



## SCMS SCHOOL OF ENGINEERING & TECHNOLOGY

### PUBLICATION DETAILS 2019

| SI No: | Name                   | First Author | Second Author   | Third Author         | Fourth Author   | INDEXING |
|--------|------------------------|--------------|-----------------|----------------------|-----------------|----------|
| 1      | Sreeja K A             | PEC1901      |                 |                      |                 | SCOPUS   |
| 2      | Dr.Sunil Jacob         | PEC1902      | PEC1903,PCS1906 | PCS1905              |                 | SCI      |
| 3      | Dr.Saira Joseph        |              |                 | PCS1906              |                 |          |
| 4      | Vinoj PG               | PEC1903      |                 |                      | PEC1902,PCS1905 | SCI      |
| 5      | Dr.Varun Menon         | PCS1906      | PEC1902         | PEC1901,PCS1902(SCO) | PCS1909(SCO)    | SCI      |
| 6      |                        |              | PCS1905         | PCS1903,PCS1904      |                 |          |
| 7      | Sreeja Rajesh          |              |                 |                      | PEC1903         | SCI      |
| 8      | Dr. Sheeja Janardhanan |              | PME1901         |                      |                 | SCOPUS   |
| 9      | Rathesh Menon          | PCE1901      |                 |                      |                 | SCI      |
| 10     | MG Airin               | PCE1902      |                 |                      |                 | SCOPUS   |
| 11     | Dr. Vinod P            | PCS1907      |                 |                      | PCS1908         | SCI      |
| 12     | Sonal Ayyappan         | PCS1902(SCO) |                 |                      |                 | SCOPUS   |

**Total Publication for the calender year 2019**

**14**



  
 DR. PRAVEENSAL C.J.  
 PRINCIPAL  
 SCMS SCHOOL OF ENGINEERING & TECHNOLOGY

Article

**A Secure Reversible Data Hiding System for Embedding EPR in Medical Images**

March 2019 · [Current Signal Transduction Therapy](#) 14(2) · [Follow journal](#)

DOI: [10.2174/1574362414666190304162411](#)

License · [CC BY 4.0](#)

[Sonal Ayyappan](#) · [C Lakshmi](#) · [Varun Menon](#)

|   |     |
|---|-----|
| Research Interest Score   | 5.1 |
| Citations   | 9   |
| Recommendations   | 1   |
| Reads  | 63  |

[Learn about stats on ResearchGate](#)


[Request full-text](#) Share ▾ More ▾

- Overview
- Stats
- Comments
- Citations (9)
- References (88)
- Related research (10+)

Abstract




Background Recent advances in medical associated technologies have drastically increased the amount of electronic medical records collected, stored and transferred through the network. Considering the significance and level of sensitivity of the collected medical data, the security of the transmitted data has become a very vital and challenging task for researchers. The protection of these medical images with embedded data is usually guaranteed using encryption or data hiding techniques. Conventional techniques that employ encryption or data hiding are often insecure and also time-consuming during transmission through the network. Materials and Methods A method combining encryption and data hiding together can result in compression of data that reduces the transmission time and increases the security level. Reversible data hiding in images can reestablish the cover image after extracting the hidden embedded data exclusive of alterations. Here a new reversible crypto-watermarking system is proposed using cryptographic algorithms that encrypts and hides an Electronic Patient Record (EPR) into an image corresponding to that patient using Rhombus Prediction Scheme. It embeds a big amount of encrypted data into an image with hardly noticeable modification using spatial pixel manipulations based on prediction errors. The marked image is hashed using SHA-256 algorithm. Results and Conclusion Hashing and cryptography increases the robustness and guarantees authenticity with integrity. The proposed method results in improved safety with a lower transmission time than the existing methods.

Methods

 Top methods in this publication

|  |  |
|--|--|
| <p><b>Electron Spin Resonance</b><br/>612 Method publications · 220 Method questions</p> <p><a href="#">View</a></p> | <p><b>Encryption</b><br/>42 Method publications · 331 Method questions</p> <p><a href="#">View</a></p> |
|--|--|

 Top related publications

|   |   |
|---|---|
| <p> Most cited</p> <p><b>Enhanced Permeability and Retention (EPR) Effect for Anticancer Nanomedicine Drug Targeting</b></p> <p>Article <a href="#">Method details available</a> <a href="#">Full-text available</a></p> | <p><b>Electron paramagnetic resonance</b></p> <p>Article <a href="#">Method details available</a></p> <p>December 1993 · <a href="#">Methods in Enzymology</a></p> <p> John R Pilbrow ·  Graeme R Hanson</p> |
|---|---|

[View more methods papers](#)

[Public Full-texts](#)



Request a copy of this research directly from the authors.

[Request full-text](#)

## ResearchGate

### Company

[About us](#)

[Blog](#)

[Careers](#)

### Resources

[ResearchGate Updates](#)

[Help Center](#)

[Contact us](#)

### Business Solutions

[Marketing Solutions](#)

[Scientific Recruitment](#)

[Publisher Solutions](#)



[Terms](#) [Privacy](#) [Copyright](#) [Imprint](#)

ℝ © 2008 - 2023 ResearchGate GmbH. All rights reserved.

[Recommend this work](#)

[Get updates](#)

[Share in a message](#)

Article

# A Secure and Efficient Lightweight Symmetric Encryption Scheme for Transfer of Text Files between Embedded IoT Devices

Sreeja Rajesh <sup>1</sup>, Varghese Paul <sup>2</sup>, Varun G. Menon <sup>3,\*</sup> and Mohammad R. Khosravi <sup>4</sup> 

<sup>1</sup> Department of Computer Science, Bharathiar University, Coimbatore 641046, Tamil Nadu, India; m.sreeja79@gmail.com

<sup>2</sup> Department of Information Technology, Cochin University of Science and Technology, Ernakulam 682022, Kerala, India; vp.itcusat@gmail.com

<sup>3</sup> Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Ernakulam 683582, Kerala, India

<sup>4</sup> Department of Electrical and Electronic Engineering, Shiraz University of Technology, Shiraz 71555-313, Iran; m.khosravi@sutech.ac.ir

\* Correspondence: varunmenon@scmsgroup.org; Tel.: +918714504684

Received: 29 January 2019; Accepted: 20 February 2019; Published: 24 February 2019



**Abstract:** Recent advancements in wireless technology have created an exponential rise in the number of connected devices leading to the internet of things (IoT) revolution. Large amounts of data are captured, processed and transmitted through the network by these embedded devices. Security of the transmitted data is a major area of concern in IoT networks. Numerous encryption algorithms have been proposed in these years to ensure security of transmitted data through the IoT network. Tiny encryption algorithm (TEA) is the most attractive among all, with its lower memory utilization and ease of implementation on both hardware and software scales. But one of the major issues of TEA and its numerous developed versions is the usage of the same key through all rounds of encryption, which yields a reduced security evident from the avalanche effect of the algorithm. Also, the encryption and decryption time for text is high, leading to lower efficiency in IoT networks with embedded devices. This paper proposes a novel tiny symmetric encryption algorithm (NTSA) which provides enhanced security for the transfer of text files through the IoT network by introducing additional key confusions dynamically for each round of encryption. Experiments are carried out to analyze the avalanche effect, encryption and decryption time of NTSA in an IoT network including embedded devices. The results show that the proposed NTSA algorithm is much more secure and efficient compared to state-of-the-art existing encryption algorithms.

**Keywords:** avalanche effect; efficiency; encryption time; key confusions; NTSA; symmetric encryption; tiny encryption algorithm

## 1. Introduction

Internets of things (IoT) includes millions of connected devices that can sense, compute and communicate data [1–6]. Every second, large amounts of data are transferred among these devices. Considering the sensitivity of applications in the IoT network, such as connected vehicles or wearable health devices, security of transmitted information has remained a major area of concern [7–9]. The increasing number of intruders and hackers has made this task very challenging. Over the years, numerous cryptographic algorithms have been used to ensure the security of transmitted data. The strength of the cryptographic algorithms depended on the techniques used for managing, establishing and distributing the secret keys. Secret keys that are poorly maintained make the

cryptographic algorithm useless, even if the algorithm is theoretically and also, practically ideal [10,11]. Cryptographic algorithms proposed for IoT networks can be classified into the symmetric and asymmetric algorithms. Symmetric algorithms use the same key for both encryption and decryption. The strength of the symmetric algorithms truly depends on how the key is securely exchanged between the sender and receiver. Asymmetric algorithms indeed avail two different keys including the public and private keys. The private key is never transmitted through the network and hence it is secure. The public key is sent through the network to the receiver. During encryption, the sender encrypts the plaintext using the public key of the receiver and sends the resultant cipher text to the receiver using the network. Even if the public key is known to the hacker, he cannot read the scrambled (or hashed) message because secret key is not known for him. During decryption, the receiver will use his private key to decrypt the cipher text. Asymmetric algorithms are more complex to implement and utilize more resources than symmetric algorithms [12,13]. Thus, most of the modern applications in IoT networks use symmetric algorithms to provide security to the transmitted information. Further, they are easy to implement, utilize fewer resources with low overhead and are secure as long as the key is kept secret.

Symmetric algorithms are classified into block and stream ciphers. Encryption of plaintext is done bit-by-bit in case of stream cipher [14] and a group of bits (i.e., 64 bits) is taken for encryption in block cipher as a unit. The block cipher algorithm is preferred to the stream cipher for faster computations. Most of the symmetric algorithms use Feistel ciphers [15,16]. In the Feistel cipher, the encrypted plaintext is decomposed into two parts. A transformation function known as the round function is applied to one half using a sub-key and the output of the round function is XOR'ed with the other half. These two parts are then swapped with each other. This step is performed iteratively on the number of times specified in the algorithm. The Feistel cipher is an efficient method for implementing block symmetric algorithms. So, we focus on improving the security of symmetric algorithms that use the Feistel ciphers for encryption of text files.

With numerous IoT devices having different computational capabilities, one of the major requirements for an efficient security protocol in IoT networks is that it should be light weight. The processing time taken by the protocol should be minimal for less delay and better performance. Also, the security algorithm needs to be less complex with minimal overhead. Because of these reasons many protocols used with normal computer networks do not give good performance in IoT networks and are not preferred. Considering these features, tiny encryption algorithm (TEA) [17–19] is the most widely used symmetric algorithm with a Feistel cipher for secure transmission of data through the IoT network. The popularity of TEA is mainly due to the ease of implementation and less memory utilization compared to all other encryption algorithms. But one of the major issues with TEA is the usage of the same keys through all the rounds of encryption which leads to reduced security. This is undoubtedly observed from the avalanche effect of TEA. Moreover, the time taken for encryption and decryption is high, leading to reduced efficiency of TEA. Although many versions of TEA have been proposed over these years [20–23], none of them have given concrete solutions to the above problems.

This paper proposes an algorithm named NTSA (novel tiny symmetric encryption algorithm) that improves the security features of TEA by introducing more key confusions. Most of the works with TEA and its variations has focused only on decreasing the delay in delivery. Very few researches have been done on key alteration as a method to enhance the security of the transmission algorithm. In the proposed method we introduce multiple key alterations dynamically and secure the key from intruders. Since the key is computed dynamically, the key values are changed during the execution time and cannot be pre-computed. Furthermore, our proposed algorithm (NTSA) takes less time for encryption and decryption compared to TEA and thus provides both better security and efficiency for all the modern applications in IoT networks. The rest of the research is organized into four sections as follows. Section 2 discusses different existing encryption mechanisms for the secure transmission of data through IoT networks. This section further explains the implementation of the TEA algorithm in detail. Few variations of the TEA algorithm are also discussed in this section. Our proposed NTSA is

explained in the Section 3. Section 4 presents the experimental results of the NTSA algorithm and we conclude in Section 5 and express some potential future works.

## 2. Related Work

In here, we discuss the major encryption algorithms proposed for transmission of data in IoT networks. Specifically, we discuss the design and implementation of these algorithms and highlight their issues and drawbacks. We also discuss the design, implementation and issues with the TEA and its latest versions in detail.

One of the earliest works in this area was the RC5 symmetric key block cipher [24]. RC5 uses variable sized blocks, 32, 64, 128 bits etc. The rounds used are 0–255 with key size of 0 to 2040 bits. The case RC5 is determined suitable for wireless sensor network (WSN) applications, but the key schedule must be calculated a priori based on 104 additional bytes of RAM for each key. Also, the variable-bit rotation instruction used by RC5 is rarely supported by the embedded systems [24]. Skipjack algorithm is another block cipher algorithm developed by the US National Security Agency. Skipjack and its variants, TinySec and MiniSec, are used for transmission of data in WSNs. But the algorithm is not efficient in embedded IoT devices with multiple issues in implementation [25–27]. Standaert et al. gave the scalable encryption algorithm (SEA) [28] generated for processing units that have limited the instruction set. It provides cost-effective encryption and authentication, but does not address secure search of the substring. Hong et al. proposed the HIGHT algorithm [29] that is very useful for pervasive computing devices like devices of a wireless sensory system or network. It uses Feistel network and basic operations like addition mod  $2^8$  or XOR. There are 32 rounds with 128-bit key and 64-bit block size. But the noted algorithm is vulnerable to saturation attack. Usman et al. proposed SIT—a lightweight encryption algorithm [30] that provides enhanced security for data transmission between IoT devices. SIT uses a combinational form of Feistel structure and network with a uniform substitution-permutation. But the detailed study on performance evaluation and cryptanalysis for possible attacks have not been performed. Liang C et al. [31] proposed the hybrid encryption algorithm for lightweight data in cloud storage. This was an improved method on the RSA algorithm and it combined with advanced encryption standard (AES) to introduce a hybrid encryption algorithm. The proposed algorithm improves the efficiency of generating large primes. But the algorithm was mainly focused on enhancing the data confidentiality in the cloud. M-SSE proposed by Chongzhi Gao et al. [32] is different from existing searchable symmetric encryption algorithms as it provides privacy in both forward and backward directions using a technique of multi-cloud computing. But the algorithms and its variations are prone to information leakage. International data encryption algorithm (IDEA) [33] is a block symmetric algorithm that uses 64-bit plain text and a key size of 128 permuted into 52 sub-keys of 128 bits. It includes a Feistel structure and has eight rounds. The degree of diffusion and non-linearity properties of the round function decides the strength of the Feistel structure. IDEA does not use substitution and permutation boxes and is based on operations like XOR, addition and multiplication, thus reducing the memory overhead. The use of the multiplication operation provides diffusion. IDEA does not support any change in the Feistel structure and hence is not flexible. MARS [34] is another symmetric block algorithm that uses 128-bit plaintext with key size varying between 128–448 bits. It follows Feistel structure and has only one substitution box. This algorithm is faster than DES and it is susceptible to many attacks. The involvement of various components makes MARS very complex to analyze and implement in hardware. Abdelhalim et al. proposed the modified TEA algorithm (MTEA) [35], which improves the security of TEA and power consumption. The linear feedback shift register (LFSR) is used as a pseudo-random number generator to improve the security of the TEA and power utilization. The pseudo-random number generator frequently changes the MTEA key in each round. Zhdanov and Sokolov proposed an algorithm [36] based on the principles of many-valued logic and variable block length. The encryption process is performed iteratively with five rounds. The number of rounds can be varied, with round 1 consisting of gamma and permutations procedures, remaining rounds include substitution and gamma procedures.



The proposed method can process binary information after representing as a ternary vector. But there is no method developed that does this conversion directly. LEA (lightweight encryption algorithm) is a block encryption algorithm [37] that is designed to provide confidentiality in lightweight environment like mobile devices. This algorithm uses plain text of 128 bits and varying modes can be selected depending on the size of the key (128, 192, or 256 bits). Based on the modes, the number of rounds can be changed between 24, 28, and 32 bits. This algorithm does not use S-box, instead addition, rotation and XOR arithmetic operation is processed in 32-bit unit [38]. Abdullah et al. proposed a super-encryption cryptography [39] with IDEA (international data encryption algorithm) and WAKE (word auto key encryption) algorithm. The technique of super encryption combines two or more symmetric cryptographic algorithms so as to provide more security to data. Anderson et al. proposed the serpent algorithm [40] that was an AES candidate. The main aim of this algorithm is to maximize the avalanche effect within the cipher text. Serpent has substitution permutation structure that uses 128-bit plain text and accepts keys of 128, 192, or 256 bits. The 32 rounds of serpent make it a bit slower and complex to implement on small blocks. Data encryption standard (DES) is one of the widely used symmetric key block cipher that uses the Feistel structure. The plaintext of 64-bit and a key size of 56 bits are used for the encryption process that includes 16 rounds. The DES algorithm does not allow flexibility in Feistel structure and hence does not support any changes in it [41].

Tiny encryption algorithm (TEA) developed by David Wheeler and Roger Needham [42] is the most efficient for use with embedded devices in IoT networks compared to all the discussed encryption algorithms. Some of the interesting features of TEA are ease of implementation, the absence of specialized tables, good performance and short enough to integrate into any embedded device. The main focus of TEA is reduced memory usage and maximized speed. Encryption routine of TEA is shown in Figure 1 and the decryption routine is shown in Figure 2.

TEA uses Feistel structure with 64 rounds or 32 cycles where one cycle is composed of two rounds [43]. The plaintext block size is 64 bits (operate on two 32-bit unsigned integers and stored in  $v[0]$  and  $v[1]$ ). The recommended key size is 128 bits. The key is split into four 32-bit blocks,  $k[0]$  to  $k[3]$ . The XOR and AND operations are used alternatively. Also repeated mixing of all the bits of plaintext and key is achieved by the dual shift operation. A simple key schedule is used for both encryption and decryption and the four 32-bit blocks of the key are mixed exactly the same way for each cycle. Magic constant is used to compute the key. For preventing the attacks caused by the symmetry of rounds, each cycle (one cycle constitutes of two rounds) uses different multiples of magic constants. Magic constant is 2,654,435,769 or  $9E3779B9_{16}$  and would be selected as  $2^{31} / \phi$  ( $\phi$  is named the golden ratio). During the encryption process, the plaintext is partitioned into two parts Left[0] and Right[0]. Each of the parts utilizes another half part for doing the encryption process. There will be 64 rounds along with two other rounds that constitute one cycle, so there are 32 cycles. After the 64th round, both parts will be composed to create the cipher text. In each of the rounds, all the inputs include "Left[ $i - 1$ ]" and "Right[ $i - 1$ ]" which is derived from the previous round and sub-key  $K_i$  extracted from the 128-bit key  $K$ . The constant  $\delta = 0 \times 9E3779B9$  is chosen to be  $2^{31} / \phi$ . This is to confirm that the sub-keys are distinct and that the accurate value of it does not have a cryptographic significance. In each round, the integer "addition" modulo of  $2^{32}$  is applied instead of XOR. The round function  $F$  uses addition, bitwise XOR, left and right shift operation.

For the  $i$ -th cycle,

$$\text{Left}[i] = \text{Left}[i - 1] + F(\text{Right}[i - 1], \text{key}[0, 1], \text{delta}[i]),$$

$$\text{Right}[i] = \text{Right}[i - 1] + F(\text{Left}[i - 1], \text{key}[2, 3], \text{delta}[i]),$$

$$\text{Delta}[i] = \text{Floor}((i + 1)/2) * \text{delta}$$

Round function  $F$  is

$$F(M, K[a, b], \text{delta}[i]) = ((M \ll 4) \text{AND } k[a]) \text{ XOR } (M \text{ AND } \text{delta}[i]) \text{ XOR } ((M \gg 5) \text{AND } k[b]).$$

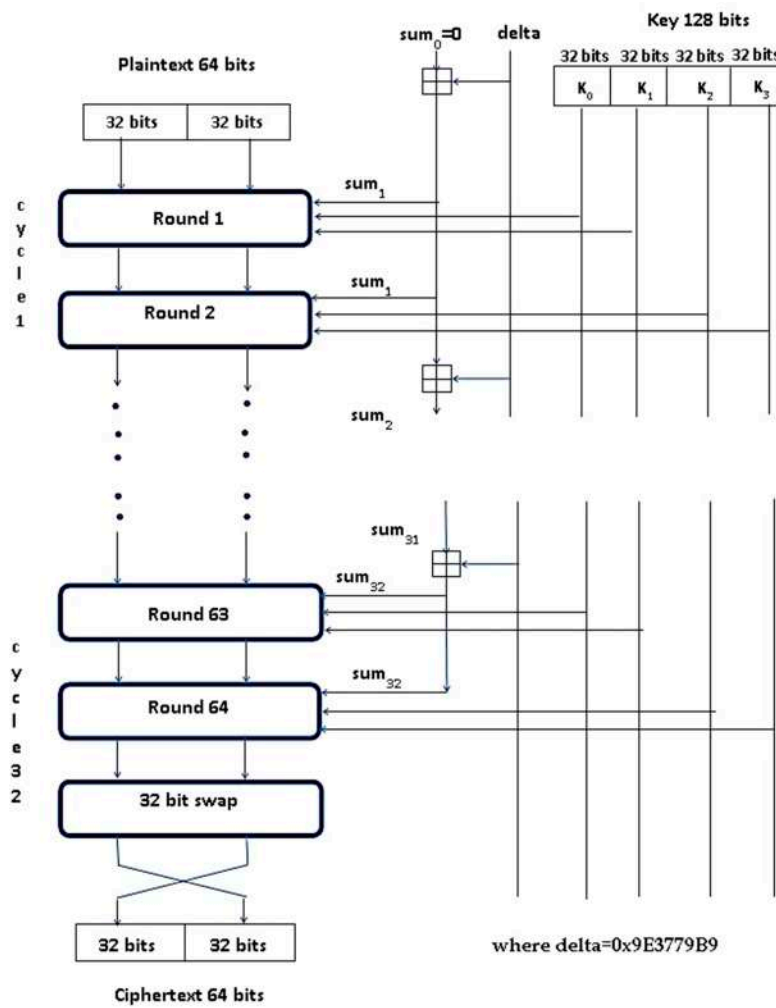


Figure 1. Encryption routine of the tiny encryption algorithm (TEA).

The 128-bit key is divided into four 32-bit blocks  $K=(k[0], k[1], k[2], k[3])$  where odd rounds use keys  $k[0]$  and  $k[1]$  and even rounds use  $k[2]$  and  $k[3]$ . One cycle constitutes two rounds and the  $i$ -th round is shown in Figure 3.

Many variations of the TEA algorithm have been proposed recently. Dian Rachmawati et al. proposed an algorithm [44] that uses a combined asymmetric and symmetric encryption for secure file transfer. The security of the file is taken care by the symmetric algorithm TEA and security of the key by the asymmetric algorithm LUC based on Lucas function. But the method used the same key for all rounds of encryption leading to reduced security. Novelan et al. developed an SMS security system for mobile devices using the Tiny Encryption algorithm [45]. This system ensures that the confidential messages are encrypted in the presence of a key to obtain the encrypted SMS message that is sent to the destination mobile number. Cipher text at the receiver side can be decrypted using the same key to get the SMS. The drawback with this method is that the size of the SMS decides the encryption and decryption time taken for the process. XTEA is a block symmetric encryption algorithm that uses the Feistel structure [46]. This algorithm uses 64-bit block plaintext, 128-bit key and 64 rounds of encryption. This algorithm uses a more complex key-schedule than TEA with rearrangements of the shifts, XOR's and additions [47]. XXTEA, also called block TEA uses the same round function as XTEA but applies it cyclically across an entire message for several iterations [48]. Table 1 presents a summary of all the existing security algorithms.



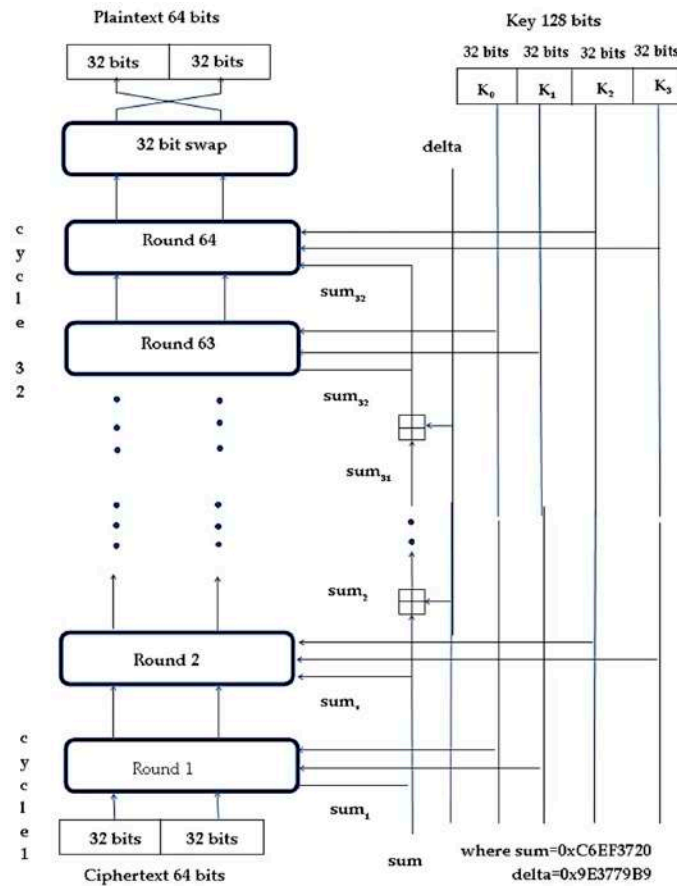


Figure 2. Decryption routine of TEA.

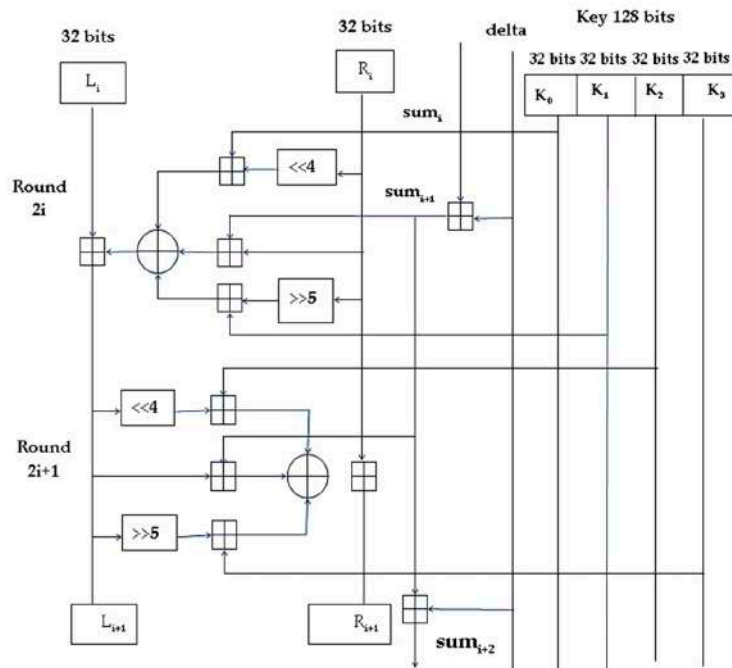


Figure 3. The  $i$ -th cycle of TEA.

Of all the discussed algorithms, TEA remains the most efficient for use in IoT networks for secure and quick transfer of text files between simple embedded devices. But one of the major issues with

TEA and its latest variations is the usage of same keys through all rounds of encryption, resulting in reduced security, which is evident from the avalanche effect of the algorithm. Also, the encryption and decryption time for text is high, leading to lower efficiency in IoT networks with embedded devices. This paper proposes a NTSA which provides enhanced security for the transfer of text files through the IoT network by introducing additional key confusions dynamically for each round of encryption.

**Table 1.** Summary of the symmetric encryption techniques.

| Algorithm     | Developer                      | Block/Stream Cipher           | Key Size           | Attack                          | Algorithm Structure                                 |
|---------------|--------------------------------|-------------------------------|--------------------|---------------------------------|---|
| DES [41]      | IBM                            | Block cipher (64 bits)        | 56 bits            | Brute Force Attack              | 16 rounds Feistel Structure                         |
| 3DES [49]     | IBM                            | Block cipher (64 bits)        | 112 or 168 bits    | chosen-plaintext attack         | 48 rounds Feistel Structure                         |
| IDEA [33]     | Lai and James                  | Block cipher (64 bits)        | 128 bits           | weak keys                       | 8 rounds Feistel Structure                          |
| RC5 [24]      | Ron Rivest                     | Block cipher (32,64,128 bits) | 0–2040 bits        | differential attack             | (12 round suggested) Feistel Structure              |
| TEA [45]      | Wheeler and Needham            | Block cipher (64 bits)        | 128 bits           | equivalent key attack           | Variable round Feistel Structure                    |
| XTEA [46]     | Wheeler and Needham            | Block cipher (64 bits)        | 128 bits           | related key differential attack | Variable round nested Feistel Structure             |
| XXTEA [47]    | Wheeler and Needham            | Block cipher (64 bits)        | 128 bits           | chosen-plaintext attack         | unbalanced Feistel Network                          |
| SKIPJACK [50] | National Security Agency (NSA) | Block cipher (64 bits)        | 80 bits            | slide attack                    | 32 rounds, unbalanced Feistel Structure             |
| AES [40]      | Daemen and Rijmen              | Block cipher (128 bits)       | 128, 192, 256 bits | known plaintext                 | 20 rounds Feistel Structure                         |
| MARS [34]     | IBM                            | Block cipher (128 bits)       | 128, 192, 256 bits | meet-in-the-middle              | 32 rounds Feistel Structure                         |
| HIGHT [29]    | Hong et al.                    | Block cipher (64 bits)        | 128 bits           | Impossible Differential attack  | light weight block algorithm, effective in hardware |

### 3. Novel Tiny Symmetric Encryption Algorithm (NTSA)

The TEA algorithm and its variations use the same key in all rounds of encryption and are thus more prone to relative key attack where the attacker tries to realize some relationship between different keys used by the user. The proposed NTSA algorithm is intended to provide more confusion to the keys in each round dynamically. It uses 64-bit plaintext and key of 128 bits. There are 32 cycles and each cycle is composed of two rounds, resulting in 64 rounds. The plaintext is divided into two halves,  $v_0$  and  $v_1$ , with 32 bits each. The round function  $op$  is applied to each half of plaintext. The 128-bit key is divided into four 32-bit partial keys  $k_1$ ,  $k_2$ ,  $k_3$ , and  $k_4$ . Partial keys  $k_1$  and  $k_3$  are applied to the odd numbered round and partial keys  $k_2$  and  $k_4$  are applied to even numbered round. Compute key schedule constant  $ksc = \text{floor}(2^{31}/\phi)$  where  $\phi$  is the golden ratio. The golden ratio  $\phi$  is 1.618033988749895 and computed as  $(1 + \sqrt{5})/2$ .

NTSA round function is as follows:

Round  $i$  ( $i$  is odd):

$$v_0 += ((v_1 \text{ LSHIFT } 4) \text{ AND } k_0) \text{ XOR } (v_1 \text{ AND } k_c) \text{ XOR } ((v_1 \text{ RSHIFT } 5) \text{ AND } k_1)$$

Round  $i$  ( $i$  is even):

$$v_1 += ((v_0 \text{ LSHIFT } 4) \text{ AND } k_2) \text{ XOR } (v_0 \text{ AND } k_c) \text{ XOR } ((v_0 \text{ RSHIFT } 5) \text{ AND } k_3)$$

For 1st cycle: the partial keys are  $k_0$ ,  $k_1$ ,  $k_2$  and  $k_3$ .

From 2nd cycle onwards:

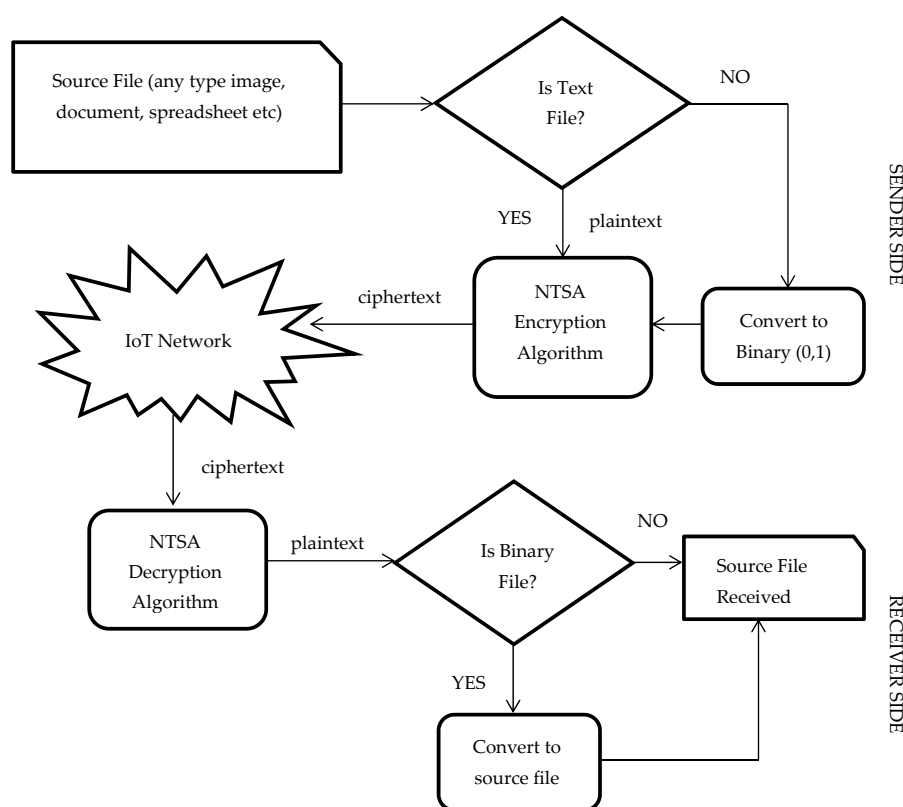
For odd round  $k_0$  is kept constant but  $k_1$  changes for all odd rounds as follows,

$$k_1 = k_1 + (k_0 \text{ XOR}(\text{xtract}(v_0)))$$

For even round  $k_2$  is kept constant but  $k_3$  changes for all even rounds as follows,

$$k_3 = k_3 + (k_2 \text{ XOR}(\text{xtract}(v_1)))$$

The function  $\text{xtract}()$  will compute an integer in the range 0 to 32 from  $v_0$  or  $v_1$  depending upon the parameter being passed. This integer value is an index to an array that is generated dynamically based on the key value selection. The  $\text{xtract}()$  function will return the value from the array that is pointed by the index value computed. Thus, the key confusion is created dynamically and cannot be predicted prior to execution and the value changes on each execution of the algorithm. The NTSA encryption and decryption model is shown in Figure 4.



**Figure 4.** System model: novel tiny symmetric encryption algorithm (NTSA) encryption and decryption.

The source file can be a file of any type such as a document, spreadsheet, pdf, presentation, image, text file etc. The text file can be sent directly to the NTSA encryption algorithm to obtain the cipher text. All the other types of files are converted into binary, the streams of ones and zeros. This binary stream is sent to the NTSA encryption algorithm to get the cipher text using the secret key which has already been agreed upon by the sender and the receiver. On reception of cipher text at the receiver end, the NTSA decryption algorithm converts the cipher text to plaintext. If the converted file is binary (that is streams of zeros and ones) the file is converted to the respective source file, otherwise the plaintext is already received. The NTSA Encryption technique is presented as Algorithm 1 and Decryption technique is presented as Algorithm 2.

**Algorithm 1** Novel tiny symmetric encryption algorithm (NTSA) symmetric encryption algorithm

Encrypt (plaintext  $v$ , key  $k$ ):

1: Start

2: Assign key constant  $kc = 0$

3: Assign cycle = 0

4:  $kc = kc + ksc$

5: 32-bit block  $v0$  is recomputed as

$v0 += ((v1 \text{ LSHIFT } 4) \text{ AND } k0) \text{ XOR } (v1 \text{ AND } kc) \text{ XOR } ((v1 \text{ RSHIFT } 5) \text{ AND } k1)$

6: Partial key  $k1$  is recomputed as

$k1 += (k0 \text{ XOR}(xtract(v0)))$  where function  $xtract()$  returns value of array indexed  $v0$ .

7: 32-bit block  $v1$  is recomputed as

$v1 += ((v0 \text{ LSHIFT } 4) \text{ AND } k2) \text{ XOR } (v0 \text{ AND } kc) \text{ XOR } ((v0 \text{ RSHIFT } 5) \text{ AND } k3)$

8: Partial key  $k3$  is recomputed as

$k3 += (k2 \text{ XOR}(xtract(v1)))$  where function  $xtract()$  returns value of array indexed  $v1$ .

9: Increment cycle by 1

10: Repeat step 4 through step 9 until cycle = 32

11: Assign value of  $k1$  to  $newk1$  and  $k3$  to  $newk3$

12: Return  $newk1$  and  $newk3$

The NTSA symmetric encryption algorithm uses the plaintext to encrypt with the key that was already agreed upon by the two parties in communication. The key constant is initialized to zero. The key schedule constant  $ksc$  is computed as  $\text{floor}(2^{31}/\phi)$  where  $\phi$  is the golden ratio. The golden ratio  $\phi$  is 1.618033988749895. The 32-bit block plaintext  $v0$  and  $v1$  are recomputed each time for 32 cycles and partial keys  $k1$  and  $k3$  are recomputed for even and odd rounds respectively to induce key confusion. The computation of  $v0$ ,  $k1$ ,  $v1$ ,  $k3$  are shown in the following equations.

$$v0 += ((v1 \text{ LSHIFT } 4) \text{ AND } k0) \text{ XOR } (v1 \text{ AND } kc) \text{ XOR } ((v1 \text{ RSHIFT } 5) \text{ AND } k1)$$

$$k1 += (k0 \text{ XOR}(xtract(v0))) \text{ where function } xtract() \text{ returns value of array indexed } v0.$$

$$v1 += ((v0 \text{ LSHIFT } 4) \text{ AND } k2) \text{ XOR } (v0 \text{ AND } kc) \text{ XOR } ((v0 \text{ RSHIFT } 5) \text{ AND } k3)$$

$$k3 += (k2 \text{ XOR}(xtract(v1))) \text{ where function } xtract() \text{ returns value of array indexed } v1.$$

$$kc \text{ is recomputed each time as } kc = kc + ksc$$

This process is repeated for 32 cycles and after the last cycle the values of partial keys  $k1$  and  $k3$  are the new values computed and these new partial keys and the cipher text are sent to the decryption process. The NTSA symmetric decryption algorithm uses the cipher text, the key that was already agreed upon by the two parties in communication and the newly computed partial keys  $k1$  and  $k3$  for the decryption purpose. The key constant is initialized to 0XC6EF3720. The key schedule constant  $ksc$  is computed as  $\text{floor}(2^{31}/\phi)$ . The golden ratio  $\phi$  is 1.618033988749895. The 32-bit blocks  $v1$  and  $v0$  are recomputed each time for 32 cycles and partial keys  $k3$  and  $k1$  are recomputed for odd and even rounds respectively to induce key confusion. The computation of  $k3$ ,  $v1$ ,  $k1$  and  $v0$  are shown in the following equations.

$$k3 - = (k2 \text{ XOR}(xtract(v1))) \text{ where function } xtract() \text{ returns value of array indexed } v1$$

$$v1 - = ((v0 \text{ LSHIFT } 4) \text{ AND } k2) \text{ XOR } (v0 \text{ AND } kc) \text{ XOR } ((v0 \text{ RSHIFT } 5) \text{ AND } k3)$$

$$k1 - = (k0 \text{ XOR}(xtract(v0))) \text{ where function } xtract() \text{ returns value of array indexed } v0$$

$$v0 - = ((v1 \text{ LSHIFT } 4) \text{ AND } k0) \text{ XOR } (v1 \text{ AND } kc) \text{ XOR } ((v1 \text{ RSHIFT } 5) \text{ AND } k1)$$

$$kc \text{ is recomputed each time as } kc = kc - ksc$$

This process is repeated for 32 cycles and after the last cycle the 32-bit block v0 and v1 contains the decrypted contents.

**Algorithm 2.** NTSA symmetric decryption algorithm

Encrypt (plaintext  $v$ , key  $k$ ):

- 1: Start
- 2: Assign key constant  $kc = 0XC6EF3720$
- 3: Assign  $k1 = newk1$  and  $k3 = newk3$
- 4: Assign  $cycle=0$
- 5: Partial key  $k3$  is recomputed as  
 $k3 = (k2 \text{ XOR}(\text{xtract}(v1)))$  where function  $\text{xtract}()$  returns value of array indexed  $v1$ .
- 6: 32-bit block  $v1$  is recomputed as  
 $v1 = ((v0 \text{ LSHIFT } 4) \text{ AND } k2) \text{ XOR } (v0 \text{ AND } kc) \text{ XOR } ((v0 \text{ RSHIFT } 5) \text{ AND } k3)$
- 7: Partial key  $k1$  is recomputed as  
 $k1 = (k0 \text{ XOR}(\text{xtract}(v0)))$  where function  $\text{xtract}()$  returns value of array indexed  $v0$ .
- 8: 32-bit block  $v0$  is recomputed as  
 $v0 = ((v1 \text{ LSHIFT } 4) \text{ AND } k0) \text{ XOR } (v1 \text{ AND } kc) \text{ XOR } ((v1 \text{ RSHIFT } 5) \text{ AND } k1)$
- 9:  $kc = kc - ksc$
- 10: Increment cycle by 1
- 11: Repeat step 5 through step 10 until  $cycle=32$
- 12: Return

Figures 5 and 6 show the structure of NTSA encryption and decryption algorithm.

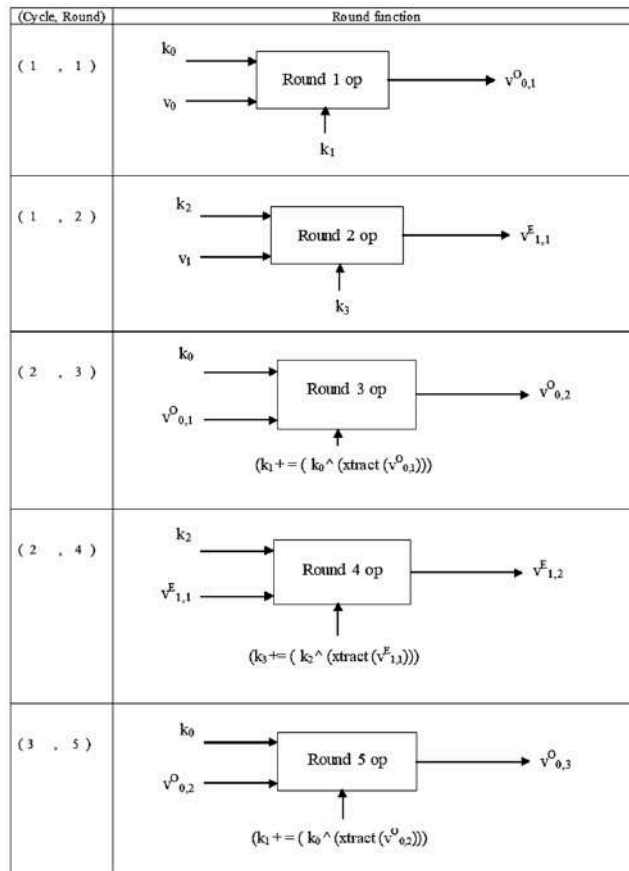


Figure 5. Cont.

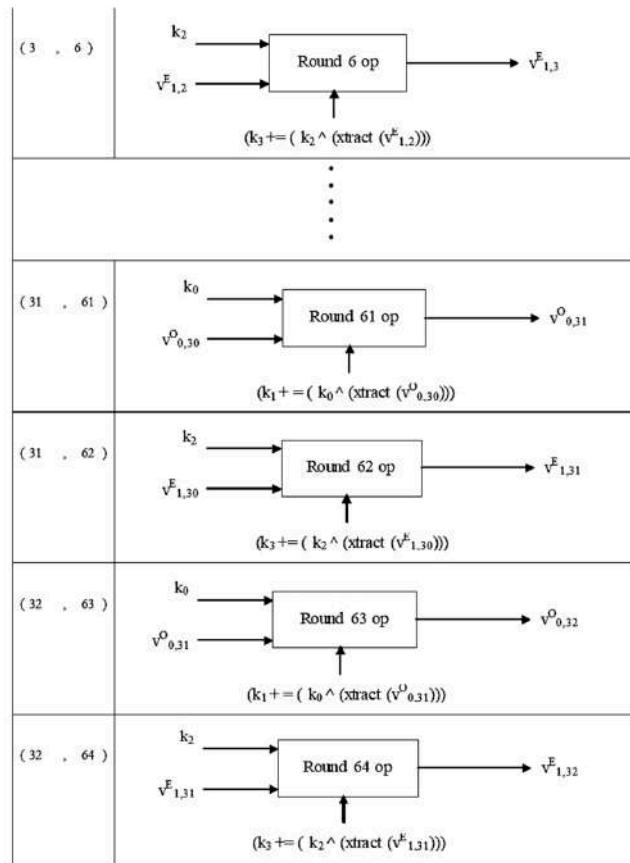


Figure 5. Structure of NTSA encryption algorithm.

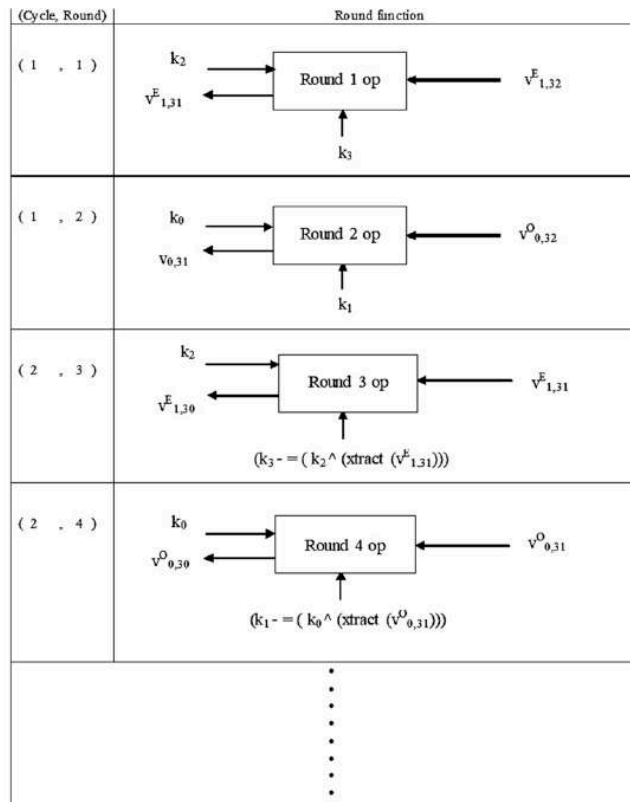


Figure 6. Cont.

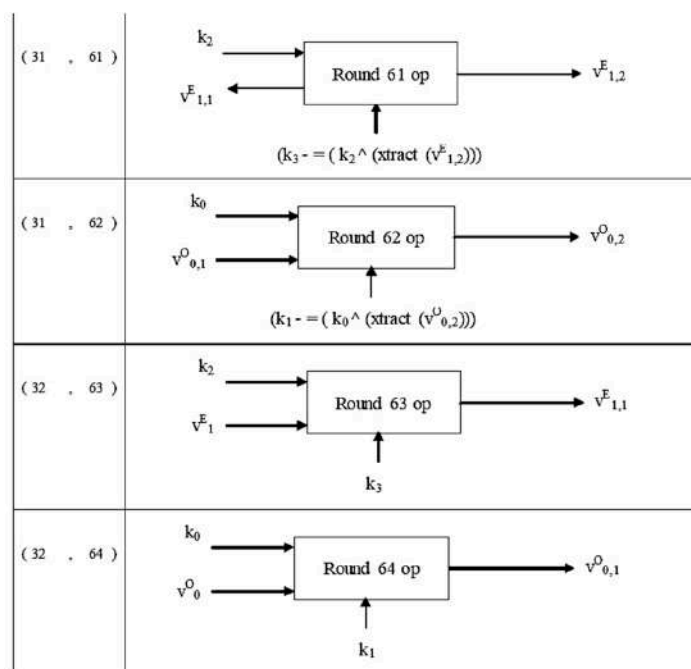


Figure 6. Structure of NTSA decryption algorithm.

The notation:

in  $v^{O,1}$ ; O indicates an odd round, and 0,1 indicate the 0th cycle, round 1;

in  $v^{E,1}$ ; E indicates an even round, and 1,1 indicate the 1st cycle, round 1.

For computing  $v^{O,1}$ , the second half of the plaintext  $v_1$  is used and shift, AND, and XOR operations are performed on  $v_1$ . Similarly, for computing  $v^{E,1}$ , the first half (32 bits) of plain text  $v_0$  is used and shift, AND and XOR operations are performed on  $v_0$ .

#### 4. Experimental Results and Discussion

In this section we discuss the results obtained with our experiments. The performance of NTSA is analyzed and compared with TEA and its latest variations XTEA and XXTEA. A network with LPWAN and IoT infrastructures was set up in our lab. NTSA, TEA, XTEA and XXTEA algorithms were implemented in embedded devices. System architecture similar to [51] was used for the experimental set up. IoT configured mobile devices connected with LPWAN and interfaced with IoT cloud via the IoT gateway was set up. The text files were then transmitted from these devices to the IoT cloud configured in a mobile device through the IoT gateway platform. The text files were then stored in the database in the cloud server. The text files were then encrypted using the four algorithms separately in four different scenarios and were send to the IoT configured mobile devices. The encryption and decryption times for each algorithm was measured for varying file sizes and key sizes.

##### 4.1. Performance Comparison of NTSA with TEA, XTEA and XXTEA

Table 2 and 3 presents the encryption and decryption times of the various security algorithms for 48-bit key with varying file sizes from 0.37 kilobytes to 26.7 kilobytes. It is evident from Table 2 that the encryption time for text files using the proposed method NTSA was lower than the other existing security algorithms. NTSA achieved an encryption time of 0.041 ms for a 0.37 kB text file which is much lower compared to 0.059 ms obtained by the TEA algorithm. The two other variations of TEA, XTEA and XXTEA had much higher encryption times because of their complexity in design and implementation. It is observed from the results that, even when the text file size increased, NTSA maintained a lower encryption time compared to the other existing security encryption schemes. NTSA achieved a much lower encryption time of 0.857 ms, 1.211 ms and 1.603 ms for text file size



12.2 kB, 16.2 kB, and 26.7 kB, respectively. This asserts the excellent performance of NTSA even with higher text file sizes.

**Table 2.** Encryption time for key size of 48 bits.

| FILE SIZE<br>(IN KILO BYTES) | ENCRYPTION TIME (in milliseconds) |       |                   |       |
|------------------------------|-----------------------------------|-------|-------------------|-------|
|                              | TEA                               | XTEA  | BLOCK TEA (XXTEA) | NTSA  |
| 0.37                         | 0.059                             | 0.174 | 0.083             | 0.041 |
| 0.95                         | 0.125                             | 0.244 | 0.155             | 0.112 |
| 1.6                          | 0.214                             | 0.451 | 0.271             | 0.201 |
| 2.6                          | 0.351                             | 0.683 | 0.429             | 0.289 |
| 6.8                          | 0.771                             | 1.384 | 1.768             | 0.551 |
| 8.6                          | 0.817                             | 2.120 | 1.192             | 0.801 |
| 12.2                         | 0.916                             | 2.306 | 1.379             | 0.857 |
| 16.2                         | 1.544                             | 3.744 | 1.981             | 1.211 |
| 26.7                         | 1.802                             | 4.176 | 2.712             | 1.603 |

From the results presented in Table 3, it is evident that NTSA achieved a lower decryption time for various text file sizes compared to the other three existing security algorithms in IoT networks. NTSA achieved a decryption time of 0.055 ms for a 0.37 kB text file, which is much lower than the decryption time achieved by other algorithms. For higher file sizes of 12.2 kB, 16.2 kB and 26.7 kB, NTSA achieved 0.890 ms, 1.234 ms, and 1.645 ms decryption times, respectively. So even with higher text file sizes, NTSA achieved lower decryption times similar to the results obtained during encryption. Lower encryption and decryption times are a very important parameter determining the efficiency of a security algorithm in an IoT network. With most of the devices having limited computational capabilities, it is very much required to have a security algorithm that can provide maximum security with less complexity and minimum encryption and decryption times. Thus, the results obtained from our experiments with 48-bit key encryption confirms that the proposed method achieves much lower encryption and decryption times compared to the existing security algorithms in IoT networks. This result is achieved, especially due to the simplicity in design of the proposed algorithm, without compromising the strength in security. The improved strength in security of the algorithm was later verified using the avalanche effect parameter. With lower encryption and decryption time, this algorithm would be highly beneficial for the users to transmit text files through the IoT networks more efficiently.

**Table 3.** Time for key size of 48 bits.

| FILE SIZE<br>(IN KILO BYTES) | DECRYPTION TIME (in milliseconds) |       |                   |       |
|------------------------------|-----------------------------------|-------|-------------------|-------|
|                              | TEA                               | XTEA  | BLOCK TEA (XXTEA) | NTSA  |
| 0.37                         | 0.058                             | 0.136 | 0.068             | 0.055 |
| 0.95                         | 0.123                             | 0.289 | 0.156             | 0.112 |
| 1.6                          | 0.209                             | 0.474 | 0.254             | 0.201 |
| 2.6                          | 0.332                             | 0.691 | 0.371             | 0.323 |
| 6.8                          | 0.753                             | 1.369 | 1.73              | 0.655 |
| 8.6                          | 0.806                             | 2.095 | 1.16              | 0.789 |
| 12.2                         | 0.903                             | 2.228 | 1.365             | 0.890 |
| 16.2                         | 1.537                             | 3.698 | 1.959             | 1.234 |
| 26.7                         | 1.78                              | 4.241 | 2.799             | 1.645 |

Tables 4 and 5 present the comparison of encryption and decryption time of NTSA with TEA, XTEA and XXTEA for a 128-bit key with varying file sizes from 0.37 kilobytes to 26.7 kilobytes. It is interesting to observe from the results presented in Table 4 that with a larger key size, NTSA achieved lower encryption time compared to all the existing security algorithms in IoT networks. The encryption time for a text file of size 0.37 kB with 128-bit key is 0.51 ms for NTSA which was much lower compared

to the encryption time achieved by TEA, XTEA and XXTEA algorithms. The simplicity in design of NTSA helped the algorithm to achieve lower encryption time with varying key and file sizes.

**Table 4.** Time for key size of 128 bits.

| FILE SIZE<br>(IN KILO BYTES) | ENCRYPTION TIME (in milliseconds) |       |                   |       |
|------------------------------|-----------------------------------|-------|-------------------|-------|
|                              | TEA                               | XTEA  | BLOCK TEA (XXTEA) | NTSA  |
| 0.37                         | 0.059                             | 0.125 | 0.068             | 0.51  |
| 0.95                         | 0.126                             | 0.264 | 0.158             | 0.109 |
| 1.6                          | 0.198                             | 0.423 | 0.232             | 0.189 |
| 2.6                          | 0.332                             | 0.686 | 0.384             | 0.221 |
| 6.8                          | 0.696                             | 1.584 | 0.743             | 0.548 |
| 8.6                          | 0.948                             | 1.669 | 1.171             | 0.899 |
| 12.2                         | 1.277                             | 2.807 | 1.535             | 1.02  |
| 16.2                         | 1.12                              | 3.263 | 1.864             | 1.10  |
| 26.7                         | 2.209                             | 5.207 | 2.224             | 1.983 |

**Table 5.** Time for key size of 128 bits.

| FILE SIZE<br>(IN KILO BYTES) | DECRYPTION TIME (in milliseconds) |       |                   |       |
|------------------------------|-----------------------------------|-------|-------------------|-------|
|                              | TEA                               | XTEA  | BLOCK TEA (XXTEA) | NTSA  |
| 0.37                         | 0.058                             | 0.143 | 0.068             | 0.49  |
| 0.95                         | 0.125                             | 0.276 | 0.179             | 0.101 |
| 1.6                          | 0.195                             | 0.43  | 0.233             | 0.174 |
| 2.6                          | 0.324                             | 0.673 | 0.388             | 0.311 |
| 6.8                          | 0.678                             | 1.57  | 0.75              | 0.556 |
| 8.6                          | 0.936                             | 1.641 | 1.21              | 0.889 |
| 12.2                         | 1.241                             | 2.764 | 1.538             | 1.03  |
| 16.2                         | 1.111                             | 3.184 | 1.956             | 1.10  |
| 26.7                         | 2.179                             | 5.178 | 2.193             | 1.989 |

This scenario was also observed with the decryption times presented in Table 5. With decryption also, NTSA achieved lower times compared to its compatriots with a 128-bit key and varying file sizes. NTSA achieved a decryption time of 0.49 ms for a 0.37 kB text file compared to 0.058 ms, 0.143 ms and 0.068 ms achieved by TEA, XTEA and XXTEA respectively for similar text file size. For higher file sizes of 12.2 kB, 16.2 kB, and 26.7 kB, NTSA achieved 1.03 ms, 1.10 ms, and 1.989 ms decryption times, respectively. So even with higher text file sizes, NTSA achieved lower decryption times similar to the results obtained during encryption. With lower encryption and decryption times at 128-bit key, NTSA can become the preferred security algorithm for hand held devices and other embedded IoT devices with different computational capabilities for efficiently transferring text files.

Tables 6 and 7 show the encryption and decryption times of the security algorithms for the transfer of a text file with size 0.95 kB. The better performance of NTSA compared to all the existing security algorithms is evident from the obtained results. This is because the NTSA algorithm has a very simple implementation strategy. The TEA and its different variations use complex computations with the key and hence the encryption and decryption time is greater. In Table 6, the encryption time obtained by NTSA for a file size of 0.95 kB with varying key size is compared with the existing algorithms. The key size is varied from 32 bits to 240 bits and the corresponding encryption time is observed. TEA achieved an encryption time of 0.125 ms for a key size of 32 bits while XTEA and XXTEA achieved 0.287ms and 0.145 ms, respectively. For the same key size, NTSA had an encryption time of 0.07 ms which was much lower compared to all the other security algorithms. For the 96-bit key, XTEA had an encryption time of 0.126 ms, while XTEA and XXTEA had encryption times of 0.265 ms and 0.158 ms, respectively. The encryption time obtained by NTSA for similar key size was 0.093 ms which was much lower than the time achieved by the existing algorithms. This demonstrates the better performance of the

proposed approach NTSA, compared to all the existing security algorithms in IoT networks with varying key sizes.

**Table 6.** Encryption time for file size 0.95 kB.

| KEY SIZE<br>(IN BITS) | ENCRYPTION TIME (in milliseconds) |       |                   |       |
|-----------------------|-----------------------------------|-------|-------------------|-------|
|                       | TEA                               | XTEA  | BLOCK TEA (XXTEA) | NTSA  |
| 32                    | 0.125                             | 0.287 | 0.145             | 0.07  |
| 48                    | 0.125                             | 0.264 | 0.162             | 0.083 |
| 64                    | 0.125                             | 0.246 | 0.17              | 0.088 |
| 96                    | 0.126                             | 0.265 | 0.158             | 0.093 |
| 128                   | 0.126                             | 0.264 | 0.158             | 0.097 |
| 160                   | 0.114                             | 0.271 | 0.154             | 0.100 |
| 192                   | 0.125                             | 0.279 | 0.144             | 0.100 |
| 240                   | 0.125                             | 0.279 | 0.145             | 0.113 |

**Table 7.** Time for file size 0.95 kB.

| KEY SIZE<br>(IN BITS) | DECRYPTION TIME (in milliseconds) |       |                   |       |
|-----------------------|-----------------------------------|-------|-------------------|-------|
|                       | TEA                               | XTEA  | BLOCK TEA (XXTEA) | NTSA  |
| 32                    | 0.124                             | 0.281 | 0.146             | 0.068 |
| 48                    | 0.136                             | 0.257 | 0.15              | 0.087 |
| 64                    | 0.123                             | 0.214 | 0.152             | 0.088 |
| 96                    | 0.123                             | 0.259 | 0.158             | 0.091 |
| 128                   | 0.125                             | 0.276 | 0.179             | 0.090 |
| 160                   | 0.113                             | 0.267 | 0.155             | 0.101 |
| 192                   | 0.126                             | 0.26  | 0.159             | 0.119 |
| 240                   | 0.123                             | 0.259 | 0.157             | 0.119 |

Tables 8 and 9 show the encryption and decryption times of the security algorithms for the transfer of a text file with size 12.2 kB with varying key sizes. The encryption time achieved by TEA, XTEA and XXTEA for a key size of 32 bits was 1.173 ms, 2.287 ms, and 1.649 ms, respectively, which was much higher compared to 1.009 ms obtained by NTSA for a similar key size. Even for a key size of 96 bits, NTSA achieved an encryption time of 1.10 ms which is lower than the values obtained by all the other existing security algorithms for similar file size. For a key size of 240 bits, NTSA had an encryption time of 1.2 ms which was much lower compared to all the existing algorithms. Thus, for smaller and larger key sizes, NTSA achieved lower encryption time compared to all the existing security algorithms in IoT networks. This scenario is also observed with the decryption times presented in Table 9. NTSA achieved a decryption time of 1.025 ms, 1.155 ms, and 1.388 ms for a key size 160 bits, 192 bits, and 240 bits, respectively. This time achieved by NTSA was lower than the times obtained by TEA, XTEA and XXTEA for similar key sizes in the IoT network. This assures the better performance of NTSA compared to all the existing algorithms with varying key sizes in IoT networks.

Tables 10 and 11 presents the results obtained in encryption and decryption time with NTSA, TEA, XTEA and XXTEA for a text file size of 26.7 kB with varying key sizes from 32 bits to 240 bits. The encryption time achieved by TEA, XTEA and XXTEA for a key size of 32 bits is 2.253 ms, 4.459 ms, and 2.339 ms, respectively, which is much higher compared to 1.772 ms obtained by NTSA for a similar key size. Even for a key size of 96 bits, NTSA achieved an encryption time of 1.856 ms which was lower than the values obtained by all the other existing security algorithms for similar file size. NTSA also achieved an encryption time of 1.887 ms, 1.662 ms, and 1.912 ms for 160 bits, 192 bits and 240 bits' key sizes. Thus, from the results it is evident that NTSA achieved much lower encryption times compared to all the existing algorithms in IoT networks. This scenario is also verified in Table 11 which presents the decryption time obtained by these algorithms for varying key sizes. The simplicity in design enables NTSA to achieve much lower encryption and decryption times in IoT networks. This would

definitely enable IoT devices with varying computational and storage capabilities to efficiently and securely transmit text files through the network.

**Table 8.** Time for file size 12.2 kB.

| KEY SIZE<br>(IN BITS) | ENCRYPTION TIME (in milliseconds) |       |                   |       |
|-----------------------|-----------------------------------|-------|-------------------|-------|
|                       | TEA                               | XTEA  | BLOCK TEA (XXTEA) | NTSA  |
| 32                    | 1.173                             | 2.287 | 1.649             | 1.009 |
| 48                    | 1.178                             | 2.572 | 1.393             | 1.010 |
| 64                    | 1.248                             | 2.089 | 1.178             | 1.006 |
| 96                    | 1.208                             | 2.32  | 1.502             | 1.10  |
| 128                   | 1.067                             | 2.301 | 1.534             | 1.04  |
| 160                   | 1.137                             | 2.608 | 1.076             | 1.03  |
| 192                   | 1.39                              | 2.327 | 1.148             | 1.11  |
| 240                   | 1.439                             | 2.866 | 1.413             | 1.2   |

**Table 9.** Decryption time for file size 12.2 kB.

| KEY SIZE<br>(IN BITS) | DECRYPTION TIME (in milliseconds) |       |                   |       |
|-----------------------|-----------------------------------|-------|-------------------|-------|
|                       | TEA                               | XTEA  | BLOCK TEA (XXTEA) | NTSA  |
| 32                    | 1.127                             | 2.249 | 1.641             | 1.08  |
| 48                    | 1.195                             | 2.572 | 1.396             | 1.083 |
| 64                    | 1.241                             | 2.084 | 1.179             | 1.112 |
| 96                    | 1.226                             | 2.299 | 1.477             | 1.117 |
| 128                   | 1.029                             | 2.265 | 1.583             | 1.020 |
| 160                   | 1.093                             | 2.645 | 1.074             | 1.025 |
| 192                   | 1.363                             | 2.278 | 1.163             | 1.155 |
| 240                   | 1.402                             | 2.827 | 1.414             | 1.388 |

**Table 10.** Time for file size 26.7 kB.

| KEY SIZE<br>(IN BITS) | ENCRYPTION TIME (in milliseconds) |       |                   |       |
|-----------------------|-----------------------------------|-------|-------------------|-------|
|                       | TEA                               | XTEA  | BLOCK TEA (XXTEA) | NTSA  |
| 32                    | 2.253                             | 4.459 | 2.339             | 1.772 |
| 48                    | 1.883                             | 3.734 | 2.111             | 1.789 |
| 64                    | 1.933                             | 3.349 | 2.485             | 1.812 |
| 96                    | 2.812                             | 4.856 | 2.246             | 1.856 |
| 128                   | 2.209                             | 5.207 | 2.224             | 1.825 |
| 160                   | 2.925                             | 3.687 | 2.731             | 1.887 |
| 192                   | 1.869                             | 4.562 | 1.958             | 1.662 |
| 240                   | 1.989                             | 4.213 | 2.43              | 1.912 |

**Table 11.** Time for file size 26.7 kB.

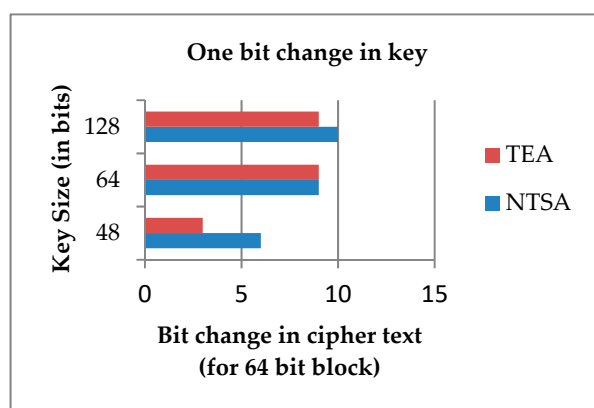
| KEY SIZE<br>(IN BITS) | DECRYPTION TIME (in milliseconds) |       |                   |       |
|-----------------------|-----------------------------------|-------|-------------------|-------|
|                       | TEA                               | XTEA  | BLOCK TEA (XXTEA) | NTSA  |
| 32                    | 2.212                             | 4.422 | 2.387             | 1.701 |
| 48                    | 1.854                             | 3.713 | 2.136             | 1.746 |
| 64                    | 1.888                             | 3.307 | 2.516             | 1.777 |
| 96                    | 2.726                             | 4.892 | 2.289             | 1.834 |
| 128                   | 2.179                             | 5.178 | 2.193             | 1.820 |
| 160                   | 2.883                             | 3.668 | 2.711             | 1.811 |
| 192                   | 1.853                             | 4.498 | 1.935             | 1.812 |
| 240                   | 1.934                             | 4.073 | 2.456             | 1.936 |

From the results presented in Tables 2–11, it is very evident that the NTSA algorithm give better performance compared to all the existing algorithms with variable file sizes and key sizes. NTSA gave much lower encryption and decryption times for variable size text files using multiple key sizes in IoT networks. This is due to the simple and efficient design of NTSA. One of the most important features of NTSA is that it provides enhanced security to all the applications in IoT devices with lower encryption and decryption times. Thus, the proposed approach NTSA can be used for efficient and secure transfer of text files between devices in IoT networks.

#### Avalanche Effect

The avalanche effect is the property wherein a very small change in input results in significant changes on the output. An encryption algorithm is considered good if a one-bit change in key results in significant changes in the cipher text. With reference to the avalanche effect, we compared the strength of NTSA and TEA algorithms.

Experiment 1: an encryption was performed for NTSA and TEA algorithms using keys with varying key sizes of 48, 64 and 128 bits and same plaintext. Then one bit was changed on the key and the experiment was repeated. It is observed that for every 64-bit block, a one-bit change in key resulted in significant changes on the cipher text. Drastic changes were observed for the NTSA algorithm when compared to TEA. Figure 7 shows, for every 64-bit block, a change in one bit of the key with various key sizes and the corresponding change in cipher text for NTSA and TEA.



**Figure 7.** Change in key and the corresponding change in cipher text for a 64-bit block.

From Figure 7, it is very evident that when a bit in the key was changed, the cipher text generated using NTSA algorithm had more drastic change than the cipher text created using TEA. This shows the increased security offered by the NTSA algorithm compared to TEA.

Experiment 2: an encryption was performed for NTSA and TEA algorithms using keys with varying key sizes 48, 64 and 128 bits. Then one bit was changed on the plaintext and the experiment is repeated. It was observed that for every 64-bit block, one-bit change in plaintext resulted in significant changes on the cipher text. Drastic changes were observed for the NTSA algorithm when compared to the tiny encryption algorithm. Figure 8 shows that for every 64-bit block a change in one bit of key with various key sizes and the corresponding change in cipher text for NTSA and TEA.

From Figure 8 it is very evident that when a bit in the plaintext was changed, the cipher text generated using NTSA algorithm had more drastic change than the cipher text created using TEA. This verifies the increased security offered by the NTSA algorithm compared to TEA. Thus, the proposed method NTSA is more efficient and secure than all previously proposed encryption schemes for transfer of text files between embedded devices in IoT network.

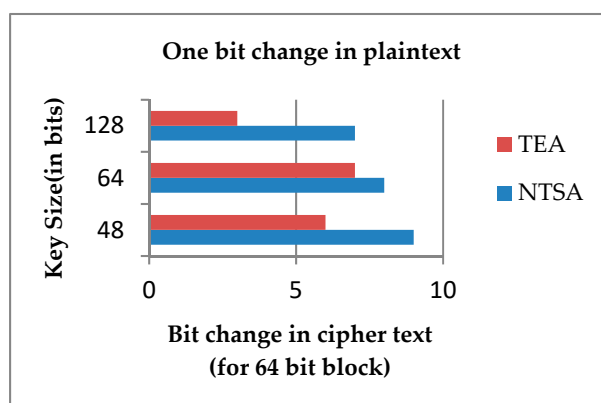


Figure 8. One-bit change in plaintext corresponding change in cipher text for 64-bit block.

## 5. Conclusions

TEA showed better performance in terms of both encryption and decryption execution times than XTEA and XXTEA. The XTEA was proposed to set the key schedule and XXTEA was proposed in order to present the key material slowly. The proposed algorithm NTSA does the same, and experiments performed proved that the performance of NTSA is better than TEA. In addition to this, NTSA created more confusion on the key than the tiny encryption algorithm. The avalanche effect showed a positive result to NTSA when compared to TEA. Thus, NTSA can be used by all the latest applications in IoT devices with different computational and storage facilities to transfer text files efficiently and securely through the network. The NTSA algorithm security can be further increased by encrypting the compressed file. In future we also aim to integrate and implement this algorithm for data transfer in ad hoc, sensor and fog networks [8,52–57].

**Author Contributions:** Conceptualization, S.R.; formal analysis, S.R. and V.M.; funding acquisition, V.M.; investigation, S.R.; methodology, S.R.; project administration, V.P., V.M. and M.K.; resources, V.P. and V.M.; software, M.K.; supervision, V.P.; validation, S.R. and M.K.; visualization, S.R.; writing—original draft, S.R., V.P. and V.M.; writing—review and editing, V.M. and M.K.

**Acknowledgments:** Authors would like to thank the Management and Principal of SCMS School of Engineering and Technology for providing the infrastructure and facilities to carry out the research. Authors would also like to thank Linda Cui, Assistant Editor for all the support handling the manuscript and the reviewers for providing valuable suggestions and comments in improving the manuscript.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Porambage, P.; Okwuibe, J.; Liyanage, M.; Ylianttila, M.; Taleb, T. Survey on Multi-Access Edge Computing for Internet of Things Realization. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2961–2991. [CrossRef]
2. Ploennigs, J.; Cohn, J.; Stanford-Clark, A. The Future of IoT. *IEEE Internet Things Mag.* **2018**, *1*, 28–33. [CrossRef]
3. Philip, V.; Suman, V.K.; Menon, V.G.; Dhanya, K. A Review on latest Internet of Things based Healthcare Applications. *Int. J. Comput. Sci. Inf. Secur.* **2017**, *15*, 248–254.
4. Deshkar, S.; Thanseeh, R.A.; Menon, V.G. A Review on IoT based m-Health Systems for Diabetes. *Int. J. Comput. Sci. Telecommun.* **2017**, *8*, 13–18.
5. Vinoj, P.G.; Jacob, S.; Menon, V.G. Hybrid brainactuated muscle interface for the physically disabled. In *Basic and Clinical Pharmacology and Toxicology*; Wiley: Hoboken, NJ, USA, 2018; Volume 123.
6. Keerthi, K.S.; Mahapatra, B.; Menon, V.G. Into the World of Underwater Swarm Robotics: Architecture, Communication, Applications and Challenges. *Recent Pat. Comput. Sci.* **2019**, *12*, 1.
7. Bordel, B.; Alcarria, R.; De Andres, D.M.; You, I.; Martin, D. Securing Internet-of-Things Systems through Implicit and Explicit Reputation Models. *IEEE Access* **2018**, *6*, 47472–47488. [CrossRef]

8. Menon, V.G.; Prathap, J. Vehicular Fog Computing: Challenges applications and future directions. *Int. J. Veh. Telemat. Infotain. Syst.* **2017**, *1*, 15–23. [[CrossRef](#)]
9. Frustaci, M.; Pace, P.; Aloï, G.; Fortino, G. Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. *IEEE Internet Things J.* **2018**, *5*, 2483–2495. [[CrossRef](#)]
10. Wang, B.; Zhan, Y.; Zhang, Z. Cryptanalysis of a Symmetric Fully Homomorphic Encryption Scheme. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 1460–1467. [[CrossRef](#)]
11. Maimuț, D.; Reyhanitabar, R. Authenticated Encryption: Toward Next-Generation Algorithms. *IEEE Secur. Privacy* **2014**, *12*, 70–72. [[CrossRef](#)]
12. Ahmad, S.; Alam, K.M.R.; Rahman, H.; Tamura, S. A comparison between symmetric and asymmetric key encryption algorithm based decryption mixnets. In Proceedings of the 2015 International Conference on Networking Systems and Security (NSysS), Dhaka, Bangladesh, 5–7 January 2015; pp. 1–5.
13. Yassein, M.B.; Aljawarneh, S.; Qawasmeh, E.; Mardini, W.; Khamayseh, Y. Comprehensive study of symmetric key and asymmetric key encryption algorithms. In Proceedings of the 2017 International Conference on Engineering and Technology (ICET), Antalya, Turkey, 21–23 August 2017; pp. 1–7.
14. Lamba, C.S. Design and Analysis of Stream Cipher for Network Security. In Proceedings of the 2010 Second International Conference on Communication Software and Networks, Singapore, 26–28 February 2010; pp. 562–567.
15. Baker, S.I.B.; Al-Hamami, A.H. Novel Algorithm in Symmetric Encryption (NASE): Based on Feistel Cipher. In Proceedings of the 2017 International Conference on New Trends in Computing Sciences (ICTCS), Amman, Jordan, 9–11 October 2017; pp. 191–196.
16. Rebeiro, C.; Nguyen, P.H.; Mukhopadhyay, D.; Poschmann, A. Formalizing the Effect of Feistel Cipher Structures on Differential Cache Attacks. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1274–1279. [[CrossRef](#)]
17. Wheeler, D.; Needham, R. TEA, a tiny encryption algorithm. In Proceedings of the 1995 Fast Software En-Cryption Workshop, Leuven, Belgium, 14–16 December 1995; Springer: Berlin/Heidelberg, Germany, 1995; pp. 97–110.
18. Amrutha George, A.; Riyadh, M.; Prajitha, M.V. Secure image transferring using KBRP and TEA algorithms. In Proceedings of the 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India, 19–20 March 2015; pp. 1–5.
19. Abdelhalim, M.B.; El-Mahallawy, M.; Ayyad, M.; Elhennawy, A. Implementation of a modified lightweight cryptographic TEA algorithm in RFID system. In Proceedings of the 2011 International Conference for Internet Technology and Secured Transactions, Abu Dhabi, UAE, 11–14 December 2011; pp. 509–513.
20. Shepherd, S.J. The Tiny Encryption Algorithm. *Cryptologia* **2007**, *31*, 233–245. [[CrossRef](#)]
21. Sima, I.; Tarmurean, D.; Greu, V.; Diaconu, A. XXTEA, an alternative replacement of KASUMI cipher algorithm in A5/3 GSM and f8, f9 UMTS data security functions. In Proceedings of the 2012 9th International Conference on Communications (COMM), Bucharest, Romania, 21–23 June 2012; pp. 323–326.
22. Lu, J. Related-key rectangle attack on 36 rounds of the XTEA block cipher. *Int. J. Inf. Sec.* **2009**, *8*, 1–11.
23. Holden, J. Demitasse: A “Small” Version of the Tiny Encryption Algorithm and Its Use in a Classroom Setting. *Cryptologia* **2013**, *37*, 74–83. [[CrossRef](#)]
24. De Dormale, G.M.; Bass, J.; Quisquater, J.-J. On Solving RC5 Challenges with FPGAs. In Proceedings of the 15th Annual IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM 2007), Napa, CA, USA, 23–25 April 2007; pp. 281–282.
25. Li, T.; Wu, H.; Wang, X.; Bao, F. *SenSec Design Technical Report-TR v1.1*; InfoComm Security Department, Institute for Infocomm Research: Singapore, 2005.
26. Karlof, C.; Sastry, N.; Wagner, D. TinySec: A link layer security architecture for wireless sensor networks. In Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems (SenSys '04), Baltimore, MD, USA, 3–5 November 2004; pp. 162–175.
27. Luk, M.; Mezzour, G.; Perrig, A.; Gligor, V. MiniSec: A secure sensor network communication architecture. In Proceedings of the 6th International Symposium on Information Processing in Sensor Networks (IPSN '07), Cambridge, MA, USA, 25–27 April 2007; pp. 479–488.
28. Standaert, F.-X.; Piret, G.; Gershenfeld, N.; Quisquater, J.-J. SEA: A scalable encryption algorithm for small embedded applications. In Proceedings of the Workshop on RFIP and Light weight Crypto, Graz, Austria, 14–15 July 2005.



29. Hong, D.; Sung, J.; Hong, S.; Lim, J.; Lee, S.; Koo, B.-S.; Lee, C.; Chang, D.; Lee, J.; Jeong, K.; et al. HIGHT: A new block cipher suitable for low-resource device. In *Cryptographic Hardware and Embedded Systems—CHES 2006: 8th International Workshop, Yokohama, Japan, 10–13 October 2006*; Volume 4249 of Lecture Notes in Computer Science; Springer: Berlin, Germany, 2006; pp. 46–59.
30. Usman, M.; Ahmed, I.; Aslam, M.I.; Khan, S.; Shah, U.A. SIT: A Lightweight Encryption Algorithm for Secure Internet of Things. *Int. J. Adv. Comput. Sci. Appl.* **2017**, *8*. [[CrossRef](#)]
31. Liang, C.; Ye, N.; Malekian, R.; Wang, R. The hybrid encryption algorithm of lightweight data in cloud storage. In *Proceedings of the 2016 2nd International Symposium on Agent, Multi-Agent Systems, and Robotics (ISAMSR), Bangi, Malaysia, 23–24 August 2016*; pp. 160–166.
32. Gao, C.; Lv, S.; Wei, Y.; Wang, Z.; Liu, Z.; Cheng, X. M-SSE: An Effective Searchable Symmetric Encryption with Enhanced Security for Mobile Devices. *IEEE Access* **2018**, *6*, 38860–38869. [[CrossRef](#)]
33. Schneier, B. The IDEA Encryption Algorithm. *Dr. Dobbs's J.* **1990**, *18*, 50–56.
34. Burwick, C.; Coppersmith, D.; D'Avignon, E.; Gennaro, R.; Halevi, S.; Jutla, C.; Matyas, S.M.; O'Connor, L.; Peyravian, M.; Safford, D.; et al. MARS—A candidate cipher for AES. 1998. Available online: <http://www.research.ibm.com/security/mars.html> (accessed on 29 April 2018).
35. Abdelhalim, M.B.; El-Mahallawy, M.; Elhennawy, M.A.A. Design and Implementation of an Encryption Algorithm for use in RFID System. *Int. J. RFID Secur. Cryptogr.* **2013**, *2*. [[CrossRef](#)]
36. Zhdanov, O.N.; Sokolov, A.V. Block Symmetric Cryptographic Algorithm based on Principles of variable block length and many-valued logic. *Far East J. Electron. Commun.* **2016**, *16*, 573–589. [[CrossRef](#)]
37. Korea Telecommunication Technology Association. *128 Bit Light Weight Block Cipher LEA*, Information Telecommunication Organization Standard (Korean Standard). 2013.
38. Park, J.H. 128 bit block cipher LEA. *TTA J.* **2015**, *157*.
39. Abdullah, D.; Rahim, R.; Siahaan, A.P.U.; Ulva, A.F.; Fitri, Z.; Malahayati, M.; Harun, H. Super-Encryption Cryptography with IDEA and WAKE Algorithm. *J. Phys. Conf. Ser.* **2018**, *1019*, 012039. [[CrossRef](#)]
40. Anderson, R.; Biham, E.; Knudsen, L. Serpent: A Proposal for the Advanced Encryption Standard. In *Proceedings of the First Advanced Encryption Standard (AES) Conference, Ventura, CA, USA, 20–22 August 1998*.
41. Ren, W.; Miao, Z. A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication. In *Proceedings of the 2010 Second International Conference on Modeling, Simulation and Visualization Methods, Sanya, China, 15–16 May 2010*; pp. 221–225.
42. Wheeler, D.; Needham, R. TEA, A Tiny Encryption Algorithm. Available online: <http://www.cix.co.uk/~klockstone/tea.pdf> (accessed on 22 April 2018).
43. Andem, V.R. *A Cryptanalysis of the Tiny Encryption Algorithm*; The University of Alabama: Tuscaloosa, AL, USA, 2003.
44. Rachmawati, D.; Sharif, A.; Jaysilen; Budiman, M.A. Hybrid Cryptosystem Using Tiny Encryption Algorithm and LUC Algorithm. *IOP Conf. Ser. Mater. Sci. Eng.* **2018**, *300*, 012042. [[CrossRef](#)]
45. Novelan, M.S.; Husein, A.M.; Harahap, M.; Aisyah, S. SMS Security System on Mobile Devices Using Tiny Encryption Algorithm. *IOP Conf. Ser. J. Phys. Conf. Ser.* **2018**, *1007*, 012037. [[CrossRef](#)]
46. Needham, R.M.; Wheeler, D.J. *TEA Extensions*; Technical Report; Computer Laboratory, University of Cambridge: Cambridge, MA, USA, 1997.
47. Kaps, J.-P. Chai-tea, Cryptographic Hardware Implementations of XTEA. In *Proceedings of the INDOCRYPT 08 Proceedings of the 9th International Conference on Cryptology in India: Progress in Cryptology, Kharagpur, India, 14–17 December 2008*.
48. Wheeler, D.; Needham, R. *XXTEA: Correction to XTEA*; Technical report; Computer Laboratory, University of Cambridge: Cambridge, MA, USA, 1998.
49. Coppersmith, D.; Johnson, D.B.; Matyas, S.M. A proposed mode for triple-DES encryption. *IBM J. Res. Dev.* **1996**, *40*, 253–262. [[CrossRef](#)]
50. Milad, A.A.; Muda, H.Z.; Noh, Z.A.; Algaet, M.A. Comparative Study of Performance in Cryptography Algorithms (Blowfish and Skipjack). *J. Comput. Sci.* **2012**, *8*, 1191–1197.
51. Wu, F.; Wu, T.; Yuce, M.R. An Internet-of-Things (IoT) Network System for Connected Safety and Health Monitoring Applications. *Sensors* **2019**, *19*, 21. [[CrossRef](#)] [[PubMed](#)]
52. Menon, V.G.; Prathap, J.; Priya, J. Ensuring reliable communication in disaster recovery operations with reliable routing technique. *Mobile Inf. Syst.* **2016**, *2016*, 9141329. [[CrossRef](#)]

53. Menon, V.G.; Prathap, J. Comparative analysis of opportunistic routing protocols for underwater acoustic sensor networks. In Proceedings of the 2016 International Conference on Emerging Technological Trends (ICETT), Kollam, India, 21–22 October 2016.
54. Menon, V. Optimized Opportunistic Routing in Highly Dynamic Ad hoc Networks. *Preprints* **2019**, *2019*, 020130.
55. Menon, V.G.; Prathap, J. Performance of various Routing Protocols in Mobile Ad Hoc Networks-A Survey. *Res. J. Appl. Sci. Eng. Technol.* **2013**, *6*, 4181–4185. [[CrossRef](#)]
56. Menon, V.G.; Prathap, J. Analyzing the behavior and performance of opportunistic routing protocols in highly mobile wireless ad hoc networks. *Int. J. Eng. Technol.* **2016**, *8*, 1916–1924. [[CrossRef](#)]
57. Menon, V.G.; Prathap, P.M.J. Opportunistic routing with virtual coordinates to handle communication voids in mobile ad hoc networks. In *Advances in Signal Processing and Intelligent Recognition Systems*; Springer: Cham, Switzerland, 2016; pp. 323–334.



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

Access through SCMS School of Engine...

Purchase P...

Access through

Article preview

Abstract

Introduction

Section snippets

References (61)

Cited by (62)



## Future Generation Computer Systems

Volume 94, May 2019, Pages 333-350



# A machine learning based approach to detect malicious android apps using discriminant system calls

Vinod P. <sup>a</sup>, Akka Zemmani <sup>b</sup>, Mauro Conti <sup>c</sup>

Show more ▾

+ Add to Mendeley ⚡ Share 🗨 Cite

<https://doi.org/10.1016/j.future.2018.11.021>

[Get rights and content](#) ↗

### Abstract

The openness of Android framework and the enhancement of users trust have gained the attention of malware writers. The momentum of downloaded applications(app for short) from numerous app stores has stimulated the

Author

X



**Vinod P.**, is Post Doc at Department of Mathematics, University of Padua, Italy. Prior to joining Padua he was working as Professor in SCMS School of Engineering & Technology, Cochin, India. He holds his Ph.D. in Computer Engineering from Malaviya National Institute of Technology, Jaipur, India. He has more than 50 research articles published in peer reviewed Journals and International Conferences. He is reviewer of number [FEEDBACK](#) 🗨

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/337362793>

# PERIÓDICO TCHÊ QUÍMICA ARTIGO ORIGINAL RUMO À REDUÇÃO DO ESFORÇO COMPUTACIONAL NAS PREDIÇÕES DE VIBRAÇÕES INDUZIDAS POR VÓRTICES DE UM RISCADOR CILÍNDRICO TOWARDS REDUCIN....

Article in *Periodico Tche Quimica* · November 2019

CITATIONS

0

READS

226

3 authors:



**Vidya Chandran**

SCMS School of Engineering and Technology, Karukutty

24 PUBLICATIONS 31 CITATIONS

[SEE PROFILE](#)



**Sheeja Janardhanan**

Indian Maritime University

66 PUBLICATIONS 77 CITATIONS

[SEE PROFILE](#)



**M. Sekar**

37 PUBLICATIONS 514 CITATIONS

[SEE PROFILE](#)

Some of the authors of this publication are also working on these related projects:



Design and Propulsion of an Autonomous Underwater Vehicle [View project](#)



Numerical Manoeuvring [View project](#)

## RUMO À REDUÇÃO DO ESFORÇO COMPUTACIONAL NAS PREDIÇÕES DE VIBRAÇÕES INDUZIDAS POR VÓRTICES DE UM RISCADOR CILÍNDRICO

## TOWARDS REDUCING COMPUTATIONAL EFFORT IN VORTEX INDUCED VIBRATION PREDICTIONS OF A CYLINDRICAL RISER.

VIDYA, Chandran<sup>1</sup>; SHEEJA, Janardhanan<sup>2</sup>; SEKAR, M<sup>3\*</sup>;<sup>1</sup>Department of Mechanical Engineering, Karunya Institute of Technology and Sciences, Tamil Nadu, India<sup>2</sup>Department of Mechanical Engineering, SCMS School of Engineering and Technology, Kerala, India<sup>3</sup>Department of Mechanical Engineering, AAA College of Engineering and Technology, Tamil Nadu, India

\* Correspondence author

e-mail: mailtosekar@gmail.com

Received 23 August 2019; received in revised form 30 October 2019; accepted 18 November 2019

## RESUMO

As vibrações induzidas pelo fluxo geralmente denominadas vibrações induzidas por vórtices são de grande importância no projeto de *risers* marinhos. Esses *risers* cilíndricos flexíveis sofrem vibrações de amplitude muito alta quando a frequência de derramamento de vórtice corresponde à frequência natural do riser. Tais vibrações são capazes de colocar a segurança da tripulação trabalhando em plataformas *offshore* em questão. Portanto, a previsão de resposta de tais estruturas é considerada muito importante. Embora muito trabalho numérico tenha sido feito neste campo, tratando o problema como uma interação fluido-estrutura bidirecional, o fato de esses trabalhos exigirem esforços computacionais muito altos não o tornou pertinente quando os recursos computacionais de ponta não estão prontamente disponíveis. Uma rápida previsão da resposta estrutural de tais estruturas esbeltas precisa ser útil para os engenheiros em momentos de necessidade. Este artigo aborda uma técnica de solução para esse problema através de um método econômico para previsão rápida e confiável da resposta do riser sob vibração induzida por vórtice, utilizando o esforço computacional mínimo para o número moderado de Reynolds ( $Re \leq 3 \times 10^5$ ). As simulações de fluxo bidimensionais são realizadas usando CFD baseado em RANSE, seguido pelo mapeamento uniforme das forças hidrodinâmicas no *riser* tridimensional. A grade usada para a simulação numérica foi validada com relação aos resultados experimentais do túnel de vento para  $Re = 5,3 \times 10^4$ . As forças hidrodinâmicas correspondentes aos três primeiros harmônicos da frequência natural do *riser* foram usadas como entrada no solucionador estrutural para analisar a resposta usando o método dos elementos finitos. Obtiveram-se trajetórias do cilindro nos três primeiros modos de vibração, um padrão típico de oito algarismos, característico da vibração de bloqueio. Verificou-se que o método é bastante eficaz no cálculo rápido de problemas de vibração induzidos por fluxo para números de Reynolds baixos e moderados.

**Palavras-chave:** CFD; cilindros de fluxo passado; lock-in; resposta estrutural; vibrações induzidas por vórtices

## ABSTRACT

Vibrations induced by flow, generally referred to as vortex induced vibrations, are of great importance in the design of marine risers. These flexible cylindrical risers undergo vibrations of very high amplitude when the vortex shedding frequency matches the natural frequency of the riser. Such vibrations are capable of putting the safety of crew working on offshore platforms in question. Hence the prediction of response of such structures is considered very important. Although a lot of numerical work has been done in this field treating the problem as a two-way fluid structure interaction, the fact that these works demand very high computational efforts has not made it pertinent where high end computing resources are not readily available. A quick prediction of the structural response of such slender structures needs to be handy to the engineers at times of need. This paper addresses a solution technique for such a problem through an economical method for quick and reliable prediction of riser response under vortex induced vibration utilizing minimum computational effort for moderate Reynolds number ( $Re \leq 3 \times 10^5$ ). Two dimensional flow simulations are carried out using RANSE based CFD followed by the uniform mapping of hydrodynamic forces on to the three dimensional riser. The grid used for the numerical simulation has been well validated against wind-tunnel experimental results for  $Re = 5.3 \times 10^4$ . Hydrodynamic forces corresponding to the first three harmonics of natural frequency of the riser have been used as input in the structural

solver to analyse the response using finite element method. Trajectories of the cylinder in the first three modes of vibration have been obtained, a typical eight figure pattern which is characteristic for lock-in vibration. It is found that the method is quite effective in the quick computation of flow induced vibration problems for low and moderate Reynolds numbers.

**Keywords:** CFD; flow past cylinders; lock-in; structural response; vortex-induced-vibrations.

## 1. INTRODUCTION

Vortex shedding around bluff bodies is natural yet a phenomenon that consumed years of comprehensive studies, for it is well known for the imminent catastrophes it brings with it. Tacoma Narrows Bridge disaster is the worst case one could recall while thinking about vortex shedding. With the ever-rising demand for petroleum products, the development of offshore oilfields has been growing fast over the past century. The drilling facilities are designed in such a way that it enables a prolonged offshore operation for a large period of time starting from a few months to several decades. Numerous studies are being carried out in this field for the proper design of the slender marine risers in ocean. The stability of structures especially those carrying pressurised fluid in them is a topic of research interest. (Ramírez *et al.* 2017, Pezzini, *et al.*, 2017) If the bluff structure is not mounted rigidly and the frequency of vortex shedding matches the natural frequency of the structure, the structure begins to resonate, vibrating with harmonic oscillations of large amplitude (Bourguet, 2011). This phenomenon is known as lock-in. During lock-in, vortex shedding frequency shifts to the natural frequency of the structure leading to large amplitude vibrations.

The vortex shedding occurs at a discrete frequency and is a function of the Reynolds number, defined by Equation 1.

$$Re = \frac{\rho V D}{\mu} \quad (\text{Eq. 1})$$

The dimensionless frequency of the vortex shedding, the shedding Strouhal number,  $St = f_v D/V$ , is approximately equal to 0.2 when the Reynolds number is greater than 1,000. When vortices are shed from the cylinder, uneven pressure distribution develops around the upper and lower surfaces of the cylinder, generating an oscillatory hydrodynamic loading (lift) on the cylinder. This unsteady force given by Equation 2

can induce significant cross flow vibrations on a structure, especially if the "resonance" condition is met.

$$F_L = \frac{1}{2} C_L \rho A V^2 \quad (\text{Eq. 2})$$

$C_L$  is the coefficient of lift. The cylinder also experiences a net force along the flow direction and is called the drag force and is given by Equation 3.

$$F_D = \frac{1}{2} C_D \rho A V^2 \quad (\text{Eq. 3})$$

where  $C_D$  is the drag coefficient.

The phenomenon of lock-in was first observed by Feng during his classical experiment (Feng, 1968). He described the phenomenon observed as matching the frequency of cylinder vibration and fluid force to the natural frequency in a vacuum. Later it was observed that this matching of frequency holds good only for higher values of mass ratio,  $m^*$  (Blevins, 1990). Further research in the field explains the phenomenon as either large amplitude vibration of the cylinder (Sarpkaya, 1977) or matching of the frequency of cylinder vibration and fluid force (Khalak and Williamson, 1999). Synchronization and lock-in, are often used synonymously, but from the experiments it was shown that, for zero damping and sinusoidal motion, synchronization ( $f = f_n$ ) occurs at only one condition, effective stiffness ratio,  $k_{\text{eff}}^* = 0$  (Sheils *et al.*, 2001), where  $k_{\text{eff}}^*$  is defined as in Equation 4.

$$k_{\text{eff}}^* = \frac{m^*}{V_R^2} \quad (\text{Eq. 4})$$

Matching of vortex shedding frequency with one of the natural frequencies of the structure may not always be the only (sole) reason for lock-in. Contrary to classical lock-in, whereby the

oscillation frequency matches the structural natural frequency, in the experiments on stationary cylinder free to oscillate, it was found that the oscillation frequency increases markedly above the natural frequency, through the excitation regime while at the same time it is below the vortex shedding frequency (of the non-oscillating structures) (Khalak and Williamson, 1999). Even though vortex shedding and the vibration induced by it has been a topic of extensive research for several years, due to its intrinsic nature, the researchers are still not able to confidently define the phenomenon and describe the flow physics behind shifting of shedding frequency. Numerous analytical, experimental, and numerical investigations have been carried out in the field of vortex induced vibration (VIV) of long flexible cylinders. Most of these studies focused on the structural response of the cylinders rather than the phenomenon of lock-in (Trim *et al.*, 2005; Vandiver *et al.*, 2009). Freely oscillating cylinders were modelling as a spring mass system with single or two degrees of freedom (Sekar *et al.*, 2009). Experiments in wind tunnels using particle induced velocimetry (PIV) have proved to predict the flow characteristics and structural response with much accuracy (Wang *et al.*, 2015). Laboratory experiments and offshore large scale experiments have also been recognized as effective tools for analysis of VIV (Domal and Sharma, 2017; Gao *et al.*, 2017). However, for case specific analysis of the problem, experiments are not always possible, and hence most of the researchers rely on computational fluid dynamics (CFD) as a tool for predicting VIV (Daniels *et al.*, 2016). Unlike the experiments CFD facilitates detailed study of the flow physics which is otherwise impossible. Three dimensional (3D) numerical simulations are widely accepted in the research community as capable of predicting VIV characteristics accurately. Researchers were under the notion that two dimensional (2D) simulations are acceptable only for lower Reynolds numbers ( $Re < 250$ ) because of the inherent 3D characteristics of vortices. Later on several researchers have proved that 2D simulations are capable of accurately predicting VIV phenomenon in rigid structure cases (Xie *et al.*, 2012). 3D numerical simulation demands high computational resources for flow analysis and also for generation of the 3D computational grid. The objective of the present work is to test the accuracy of 2D numerical simulations in predicting flow characteristics of VIV and to develop an easy and economical tool for comprehensive analysis of vortex shedding and the structural response during VIV. RANSE-based Commercial solver

ANSYS Fluent -15, as well as ANSYS Workbench -15, have been used as the tools for the study.

## 2. MATERIALS AND METHODS

The grid generated for the analysis has been validated using the experimental method. Experiments have been carried out on a subsonic wind tunnel, and the results have been compared with those of numerical studies for the same value of Reynold's number. Details of the material and dimensions of the test cylinder are shown in Table 1.

**Table 1.** Geometric specification of the riser and fluid domain

|  |        |
|--|--------|
| The diameter of the riser (D)                | 0.05 m |
| Distance from inlet to the riser             | 9 D    |
| Distance from riser to outlet                | 27 D   |
| Lateral distance from cylinder to both sides | 7 D    |
| Cylinder Material (Hollow)                   | PVC    |

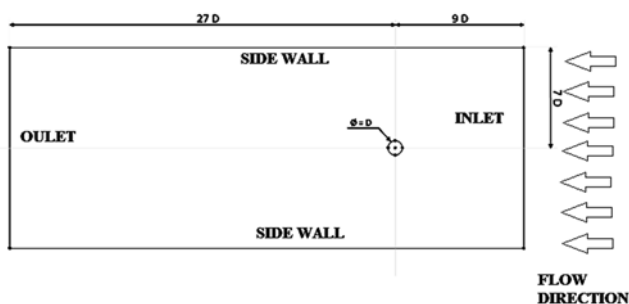
### 2.1. CFD Prediction for Vortex Shedding

Geometric modeling and the generation of computational grids around the riser placed in a fluid domain, mimicking ocean environment (still water conditions) have been carried out using ANSYS ICEM CFD.

#### 2.1.1. Creating a computational domain

The geometric specifications of the riser model and the fluid domain with respect to the diameter of the riser are given in Table 1. The length of the riser (L) has been chosen to be 0.4 m, so that the aspect ratio (L/D) is 20. At this value of aspect ratio, the model has been found to account for the three dimensional effects of vortex shedding (Vandiver *et al.*, 2009). Figure 1 shows the representation of fluid domain. Domain size has been fixed based on the published domain independency test results (Gutafsson, 2012).





**Figure 1.** Dimensions of the fluid domain with the riser

Meshing or generating the computational grid in the fluid domain around the riser effectively is most important in capturing the vortex shedding phenomenon. The vorticity transport equation represented by Equation 5 gives an insight into the mechanism of generation and transport of vortices.

$$\frac{\partial \omega}{\partial t} + \mathbf{u} \cdot \nabla \omega + \omega(\nabla \cdot \mathbf{u}) = \omega \cdot \nabla \mathbf{u} + \frac{1}{\rho^2} \nabla p + \nu \nabla^2 \omega \quad (\text{Eq. 5})$$

The third term on the right hand side of the equation represents the diffusion of vorticity by viscosity. Due to this term, vorticity is generated along solid wall boundaries because of steep velocity gradients. These steep gradients make vortical motion susceptible to numerical dissipation. But in the near wall region, where the mesh is usually very fine, this is not an issue since the fine mesh can capture viscous effects. It is a bigger issue in the far field, where poor resolution can severely weaken and distort the vertical structures (Kamkar, 2011). Hence importance must be given even to the far field wake, where the major concern is the mesh resolution.

### 2.1.2. Mesh Generation

Mesh element size near the surface of the cylinder is of great importance in case of turbulent flow compared to laminar flow. The interaction between the mean flow and the boundary layer flow is more in turbulent flow, and turbulence plays the most important role in the transport of momentum and hence must be properly resolved, especially at the boundary for better results. To accurately capture the features of flow near the boundary, the spacing of the first grid point should be such that it is well within the laminar sub layer of the boundary layer for turbulent flow and within the boundary layer for laminar flow. In the outset a mesh has been generated, and the drag force computed has been compared with the value

obtained through experiments. The experimental set up is described in the previous section. The flow over the cylinder corresponds to a  $Re = 5.3 \times 10^4$  which is in the laminar flow regime. The boundary layer at  $Re = 5.3 \times 10^4$  is laminar before separation, but during vortex shedding the wake of the cylinder turns turbulent in nature at any  $Re > 300$ . Hence while meshing the geometry due consideration must given to the possible influence of turbulence on the boundary layer.

From Blasius's solution of the equation for the boundary layer in laminar flow, represented by Equation 6, the boundary layer thickness, considering the boundary layer to be completely laminar, is  $1 \times 10^{-3}$  m.

$$\delta = \frac{4.91 D}{\sqrt{Re_D}} \quad (\text{Eq. 6})$$

If, for an additional factor of safety, we consider the influence of turbulence on the boundary layer, then the minimum element size near the cylinder wall must be chosen so that it is well with the laminar sub-layer of the boundary layer. The thickness of the laminar sub-layer is obtained from Equation 7.

$$\delta' = \frac{11.6 \nu}{V^*} \quad (\text{Eq. 7})$$

Where  $V^*$  is the frictional velocity given by Equation 8.

$$V^* = \sqrt{\frac{\tau_0}{\rho}} \quad (\text{Eq. 8})$$

And  $\tau_0$  the wall shear stress is obtained as in Equation 9.

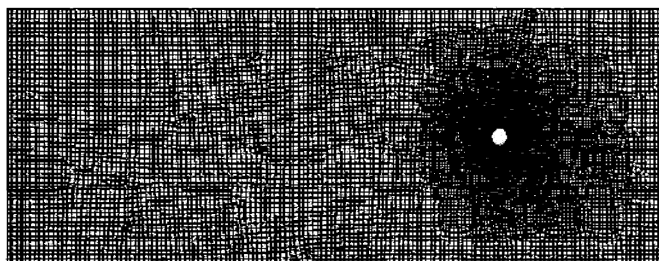
$$\tau_0 = \frac{0.664 \rho V^2}{2\sqrt{Re_D}} \quad (\text{Eq. 9})$$

For  $Re = 5.3 \times 10^4$ , the thickness of the laminar sub-layer has been obtained from the Von-Karman momentum integral equation as  $2.8 \times 10^{-4}$  m. While generating mesh for computation,  $3 \times 10^{-4}$  m has been fixed as the global minimum seed element size with a scale factor of 1. An unstructured mesh has been generated with view that the same mesh may be used for analyzing the

variation in flow characteristics with oscillating cylinder. Quad dominant mesh type has been preferred in shell meshing parameters as it suits accurate meshing of curved cylindrical surface. Patch dependent mesh method has been selected since it gives the best quad dominant quality while capturing surface details. Tetra/Mixed mesh type and Robust (Octree) mesh method have been selected for surface meshing. Moreover it is to be observed that the first grid point should exhibit a  $Y^+$  (wall normal dimensionless distance) value of less than 1 in case of RANS simulations. Near wall spacing or element size has been calculated as  $2 \times 10^{-5}$  from Equation 10.

$$\Delta S = \frac{\mu Y^+}{\rho V^*} \quad (\text{Eq. 10})$$

This value of near wall spacing is ensured by fixing maximum element size and height  $3 \times 10^{-5}$  m and height ratio 1.05 with 20 numbers of prism layers to cover the entire boundary layer in the part mesh set up of cylinder surface. After a thorough grid independency study, the final mesh for analysis has been chosen with 41,932 elements. Unstructured mesh used for the flow analysis using ANSYS 15 is shown in Figure 2.



**Figure 2.** Unstructured 2D mesh generated in ANSYS ICEM CFD

### 2.1.3. Flow Analysis

Flow past the cylinder at  $Re = 5.3 \times 10^4$  has been simulated using the generated unstructured mesh in ANSYS Fluent -15. Pressure based transient analysis has been carried out. Fluid flowing has been chosen to be water at density  $998.2 \text{ kg/m}^3$ , and the inlet velocity  $1.06 \text{ m/s}$  in order to match the  $Re$  value.  $k-\omega$  SST turbulence model has been selected, which has been tested against other models and proven to be the most adaptable model to predict the near cylinder and wake flow characteristics (Chandran *et al.*, 2018). Velocity inlet boundary condition has been given at the inlet, pressure outlet at the outlet boundary, and

for both sides of the domain, symmetry boundary condition (Chandran *et al.*, 2019). Pressure velocity coupling has been done using PISO scheme. Second order upwind spatial discretization has been selected for momentum and turbulent kinetic energy. Second order implicit transient formulation has been used. The spatial discretization gradient is least squares cell based. Since the simulation has been compared with the results obtained from wind tunnel experiments turbulent intensity has been calculated from the empirical correlation for a duct flow given by Equation 11.

$$I = \frac{V'}{V_{\text{avg}}} = 0.16 (Re_D)^{\frac{1}{8}} \quad (\text{Eq. 11})$$

Where  $V$  the root mean square of velocity fluctuations and  $V_{\text{avg}}$  is the mean flow velocity. For  $Re = 5.3 \times 10^4$ , the turbulence intensity will be 4 % according to Equation 11 and hence so chosen for analysis. The time step size for the transient simulation has been calculated based on vortex shedding frequency corresponding to  $Re = 5.3 \times 10^4$ . The time period of vortex shedding has been calculated from the definition of Strouhal number ( $St$ ) given by Equation 12.

$$St = \frac{fD}{V} \quad (\text{Eq. 12})$$

where  $f$  is the vortex shedding frequency.

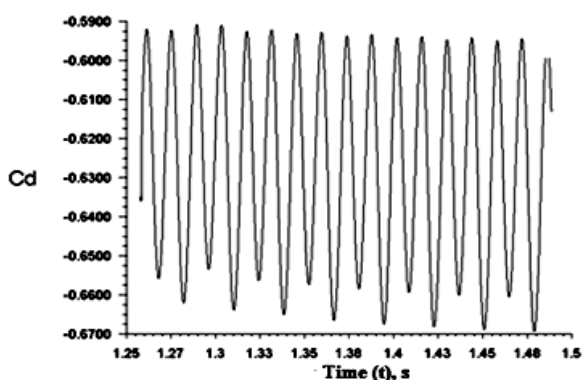
The time period has been obtained as 0.25 seconds from the value of frequency. For accurately capturing the shedding phenomenon one-time period should contain at least 20 time steps. Accommodating 25 time steps per time period, the time step size obtained is 0.01 seconds. Further for ensuring stability of the solution, Courant Friedrichs Lewy (CFL) condition must be satisfied as given by Equation 13.

$$\Delta t = \frac{C_m \Delta x}{V} \quad (\text{Eq. 13})$$

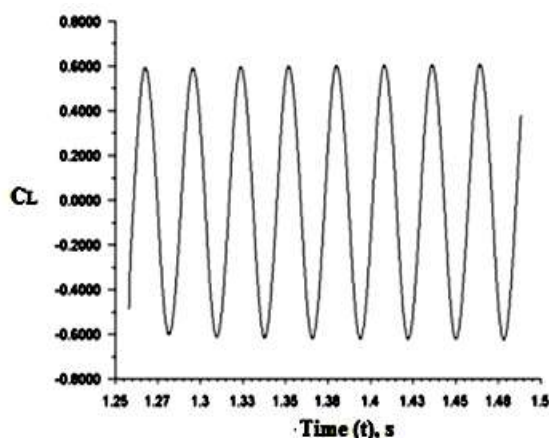
where  $C_m$  is the maximum allowable CFL number.

For explicit solver  $C_m = 1$ .  $\Delta x$  is the minimum element size. The time step size obtained from Equation 13 is  $3 \times 10^{-4}$  seconds. A time step size of  $1 \times 10^{-4}$  seconds has been selected for the transient analysis of the flow with a safety factor. Simulations have been performed for various time step sizes ranging from  $1 \times 10^{-3}$  to

$5 \times 10^{-5}$ . Above a value of  $1 \times 10^{-4}$  the results have been found to be independent of time step size. Simulations have been run for 5 seconds, and it took nearly 1.5 hours of physical time to complete the runs on an 8 GB RAM machine. Analysis of flow took 1.36 seconds computational time for reaching convergence. RMS value of coefficient of drag ( $C_D$ ) obtained from the analysis is 0.63, and that of coefficient of lift ( $C_L$ ) is 0.61. Shedding frequency has been calculated from the period of oscillation of the lift force. Lift force oscillates about zero mean value at the same frequency as that of vortex shedding. The frequency of oscillation of  $C_L$ , and hence that of shedding, has been found to be equal to be 35.7 Hz, which corresponds to a  $St = 0.28$ . A relationship between  $St$  and  $Re$  (Techet, 2005) it is observed that at  $Re = 5.3 \times 10^4$  for a smooth cylinder, Strouhal number value is just above 0.3. Hence the obtained shedding frequency value from the numerical simulation has been proved to be in acceptable range.  $C_D$  and  $C_L$  time histories after convergence for a number of time periods are presented in Figure 3 and Figure 4.



**Figure 3.** Time history of the coefficient of drag ( $C_D$ ) at  $Re = 5.3 \times 10^4$



**Figure 4.** Time history of the coefficient of lift ( $C_L$ ) at  $Re = 5.3 \times 10^4$

## 2.2. Experiment - Flow Past Horizontal Cylinder

Experiments have been conducted with two folded objectives. The first one does a quantitative comparison, and the other one for a qualitative comparison. Quantitative comparisons with the numerical study have been established through a test at moderate  $Re = 5.3 \times 10^4$  while the qualitative ones employed lower  $Re$  tests for flow visualizations, thus proving the efficacy of the mesh at moderate and low  $Re$ .

### 2.2.1. Quantitative Comparisons

A smoke test was carried out in the subsonic wind tunnel of Aerospace Laboratory of Karunya Institute of Technology and Sciences, Coimbatore, India. A horizontal cylinder of diameter 50 mm and length 600 mm fitted with pressure tapings has been used as the model for testing. The compressor of the wind tunnel unit was operated at 600 rpm, which corresponds to 16.4 m/s ( $Re = 5.3 \times 10^4$ ) velocity at the test section. Smoke was inducted into the test section by burning liquid paraffin. Flow patterns and vortex shedding around the cylinder were captured using a high resolution camera.  $C_D$  and  $C_L$  values have been calculated from the measured pressure distribution. Details of the wind tunnel are as follows.

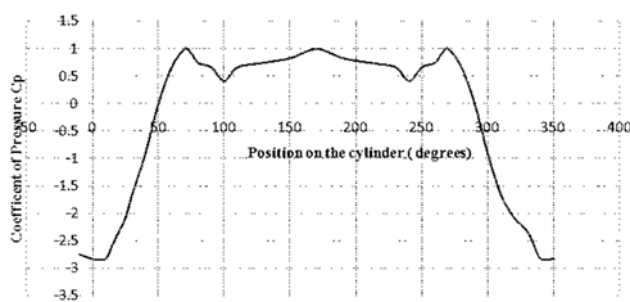
#### 2.2.1.1. Wind tunnel specification

|                    |   |                                     |
|--------------------|---|-------------------------------------|
| Test Section Size  | : | Cross section =<br>600 x 600 mm     |
| Length             | : | 4000 mm                             |
| Maximum Speed      | : | 45 m/s                              |
| Contraction Ratio  | : | 6:1                                 |
| Contraction Length | : | 1.8 m                               |
| Entry Section      | : | Bell mouthed.                       |
| Smoke              | : | Provided in the<br>contraction cone |
| Power              | : | 22 kW/30 HP AC<br>motor.            |

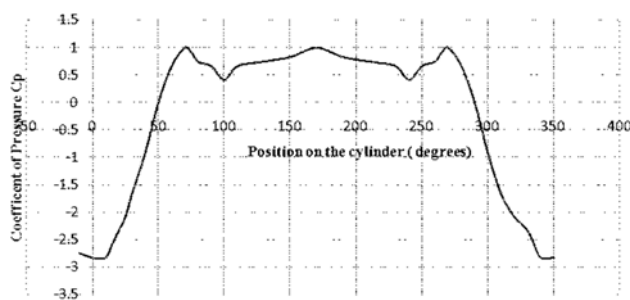
An inclined manometer with ethanol as the manometric fluid is fixed on the tunnel. The two limbs of the manometer are connected to the static pressure holes one in the settling chamber just before the contraction and the other to that at the entrance of the test section. The reading on the manometer is very near to the dynamic head of the fluid in the test section, and it serves as a reference for keeping the tunnel speed constant. The tunnel is also provided with a pitot static tube

which can be traversed across the tunnel cross section.

Pressure readings have been observed from the pressure ports provided on the circumference of the cylinder. Static and stagnation pressure have also been observed. Plots of pressure distributions around the cylinder and coefficient of pressure are represented in graphs Figure 5(a) and 5(b).  $C_D$  has been calculated by integrating  $C_p \cos \theta$  over  $360^\circ$  using Simpson's method of integration. The value of  $C_D$  obtained from the wind tunnel experiment is 0.62. A comparison of the results obtained from the simulations and experiment are given in Table 2.



a)



b)

**Figure 5.** (a) Pressure distribution around the cylinder at  $Re = 5.3 \times 10^4$  (b) Coefficient of pressure around the cylinder at  $Re = 5.3 \times 10^4$

### 2.2.2. Qualitative Comparisons

An experiment to visualize, study, and analyze the characteristics of wake behind the horizontal cylindrical model has been conducted through smoke injection tests in the wind tunnel. A 50 mm diameter cylinder with 600 mm length has been used for flow visualization. The model is exactly similar to the one used for pressure measurement but without pressure ports. The model which had been used for pressure measurement cannot be used in this scenario because of the risk of the pressure ports getting

clogged with smoke particles. The recommended maximum tunnel speed for smoke visualization experiments is 4 m/s. Smoke tests have been performed at 0.6 m/s which corresponds to  $Re = 2000$ . Numerical simulations also have been performed using ANSYS Fluent 15 for the same Reynolds number using the previously generated mesh. Results obtained from the experiment and simulations are compared in Table 2.  $St$  has been calculated from the frequency of vortex shedding using Equation 12. In numerical simulations the shedding frequency is taken to be equal to the oscillation frequency of lift coefficient. Shedding frequency is obtained as 0.99 Hz and Strouhal number as 0.1995 for  $Re = 2000$ . Vortex shedding frequency from the wind tunnel experiment has been calculated by repeatedly noting from the recorded video of shedding phenomenon, the time is taken for shedding 20 vortices from the upper boundary of the cylinder, and then taking the average time observed for the calculation. Results obtained are presented in Table 2 for comparison with those obtained from numerical simulations.

Figures 6(a) and 6(b) represent the flow pattern obtained from the numerical study after convergence at 1.6 seconds of flow and wind tunnel test respectively for flow past cylinder at  $Re = 2000$ . Distances to the lower pressure zones (vortices) shed from the cylinder are indicated on a scale of the diameter of the cylinder. The length of the line segment in both figures corresponds to the diameter of the cylinder. The angle of separation of the boundary layer is shown in the wake patterns given in Figures 7(a) and 7(b). The numerical value of the separation angle is given in Table 2. For verification of the results from the present grid, flow analysis has been carried out at  $Re = 1000$ , in order to validate the grid using other published numerical works. The RMS value of  $C_D$  is found to be 1.24, which is very much comparable with the published results at  $Re=1000$  ( $C_D= 1.15$ ) (Braza. *et al.*, 1986).

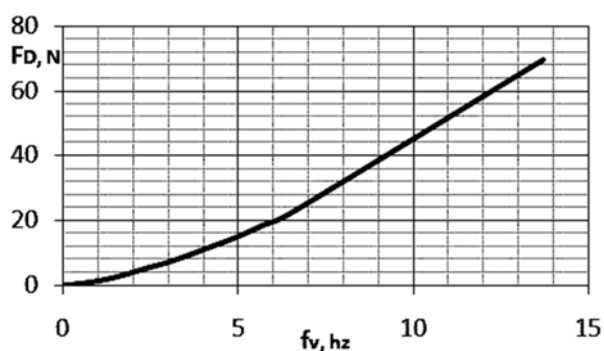
### 2.3. Force - Frequency Plot and Structural Analysis

Characteristics of flow past cylinder is a topic extensively investigated by researchers. Many have proposed plots from experimental, analytical, and numerical simulation results, which show the relationship between various flow parameters such as. with  $Re$ . The present work focuses on a marine riser model of specified dimension. A methodology has been developed to predict the structural response especially the trajectory of any section of the riser under vortex induced vibration. As the first phase, a data sheet has been created using the unstructured 2D mesh

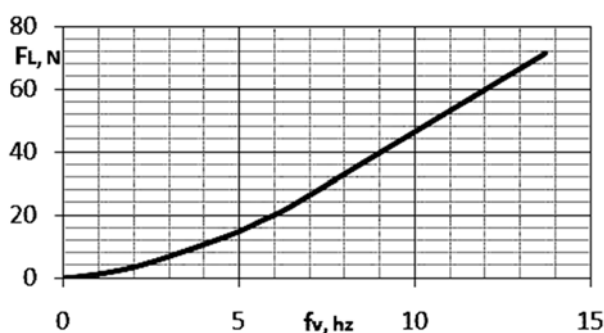
given in Figure 2. The sheet gives the numerical results of  $C_D$ ,  $C_L$ , and vortex shedding frequency ( $f_v$ ) from the 2D simulations performed in ANSYS Fluent-15 for a range of Reynolds number up to the sub critical value and the values have been mapped over the entire length of a 3D cylinder

Simulations have been performed for  $Re = 100$  to  $20,000$ . The velocity of flow has been assumed to be uniform along the span of the cylinder. Using the values of  $C_D$  and  $C_L$  obtained from the flow analysis lift and drag force acting on a cylindrical riser of 8 m length, and 0.05 m diameter has been estimated. Figures 8(a) and 8(b) show the plot for drag and lift forces on a cylindrical riser model of 0.05 diameter and 8 m length against its vortex shedding frequency.

From the plot, the hydrodynamic forces acting on the cylinder at various frequencies can be obtained. The value of hydrodynamic loads obtained from the plot at a specific frequency has been used as the input for predicting the structural response of the cylinder and the trajectory of any point on the surface of the cylinder.



a)



b)

**Figure 8.** (a) Drag Force – Frequency plot  
(b) Lift Force – Frequency plot

Structural analysis of the cylinder model has been performed in ANSYS Workbench-15. Drag and lift forces acting on the cylinder as a

result of vortex shedding have been given as input in the solver. It has been treated as an oscillating force having an amplitude equal to maximum lift in the direction perpendicular to the flow (cross flow) and equal to maximum drag in the direction of flow (in line). The frequency of oscillation of lift and drag forces has also been obtained from flow analysis. It has been observed that the drag coefficient is oscillating about a non-zero value at double the frequency of the lift coefficient. Vortices are shed behind the cylinder at the same frequency as that of the oscillating lift force. When the vortex shedding frequency matches the natural frequency of oscillation of the cylindrical structure, a resonance condition, well known as lock – in vibration occurs, which gives rise to oscillations of very high amplitude. This may bring in extensive damage to the structure and to the working crew. Hence the analysis of the response of structures vibrating at their natural frequencies due to vortex shedding is considered to be most desirable in design of offshore structures.

The cylinder has been modeled in ANSYS Workbench-15 as a hollow vertical, having a thickness of  $2.5 \times 10^{-3}$  mm. The material of the riser model has been chosen to be Poly Vinyl Chloride (PVC) of density  $1400 \text{ kg/m}^3$ . The simulation has been performed as a transient case since it involves time varying forces and deformation. The top end has been modeled fixed in the x and y directions, and the bottom end with motion in x, y, and z direction arrested. Since the riser is a flexible structure, Mechanical ANSYS Parametric Design Language (APDL) has been used as the solver. Stiffness and mass coefficients were provided as input in the damping control of analysis settings of the solver. After performing a grid independency analysis, a mesh having 66,158 elements have been chosen for the response analysis. The meshing of the geometry has been done using tetrahedral elements. The time step size has been chosen to be  $5 \times 10^{-2}$  based on the oscillating frequency of hydrodynamic loads. Transient simulation has been performed for 10 seconds. Local displacements at estimated locations of maximum vibration amplitude at the first three modes of vibration were obtained by inserting a displacement probe at the respective locations on the cylinder. Time histories of displacement in the X and Y directions and the trajectory of the cylinder during vibration have been plotted from the probe data.

The first three modes of vibration and the corresponding natural frequencies of the riser in the air have been obtained as 2.99, 9.7, and 20.23

Hz, respectively, from the modal analysis. Natural frequencies of the riser in water have been obtained solving Equation 14, considering added mass to be 70% of the total system mass,  $m_a = 1.12$  kg, and stiffness of the riser  $k = 17.73$  N/m. The first three natural frequencies of the riser in water have been obtained as 2.88 Hz, 7.16 Hz, and 9.41 Hz, respectively.

$$\frac{1}{\omega_{n\text{ water}}^2} = \frac{1}{\omega_{n\text{ air}}^2} + \frac{m_a}{k} \quad (\text{Eq. 14})$$

Drag and lift forces, corresponding to the identified natural frequencies of the riser, have been obtained from the plotted frequency – force graph. The amplitude of variation of drag force has been observed to be much less compared to the lift force. Lift force has been considered as periodically varying force, which oscillates about zero and acting in the cross flow direction as given in Equation.15 in the structural solver.

$$F(t) = F_0 \cos(\omega_v t) \quad (\text{Eq. 15})$$

Drag force oscillates with double the frequency of lift force, and it oscillates about a non-zero value. Drag force has two components, viz. average drag and the fluctuating component of drag force. From the numerical simulation, both RMS value and fluctuation about RMS value of drag forces have been obtained. Drag force is applied to the cylinder in the structural solver, as given by Equation 16.

$$F_D(t) = F_{D\text{ avg}} + F'_D \cos(2\omega_v t) \quad (\text{Eq. 16})$$

Where  $F_{D\text{ avg}}$  is the RMS value of drag force, and  $F'_D$  is its fluctuating component. The lift and drag forces obtained from the flow analysis corresponding to the flow regimes at which vortex shedding frequency ( $\omega_v$ ) matches the first three harmonics of the natural frequency of the cylinder ( $\omega_n$ ) have been used for structural analysis. This condition is generally referred to as lock-in condition. The drag force oscillates at double the frequency of lift coefficient. This phenomenon is well established in published literature (Durbin, 2007).

For the identified natural frequencies, structural analysis has been carried out to study various response parameters. A deformation probe has been inserted at  $z = 4$  m for first and third modes of vibrations and at  $z = 2$  m for the second mode to observe the response of the

cylinder under oscillating load.

### 3. RESULTS AND DISCUSSION

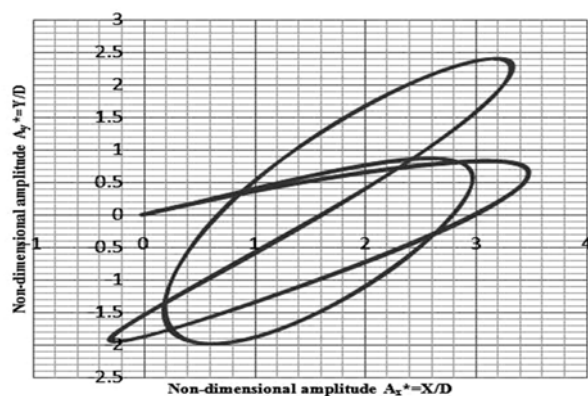
It can be observed that the numerical simulation with the grid generated, as shown in Figure 2 in the present work, is capable of replicating the wake pattern behind the cylinder exactly in the way the experiments do. Wake dimensions are comparable in both cases in terms of the span and angle of separation. Quantitative comparisons between the experimental and numerical values presented in Table 2 indicate the reliability in the present numerical predictions. Here the important observation is that at lower  $Re = 2000$ , a better prediction of  $St$  is achieved (9% deviation from the experimental ones) while at higher  $Re = 4000$ , a deviation of 22% is observed from the corresponding experimental value.

From the history of cylinder displacement during the lock-in, it can be observed that, as the frequency of shedding increases, the amplitude of displacement in cross flow direction goes on decreasing and that in the inline direction increases. This is because, at higher  $Re$  corresponding to higher shedding frequencies, the value of  $C_D$  is also high. A huge number of researchers are focusing on the cross flow response of cylinder. The observation made here emphasizes the need for investigating the inline response during lock-in at higher harmonics of natural frequency.

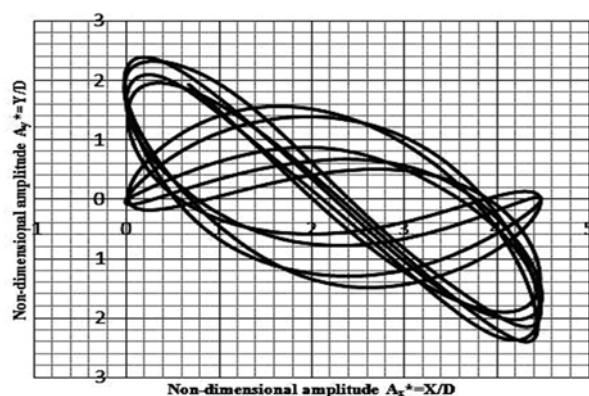
By plotting the non-dimensional amplitude of the cylinder in IL and CF directions, the trajectory of the probe location has been traced, as shown in Figures 9 (a) – (c) for all three frequency regimes. It can be observed that the cylinder point follows an eight figure trajectory during lock - in. The cylinder is expected to follow an eight figure trajectory due to oscillating lift and drag forces induced by vortex shedding at its wake. In lock-in condition the frequency of the inline vibration is twice that of cross flow vibration, and the trajectory of the cylinder corresponds to “Lissajou figure 8” (Vandiver *et al.*, 2009). Trajectory obtained from the numerical study is very much comparable with the response of an 8 m riser model obtained from the experimental study (Liangjie *et al.*, 2004). The trajectory from the experiment is given in Figure 10.

The trajectories traced show the increasing importance of accounting for IL response at higher harmonics of natural frequency. The maximum amplitude in the CF direction is obtained to be equal to 2.5D, where D is the diameter of the cylinder when the cylinder locks on to the first

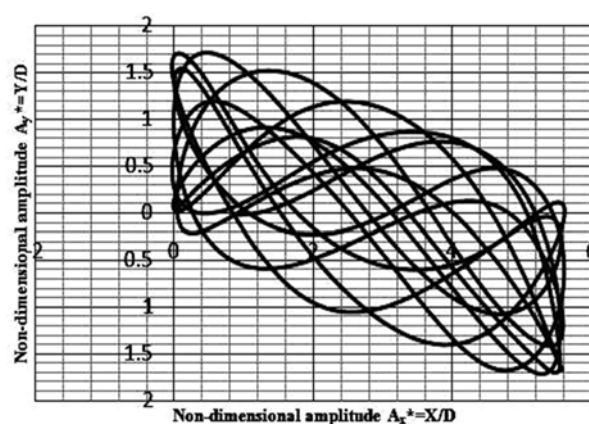
natural frequency. During the first natural frequency lock-in vibration, the cylinder traces the same path repeatedly for several cycles of oscillation. But moving to higher harmonics, there is considerable uncertainty in the case of exact path traced. The magnitude of the non-dimensional amplitude of oscillation and the pattern of trajectory matches reasonably well with the published experimental and numerical results.



a)



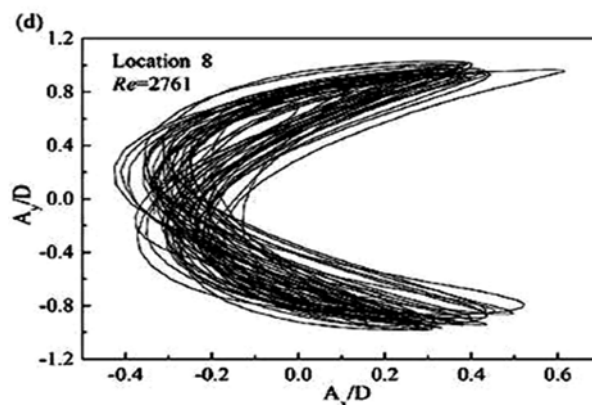
b)



c)

**Figure 9.** Trajectory of the cylinder (a) shedding frequency equal to the first harmonic of natural frequency (b) shedding frequency equal to second harmonic of natural

frequency (c) shedding frequency equal to third harmonic of natural frequency



**Figure 10.** Trajectory obtained from an experimental study of the response of cylindrical riser

#### 4. CONCLUSIONS

This paper presents a method that is computationally economic at the same time efficient in predicting VIV of cylindrical risers. Two dimensional flow analysis is capable of predicting the numerical values of hydrodynamics loads, pressure patterns during vortex shedding, the amplitude of oscillation and the trajectory as well for VIV problems. Vortex induced vibration of slender structures especially petroleum risers and mooring cables are one of the important aspects that should never be neglected in their design. Hence a thorough understanding of the loads and responses of such slender structures is essential before its design and deployment. Numerical analysis using two way fluid structure interaction (FSI), which can predict the parameters with considerable accuracy is always not handy for everyone dealing with this type of problem because of the heavy computational requirement needed for such solvers. This method has been proposed in a view to supporting young researchers in the field of the intrinsic flow phenomenon of vortex shedding, who lack high computational facility but may also understand the phenomenon without compromising much accuracy.

The method has been well validated in two stages, initially the grid, which yields the same flow physics as that of conventional experiments and then the structural behaviour which also is in good agreement with similarly published works (Liangjieet *al.*,2004 ,Vandiveret *al.*,2009). On the whole, it is found that the method is quite effective in the quick computation of VIV problems for low and moderate Re. At high Re, 3D studies find their



use as 2D predictions do not suffice in providing the minute details of flow physics.

## 5. ACKNOWLEDGEMENT

The authors of this paper wholeheartedly express their gratitude and acknowledgement to Mr. K. Alfred Sunny and Mr. Kumar of Karunya Institute of Science and Technology, Coimbatore, India, for the technical support rendered by them while conducting experiments on the sub-sonic wind tunnel. We also extend our deepest sense of gratefulness to Prof. M. Madhavan, former Principal, SCMS School of Engineering and Technology, Eranakulam, India, for his timely advice and support.

## 6. REFERENCES

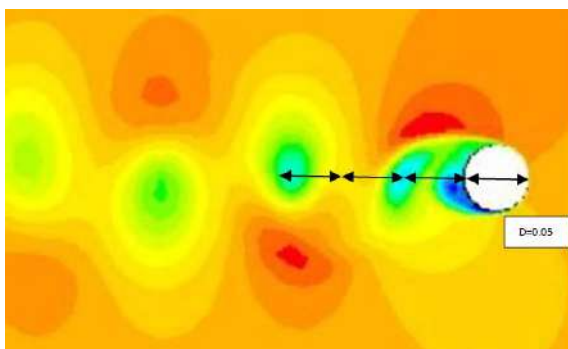
1. Gustafsson, A. Analysis of Vortex-Induced Vibration of Risers, Master's thesis in Applied Mechanics, Chalmers University of Technology, Sweden, **2012**.
2. Blevins, R.D. Flow-Induced Vibration, second ed., Van Nostrand Reinhold, New York, **1990**.
3. Bourguet, R., Karniadakis, G.E., Michael, S., and Triantafyllou, M.S. Lock-in of the vortex-induced vibrations of a long tensioned beam in shear flow, *Journal of Fluids and Structures*, **2011**, 27, 838–847.
4. Braza, M., Chassaing, P., and Minh, H.H. The Numerical Study and Physical Analysis of the Pressure and Velocity Fields in the Near Wake of a Circular Cylinder, *Journal of Fluid Mechanics*, **1986**, 165, 79–130.
5. Chandran, V., Sekar, M., Janardhanan, S., and Menon, V.A. numerical study on the influence of mass and stiffness ratios on the vortex induced motion of an elastically mounted cylinder for harnessing the power. *Energies*, **2018**, 11, 2580.
6. Chandran, V., Sekar, M., Janardhanan, S., Influence of Frequency Ratio on Hydroelastic Response of a Cylinder with Degrees of Freedom under Vortex Induced Vibration., *International Journal of Innovative Technology and Exploring Engineering*, **2019**, 8, 9S3, 307 -312.
7. Daniels, S.J., Castro, I.P., and Xie, Z. Numerical analysis of free stream turbulence effects on the vortex-induced vibrations of a rectangular cylinder, *Journal of Wind Engineering and Industrial Aerodynamics*, **2016**, 153, 13–25.
8. Domala, V., and Sharma, R. An experimental study on vortex-induced vibration response of marine riser with and without semi-submersible, *Journal of Engineering for the Maritime Environment*, **2017**.
9. Durbin, P.A., and Medic, G. Fluid dynamics with a computational perspective, **2007**, Cambridge University Press, Newyork.
10. Feng, C.C., The measurement of vortex-induced effects in flow past stationary and oscillating circular and D-section cylinders, Master's thesis, **1968**, University of British Columbia.
11. Gao, Y., Fu, S., Xiong, Y., Zhao, Y., and Liu, L. Experimental study on response performance of vortex-induced vibration on a flexible cylinder, *Ships, and Offshore Structures*, **2017**, 12, 116–134.
12. Kamkar S.J. Mesh Adaptation Strategies for vortex dominated flows, Ph. D Thesis, **2011**, Stanford University.
13. Keshavarzian, B., and Khosravi, M. Numerical Investigation of the Structural Frequencies Effects on Flow Induced Vibration and Heat Transfer, *Journal of Material and Environmental Science*, **2015**, 6 (7), 1949–1956.
14. Khalak, A., and Williamson, C.H.K. Motions, forces, and mode transitions in vortex-induced vibrations at low mass-damping, *Journal of Fluids and Structures*, **1999**, 13, 813–851.
15. Liangjie, M., Qingyou, L., and Shouwei, Z. Experimental Study of the Vortex-Induced Vibration of Drilling Risers under the Shear Flow with the Same Shear Parameter at the Different Reynolds Numbers, *PLoS ONE*, **2004**, 9, e104806.
16. Pezzini, A., Brião, V.B., and DE BONI, L.A. B. Preliminary study for a cleaning and water reuse system, *PERIÓDICO TCHÊ QUÍMICA*, **2017**, 28, 127–132.
17. Ramírez, Ann-Katrin, P., Wolff, and Carl, F. Building quality infrastructure services for water and sanitation providers in latinamerica – examples from german development cooperation, *PERIÓDICO TCHÊ QUÍMICA*, **2017**, 28, 18–28.
18. Sarpkaya, T., Transverse Oscillations of

Circular Cylinder in Uniform Flow, Part I Report No. NPS-69L 77071-R, **1997**, Naval Postgraduate School, Monterey, Calif.

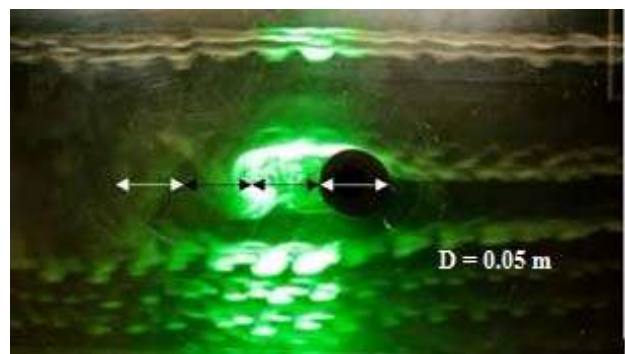
19. Sekar, M., Srinivas, J., Kotaiah, K.R., and Yang, S.H. Stability analysis of turning process with the tailstock-supported workpiece, *Int J Adv. Manuf. Technol*, **2009**, 43, 9–10, 862–871.
20. Shiels, D., Leonard, A., and Roshko, A. Flow-Induced Vibration of a Circular Cylinder at Limiting Structural Parameters, *Journal Of Fluids And Structures*, **2001**, 15, 3–21.
21. Techet, A., 13.42 Lecture: Vortex induced vibration – MIT open courseware, **2005**, Massachusetts Institute of Technology, USA.
22. Trim, A.D., Braaten, H., Lie, H., and Tognarelli, M.A. Experimental investigation of vortex-Induced vibration of long marine risers. *Journal of Fluids and Structures*, **2005**, 21, 335–361.
23. Vandiver, J.K., Jaiswal, V., and Jhingran, V. Insights on vortex-induced, traveling waves on long risers. *Journal of Fluids and Structures*, **2009**, 25: 641–653
24. Wang, Q., Li, M., and Xu, S., Experimental study on vortex induced vibration (VIV) of a wide-D-section cylinder in a cross flow, *Theoretical and Applied Mechanics Letters*, **2015**, 5: 39–44.
25. Xie, F., Deng, J., Xiao, Q., and Zheng, Y.A. Numerical simulation of VIV on a flexible circular cylinder, *Fluid Dynamics Research*, **2012**, 44, 21.

**Table 2.** Comparison between wind tunnel experiments and numerical simulations.

| Reynolds Number (Re) | Coefficient of Drag ( $C_D$ ) |           | Strouhal Number (St) (Non-dimensional Frequency) |           | Wake Dimension       |                      |
|----------------------|-------------------------------|-----------|--|-----------|----------------------|----------------------|
|                      | Experiment                    | Numerical | Experiment                                       | Numerical | Experiment           | Numerical            |
| <b>53000</b>         | 0.62                          | 0.63      | NA   |           | NA                   |                      |
| <b>4000</b>          | -                             | -         | 0.178  | 0.22      | $\theta = 126^\circ$ | $\theta = 120^\circ$ |
| <b>2000</b>          | -                             | -         | 0.183  | 0.1995    | D = 0.05m            | D = 0.02m            |

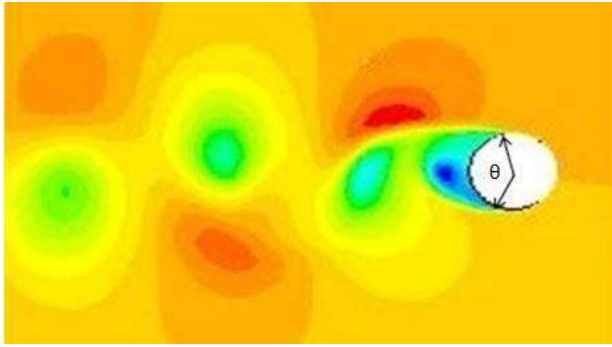


a)

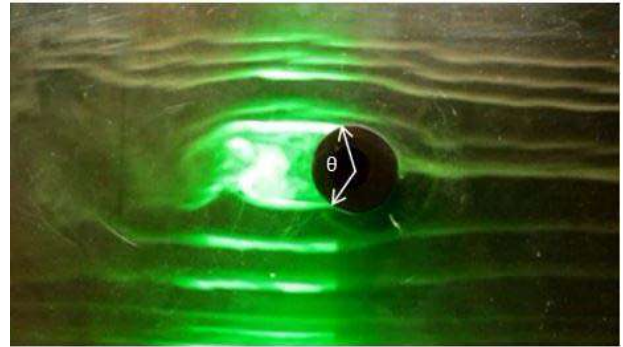


b)

**Figure 6.** Pressure pattern at the wake of the cylinder at  $Re = 2000$  (a) obtained from numerical simulations (b) obtained from the smoke test conducted in the subsonic wind tunnel



a)






b)

**Figure 7.** Boundary layer separation at the wake of the cylinder at  $Re = 4000$ . (a) obtained from numerical simulations (b) obtained from the smoke test conducted in the subsonic wind tunnel

# Chapter 6

## Automated Detection of Retinal Hemorrhage Based on Supervised Classifiers and Implementation in Hardware



K. A. Sreeja , S. S. Kumar , and Arun Pradeep 

**Abstract** Supervised machine learning algorithm based retinal hemorrhage detection and classification is presented. For developing an automated diabetic retinopathy screening system, efficient detection of retinal hemorrhage is important. Splat, which is a high level entity in image segmentation is used to mark out hemorrhage in the pre-processed fundus image. Here, color images of retina are portioned into different segments (splats) covering the whole image. With the help of splat level and GLCM features extracted from the splats, two classifiers are trained and tested using the relevant features. The ground-truth is established with the help of a retinal expert and using dataset and clinical images the validation was done. The trained classifier's output is evaluated and the classifier with the best output is chosen for implementation in hardware.

**Keywords** Retinal hemorrhage · Diabetic retinopathy · Fundus image · Splat feature classification · GLCM features · Raspberry Pi

### 6.1. Introduction

The World Health Organization estimated that by 2030, there will be nearly 366 million people with Diabetic Mellitus (DM) [1]. A microvascular complication of DM that is responsible for a major share of cases of blindness in the world is the Diabetic Retinopathy (DR). The severe complications like Microaneurysms, Exudates,

---

K. A. Sreeja (✉)  
SCMS School of Engineering and Technology, Ernakulam, India  
e-mail: ka.sreeja@gmail.com

S. S. Kumar · A. Pradeep  
Noorul Islam University, Kanyakumari, India  
e-mail: kumarss@live.com

A. Pradeep  
e-mail: arunpradeep@msn.com



Received August 17, 2019, accepted September 7, 2019, date of publication September 16, 2019,  
date of current version September 26, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2941491

# Artificial Muscle Intelligence System With Deep Learning for Post-Stroke Assistance and Rehabilitation

SUNIL JACOB<sup>1,2</sup>, VARUN G. MENON<sup>3</sup>, FADI AL-TURJMAN<sup>4</sup>, (Member, IEEE), VINOJ P. G.<sup>2,5</sup>,  
AND LEONARDO MOSTARDA<sup>6</sup>

<sup>1</sup>Center for Robotics, SCMS School of Engineering and Technology, Ernakulam 683576, India

<sup>2</sup>Department of Electronics and Communication Engineering, SCMS School of Engineering and Technology, Ernakulam 683576, India

<sup>3</sup>Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Ernakulam 683576, India

<sup>4</sup>Computer Engineering Department, Antalya Bilim University, 07190 Antalya, Turkey

<sup>5</sup>Department of Electronics and Communication Engineering, APJ Abdul Kalam Technological University, Thiruvananthapuram 695016, India

<sup>6</sup>Computer Science Division, University of Camerino, 62032 Camerino, Italy

Corresponding author: Varun G. Menon (varunmenon@scmsgroup.org)

This work was supported by The Institute of Electrical and Electronics Engineers (IEEE) EPICS, USA, under Grant 2016-12.

**ABSTRACT** Stroke is one of the prime reasons for paralysis throughout the world caused due to impaired nervous system and resulting in disability to move the affected body parts. Rehabilitation is the natural remedy for recovering from paralysis and enhancing the quality of life. Brain Computer Interface (BCI) controlled assistive technology is the new paradigm, providing assistance and rehabilitation for the paralyzed. But, most of these devices are error prone and also hard to get continuous control because of the dynamic nature of the brain signals. Moreover, existing devices like exoskeletons brings additional burden on the patient and the caregivers and also results in mental fatigue and frustration. To solve these issues Artificial Muscle Intelligence with Deep Learning (AMIDL) system is proposed in this paper. AMIDL integrates user intentions with artificial muscle movements in an efficient way to improve the performance. Human thoughts captured using Electroencephalogram (EEG) sensors are transformed into body movements, by utilising microcontroller and Transcutaneous Electrical Nerve Stimulation (TENS) device. EEG signals are subjected to pre-processing, feature extraction and classification, before being passed on to the affected body part. The received EEG signal is correlated with the recorded artificial muscle movements. If the captured EEG signal falls below the desired level, the affected body part will be stimulated by the recorded artificial muscle movements. The system also provides a feature for communicating human intentions as alert message to caregivers, in case of emergency situations. This is achieved by offline training of specific gesture and online gesture recognition algorithm. The recognised gesture is transformed into speech, thus enabling the paralyzed to express their feelings to the relatives or friends. Experiments were carried out with the aid of healthy and paralyzed subjects. The AMIDL system helped to reduce mental fatigue, miss-operation, frustration and provided continuous control. The thrust of lifting the exoskeleton is also reduced by using light weight wireless electrodes. The proposed system will be a great communication aid for paralyzed to express their thoughts and feelings with dear and near ones, thereby enhancing the quality of life.

**INDEX TERMS** Artificial muscle intelligence, assistive technologies, BCI, EEG, exoskeleton, healthcare, intelligent solutions, deep learning system, paralyzed, stroke.

## I. INTRODUCTION

The recent survey by reeve foundation revealed the impact of paralysis on world population, affecting approximately 5.4 million people [1], [2]. The survey also identified stroke (33.7%) as the major cause for paralysis. Paralysis is the deficiency of brain to activate muscle function of any body

The associate editor coordinating the review of this manuscript and approving it for publication was Shadi Aljawarneh.

part. Paralyzed persons find it difficult to perform their routine activities without assistance. Rehabilitation is one of the natural ways of healing paralysis. Because of this there is increasing interest and involvement in the field of post stroke rehabilitation. Exoskeleton-assisted technologies have emerged as a reliable means for rehabilitation of the affected upper and lower limbs [3]. Exoskeleton movements were controlled using sensors like gyroscopes, accelerometers, and potentiometers. Recently the focus is on controlling



Received May 21, 2019, accepted June 3, 2019, date of publication June 6, 2019, date of current version September 26, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2921375

# Brain-Controlled Adaptive Lower Limb Exoskeleton for Rehabilitation of Post-Stroke Paralyzed

P. G. VINOJ<sup>1,2</sup>, SUNIL JACOB<sup>1,3</sup>, VARUN G. MENON<sup>4</sup>, SREEJA RAJESH<sup>4</sup>,  
AND MOHAMMAD REZA KHOSRAVI<sup>5</sup>

<sup>1</sup>Department of Electronics and Communication Engineering, SCMS School of Engineering and Technology, Ernakulam 683576, India

<sup>2</sup>Department of Electronics and Communication Engineering, APJ Abdul Kalam Technological University, Thiruvananthapuram 695016, India

<sup>3</sup>Center for Robotics, SCMS School of Engineering and Technology, Ernakulam 683576, India

<sup>4</sup>Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Ernakulam 683576, India

<sup>5</sup>Department of Electrical and Electronic Engineering, Shiraz University of Technology, Shiraz 71355-311, Iran

Corresponding author: Varun G. Menon (varunmenon@scmsgroup.org)

This work was supported by the EPICS, Institute of Electrical and Electronics Engineers (IEEE), USA, under Grant 2016-12.

**ABSTRACT** Stroke is a standout amongst the most imperative reasons of incapacity on the planet. Due to partial or full paralysis, the majority of patients are compelled to rely upon parental figures and caregivers in residual life. With post-stroke rehabilitation, different types of assistive technologies have been proposed to offer developments to the influenced body parts of the incapacitated. In a large portion of these devices, the clients neither have control over the tasks nor can get feedback concerning the status of the exoskeleton. Additionally, there is no arrangement to detect user movements or accidental fall. The proposed framework tackles these issues utilizing a brain-controlled lower limb exoskeleton (BCLLE) in which the exoskeleton movements are controlled based on user intentions. An adaptive mechanism based on sensory feedback is integrated to reduce the system false rate. The BCLLE uses a flexible design which can be customized according to the degree of disability. The exoskeleton is modeled according to the human body anatomy, which makes it a perfect fit for the affected body part. The BCLLE system also automatically identifies the status of the paralyzed person and transmits information securely using Novel-T Symmetric Encryption Algorithm (NTSA) to caregivers in case of emergencies. The exoskeleton is fitted with motors which are controlled by the brain waves of the user with an electroencephalogram (EEG) headset. The EEG headset captures the human intentions based on the signals acquired from the brain. The brain-computer interface converts these signals into digital data and is interfaced with the motors via a microcontroller. The microcontroller controls the high torque motors connected to the exoskeleton's joints based on user intentions. Classification accuracy of more than 80% is obtained with our proposed method which is much higher compared with all existing solutions.

**INDEX TERMS** Artificial skin, assistive technologies, brain-computer interface (BCI), electroencephalogram (EEG), brain-controlled exoskeleton, paralyzed, stroke.

## I. INTRODUCTION

Stroke is an important reason of physical disability in developed countries, and in fact the third most common reason [1]. Almost 80% of survivors of stroke have experienced movement impairment on one side of the body [2-3]. Hand or arm impairment is particularly disabling and persistent, and lead to reduced quality of life [3-4]. Many of the stroke survivors

have a less physical disability by the end of the first three months (almost in all cases). Nearly, 35% of survivors having an initial paralysis of the leg do not regain the basic and essential function, and 20 to 25% of all the survivors are not able to walk without complete physical assistance [5]. Within six months, nearly 65% of patients are unable to use the affected hands for doing common life activities. Most of the patients are thus forced to be dependent on others in the remaining part of life.

The associate editor coordinating the review of this manuscript and approving it for publication was Mohammad Zia Ur Rahman.

# Secure Brain-to-Brain Communication With Edge Computing for Assisting Post-Stroke Paralyzed Patients

Sreeja Rajesh, Varghese Paul, Varun G. Menon<sup>1b</sup>, Member, IEEE, Sunil Jacob, and P. Vinod

**Abstract**—Stroke affects 33 million individuals worldwide every year and is one of the prime causes of paralysis. Due to partial or full paralysis, most of the patients affected by stroke depend on caregivers for the rest of their lives. Easy and efficient communication from the patient to the caregiver is a vital parameter determining the quality of life during rehabilitation. Several solutions, such as brain-computer interface (BCI) systems and exoskeletons, are proposed for post-stroke rehabilitation. But, most of these devices are expensive, sophisticated, and put an additional burden on the patient. Also, the communication between the patient and the caregiver is insecure. In this article, the brain-to-brain interface technique is integrated with an efficient encryption algorithm to enable secure transmission of information from the patient's brain to the caregiver. When a patient thinks of a word or a number, the thought is transmitted with the help of an electroencephalogram (EEG) headset through a wireless medium to the recipient, who correctly interprets the thoughts conveyed by the sender and types the same alphabet on the keyboard at his/her end. The transmitted message at the edge is encrypted with a lightweight novel tiny symmetric algorithm (NTSA), which can only be decrypted at the edge receiver. The Internet of Things integrated system is also flexible to send signals to multiple caregivers at the same time. The proposed method tested on ten users gave an average effective concentration percentage of 78.9% along with the secure transmission, which is a significant result compared with existing solutions.

**Index Terms**—Brain-to-brain interface, edge computing, electroencephalogram (EEG), Internet of Things, post-stroke paralysis, secure communication, security and privacy, TMS.

Manuscript received June 22, 2019; revised August 26, 2019, September 18, 2019, and October 22, 2019; accepted October 30, 2019. **Date of publication November 5, 2019**; date of current version April 14, 2020. This work was supported in part by EPICS in IEEE under Grant 2016-12. (Corresponding author: Varun G. Menon.)

S. Rajesh is with the Department of Computer Science, Bharathiar University, Coimbatore 641046, India (e-mail: m.sreeja79@gmail.com).

V. Paul is with the Department of Information Technology, Rajagiri School of Engineering and Technology, Ernakulam 682039, India (e-mail: vp.itcusat@gmail.com).

V. G. Menon and P. Vinod are with the Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Karukutty 683576, India (e-mail: varunmenon@scmsgroup.org; vinodp@scmsgroup.org).

S. Jacob is with the Center for Robotics, SCMS School of Engineering and Technology, Karukutty 683576, India (e-mail: suniljacob@scmsgroup.org).

Digital Object Identifier 10.1109/JIOT.2019.2951405

## I. INTRODUCTION

**S**TROKE is a major cause of full or partial paralysis among people, especially, prevalent in developing countries. Thirty five percent of survivors have permanent disability one year after a stroke [1] and all of them need care in a nursing home or other long-term assistance. Communicating ideas and requests from the patient to the caregiver is a significant challenge in these conditions. Communicating the feelings can often be unclear and hard to understand, depending on how a person describes or expresses them in words. It is more challenging when the patient and the caregiver are far apart. Exoskeletons have been proposed in recent years as a possible solution to this issue. Regaining the ability to walk has been major focus of most of the exoskeleton systems. Progressive, task-specific, and repetitive training based on the principles of motor learning and neuroplasticity is carried out with the help of exoskeletons. Wearable robots strapped onto legs, and actuated motors are also used for rehabilitation in many scenarios [2]. Numerous alternate brain-computer interface (BCI) [3], [4] systems have also emerged for stroke rehabilitation. Most of the proposed solutions are expensive, sophisticated, put an additional burden on the patient, and also do not ensure secure and efficient communication between the patient and the caregiver [5].

Recently, the brain-to-brain interface systems [6]–[9] have opened numerous possibilities in efficient post-stroke rehabilitation, including provision for direct communication of the ideas and thoughts between the patient and the caregiver. This technology involves the transmission of information from one person's brain to another using a wireless medium. The significant advantage of this technology is that it is noninvasive and does not have the complications of using bulky devices like exoskeletons and comes with less cost. This technology is still in its early stages and has numerous limitations and challenges. The recent research in post-stroke rehabilitation has thus focused on developing efficient systems using the brain-to-brain interface. Most of the existing brain-to-brain interface systems work only with simulations and fail to deliver in real-time environments. Another major limitation of current systems is the lack of security in the transmitted message. Whenever the information is transmitted through a wireless medium or any public medium like the Internet, it is essential to have a suitable security mechanism. Securing the sensitive data transferred between the patient and the caregiver is vital for regaining the confidence during the rehabilitation phase.



Very few works have been done in this article direction, and this article focuses on proposing an efficient solution to this problem.

In the proposed system, the secrecy of information transferred is attained using cryptography wherein the transferred file is scrambled into a nonreadable form by the sender. The recipient on receiving the scrambled message from the sender de-scrambles it into a readable form. The tiny encryption algorithm (TEA) [10]–[12], which is one of the most widely used symmetric algorithms due to the ease of implementation and less memory utilization, is improved and used in the system as the novel tiny symmetric algorithm (NTSA). It enhances the security features of TEA by introducing more key confusions [13]–[15]. The keys are altered dynamically, thus making it secure from the intruders. Since the key is computed dynamically, the key values change during execution time and cannot be precomputed. This algorithm is then used in the proposed system for the secure transmission of information from the patient to the caregiver. As the computation happens at the edge of the network, it eliminates the delay in transmission and processing of the data that exists in systems with centralized data processing centers. The contributions of this article are as follows.

- 1) A simple, noninvasive, and efficient brain-to-brain thought transfer system that helps to share the thoughts between the patient and the caregiver with electroencephalogram (EEG) headset at the transmitting end and magnetic stimulation at the receiving end.
- 2) Edge computing powered secured transmission of message between the patient and the caregiver using an efficient and lightweight symmetric encryption algorithm.
- 3) Real-time implementation with analysis of the results obtained is provided.

The remainder of this article is organized into six sections. Section II reviews the related work in brain-to-brain communication. Section III describes the theoretical analysis of the proposed system. Section IV provides the details of the proposed system, its working, and discussion. Section V presents the results obtained with experiments and proves that the proposed method achieves secured data transmission between the patient and the caregiver. Finally, Section VI summarizes the findings and presents the conclusion and future work.

## II. RELATED WORKS

This section presents the discussion on few latest related works in the brain-to-brain communication and BCI. The usage of BCI facilitates a person to communicate without the intervention of the brain's normal output pathways of peripheral nerves and muscles. The EEG features are used to identify the message or commands from the brain. The two methods used in BCI are invasive and noninvasive BCI. The invasive BCI uses implanted electrodes in brain tissue, and noninvasive uses EEG recordings obtained by placing electrodes at various points on the scalp of a person. In [16], multiple

TABLE I  
FREQUENTLY USED NOTATIONS

| Notation           | Definition  |
|--------------------|---|
| $T_X$              | transmitter headset   |
| $R_X$              | receiver headset.   |
| $L_B$              | height of $T_X$ from ground   |
| $\beta_B$          | angle of incidence  |
| $\beta_D$          | angle of reflection   |
| $D_{Total}$        | total distance between $T_X$ and $R_X$  |
| $\epsilon_{B-D}$   | signal strength of the directly transmitted signal                            |
| $\epsilon'_{B-D}$  | signal strength of the reflected part   |
| $\epsilon_{Total}$ | total transmitted signal energy   |
| $\Delta D$         | difference of the distance travelled by the reflected and line of sight waves |
| $\mu_F$            | propagation loss in the environment   |
| $\beta_{LU}$       | incident and reflection loss of the transmitted signal                        |
| $\gamma(L_B)$      | $T_X$ side gain   |
| $\gamma(L_D)$      | $R_X$ side gain   |
| $\mu_{env}$        | environmental gain factor   |

variations of using BCI in communication and motor control are discussed. Wolpaw *et al.* [17] conducted a survey and identified that the BCI systems were efficient in providing communication and controls the options to those with a disability. Mason and Birch [18] discussed a prototype of an asynchronous switch known as LF-ASD. For people who are paralyzed and have no voluntary muscle control, a BCI might give the ability to answer simple questions quickly and control the environment [19]. Zhang *et al.* [20] proposed a brain interface system to control a rat implanted with micro-electrodes. Maksimenko *et al.* [21] proposed a system for distributing the cognitive load among all members of the group toward achieving a common task. In [22]–[24], user authentication and other security mechanism that can be introduced in the transmission of signals from the brain to other devices are discussed.

Most of the existing systems have minimal works only with simulations and fail to deliver in real-time environments. Another major limitation with most of the methods is the lack of adequate security in the transmitted message. Also, the privacy of the information transmitted from the patient to the caregiver is not provided. The proposed system is designed to overcome all the above limitations. Using the concept of brain-to-brain interface, edge computing, and a novel lightweight symmetric encryption algorithm [13], [25], [26], secure transmission of information from the patient's brain to the caregiver using wireless medium is achieved with EEG and TMS. The Internet of Things module can be further integrated into the system to transfer information securely to multiple receivers.

## III. MATHEMATICAL ANALYSIS

In this section, the theoretical analysis of the transmitted signal strength is presented and discussed. Table I presents the summary of frequently used notations in this article.

Analysis of the thought transfer signal along with the range estimation is presented in Fig. 1. The total transmitted signal from  $T_X$  is calculated from the above deployment scenario of the proposed system. The total transmitted signal is the sum of the signal that is directly transmitted and the part of the signal that is reflected from the surface. Hence, the total transmitted

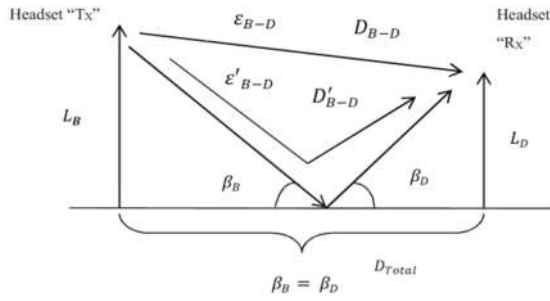


Fig. 1. Signal analysis for thought transfer.

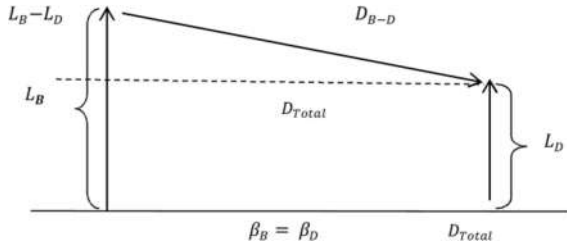


Fig. 2. Range analysis of thought processing.

signal energy is given by

$$\varepsilon_{\text{Total}} = \varepsilon_{B-D} + \varepsilon'_{B-D}. \quad (1)$$

A reference signal strength of  $\varepsilon_0$  at a distance  $D_0$  is assumed by the system, which is given by

$$\varepsilon_{B-D} = \frac{\varepsilon_0 D_0}{D_{\text{Total}}} e^{j2\pi F_c \left(t_0 - \frac{D_{B-D}}{c}\right)} \quad (2)$$

$$\varepsilon'_{B-D} = \frac{-\varepsilon_0 D_0}{D_{\text{Total}}} e^{j2\pi F_c \left(t_0 - \frac{D'_{B-D}}{c}\right)}. \quad (3)$$

Here, the negative sign in (3) is due to the phase inversion of the signal. Substituting (2) and (3) into (1) gives

$$\varepsilon_{\text{Total}} = \frac{\varepsilon_0 D_0}{D_{\text{Total}}} e^{j2\pi F_c \left(t_0 - \frac{D_{B-D}}{c}\right)} - \frac{\varepsilon_0 D_0}{D_{\text{Total}}} e^{j2\pi F_c \left(t_0 - \frac{D'_{B-D}}{c}\right)} \quad (4)$$

$$\varepsilon_{\text{Total}} = \frac{\varepsilon_0 D_0}{D_{\text{Total}}} e^{j2\pi F_c \left(t_0 - \frac{D_{B-D}}{c}\right)} \left(1 - e^{j2\pi F_c \frac{\Delta D}{c}}\right) \quad (5)$$

where  $\Delta D = D'_{B-D} - D_{B-D}$  that gives the difference of the distance traveled by the reflected wave and the distance traveled by the direct line-of-sight wave

$$\varepsilon_{\text{Total}} = \frac{\varepsilon_0 D_0}{D_{\text{Total}}} e^{-j2\pi F_c \left(t_0 - \frac{D_{B-D}}{c}\right)} \left(1 - e^{j2\pi \frac{\Delta D}{\lambda_0}}\right) \quad (6)$$

where  $(C/F_c) = \lambda_0$

$$\varepsilon_{\text{Total}} = \frac{\varepsilon_0 D_0}{D_{\text{Total}}} e^{-j2\pi F_c \left(t_0 - \frac{D_{B-D}}{c}\right)} e^{j2\pi \frac{\Delta D}{2\lambda_0}} e^{-j2\pi \frac{\Delta D}{2\lambda_0}} \quad (7)$$

$$\varepsilon_{\text{Total}} = -\frac{\varepsilon_0 D_0}{D_{\text{Total}}} e^{-j2\pi F_c \left(t_0 - \frac{D_{B-D}}{c}\right)} e^{j2\pi \frac{\Delta D}{2\lambda_0}} \sin\left(2\pi \frac{\Delta D}{2\lambda_0}\right). \quad (8)$$

The magnitude of the total signal strength is obtained as

$$|\varepsilon_{\text{Total}}| = \frac{\varepsilon_0 D_0}{D_{\text{Total}}} \left| \sin\left(2\pi \frac{\Delta D}{2\lambda_0}\right) \right|. \quad (9)$$

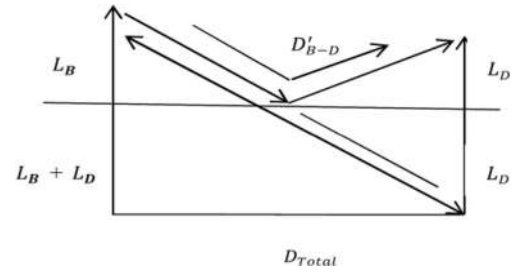


Fig. 3. Range estimation using mirror image analysis.

Fig. 2 presents the range analysis of the thought processing signal. The actual range of the line-of-sight signal is given by  $D_{B-D}$  which is obtained as

$$D_{B-D} = \sqrt{(L_B - L_D)^2 + (D_{\text{Total}})^2}. \quad (10)$$

Fig. 3 presents the range estimation of the signal using the mirror image analysis. The reflected signal in the system is given by

$$D'_{B-D} = \sqrt{(L_B + L_D)^2 + (D_{\text{Total}})^2}. \quad (11)$$

Using (11), the value of  $\Delta D$  is estimated, where  $\Delta D = D'_{B-D} - D_{B-D}$

$$\Delta D = \sqrt{(L_B + L_D)^2 + (D_{\text{Total}})^2} - \sqrt{(L_B - L_D)^2 + (D_{\text{Total}})^2} \quad (12)$$

$$\Delta D = D_{\text{Total}} \left\{ \sqrt{1 + \left(\frac{L_B + L_D}{D_{\text{Total}}}\right)^2} - \sqrt{1 + \left(\frac{L_B - L_D}{D_{\text{Total}}}\right)^2} \right\} \quad (13)$$

where  $L_B, L_D \ll D_{\text{Total}}$ .

Approximating the  $\Delta D$  value with respect to  $L_B, L_D$ , and  $D_{\text{Total}}$

$$\Delta D \approx D_{\text{Total}} \left\{ \left(1 + \frac{1}{2} \left(\frac{L_B + L_D}{D_{\text{Total}}}\right)^2\right) - \left(1 + \frac{1}{2} \left(\frac{L_B - L_D}{D_{\text{Total}}}\right)^2\right) \right\}. \quad (14)$$

Reducing the above equation, we obtain

$$\Delta D \approx 2 \frac{L_B L_D}{D_{\text{Total}}}. \quad (15)$$

Substituting the value of  $\Delta D$  in (9), the magnitude of the total signal strength is obtained as

$$|\varepsilon_{\text{Total}}| = \frac{2\varepsilon_0 D_0}{D_{\text{Total}}} \sin\left(2\pi \frac{\Delta D}{2\lambda_0}\right). \quad (16)$$

Considering a very small value of sine, the magnitude of the total signal strength is approximated as

$$|\varepsilon_{\text{Total}}| \approx \frac{2\varepsilon_0 D_0}{D_{\text{Total}}} 2\pi \frac{\Delta D}{2\lambda_0} \quad (17)$$

$$|\varepsilon_{\text{Total}}| \approx \frac{2\varepsilon_0 D_0}{D_{\text{Total}}} \frac{2\pi}{2\lambda_0} \frac{2L_B L_D}{D_{\text{Total}}}. \quad (18)$$

Finally, the approximated total strength of the thought processes signal is obtained as

$$|\varepsilon_{\text{Total}}| \approx 4\pi \frac{\varepsilon_0 D_0}{\lambda_0 (D_{\text{Total}})^2} L_B L_D. \quad (19)$$

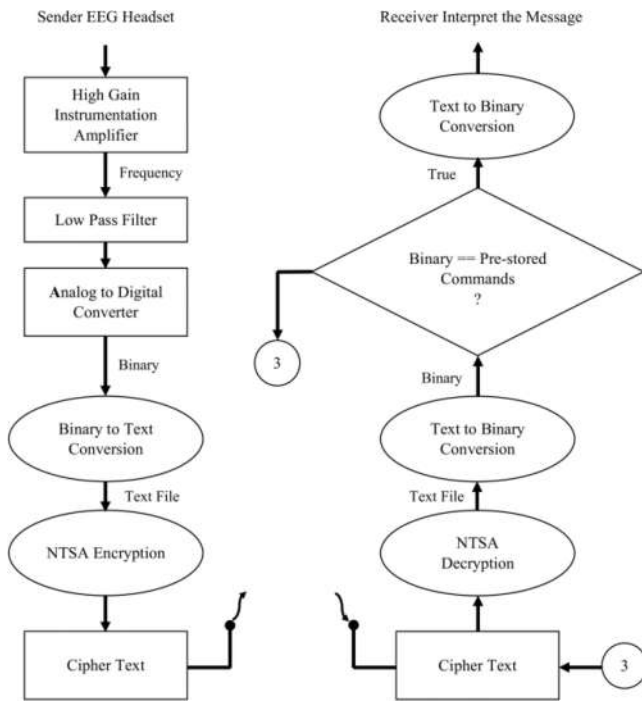


Fig. 4. System architecture.

The correctness factor introduced in the signal is discussed below. The 50th percentile loss in dB is given by

$$\mu_{50}(dB) = \mu_F + \beta_{LU} - \gamma(L_B) - \gamma(L_D) - \mu_{env}. \quad (20)$$

Here,  $\mu_F$  is the propagation loss in the environment,  $\beta_{LU}$  is the incident and reflection loss of the transmitted signal,  $\gamma(L_B)$  is the  $T_X$  side gain factor,  $\gamma(L_D)$  is the  $R_X$  side gain factor, and  $\mu_{env}$  is the environmental gain factor.

#### IV. PROPOSED SYSTEM

This article aims to securely transfer the thoughts between the paralyzed patient and the caregiver with the help of EEG headsets. The idea is to share the thoughts with EEG headset at the transmitting end and use magnetic stimulation at the receiving end. The EEG recordings from the brain are taken by placing a cap of electrodes on a person's scalp, using a 10–20 placement scheme. The electrical stimulation from the brain's cortex region is then recorded and transmitted wirelessly through the cloud. At the receiving end, the machine converts the message into the equivalent electrical signal. This electrical signal produces equivalent magnetic stimulation in the form of TMS and the receiver interprets the information based on the flashes he/she sees. Fig. 4 shows the detailed block diagram of the proposed system.

##### A. At the Sender Side

Sender wears the EEG headset which is shown in Fig. 5. Then, using the 10–20 probe placement scheme on the person's scalp, the electric impulses at the neural synapses from the brain cortex region is fetched and recorded. Fig. 5 shows the EEG headset to which EEG electrodes are attached and also the placement of electrodes on the brain. This EEG

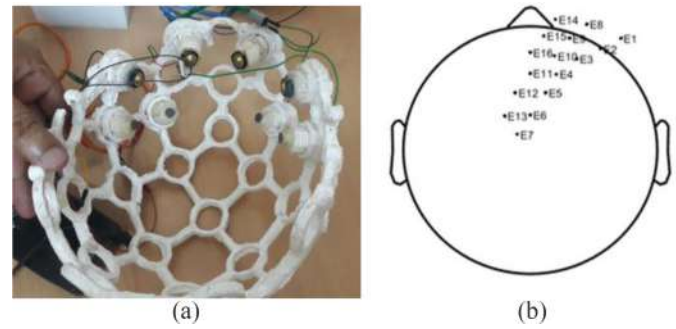


Fig. 5. (a) EEG headset. (b) Electrode placement on the brain [23].



Fig. 6. Electromagnetic coil.

recording obtained is feeble, and hence amplified using the high-gain instrumentation amplifier. The noise in the signal is mitigated by passing the signal through a low-pass filter. The resulting analog signal is digitized using the analog-to-digital convertor (ADC). This digitized signal is converted to text and can be securely sent through the public medium using the proposed NTSA encryption algorithm.

##### B. At the Receiver Side

The ciphertext transmitted by the sender reaches the receiver through the wireless medium. On reception of the ciphertext, it is decrypted using the NTSA decryption algorithm and the text file is obtained. The text file is converted into binary which is compared with the prestored commands. If it matches with the prestored commands, the TMS circuit is triggered correspondingly to generate the TMS flashes which will be interpreted by the receiver. The TMS circuit is designed with an external source of 230-V ac signal and is step down to 24-V ac signal using the step-down transformer and is passed to the coil via Triac switch. The 12-V step-down transformer is used to trigger the timer circuit. The Triac is used as a high-power switching device and is controlled by the binary value. Depending on 0s and 1s, TMS creates flash (binary 1 for vibration with flash and binary 0 for no vibration and flash). The helmet at the receiver side has two coils inside it and each coil has 30 000 turns. One coil is used to control the activity of left part of the brain and the other to control the right part of the brain. Based on the excitation signal from the coil, the brain gets stimulated to create a flash or equivalent vibration. Fig. 6 shows the electromagnetic coil with the circuit.

**Algorithm 1** Encryption

```

1: procedure E(n)encryption (plaintext[64], key[128],  $\emptyset$ )
2:   // Initialize subkeys  $sk_i$  and plaintexts  $P_i$ 
3:    $sk_0 \leftarrow key[i : i+32]$ 
4:    $sk_1 \leftarrow key[i+33 : i+64]$ 
5:    $sk_2 \leftarrow key[i+65 : i+96]$ 
6:    $sk_3 \leftarrow key[i+97 : i+128]$ 
7:    $C_0 \leftarrow plaintext[i : i+32]$ 
8:    $C_1 \leftarrow plaintext[i+33 : i+64]$ 
9:    $ksc \leftarrow (2^{31}) / \emptyset$ 
10:   $kc \leftarrow 0$ 
11:  // The loop generates cipher text  $C_0$  and  $C_1$  and the keys  $sk_1$ 
    and  $sk_3$ 
12:  for cycle  $\leftarrow 0$  to 32 do
13:     $kc \leftarrow kc + ksc$ 
14:     $C_0 \leftarrow C_0 + ((C_1 << 4 \wedge sk_0) \oplus (C_1 \wedge kc) \oplus$ 
         $((C_1 >> 5) \wedge sk_1))$ 
15:     $sk_1 \leftarrow sk_1 + (sk_0 \oplus (xtract(C_0)))$ 
16:     $C_1 \leftarrow C_1 + ((C_0 << 4 \wedge sk_2) \oplus (C_0 \wedge kc) \oplus ((C_0$ 
         $>> 5) \wedge sk_3))$ 
17:     $sk_3 \leftarrow sk_3 + (sk_2 \oplus (xtract(C_1)))$ 
18:  end for
19:   $newk1 \leftarrow sk_1$ 
20:   $newk3 \leftarrow sk_3$ 
21: end procedure

// Details of key confusion xtract function
1: procedure xtract(a)
2: while  $i = \text{lal}$  do
3:   if  $a[i] = 32$  then
4:      $a[i] \leftarrow a[i] \bmod 32$ 
5:   end if
6:    $i \leftarrow i + 1$ 
7: end while
8: return a

```

*C. Novel Tiny Symmetric-Key Algorithm*

The proposed NTSA is a symmetric cryptographic algorithm that follows the Feistel structure, having 64 rounds and 32 cycles, each cycle comprising of an odd and even round. The pseudocode for encryption and decryption is presented in Algorithms 1 and 2, respectively, and Fig. 7 presents the illustration of the encryption process. During encryption, in steps 1–8, the plain text with 64 bits is divided into two halves of 32 bit each and the key 128 bits is divided into four subkeys  $sk_0$ ,  $sk_1$ ,  $sk_2$ , and  $sk_3$  of 32 bit each. Subkey  $sk_1$  is applied to odd round and subkey  $sk_3$  is applied to even round. Different multiples of magic constant are used for each round. The value of magic constant is chosen to be floor  $(2^{31}/\emptyset)$ , where  $\emptyset$  is the golden ratio. In steps 12–18, a loop generates ciphertext  $C_0$  and  $C_1$  and the keys  $sk_1$  and  $sk_3$ .

An xtract function is used to generate additional key confusions in encryption. The xtract function given above (lines 1–8) returns the array indices value between 0 and 31. The value from the array is then selected dynamically to recompute the subkey values, thus making the algorithm secure. The decryption algorithm has the same initialization procedure and preliminary steps as in encryption which is depicted in lines 1–12. In lines 13–19, the loop generates the plain text  $P_0$  and  $P_1$  and keys  $sk_1$  and  $sk_3$ .

*D. Security and Privacy Enabled at the Edge*

The transmitted EEG signal is amplified and digitized, and encrypted at the edge using the NTSA algorithm. Instead of recording and processing the data with centralized cloud

**Algorithm 2** Decryption

```

1: procedure D(e)decryption ( $C_0, C_1, key[128], newk_1, newk_3, \emptyset$ )
2:   // Initialize
3:    $sk_0 \leftarrow key[i : i+32]$ 
4:    $sk_1 \leftarrow key[i+33 : i+64]$ 
5:    $sk_2 \leftarrow key[i+65 : i+96]$ 
6:    $sk_3 \leftarrow key[i+97 : i+128]$ 
7:    $ksc \leftarrow (2^{31}) / \emptyset$ 
8:    $kc \leftarrow 0xC6EF3720$ 
9:    $sk_1 \leftarrow newk_1$ 
10:   $sk_3 \leftarrow newk_3$ 
11:   $P_0 \leftarrow C_0$ 
12:   $P_1 \leftarrow C_1$ 
13:  for cycle  $\leftarrow 0$  to 32 do // The loop generates plaintext  $P_0$ 
    and  $P_1$ 
14:     $sk_3 \leftarrow sk_3 - (sk_2 \oplus (xtract(P_1)))$ 
15:     $P_1 \leftarrow P_1 - ((P_0 << 4) \wedge sk_2) \oplus (P_0 \wedge kc) \oplus ((P_0$ 
         $>> 5) \wedge sk_3))$ 
16:     $sk_1 \leftarrow sk_1 - (sk_0 \oplus (xtract(P_0)))$ 
17:     $P_0 \leftarrow P_0 - ((P_1 << 4) \wedge sk_0) \oplus (P_1 \wedge kc) \oplus ((P_1 >>$ 
         $5) \wedge sk_1))$ 
18:     $kc \leftarrow kc - ksc$ 
19:  end for
20: end procedure

```

centers, the proposed system encrypts and decrypts the EEG signals at the edge of the network. Only encrypted data is available in the network and without the key, decryption is not possible. Hence, the security of information is ensured at the edge of the network.

## V. RESULTS AND DISCUSSION

The sender is hooked up to an electroencephalography machine, to examine the brain signals, while the receiver has a TMS coil, attached to the side of the head to control the right side of the body. The sender watches an on-screen keyboard and urges to press a key using the right hand. The machine transmits this information securely as an encrypted file through the wireless medium. The wireless reception transfers it to the TMS, which prompts the distant located receiver's brain to do the same action of the sender.

*A. Sender Side*

The EEG signal extraction and transmission by the sender are depicted in Fig. 8. The unit comprises: 1) EEG signal extraction headset; 2) EEG signal processing unit; and 3) signal encryption and wireless transmission unit.

*B. Sender Side*

The EEG signal extraction and transmission by the sender is depicted in Fig. 8. The unit comprises: 1) EEG signal extraction headset; 2) EEG signal processing unit; and 3) signal encryption and wireless transmission unit.

*C. EEG Signal Extraction Headset*

The EEG headset is worn by the sender. The sender chooses a specific key of the onscreen keyboard by concentrating his/her thoughts on it. The electrodes on contact with the scalp extract these EEG signals from the brain. This EEG signal is passed to the EEG signal processing unit.

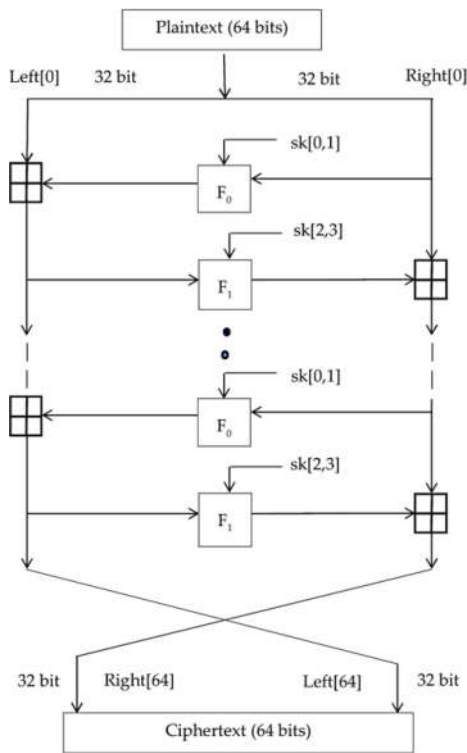


Fig. 7. Encryption in the NTSA algorithm [13].

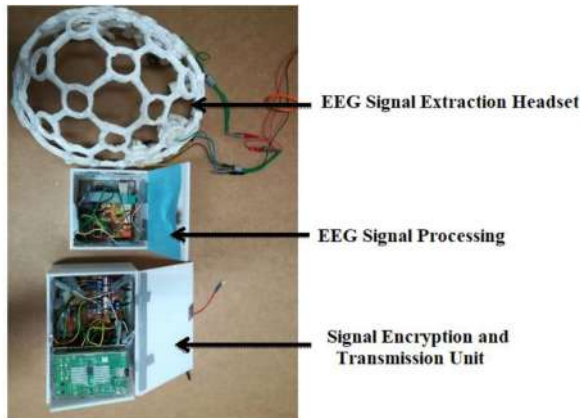


Fig. 8. Signal extraction and transmission unit.

*D. EEG Signal Processing and Wireless Transmission Unit*

Here, the EEG signals undergo high gain amplification and noise filtering for further processing. The analog signals are then converted to digitized format using the ADC. This digital data is then converted to text which is encrypted using the NTSA algorithm. The obtained ciphertext is then sent to the receiver through the Internet using the wireless transmission unit.

*E. Receiver Side*

Fig. 9 shows the ciphertext reception and decoding at the receiver side. This unit comprises: 1) wireless reception and decryption unit; 2) brain excitation control system; and 3) brain excitation headset.

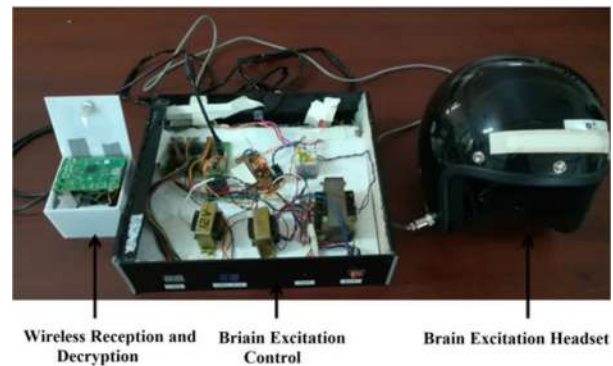


Fig. 9. Signal reception and end user.

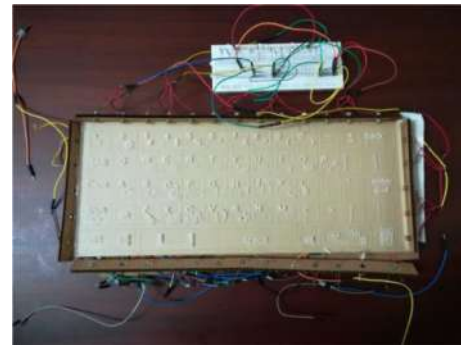


Fig. 10. End user interface.

*F. Wireless Reception and Decryption and Signal Processing Unit*

On reception of the ciphertext by the wireless receiver unit, decoding is performed using the NTSA decryption algorithm to get the text message which is then digitized. This digitized code is compared with the prestored commands stored in the data library. If there is a match, then the corresponding command is passed to the brain excitation control system.

*G. Brain Excitation Control System*

The exciter circuit (TMS) will generate the signal corresponding to the command passed. This signal will reach the receiver who will be wearing the helmet connected to TMS. The excitation impulses prompt the receiver (end user) to press the specific key on the customized keyboard (shown in Fig. 10) that was chosen by the sender.

*H. EEG Signal Extraction and Reception*

The brain pattern generated by concentrating on the virtual keyboard for letter ‘‘A’’ and the stimulated pattern of the transmitted character A received at the receiver end is shown in Fig. 8. It is observed that the pattern transmitted at the sender side and the pattern received at the receiver end are the same. Similarly, brain pattern generated for single character B, combination of characters AN, combination of numbers 12 are depicted in Figs. 11–13, respectively.



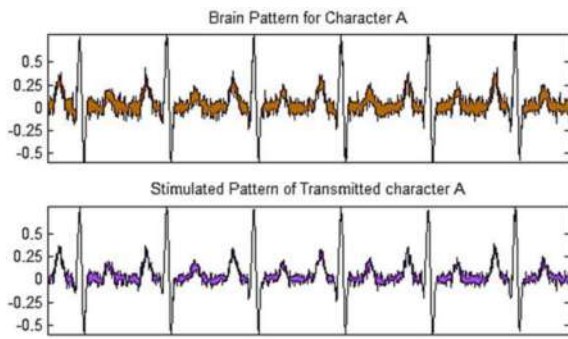


Fig. 11. Brain pattern transmitted and received for character A.

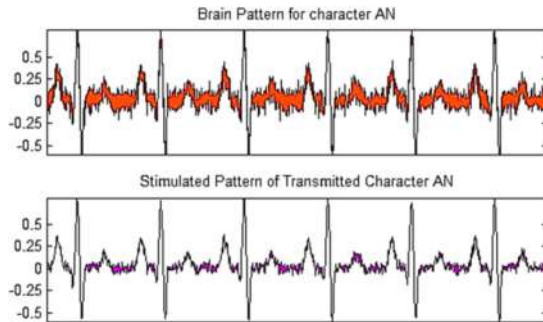


Fig. 12. Brain pattern transmitted and received for character AN.

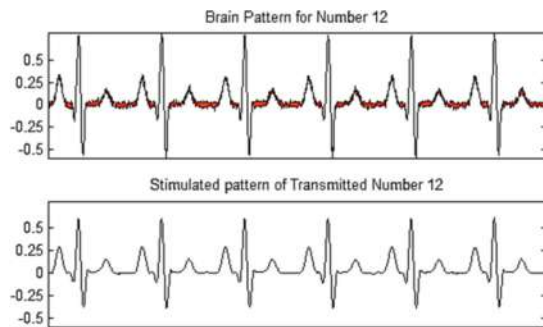


Fig. 13. Brain pattern transmitted and received for number 12.

*I. NTSA Avalanche Effect*

Additionally, the strength of the proposed encryption algorithm is evaluated using the concept of the avalanche effect. It is one of the desired properties of a block cipher algorithm, in that a very small change in the input creates a significant change in the output. The NTSA and TEA encryption algorithms were executed with varying key sizes of 48, 64, and 128 bits as one input and same plaintext as another input. The same experiment is repeated with the same key but by changing only one bit of it. The observation made was that for every 64-bit block, one-bit change in key produces a significant change on the ciphertext for NTSA when compared to TEA. Fig. 14 shows for every 64-bit block a change in one-bit of key with various key sizes and the corresponding change in ciphertext for NTSA and TEA.

The same experiment is repeated, but now one-bit change is made on the plaintext. The observations made are: NTSA shows drastic changes in the ciphertext than the TEA algorithm. Fig. 15 shows that for every 64-bit block

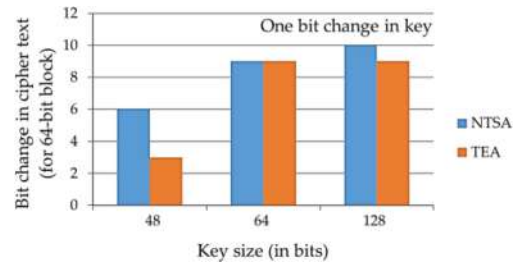


Fig. 14. One-bit change in key and the corresponding change in ciphertext for 64-bit block.

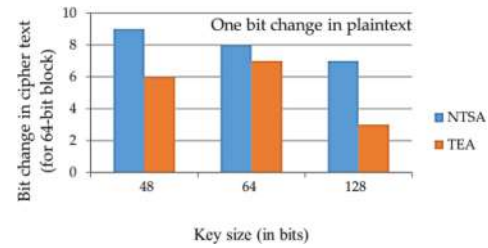


Fig. 15. One-bit change in plaintext and the corresponding change in ciphertext for 64-bit block.

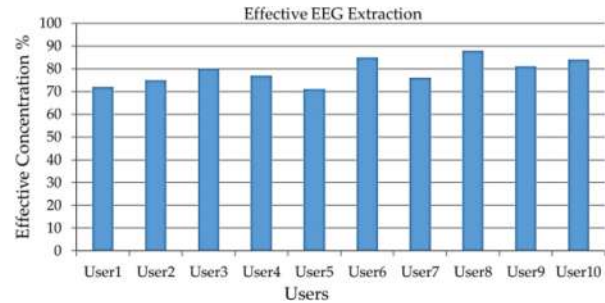


Fig. 16. Effective EEG extraction from test users.

a change in one bit of key with various key sizes and corresponding change in the ciphertext for NTSA and TEA.

*J. Effective Concentration Percentage*

The proposed system was tested on ten users and their effective concentration percentages were obtained. The results are presented in the graph as shown in Fig. 16. The result shows that the average effective concentration percentage is 78.9% which is really significant and higher value compared to most of the existing methods.

VI. CONCLUSION

This article analyzed the possibilities of brain-to-brain communication and highlighted the limitations with the existing systems. The proposed system enabled secure transmission of information from the patient’s brain to the caregiver using the wireless medium with EEG and TMS and a novel lightweight symmetric encryption algorithm, NTSA. This easy to use and secure system will be of great assistance to the paralyzed in the rehabilitation phase and will enable efficient and easy communication from the patient to the caregiver with less cost and without the help of any complex devices. In the future, the size of the system could be reduced so that it can be much more easily handled by the patients. Furthermore, the possibilities of using deep learning strategies to make the system efficient could be studied.

## ACKNOWLEDGMENT

The authors would like to thank the Principal and Management of SCMS School of Engineering and Technology, Dr. S. Joseph and Ms. A. Jacob for the valuable support extended to this article.

## REFERENCES

- [1] A. E. Hillis and D. C. Tippett, "Stroke recovery: Surprising influences and residual consequences," *Adv. Med.*, vol. 2014, pp. 1–10, Oct. 2014, doi: [10.1155/2014/378263](https://doi.org/10.1155/2014/378263).
- [2] D. R. Louie and J. J. Eng, "Powered robotic exoskeletons in post-stroke rehabilitation of gait: A scoping review," *J. Neuroeng. Rehabil.*, vol. 13, no. 1, p. 53, 2016, doi: [10.1186/s12984-016-0162-5](https://doi.org/10.1186/s12984-016-0162-5).
- [3] A. Rezeika, M. Benda, P. Stawicki, F. Gembler, A. Saboor, and I. Volosyak, "Brain-computer interface spellers: A review," *Brain Sci.*, vol. 8, no. 4, p. 57, 2018, doi: [10.3390/brainsci8040057](https://doi.org/10.3390/brainsci8040057).
- [4] F. Pichiorri *et al.*, "Brain-computer interface boosts motor imagery practice during stroke recovery," *Ann. Neurol.*, vol. 77, no. 5, pp. 851–865, 2015, doi: [10.1002/ana.24390](https://doi.org/10.1002/ana.24390).
- [5] R. Ramele, A. J. Villar, and J. M. Santos, "EEG waveform analysis of P300ERP with applications to brain computer interfaces," *Brain Sci.*, vol. 8, no. 11, p. 199, 2018, doi: [10.3390/brainsci8110199](https://doi.org/10.3390/brainsci8110199).
- [6] L. Jiang, A. Stocco, D. M. Losey, J. A. Abernethy, C. S. Prat, and R. P. N. Rao, "BrainNet: A multi-person brain-to-brain interface for direct collaboration between brains," *Sci. Rep.*, vol. 9, no. 1, p. 6115, 2019, doi: [10.1038/s41598-019-41895-7](https://doi.org/10.1038/s41598-019-41895-7).
- [7] R. P. N. Rao *et al.*, "A direct brain-to-brain interface in humans," *PLoS ONE*, vol. 9, no. 11, 2014, Art. no. e111332, doi: [10.1371/journal.pone.0111332](https://doi.org/10.1371/journal.pone.0111332).
- [8] P. G. Vinoj, S. Jacob, and V. G. Menon, "Hybrid brain-actuated muscle interface for the physically disabled," *Basic Clin. Pharmacol. Toxicol.*, vol. 123, no. 1, pp. 8–9, 2019, doi: [10.1111/bcpt.13100](https://doi.org/10.1111/bcpt.13100).
- [9] S. Jacob, V. G. Menon, F. Al-Turjman, P. G. Vinoj, and L. Mostarda, "Artificial muscle intelligence system with deep learning for post-stroke assistance and rehabilitation," *IEEE Access*, vol. 7, pp. 133463–133473, 2019, doi: [10.1109/ACCESS.2019.2941491](https://doi.org/10.1109/ACCESS.2019.2941491).
- [10] D. J. Wheeler and R. M. Needham, "TEA, a tiny encryption algorithm," in *Proc. Fast Softw. Encryption Workshop*, vol. 1008, 1994, pp. 363–366, doi: [10.1007/3-540-60590-8\\_29](https://doi.org/10.1007/3-540-60590-8_29).
- [11] A. A. George, M. Riyadh, and M. V. Prajitha, "Secure image transferring using KBRP and TEA algorithms," in *Proc. Int. Conf. Innov. Inf. Embedded Commun. Syst. (ICIECS)*, Coimbatore, India, 2015, pp. 1–5, doi: [10.1109/ICIECS.2015.7193117](https://doi.org/10.1109/ICIECS.2015.7193117).
- [12] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 26, no. 1, pp. 96–99, 1983, doi: [10.1145/357980.358017](https://doi.org/10.1145/357980.358017).
- [13] S. Rajesh, V. Paul, V. G. Menon, and M. R. Khosravi, "A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices," *Symmetry*, vol. 11, no. 2, p. 293, 2019, doi: [10.3390/sym11020293](https://doi.org/10.3390/sym11020293).
- [14] A. Jolfaei, A. Matinfar, and A. Mirghadri, "Preserving the confidentiality of digital images using a chaotic encryption scheme," *Int. J. Electron. Security Digit. Forensics*, vol. 7, no. 3, p. 258, 2015, doi: [10.1504/ijesdf.2015.070389](https://doi.org/10.1504/ijesdf.2015.070389).
- [15] A. Jolfaei, A. Vizandan, and A. Mirghadri, "Image encryption using HC-128 and HC-256 stream ciphers," *Int. J. Electron. Security Digit. Forensics*, vol. 4, no. 1, p. 19, 2012, doi: [10.1504/ijesdf.2012.045388](https://doi.org/10.1504/ijesdf.2012.045388).
- [16] N. Birbaumer, "Breaking the silence: Brain computer interfaces (BCI) for communication and motor control," *Psychophysiology*, vol. 43, no. 6, pp. 517–532, 2006, doi: [10.1111/j.1469-8986.2006.00456.x](https://doi.org/10.1111/j.1469-8986.2006.00456.x).
- [17] J. R. Wolpaw *et al.*, "Brain-computer interface technology: A review of the first international meeting," *IEEE Trans. Rehabil. Eng.*, vol. 8, no. 2, pp. 164–173, Jun. 2000, doi: [10.1109/tre.2000.847807](https://doi.org/10.1109/tre.2000.847807).
- [18] S. G. Mason and G. E. Birch, "A brain-controlled switch for asynchronous control applications," *IEEE Trans. Biomed. Eng.*, vol. 47, no. 10, pp. 1297–1307, Oct. 2000, doi: [10.1109/10.871402](https://doi.org/10.1109/10.871402).
- [19] A. Kübler, B. Kotchoubey, J. Kaiser, J. Wolpaw, and N. Birbaumer, "Brain-computer communication: Unlocking the locked in," *Psychol. Bull.*, vol. 127, no. 3, pp. 358–375, 2001, doi: [10.1037/0033-2909.127.3.358](https://doi.org/10.1037/0033-2909.127.3.358).
- [20] S. Zhang *et al.*, "Human mind control of rat cyborg's continuous locomotion with wireless brain-to-brain interface," *Sci. Rep.*, vol. 9, no. 1, p. 1321, 2019, doi: [10.1038/s41598-018-36885-0](https://doi.org/10.1038/s41598-018-36885-0).
- [21] V. A. Maksimenko *et al.*, "Increasing human performance by sharing cognitive load using brain-to-brain interface," *Front. Neurosci.*, vol. 12, p. 949, Dec. 2018, doi: [10.3389/fnins.2018.00949](https://doi.org/10.3389/fnins.2018.00949).
- [22] A. Jolfaei, X. Wu, and V. Muthukkumarasamy, "On the feasibility and performance of pass-thought authentication systems," in *Proc. 4th Int. Conf. Emerg. Security Technol.*, Cambridge, MA, USA, 2013, pp. 33–38.
- [23] P. G. Vinoj, S. Jacob, V. G. Menon, S. Rajesh, and M. R. Khosravi, "Brain-controlled adaptive lower limb exoskeleton for rehabilitation of post-stroke paralyzed," *IEEE Access*, vol. 7, pp. 132628–132648, 2019, doi: [10.1109/ACCESS.2019.2921375](https://doi.org/10.1109/ACCESS.2019.2921375).
- [24] J. F. Valenzuela-Valdes, M. A. Lopez, P. Padilla, J. L. Padilla, and J. Minguillon, "Human neuro-activity for securing body area networks: Application of brain-computer interfaces to people-centric Internet of Things," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 62–67, Feb. 2017, doi: [10.1109/mcom.2017.1600633cm](https://doi.org/10.1109/mcom.2017.1600633cm).
- [25] A. Jolfaei and A. Mirghadri, "Substitution-permutation based image cipher using chaotic Henon and Baker's maps," *Int. Rev. Comput. Softw.*, vol. 6, no. 1, pp. 40–54, 2011.
- [26] A. Jolfaei, X. Wu, and V. Muthukkumarasamy, "A secure lightweight texture encryption scheme," in *Proc. Workshops Image Video Technol. (PSIVT)*, vol. 9555, 2015, pp. 344–356.



**Sreeja Rajesh** is currently pursuing the Ph.D. degree with the Department of Computer Science, Bharathiar University, Coimbatore, India.

Her research interests are in cryptography, security and privacy, Internet of Things, fog computing, and secure communication protocols.



**Varghese Paul** received the Ph.D. degree in computer science from the Cochin University of Science and Technology (CUSAT), Kochi, India.

He was the Head of information technology with CUSAT. He is currently a Professor with the IT Department, Rajagiri School of Engineering and Technology, Ernakulam, India. His research interests are in security and privacy, cryptography, data compression, data mining, image processing, and Internet of Things.



**Varun G. Menon** (M'16) received the Ph.D. degree in computer science and engineering from Sathyabama University, Chennai, India.

He is currently an Associate Professor with the Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Karukutty, India. His research interests include Internet of Things, brain signal analysis, fog computing and networking, and underwater acoustic sensor networks.

Prof. Menon is currently serving as the Guest Editor for the *IEEE Internet of Things Magazine* and the *Journal of Supercomputing*. He is an ACM Distinguished Speaker.



**Sunil Jacob** received the Ph.D. degree in electronics and communication engineering from Bharathiar University, Coimbatore, India.

He is currently the Director of the Centre for Robotics, SCMS School of Engineering and Technology, Karukutty, India, where he is a Professor with the Department of Electronics and Communication Engineering.

Prof. Jacob is the recipient of the Young Gandhian Technological Innovation Appreciation Award in 2018 and the AICTE Chhatra Vishwakarma Award in 2017.



**P. Vinod** received the Ph.D. degree in computer engineering from MNIT, Jaipur, India.

He is currently a Professor with the Department of Computer Science and Engineering and the Dean Research with the SCMS School of Engineering and Technology, Karukutty, India. He is also a Postdoctoral Fellow with the Department of Mathematics, University of Padua, Padua, Italy. His area of interest is adversarial machine learning, malware analysis, context-aware privacy preserving data mining, ethical hacking, and natural language processing.



# SDN-Powered Humanoid With Edge Computing for Assisting Paralyzed Patients

Varun G. Menon<sup>1</sup>, Senior Member, IEEE, Sunil Jacob, Member, IEEE, Saira Joseph, Member, IEEE, and Alaa Omran Almagrabi

**Abstract**—The number of people afflicted with paralysis is increasing worldwide due to stroke, spinal cord injury, polio, and other related diseases. Exoskeletons have emerged as one of the promising technologies to provide assistance and rehabilitation for the paralyzed people. But most of the exoskeletons are limited by its bulkiness, lack of flexibility and stability, instant control and adaptability. To overcome these issues, this article proposes a novel and efficient software-defined network (SDN)-powered humanoid assistive and rehabilitation system. In the proposed system, the signals acquired by the human sensor module are processed with multiple node MCUs and transmitted via the SDN incorporated with universal software radio peripheral (USRP). Using edge computing, the signal from the USRP is sent to the receiver node MCU and is used for controlling the movements of the humanoid that provides assistance to the paralyzed patients. The experimental setup is done for controlling a humanoid hand, and the results show high quality-of-service (QoS) for hand roll-up and roll-down posture. QoS is also evaluated for different electroencephalogram (EEG) signals, and the results show that the SDN-enabled assistive humanoid system is an efficient method for providing instant control in rehabilitation of the paralyzed patients.

**Index Terms**—Electroencephalogram (EEG), exoskeleton, humanoid, Internet of Things (IoT), paralyzed, software-defined networks (SDNs), universal software radio peripheral (USRP).

## I. INTRODUCTION

RECENT studies carried out by Toyota Mobility Foundation revealed that 30% of the paralyzed population is frustrated with the current assistive technologies using exoskeletons [1]. The patients suffer from constant pain and discomfort due to the outdated design of the mobility devices [1]–[4]. The participants of the study suggested that the assistive devices should allow them to move faster and help

in daily activities and also mentioned that the design should be natural, like an extension of their body, providing them freedom and independence.

Exoskeletons are currently being used for various assistive functions. Electrically powered full body exoskeletons have been designed for transport and handling of heavy loads [5]. A modular architecture is employed to manage the complexity of the system design and has different operating conditions for walking, squatting and handling loads. But the designed machine has difficulties in maintaining equilibrium while carrying heavy loads. Exoskeletons are also used for children suffering from cerebral palsy to assist in their gait [6], [7]. These wearable devices produce physiological gait patterns for the patients at the angle joints. Translation of gait in biped exoskeleton without using crutches is demonstrated in [8]. A series actuator with required torque and speed for transition from sit-to-stand posture is designed in [9]. Many exoskeletons are introduced specifically for assisting people with lower body paralysis [10], [11]. Several other brain computer interface (BCI) technologies integrated with exoskeletons are also used for assisting the paralyzed in rehabilitation [12]–[15]. But, many of these technologies introduce additional burden to the patient and also do not provide feedback for improvement. Lack of instant control and adaptability is a major issue in most of the exoskeleton-based solutions.

Recently, brain-to-brain interface systems have gained wide acceptance in stroke rehabilitation and assistance [16]. They overcome the issues with exoskeletons and provide better assistance in rehabilitation to the paralyzed patients. The efficiency of these systems hugely depends on the accuracy of the captured electroencephalogram (EEG) signals. Recent works in full body humanoids have highlighted their advantage over previous solutions [17], [18]. The current research work proposes a full body assistive humanoid for the paralyzed by integrating the advantages offered by BCI, brain-to-brain interface and humanoid systems with software-defined network (SDN) [19]–[23] and edge computing [24], [25] technologies. SDN offers flexibility with improved network control in communication and edge computing reduces the delay in processing of the signals. These two powerful technologies provide the much-needed efficiency in the proposed system. SDN is selected with an objective of improving the network efficiency and its effective usage is implemented with universal software radio peripheral (USRP). These advantages offered by SDN are used by the proposed system to achieve simplicity, efficiency and instant control in communication.

Manuscript received September 30, 2019; revised November 30, 2019 and December 19, 2019; accepted December 28, 2019. Date of publication December 31, 2019; date of current version July 10, 2020. This work was supported by the Deanship of Scientific Research, King Abdulaziz University, Jeddah, under Grant DF-160-6115-1441. (Corresponding author: Sunil Jacob.)

Varun G. Menon is with the Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Karukutty 683576, India (e-mail: varunmenon@ieee.org).

Sunil Jacob is with the Center for Robotics, SCMS School of Engineering and Technology, Karukutty 683576, India (e-mail: suniljacob@scmsgroup.org).

Saira Joseph is with the Department of Electronics and Communication Engineering, SCMS School of Engineering and Technology, Karukutty 683576, India (e-mail: saira\_joseph@scmsgroup.org).

Alaa Omran Almagrabi is with the Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia (e-mail: aalmagrabi3@kau.edu.sa).

Digital Object Identifier 10.1109/JIOT.2019.2963288

2327-4662 © 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.

See <https://www.ieee.org/publications/rights/index.html> for more information.

A novel assistive system for paralyzed people using an SDN-powered humanoid integrated with edge computing is proposed and discussed in this article. The system consists of three modules: a human body sensor module connected to node MCU that collects EEG, electrocardiogram (ECG), electromyography (EMG), and angular motion data; a node MCU-USRP interface with edge computing; and a USRP connected assistive humanoid module. The signals captured by the human body sensors in turn help to provide instant control to the humanoid and this system is used for assisting the paralyzed. The next section presents and discusses the recent related works. The notations and abbreviations used in this article are presented in Section III. The design and theoretical analysis of the proposed system is discussed in Section IV. Section V presents the hardware implementation of the system with results and discussion. This article concludes in Section VI with suggestions for future work.

## II. RELATED WORKS

Rehabilitation of the paralyzed people using efficient and competent technologies is a major challenge. Recently, many works are carried out in this article direction and this section discusses and highlights few of them. Fontana *et al.* [5] discussed the application of exoskeletons in transportation of heavy loads. The proposed system uses a modular architecture to manage the complexity of the design. The system also has different operating conditions for walking, squatting and handling loads. One of the major limitations is that the designed machine has difficulties in maintaining equilibrium while carrying heavy loads. Zhang *et al.* [10] presented and discussed a self-balancing and software-controlled exoskeleton for the lowered body. The system is designed to give a proper balance in both the sagittal and frontal planes. For managing the stability during walking, the authors discuss the use of a balance controller based on the extrapolated center of mass concept. The association of the assistance magnitude of the exoskeleton with the energy cost gains is studied with the help of a collection of elastic actuators driven powered hip exoskeleton in [11]. The exoskeleton is designed to mimic the behavior of a human biological hip. Pichiorri *et al.* [14] discussed the use of a BCI system to improve the motor imagery practice during the rehabilitation of paralyzed patients. The study focuses on presenting BCI devices as a major solution for recovery in stroke patients with severe motor impairments. Pierre and Abderrahmane [17] presented a BCI system that enabled a user to control a humanoid. An interesting solution to rehabilitation and recovery process for paralyzed patients using humanoids is proposed in [20]. This highly powered robotic rehabilitation system is used for assisting people with upper body paralysis. Jolfaei *et al.* [26] proposed an interesting discussion on using an information-theoretic measure-based binary asymmetric channel model for measuring the performance of pass-thought authentication systems. Batula *et al.* [27] discussed a four-class motor-imagery-based online BCI system for controlling a humanoid. The system is designed to help the upper and lower limb paralyzed patients to accelerate the rehabilitation process. Most of the existing exoskeleton-based

TABLE I  
FREQUENTLY USED NOTATIONS

| Notation      | Definition   |
|---------------|--|
| $B^+, B^-$    | varying amplitudes of the EEG signal   |
| $EEG_x$       | EEG signal in the 'x' direction  |
| $EEG_y$       | EEG signal in the 'y' direction  |
| $\alpha_{mn}$ | EEG propagation constant of $m^{\text{th}}$ and $n^{\text{th}}$ electric component |
| $\mu$         | permeability of the medium   |
| $\epsilon$    | permittivity of the medium   |
| $f_{mnl}$     | resonance frequency of USRP  |
| $USRP_E$      | transmitted EEG signal at USRP   |
| $USRP_P$      | received EEG signal at USRP  |
| $P_{LT}$      | power lost in the transmission   |
| $R_S$         | resistivity of USRP  |
| $\sigma$      | effective transmission conductivity of USRP  |
| $EEG_T$       | tangential electric field at the closed cylindrical structure                      |
| $Q_{USRP}$    | Total QoS at USRP  |

TABLE II  
LIST OF ABBREVIATIONS

| Abbreviation | Description  |
|--------------|--|
| SDN          | Software Defined Network                                 |
| USRP         | Universal Software Radio Peripheral                      |
| QoS          | Quality of Service                                       |
| EEG          | Electroencephalogram                                     |
| BCI          | Brain Computer Interface                                 |
| ECG          | Electrocardiogram  |
| EMG          | Electromyography   |
| WHT          | Walsh Hadamard Transform                                 |
| CP-OFDMA     | Cyclic-Prefix Orthogonal Frequency Division Multiplexing |
| RCTF         | Raised Cosine Transmit Filter                            |
| AWGN         | Additive White Gaussian Noise                            |
| CFC          | Coarse Frequency Compensation                            |
| FFC          | Fine Frequency Compensation                              |
| PLL          | Phase Locked Loop  |
| PED          | Phase Error Detection                                    |

solutions have limitations such as bulkiness and lack of flexibility. Inability to provide instant control, lack of stability, and adaptability are major issues with humanoid-based solutions. The proposed work overcomes these issues using an SDN powered humanoid assistive and rehabilitation system that helps in efficient rehabilitation and recovery of patients with partial or full body paralysis.

## III. NOTATIONS AND PRELIMINARIES

This section describes the various notations and preliminaries used in the research. Table I presents the summary of notations and Table II presents the list of abbreviations. This section also presents and discusses the flexible humanoid structure design.

### A. Humanoid Design

The designed humanoid structure along with joints and links is presented in Fig. 1. The figure correlates the human limb with humanoid limb. The different labels used in the figure are explained:  $A$ —head joint,  $B$ —neck joint,  $C$ —shoulder joint left,  $D$ —elbow joint left,  $E$ —hand joint left,  $F$ —shoulder joint right,  $G$ —elbow joint right, and  $H$ —hand joint right.

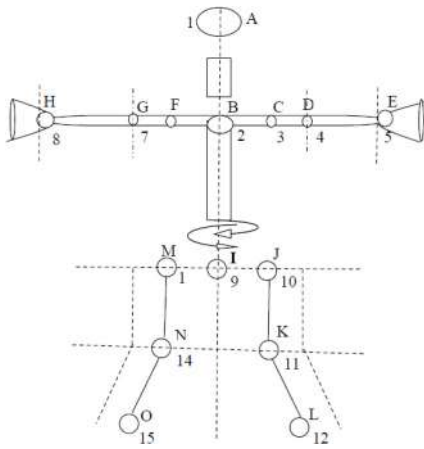


Fig. 1. Design of the humanoid.

Initially, the full body humanoid is modeled and mainly consists of five different body parts—the lower limb, upper limb, head and neck, shoulder, and hip. The modular design provides the humanoid with flexibility of use at different levels of paralysis. The design of humanoid for different human postures is explained below. The humanoid is designed to emulate the human body anatomy. The parts and joints can be attached and detached easily, allowing it to be used by people with different levels of paralysis. For the fully paralyzed, the full body humanoid structure can be used. Easier mobility and light weight features are also provided to the humanoid by constructing it using carbon fiber material. Supports are provided on the foot region and on the back side of the ankle joint to get better stability. Table III indicates the various postures and instruction execution method used in the design to ensure stability. The translation from sleeping to sitting posture is achieved by actuating the motors present in the desired joints. To maintain stability and reduce errors, a particular execution pattern is followed. The design ensures no direct transition from sleeping to standing or vice versa. To prevent falling, execution of halt command in the standing posture is rejected. In the current research work, the experimental evaluations and validations are carried out using a fully developed humanoid hand. The flexible full body humanoid will be presented in our future research work.

#### IV. PROPOSED SYSTEM

The proposed system has three modules: 1) a human body sensor module; 2) node MCU USRP interface with edge computing module; and 3) USRP-enabled humanoid. The main function of the human body sensor module is to capture the EEG, ECG, EMG signal, angular motion, positioning information and transform it into a signal acceptable by the USRP unit. The unit has USRP motherboard and has the subsystem consisting of FPGA, DAC, ADC clock synchronization and generation. The front end is a daughterboard used for up/down signal conversion, conditioning and filtering. This flexibility allows the USRP to be used from DC to GHz application. The FPGA on USRP board performs the DSP operations allowing real analog signal to be translated

TABLE III  
INSTRUCTION EXECUTION METHOD

| Posture  | Sitting | Standing | Sleeping | Halt    |
|----------|---------|----------|----------|---------|
| Sleeping | execute | rejected | retain   | execute |
| Sitting  | retain  | execute  | execute  | execute |
| Standing | execute | retain   | rejected | reject  |

into baseband digital signals. The human body sensor module uses noninvasive methods to capture the body parameter like the brain signals from the human scalp. The collected signals are then amplified using a high gain instrumentation amplifier to improve the signal strength. The signal further undergoes preprocessing and filtering. A band-pass filter is used to remove the high frequency noise. The signals are converted into frequency domain using the Walsh Hadamard transform (WHT) for feature extraction. The extracted signals are converted into digital and given to the Internet of Things (IoT) powered node MCU which transmits the signal via edge computing-enabled USRP. The main functionality of the node MCU with IoT-enabled edge computing is to classify the commands and to produce actuation signal for the corresponding body part. All the decisions for control are taken by the node MCU based on the signal received via human body sensor module.

In the offline training phase, the users will be trained for three basic commands (sitting, standing, and sleeping). The patterns for each of these commands will be recorded to create the database. The detected sensor patterns will be mapped into these three different commands. The node MCU uses this database to make the decision regarding the action to be performed. The activation signal from the IoT-enabled edge computing is received at the receiver side by USRP trans receiver daughterboard which is connected to IoT-enabled node MCU. The node MCU decodes the received signal and passes it on to the desired part of the humanoid actuation module through the motor driver circuit. A two-level sensing mechanism is given as the feedback to the node MCU to take corrective actions. Based on the angle sensor feedback received, the node MCU makes the desired corrections on the actuation signals. The accidental fall of humanoid is detected by incorporating an accelerometer on the back of the humanoid. If the measured tilt crosses a threshold, deceleration is provided to stabilize via edge computing-enabled USRP.

Now, the theoretical analysis of the data transmission in the proposed system is presented and discussed. The EEG signal processed by USRP on the humanoid can be considered as shortened at both ends of the edge forming a closed cylindrical structure. The EEG signal transmitted has an electrical component stored in the closed cylinder with power loss. The EEG signal field variation will be along three dimensions of the closed cylinder which is illustrated in Fig. 2.

The closed cylinder is of length  $b$  and radius  $c$ . Analysis is carried out considering the processing as lossless and then determining the quality-of-service (QoS) using the perturbation method and applying the boundary condition on the

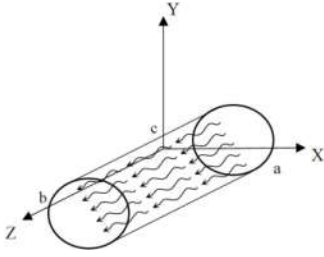


Fig. 2. Closed cylindrical structure (EEG signal processed by USRP).

circular cylinder  $X = (0, a)$  and  $Y = (0, c)$  and  $EEG_X = EEG_Y = 0$  at  $Z = (0, b)$ . The variation in transverse direction is represented by  $eeg(X, Y)$  and the varying amplitudes of the EEG signal as  $B^+$  and  $B^-$ . For the EEG signal in the “x” direction and “y” direction,  $EEG_X$  and  $EEG_Y$  are represented as

$$EEG(X, Y, Z) = eeg(X, Y)(B^+ e^{-j\alpha_{mn}Z} + B^- e^{j\alpha_{mn}Z}). \quad (1)$$

The permeability and permittivity of the medium are represented as  $\mu$  and  $\varepsilon$ , respectively, and the constant  $K = \omega\sqrt{\mu\varepsilon}$ . Now, the EEG propagation constant of  $m$ th and  $n$ th electric components is given by

$$\alpha_{mn} = \sqrt{K^2 - \frac{m\Pi^2}{a} - \frac{n\Pi^2}{b}}. \quad (2)$$

Applying the condition that  $B^+ = B^-$  at  $EEG_t = 0$  and at  $Z = 0$  gives

$$EEG_t(X, Y, b) = -eeg_t(X, Y)B^+ 2j \sin \alpha_{mn}d = 0. \quad (3)$$

The nontrivial solution ( $B^+ \neq 0$ ) is the only solution which occurs for  $\alpha_{mn}d = l\Pi$  where  $l = 1, 2, 3$  indicates that the EEG signal is an integer multiple. The variations of EEG at  $X, Y, Z$  directions are represented by  $m, n$  and  $l$  indices. Now, the EEG components for the structure is given by

$$O_{mnl} = \sqrt{\frac{m\Pi^2}{a} + \frac{n\Pi^2}{c} + \frac{l\Pi^2}{b}}. \quad (4)$$

The resonance frequency of USRP is given by

$$f_{mnl} = \frac{cO_{mnl}}{2\Pi\sqrt{\mu_r\varepsilon_r}} = \frac{c}{2\Pi\sqrt{\mu_r\varepsilon_r}} \sqrt{\frac{m\Pi^2}{a} + \frac{n\Pi^2}{c} + \frac{l\Pi^2}{b}}. \quad (5)$$

The resonance frequency of USRP shifts depending on  $a, c$ , and  $b$ . Considering the fact that  $B^+ = B^-$ , the total EEG field at different directions are given by

$$EEG_Y = B^+ \sin \frac{\Pi X}{a} (e^{-j\alpha Z} - e^{j\alpha Z}) \quad (6)$$

$$EEG_X = -\frac{B^+}{Z} \sin \frac{\Pi X}{a} (e^{-j\alpha Z} + e^{j\alpha Z}) \quad (7)$$

$$EEG_Z = \frac{j\Pi B^+}{Kna} \cos \frac{\Pi X}{a} (e^{-j\alpha Z} + e^{j\alpha Z}). \quad (8)$$

Substituting  $EEG_0 = -2jB^+$  and using  $\alpha_{mnd} = l\Pi$  into the above expression, we obtain

$$EEG_Y = EEG_0 \sin \frac{\Pi X}{a} \sin \frac{l\Pi Z}{b} \quad (9)$$

$$EEG_X = \frac{-jEEG_0}{Z} \sin \frac{\Pi X}{a} \cos \frac{l\Pi Z}{b} \quad (10)$$

$$EEG_Z = \frac{j\Pi EEG_0}{Kna} \cos \frac{\Pi X}{a} \sin \frac{l\Pi Z}{b}. \quad (11)$$

The transmitted EEG signal at USRP is given by

$$USRP_E = \frac{\varepsilon}{4} \int_0^V EEG_Y EEG_Y^* dV = \frac{\varepsilon abc}{16} EEG_0^2. \quad (12)$$

The received EEG signal at USRP is given by

$$\begin{aligned} USRP_P &= \frac{\mu}{4} \int_0^V (E_X E_X^* + E_Z E_Z^*) dV \\ &= \frac{\mu abc}{16} EEG^2 \left( \frac{1}{Z^2} + \frac{\Pi^2}{K^2 n^2 a^2} \right). \end{aligned} \quad (13)$$

Substituting  $\alpha = \sqrt{K^2 - (\frac{\Pi^2}{a})}$  in  $Z = (Kn/\alpha)$  and then substituting the result in (13), we obtain

$$USRP_P = \left( \frac{1}{Z^2} + \frac{\Pi^2}{K^2 n^2 a^2} \right) = \frac{\alpha^2 + \frac{\Pi^2}{a}}{K^2 n^2} = \frac{1}{n^2} = \frac{\varepsilon}{\mu}. \quad (14)$$

Considering  $R_S$  as the resistivity of USRP and  $EEG_T$  as the tangential electric field at the closed cylindrical structure, the power lost in the transmission is given by

$$P_{LT} = \frac{R_S}{2} \int |EEG_t|^2 dS. \quad (15)$$

Using the value of  $EEG_X$  and  $EEG_Y$  in the above equation, we obtain

$$\begin{aligned} P_{LT} &= \frac{R_S}{2} \left\{ 2 \int_{Y=0}^c \int_{X=0}^a |EEG_X(Z=0)|^2 \right. \\ &\quad + 2 \int_{Z=0}^b \int_{Y=0}^c |EEG_Z(X=0)|^2 \\ &\quad + 2 \int_{Z=0}^b \int_{X=0}^a |EEG_X(Y=0)|^2 \\ &\quad \left. + |EEG_Z(Y=0)|^2 \right\} dY dZ \\ &= \frac{R_S EEG_0^2 \lambda^2}{8n^2} \left( \frac{l^2 ac}{b^2} + \frac{cb}{a^2} + \frac{l^2 a}{2b} + \frac{b}{2a} \right). \end{aligned} \quad (16)$$

Here, the symmetry of the circular cylinder structure at  $X = 0$ ,  $Y = 0$ , and  $Z = 0$  is accumulated till  $X = a$ ,  $Y = c$ , and  $Z = b$ .

The QoS at USRP is obtained as

$$\begin{aligned} Q_{USRP(TX)} &= \frac{2\omega_0 SDR_E}{P_L} \\ &= \frac{K^3 abc n}{4\Pi^2 R_S} \frac{1}{\left[ \left( \frac{l^2 ac}{b^2} \right) + \left( \frac{cb}{a^2} \right) + \left( \frac{l^2 a}{2b} \right) + \left( \frac{b}{2a} \right) \right]} \\ &= \frac{(Kab)^3 cn}{2\Pi^2 R_S} \frac{1}{2l^2 a^3 c + 2cb^3 + l^2 a^3 b + ab^3}. \end{aligned} \quad (17)$$

The effective transmission conductivity of USRP is given by

$$\begin{aligned} \sigma &= \omega \bar{\varepsilon} = \omega \varepsilon_r \varepsilon_0 \tan \delta \\ \varepsilon &= \varepsilon' - j\varepsilon'' = \varepsilon_r \varepsilon_0 (1 - j \tan \delta) \end{aligned} \quad (18)$$

where  $\tan \delta$  denotes loss tangent.

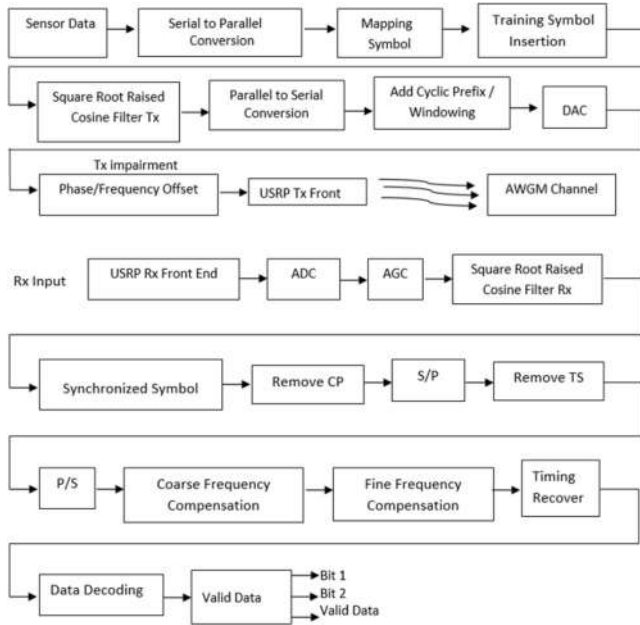


Fig. 3. System architecture.

Total received power at the received side is given by

$$P_R = \frac{1}{2} \int_0^V EEG \cdot EEG^* dV = \frac{\omega \varepsilon''}{2} \int_0^V |EEG|^2 dV$$

$$= \frac{ac b \omega \varepsilon'' |EEG|^2}{8}$$

$$\text{and } Q_{\text{USRP}(RX)} = \frac{2\omega \text{USRP}_E}{P_R} = \frac{1}{\tan \delta}. \quad (19)$$

When both USRP transmitted and received signal loss exist, the total power loss is  $(P_T + P_R)$ . A total QoS of USRP is

$$Q_{\text{USRP}} = \left( \frac{1}{Q_{\text{USRP}(TX)}} + \frac{1}{Q_{\text{USRP}(RX)}} \right)^{-1}. \quad (20)$$

Fig. 3 presents the architecture of the proposed system. Here, the transmitter side mainly includes the sensor data generation module, the cyclic-prefix orthogonal frequency-division multiplexing (CP-OFDMA) module and the raised cosine transmitter filter. The sensor data module generates the bits for each frame and the CP-OFDMA module modulates the bits into CP-OFDMA symbols. Raised cosine transmit filter (RCTF) uses a rolloff factor at 0.5 to up sample the CP-OFDMA symbol by two.

The channel used is additive white Gaussian noise (AWGN) with frequency offset and variable timing drift. At the receiver side the input data is received from the two USRP devices. The data captured has a base band signal with sampling frequency of 200 KHz. With automatic gate control (AGC), the derived amplitude level is adjusted for the received signal. The cosine receive filter with root raised, decimates the received signal by two and set a rolloff factor of 0.5. Coarse frequency compensation (CFC) calculates an approximate offset frequency of the input signal and rectifies it. Fine frequency compensation (FFC) compensates the phase and the residual frequency offset. With timing recovery, the recovered stroke

timing is used to resample the received signal such that the correct symbol decision is made for the optimized sampling frequency. Decoding module demodulates the received signal and aligns the frame bit boundary. It also resolves the ambiguity of the carrier phase caused by the FFC sub system. The three Boolean signals, bit 1 and bit 2 and the valid data are the output from the receiver. To speed up the computation, frame-based signal processing is used. In downstream bit processing, the sample-based signal is converted to frame-based signal using bit message decoding. The output demodulated bit 1 and bit 2 are valid only when the valid data is high. The bit message decoding block uses valid data to fill the delay string of bit 1 and bit 2.

The first block AGC is used to ensure a fixed and stable input to the timing and frequency recovery block. This is done by setting the amplitude of the input CFC systems as  $1/\text{up}$  sampling factor and to make sure that the phase and timing error detection gain remain constant with respect to time. The positioning of AGC before the cosine receiver is to make sure that the over sampling factor of four is used to measure the amplitude of the signal. This ensures improvement in the accuracy of the estimation. The RCTF helps with optimized SNR for the transmitted waveform using matched filtering and assures smooth downstream signal processing. The CFC corrects the required signal with approximate estimation of the frequency offset. The phase and frequency offset of the base band signal is then calculated. The received signal is raised to the power of four using the cascaded product block. The tones at the four-timing multiplication factor of the frequency offset is estimated. This estimated factor is divided by four, and the frequency offset is corrected in the original received signal. The residual frequency offset is then removed by FFC which is implemented using a phase locked loop (PLL). A correlation-based technique is used for estimating the frequency compensation with FFC which saves the hardware resources. The circuit speed is ensured by implementing the pipeline register. The phase offset and the residual frequency offset are compensated using PLL in the input signal. The maximum likelihood phase error detection (PED) will generate the error phase shift. The integral loop filter with automatic timing removes the error signal and feeds it to the phase estimation block. The phase estimation block generates the exponential signal to correct the phase offset and the residual frequency at the output signal of CFC. The timing error in the received signal is corrected by using the PLL. On average, one output sample is generated for two given input samples. It also gives a timing strobe valid data signal that has input sample rate as reference. Under normal operation, the value of the strobe signal is alternate zeroes and ones in sequence. The data decoding module performs the carrier phase error resolution and frame synchronization. Here, the frequency synchronization is achieved by matched filtering. The AWGN channel is enabled with variable delay and frequency offset. It applies frequency offset and a preset phase offset to the signal which has to be transmitted and then adds the variable delay. The next section presents the discussion on the results achieved with the proposed method.



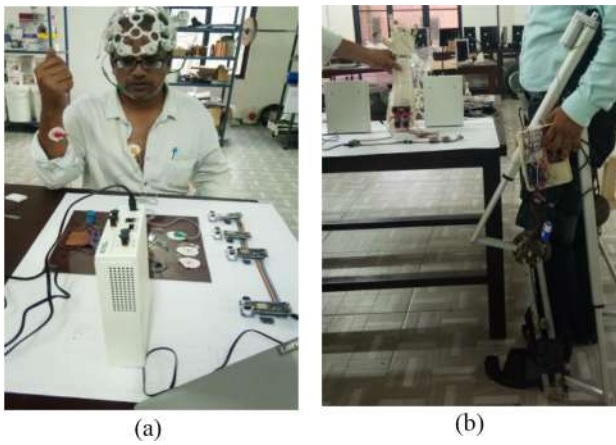


Fig. 4. Hardware setup. (a) Transmission system. (b) Receiver system.

V. RESULTS AND DISCUSSION

The hardware implementation details and the results achieved with the proposed method are presented in this section. Fig. 4(a) depicts the transmission side of the proposed system. Here, the human body sensor module consists of an EEG headset and sensors to capture EMG, ECG, positioning and angular motion information. The collected signals are amplified by using high gain instrumentation amplifier to improve the signal strength. The signal further undergoes preprocessing and filtering. A band-pass filter is used for removing high frequency noise. The signals are then converted into frequency domain using WHT for feature extraction. The extracted signals are converted into digital and given to the IoT powered node MCU which transmits the signal via edge computing-enabled USRP. Fig. 4(b) depicts the receiver side of the proposed system. The main functionality of the node MCU with IoT-enabled edge computing is to classify the commands and to produce actuation signals for the corresponding body part. All the decisions regarding control are taken by the node MCU based on the signal received via human body sensor module. An exoskeleton integrated with humanoid hand is used for the experiment and to validate the proposed system.

Fig. 5 presents the various reference components of the USRP used with the proposed system. The frequency range used in the transmission is between  $-20$  and  $20$  Hz. This is presented to depict the fundamental setting in the data transmission with SDN-USRP. In the proposed system, two USRPs are used at the transmitter side and two at the receiver side. They provide simple and efficient connectivity between the sensor module and the assistive humanoid. Further, the USRP-enabled proposed system achieves very good QoS in different humanoid hand postures. The amplitude variations with respect to frequency of EEG electrical component is shown in Fig. 6. In the proposed system, with the humanoid hand, two movements, hand roll-up and hand roll-down are performed. Amplitude variations with respect to the frequency of EEG electrical components will help in the estimation of the correct decision regarding the hand movement by the humanoid. The correct hand posture is selected based on the matching of the signal parameters with the already

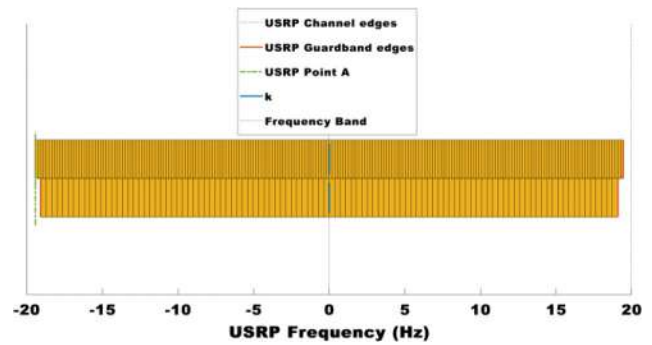


Fig. 5. Reference components of USRP.

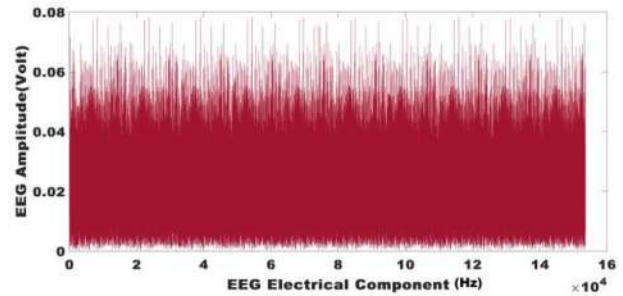


Fig. 6. Amplitude variations with respect to the frequency of EEG electrical components.

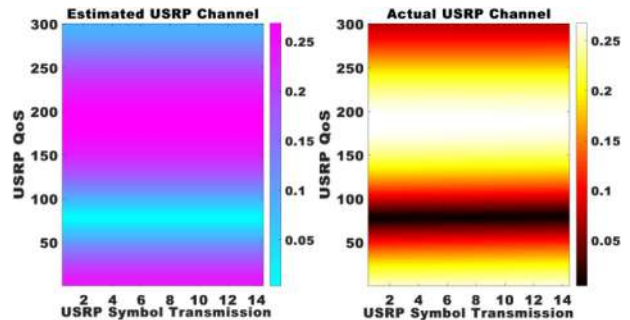


Fig. 7. Estimated and actual USRP channel estimation.

recorded values. The nearest matching value is selected and the corresponding hand movement is performed.

Fig. 7 gives the actual and estimated USRP channel for transmission and reception. This result is also very important for making the correct decision on the appropriate hand movement at the receiver end. From the results obtained with the proposed system, it is observed that the actual channel converges with the estimated channel which helps to make the right decision on the selection of the exact hand movement by the system.

Fig. 8 presents the USRP QoS variations with respect to symbols transmitted and received. The QoS of the signal at the transmitter is shown in the top half of the figure and the QoS at the receiver is shown at the bottom half. It is quite evident from the results plotted in the graph that the proposed system with USRP achieves good performance at the humanoid end. The system offers very good performance in communication and thus contributes to the overall success in

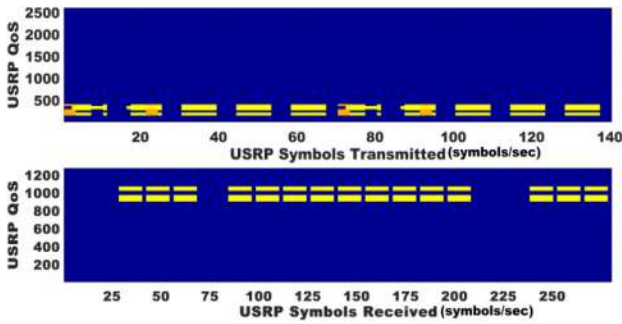


Fig. 8. USRP QoS variations with respect to symbols transmitted/received.

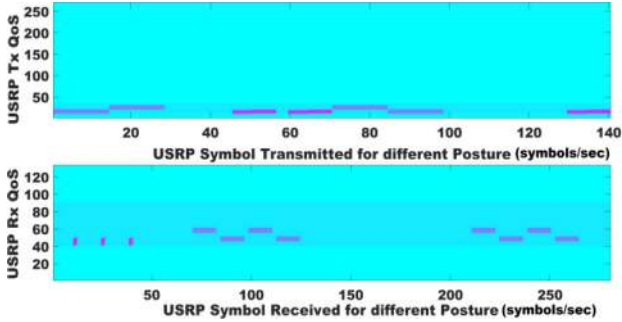


Fig. 9. USRP transmission/reception QoS with respect to symbols transmitted/received for different postures.

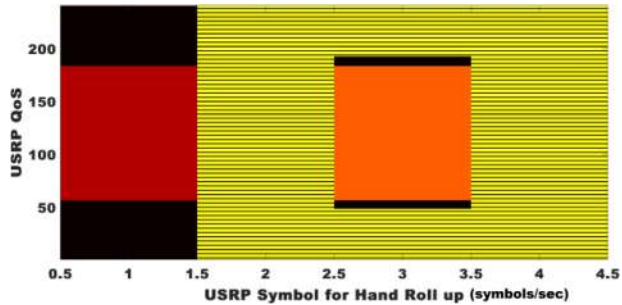


Fig. 10. USRP QoS with hand roll up.

the working of the assistive humanoid system. The USRP QoS variations with respect to symbols transmitted and received for different hand movements, hand roll-up and hand roll down is shown in Fig. 9. From the graph, it is evident that a higher QoS is achieved at the receiving end for different hand movements, which justifies the excellent performance of the proposed system. Fig. 10 presents the QoS of the proposed system with the hand roll up movement and Fig. 11 presents the QoS with the hand roll down movement. It is evident from the graph that the actual QoS achieved by proposed system while controlling the humanoid in various movements is almost equivalent to the estimated QoS and this confirms the high performance achieved by the proposed SDN powered humanoid assistive system.

Fig. 12 presents the variations in EEG components obtained for different postures. The graph is plotted based on sample results obtained with the proposed system. From the graph, it is observed that the hand roll-up posture is selected in the current scenario for activating the humanoid based on the peak

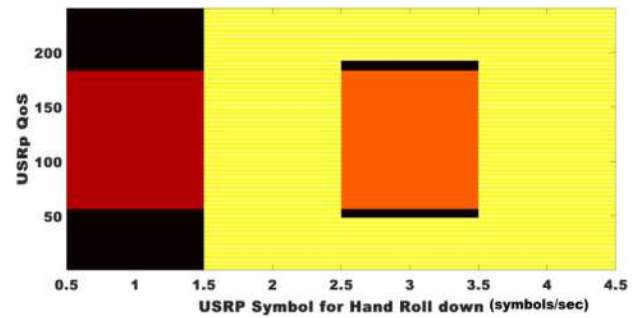


Fig. 11. USRP QoS with hand roll down.

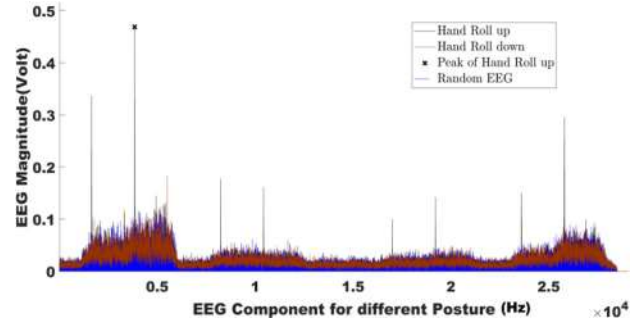


Fig. 12. EEG magnitude variation in the receiver system.

component value observed in the result. The proposed system makes the right posture decisions accurately based on the peak component values achieved. Thus, the proposed SDN-enabled assistive humanoid system is efficient and provides instant control and assistance in rehabilitation of the paralyzed.

## VI. CONCLUSION

This article proposed a novel assistive system for paralyzed people using an SDN-USRP powered humanoid integrated with edge computing. The system consists of three modules, a human body sensor module connected to node MCU to collect EEG, ECG, EMG and angular motion data, a node MCU-USRP interface with edge computing and USRP-enabled humanoid. The signals captured by the human body sensors in turn helped to control the humanoid and this system is used for assisting the paralyzed. The proposed system overcomes the limitations of normal exoskeletons used for paralysis assistance. The experimental setup was done for controlling a humanoid hand and results showed high QoS for hand roll-up and roll-down posture. The results showed that the SDN-enabled body sensor module is an efficient method for providing instant control for the assistance and rehabilitation of the paralyzed. In the future, the analysis of the system performance needs to be done with the full body humanoid and also more efficient deep learning algorithms can be integrated to improve the accuracy of movement prediction and decision making in the humanoid.

## ACKNOWLEDGMENT

The authors would like to thank Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, Saudi Arabia, for technical support.



## REFERENCES

- [1] *Mobility Devices for Lower-Limb Paralysis Flawed, Survey Reveals*, ComRes, London, U.K., and Toyota Mobility Found., Tokyo, Japan, 2019. Accessed: Jun. 20, 2019. [Online]. Available: <https://multiplesclerosisnewstoday.com/2018/06/08/mobility-devices-lower-limb-paralysis-flawed-survey>
- [2] A. Nishimoto *et al.*, "Feasibility of task-specific brain-machine interface training for upper-extremity paralysis in patients with chronic hemiparetic stroke," *J. Rehabil. Med.*, vol. 50, no. 1, pp. 52–58, 2018. doi: [10.2340/16501977-2275](https://doi.org/10.2340/16501977-2275).
- [3] S. Jacob, V. G. Menon, F. Al-Turjman, P. G. Vinoj, and L. Mostarda, "Artificial muscle intelligence system with deep learning for post-stroke assistance and rehabilitation," *IEEE Access*, vol. 7, pp. 133463–133473, 2019. doi: [10.1109/ACCESS.2019.2941491](https://doi.org/10.1109/ACCESS.2019.2941491).
- [4] S. Rajesh, V. Paul, V. G. Menon, S. Jacob, and Vinod P., "Secure brain to brain communication with edge computing for assisting post-stroke paralyzed patients," *IEEE Internet Things J.*, early access, 2019. doi: [10.1109/JIOT.2019.2951405](https://doi.org/10.1109/JIOT.2019.2951405).
- [5] M. Fontana, R. Vertechy, S. Marcheschi, F. Salsedo, and M. Bergamasco, "The body extender: A full-body exoskeleton for the transport and handling of heavy loads," *IEEE Robot. Autom. Mag.*, vol. 21, no. 4, pp. 34–44, Dec. 2014. doi: [10.1109/mra.2014.2360287](https://doi.org/10.1109/mra.2014.2360287).
- [6] A. A. Lins, J. M. de Oliveira, J. J. P. C. Rodrigues, and V. H. C. de Albuquerque, "Robot-assisted therapy for rehabilitation of children with cerebral palsy—A complementary and alternative approach," *Comput. Human Behav.*, vol. 100, pp. 152–167, Nov. 2019. doi: [10.1016/j.chb.2018.05.012](https://doi.org/10.1016/j.chb.2018.05.012).
- [7] F. Patané, S. Rossi, F. D. Sette, J. Taborri, and P. Cappa, "WAKE-up exoskeleton to assist children with cerebral palsy: Design and preliminary evaluation in level walking," *IEEE Trans. Neural Syst. Rehabil. Eng.*, vol. 25, no. 7, pp. 906–916, Jul. 2017. doi: [10.1109/tnsre.2017.2651404](https://doi.org/10.1109/tnsre.2017.2651404).
- [8] A. Agrawal *et al.*, "First steps towards translating HZD control of bipedal robots to decentralized control of exoskeletons," *IEEE Access*, vol. 5, pp. 9919–9934, 2017. doi: [10.1109/access.2017.2690407](https://doi.org/10.1109/access.2017.2690407).
- [9] M. K. Shepherd and E. J. Rouse, "Design and validation of a torque-controllable knee exoskeleton for sit-to-stand assistance," *IEEE/ASME Trans. Mechatronics*, vol. 22, no. 4, pp. 1695–1704, Aug. 2017. doi: [10.1109/tmech.2017.2704521](https://doi.org/10.1109/tmech.2017.2704521).
- [10] T. Zhang, M. Tran, and H. Huang, "Design and experimental verification of hip exoskeleton with balance capacities for walking assistance," *IEEE/ASME Trans. Mechatronics*, vol. 23, no. 1, pp. 274–285, Feb. 2018. doi: [10.1109/TMECH.2018.2790358](https://doi.org/10.1109/TMECH.2018.2790358).
- [11] I. Kang, H. Hsu, and A. Young, "The effect of hip assistance levels on human energetic cost using robotic hip exoskeletons," *IEEE Robot. Autom. Lett.*, vol. 4, no. 2, pp. 430–437, Apr. 2019. doi: [10.1109/LRA.2019.2890896](https://doi.org/10.1109/LRA.2019.2890896).
- [12] P. G. Vinoj, S. Jacob, and V. G. Menon, "Hybrid brainactuated muscle interface for the physically disabled," *Basic Clin. Pharmacol. Toxicol.*, vol. 123, no. 1, pp. 8–9, 2019. doi: [10.1111/bcpt.13100](https://doi.org/10.1111/bcpt.13100).
- [13] S. Jacob, V. Menon, and S. Joseph, "Artificial intelligence powered EEG-EMG electrodes for assisting the paralyzed," *IEEE Technol. Policy Ethics*, to be published.
- [14] F. Pichiorri *et al.*, "Brain-computer interface boosts motor imagery practice during stroke recovery," *Ann. Neurol.*, vol. 77, no. 5, pp. 851–865, 2015. doi: [10.1002/ana.24390](https://doi.org/10.1002/ana.24390).
- [15] P. G. Vinoj, S. Jacob, V. G. Menon, S. Rajesh, and M. R. Khosravi, "Brain-controlled adaptive lower limb exoskeleton for rehabilitation of post-stroke paralyzed," *IEEE Access*, vol. 7, pp. 132628–132648, 2019. doi: [10.1109/access.2019.2921375](https://doi.org/10.1109/access.2019.2921375).
- [16] W. Lee *et al.*, "Non-invasive transmission of sensorimotor information in humans using an EEG/focused ultrasound brain-to-brain interface," *PLoS ONE*, vol. 12, no. 6, 2017, Art. no. e0178476. doi: [10.1371/journal.pone.0178476](https://doi.org/10.1371/journal.pone.0178476).
- [17] G. Pierre and K. Abderrahmane, "2A1-I09 building a usable brain-computer interface for humanoid control (mobiligence and embodiment)," in *Proc. JSME Annu. Conf. Robot. Mechatronics (Robomec)*, vol. 2013, Tsukuba, Japan, May 2013, pp. 2A1-I09\_1–2A1-I09\_2. doi: [10.1299/jsmermd.2013\\_2A1-I09\\_1](https://doi.org/10.1299/jsmermd.2013_2A1-I09_1).
- [18] J. Brookes *et al.*, "Robots testing robots: ALAN-Arm, a humanoid arm for the testing of robotic rehabilitation systems," in *Proc. Int. Conf. Rehabil. Robot. (ICORR)*, London, U.K., 2017, pp. 676–681. doi: [10.1109/ICORR.2017.8009326](https://doi.org/10.1109/ICORR.2017.8009326).
- [19] S. Garg, K. Kaur, G. Kaddoum, S. H. Ahmed, and D. N. K. Jayakody, "SDN-based secure and privacy-preserving scheme for vehicular networks: A 5G perspective," *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 8421–8434, Sep. 2019. doi: [10.1109/TVT.2019.2917776](https://doi.org/10.1109/TVT.2019.2917776).
- [20] K. Kaur, S. Garg, G. Kaddoum, E. Bou-Harb, and K.-K. R. Choo, "A big data-enabled consolidated framework for energy efficient software defined data centers in IoT setups," *IEEE Trans. Ind. Informat.*, early access, 2019. doi: [10.1109/TII.2019.2939573](https://doi.org/10.1109/TII.2019.2939573).
- [21] S. Garg, K. Kaur, S. H. Ahmed, A. Bradai, G. Kaddoum, and M. Atiquzzaman, "MobQoS: Mobility-aware and QoS-driven SDN framework for autonomous vehicles," *IEEE Wireless Commun.*, vol. 26, no. 4, pp. 12–20, Aug. 2019.
- [22] S. Anbalagan, D. Kumar, Mercy Faustina J., G. Raja, W. Ejaz, and A. K. Bashir, "SDN-assisted efficient LTE-WiFi aggregation in next generation IoT networks," *Future Gen. Comput. Syst.*, Dec. 2017. doi: [10.1016/j.future.2017.12.013](https://doi.org/10.1016/j.future.2017.12.013).
- [23] S. Garg, K. Kaur, N. Kumar, G. Kaddoum, A. Y. Zomaya, and R. Ranjan, "A hybrid deep learning-based model for anomaly detection in cloud datacenter networks," *IEEE Trans. Netw. Service Manag.*, vol. 16, no. 3, pp. 924–935, Sep. 2019.
- [24] V. G. Menon and J. Prathap, "Vehicular fog computing: Challenges applications and future directions," in *Fog Computing: Breakthroughs in Research and Practice*. Hershey, PA, USA: IGI Glob., 2018, pp. 220–229.
- [25] S. Garg *et al.*, "Edge computing-based security framework for big data analytics in VANETs," *IEEE Netw.*, vol. 33, no. 2, pp. 72–81, Mar./Apr. 2019. doi: [10.1109/MNET.2019.1800239](https://doi.org/10.1109/MNET.2019.1800239).
- [26] A. Jolfaei, X.-W. Wu, and V. Muthukkumarasamy, "On the feasibility and performance of pass-thought authentication systems," in *Proc. 4th Int. Conf. Emerg. Security Technol.*, 2013, pp. 33–38.
- [27] A. M. Batula, Y. E. Kim, and H. Ayaz, "Virtual and actual humanoid robot control with four-class motor-imagery-based optical brain-computer interface," *BioMed Res. Int.*, vol. 2017, pp. 1–13, Jul. 2017. doi: [10.1155/2017/1463512](https://doi.org/10.1155/2017/1463512).

**Varun G. Menon** (Senior Member, IEEE) received the M.Tech. degree from Karunya University, Coimbatore, India, in 2011, and the Ph.D. degree in computer science and engineering from Sathyabama University, Chennai, India, in 2017.

He is currently an Associate Professor with the Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Karukutty, India. His research interests include IoT, brain signal analysis, fog computing, and underwater acoustic sensor networks.

Dr. Menon is a Guest Editor for the IEEE SENSORS JOURNAL and the IEEE Internet of Things Magazine. He is also a Distinguished Speaker of ACM.

**Sunil Jacob** (Member, IEEE) received the M.Tech. degree from Jawaharlal Nehru Technological University Hyderabad, Hyderabad, India, in 2004, and the Ph.D. degree in electronics and communication engineering from Bharathiar University, Coimbatore, India, in 2015.

He is the Director of the Centre for Robotics, SCMS School of Engineering and Technology, Karukutty, India, where he is a Professor with the Department of Electronics and Communication Engineering. His research interests include SDN, edge computing, brain computer interface, and signal processing.

Prof. Jacob is a recipient of the Young Gandhian Technological Innovation Appreciation Award 2018.

**Saira Joseph** (Member, IEEE) received the M.Tech. and Ph.D. degrees in electronics and communication engineering from the Cochin University of Science and Technology, Kochi, India, in 2006 and 2017, respectively.

She is currently an Associate Professor and the Head of the Department of Electronics and Communication Engineering, SCMS School of Engineering and Technology, Karukutty, India. Her interests include edge computing, fractal antennas, UWB, RADAR, and metamaterials.

**Alaa Omran Almagrabi** received the master's degree in information technology and the Ph.D. degree in computer science from La Trobe University, Melbourne, VIC, Australia, in 2009 and 2014, respectively.

He is with the Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia. His research interests are in information system, network, programming, modeling and analysis, Internet of Things, and SDN.

Skip to main content

Access and authentication: Please [visit our page](#).

Close X

Enter your search terms here  Advanced search

Access and purchase options

# Preventing hijacked research papers in fake (rogue) journals through social media and databases

**Varun G. Menon** (Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Kochi, India)

**Mohammad R. Khosravi** (Department of Electrical and Electronic Engineering, Shiraz University of Technology, Shiraz, Islamic Republic of Iran)

[Library Hi Tech News](#)

DOWNLOADS

ISSN: 0741-9058



Article publication date: 18 June 2019

International Standard

Serial [Permissions](#)

Number publication date: 6 August 2019

Citation

Menon, V.G. and Khosravi, M.R. (2019), "Preventing hijacked research papers in fake (rogue) journals through social media and databases", *Library Hi Tech News*, Vol. 36 No. 5, pp. 1-6.

<https://doi.org/10.1108/LHTN-11-2018-0070>

 Download as .RIS

Publisher: Emerald Publishing Limited

Copyright © 2019, Emerald Publishing Limited

## Related articles

Getting acquainted with social networks and apps: combating fake news on social media

Katie Elson Anderson, *Library Hi Tech News*, 2018

Types of hijacking in the academic world – our experiment in the scholarly publishing

Mehdi Dadkhah, *Library Hi Tech News*, 2016

Social media research in the context of emerging markets: An analysis of extant literature from information systems perspective

Kuttimani Tamilmani et al., *Journal of Advances in Management Research*, 2018

The people speak: social media on euthanasia/assisted dying

Chrystal Jaye et al., *Med Humanities*, 2021

Children's fitness and health: an epic scandal of poor methodology, inappropriate statistics, questionable editorial practices and a generation of misinformation

Jo Welsman et al., *Evid Based Med*, 2021

Promoting corporate image or preventing underage use?



### Services

[Authors](#)

[Editors](#)

[Librarians](#)

[Researchers](#)

[Reviewers](#)

### About

[About Emerald](#)

[Working for Emerald](#)

[Contact us](#)

[Publication sitemap](#)

### Policies and information

[Privacy notice](#)

[Site policies](#)

[Modern Slavery Act](#)

[Chair of Trustees governance statement](#)

[COVID-19 policy](#)

[Accessibility](#)

## Identification of Android malware using refined system calls

Deepa K., Radhamani G., Vinod P., Mohammad Shojafar ✉, Neeraj Kumar, Mauro Conti

First published: 09 May 2019

<https://doi.org/10.1002/cpe.5311>

Citations: 2

### Summary

The ever increasing number of Android malware has always been a concern for cybersecurity professionals. Even though plenty of anti-malware solutions exist, we hypothesize that the performance of existing approaches can be improved by deriving relevant attributes through effective feature selection methods. In this paper, we propose a novel two-step feature selection approach based on Rough Set and Statistical Test named as RSST to extract refined system calls, which can effectively discriminate malware from benign apps. By refined set of system call, we mean the existence of highly relevant calls that are uniformly distributed thought target classes. Moreover, an optimal attribute set is created, which is devoid of redundant system calls. To address the problem of higher dimensional attribute set, we derived suboptimal system call space by applying the proposed feature selection method to maximize the separability between malware and benign samples. Comprehensive experiments conducted on three datasets resulted in an accuracy of 99.9%, Area Under Curve (AUC) of 1.0, with 1% False Positive Rate (FPR). However, other feature selectors (Information Gain, CFSSubsetEval, ChiSquare, FreqSel, and Symmetric Uncertainty) used in the domain of malware analysis resulted in the accuracy of 95.5% with 8.5% FPR. Moreover, the empirical analysis of RSST derived system calls outperformed other attributes such as permissions, opcodes, API, methods, call graphs, Droidbox attributes, and network traces.

### REFERENCES

- 1 Smartphones Industry: Statistics & Facts. <http://www.statista.com/topics/840/smartphones/>. Accessed March 2019.  
[Google Scholar](#)
- 2 Sophos. <http://www.sophos.com/en-us/security-news-trends/whitepapers.aspx>. Accessed March 2019.  
[Google Scholar](#)
- 3 Faruki P, Bharmal A, Laxmi V, et al. Android security: a survey of issues, malware penetration, and defenses. *IEEE Commun Surv Tutor*. 2015; **17**(2): 998-1022.  
View | [Web of Science®](#) | [Google Scholar](#)
- 4 Amos B, Turner H, White J. Applying machine learning classifiers to dynamic Android malware detection at scale. Paper presented at: 9th International Wireless Communications and Mobile Computing Conference; 2013; Sardinia, Italy.  
[Google Scholar](#)
- 5 Gardiner J, Nagaraja S. On the security of machine learning in malware C&C detection: a survey. *ACM Comput Surv*. 2016; **49**(3): 59:1-59:39.  
View | [Web of Science®](#) | [Google Scholar](#)
- 6 Android Monkey. <http://developer.android.com/studio/test/monkey.html>. Accessed March 2019.  
[Google Scholar](#)
- 7 Feizollah A, Anuar NB, Salleh R, Wahab AWA. A review on feature selection in mobile malware detection. *Digit Investig*. 2015; **13**: 22-37.  
View | [Web of Science®](#) | [Google Scholar](#)
- 8 Zhang M, Yao JT. A rough sets based approach to feature selection. Paper presented at: IEEE Annual Meeting of the Fuzzy Information; 2004; Banff, Canada.  
[Google Scholar](#)
- 9 Świniarski RW. Rough sets methods in feature reduction and classification. *Int J Appl Math Comput Sci*. 2001; **11**: 565-582.  
[Google Scholar](#)
- 10 Massey A, Miller SJ. Tests of Hypotheses Using Statistics. Providence, RI: Brown University; 2006.  
[Google Scholar](#)

11 Freund Y, Schapire R, Abe N. A short introduction to boosting. *Jpn Soc Artif Intell.* 1999; **14**(771-780): 1612.

[Google Scholar](#)

---

12 Breiman L. Random forests. *Mach Learn.* 2001; **45**(1): 5-32.

View | [Web of Science®](#) | [Google Scholar](#)

---

13 Kuncheva LI, Rodríguez JJ. An experimental study on rotation forest ensembles. Paper presented at: International Workshop on Multiple Classifier Systems; 2007; Prague, Czech Republic.

[Google Scholar](#)

---

14 Droidbox. <http://github.com/pjlantz/droidbox>. Accessed March 2019.

[Google Scholar](#)

---

15 Arp D, Spreitzenbarth M, Hubner M, Gascon H, Rieck K, Siemens C. DREBIN: Effective and explainable detection of Android malware in your pocket. Paper presented at: Network and Distributed System Security Symposium; 2014; San Diego, CA.

[Google Scholar](#)

---

16 Zhou Y, Jiang X. Dissecting Android malware: Characterization and evolution. Paper presented at: 33rd IEEE Symposium on Security and Privacy; 2012; San Francisco, CA.

[Google Scholar](#)

---

17 Glodek W, Harang R. Rapid permissions-based detection and analysis of mobile malware using random decision forests. Paper presented at: Military Communications Conference; 2013; San Diego, CA.

[Google Scholar](#)

---

18 Cen L, Gates CS, Si L, Li N. A probabilistic discriminative model for android malware detection with decompiled source code. *IEEE Trans Dependable Secure Comput.* 2015; **12**(4): 400-412.

View | [Web of Science®](#) | [Google Scholar](#)

---

19 Talha KA, Alper DI, Aydin C. APK auditor: permission-based Android malware detection system. *Digit Investig.* 2015; **13**: 1-14.

View | [Web of Science®](#) | [Google Scholar](#)

---

20 Wang W, Li Y, Wang X, Liu J, Zhang X. Detecting Android malicious apps and categorizing benign apps with ensemble of classifiers. *Future Gener Comput Syst.* 2018; **78**: 987-994.

View | [Web of Science®](#) | [Google Scholar](#)

---

21 Zhao K, Zhang D, Su X, Li W. Fest: A feature extraction and selection tool for Android malware detection. Paper presented at: IEEE Symposium on Computers and Communication; 2015; Larnaca, Cyprus.

[Google Scholar](#)

---

22 Wang W, Wang X, Feng D, Liu J, Han Z, Zhang X. Exploring permission-induced risk in android applications for malicious application detection. *IEEE Trans Inf Forensics Secur.* 2014; **9**(11): 1869-1882.

View | [Web of Science®](#) | [Google Scholar](#)

---

23 Ham H-S, Choi MJ. Analysis of Android malware detection performance using machine learning classifiers. Paper presented at: International Conference on ICT Convergence; 2013; Jeju, South Korea.

[Google Scholar](#)

---

24 Amamra A, Robert J-M, Abraham A, Talhi C. Generative versus discriminative classifiers for android anomaly-based detection system using system calls filtering and abstraction process. *Secur Commun Netw.* 2016; **9**(16): 3483-3495.

View | [Web of Science®](#) | [Google Scholar](#)

---

25 Kim H-H, Choi M-J. Linux kernel-based feature selection for Android malware detection. Paper presented at: 16th Asia-Pacific Network Operations and Management Symposium; 2014; Hsinchu, Taiwan.

[Google Scholar](#)

---

26 Shabtai A, Tenenboim-Chekina L, Mimran D, Rokach L, Shapira B, Elovici Y. Mobile malware detection through analysis of deviations in application network behavior. *Comput Secur.* 2014; **43**: 1-18.

View | [Web of Science®](#) | [Google Scholar](#)

27 Narudin FA, Feizollah A, Anuar NB, Gani A. Evaluation of machine learning classifiers for mobile malware detection. *Soft Computing*. 2016; **20**(1): 343-357.

View | [Web of Science®](#) | [Google Scholar](#)

---

28 Chekina L, Mimran D, Rokach L, Elovici Y, Shapira B. Detection of Deviations in Mobile Applications Network Behavior. 2012. <http://arxiv.org/abs/1208.0564>

[Google Scholar](#)

---

29 Shabtai A, Kanonov U, Elovici Y, Glezer C, Weiss Y. Andromaly: a behavioral malware detection framework for android devices. *J Intell Inf Syst*. 2012; **38**(1): 161-190.

View | [Web of Science®](#) | [Google Scholar](#)

---

30 Tong F, Yan Z. A hybrid approach of mobile malware detection in Android. *J Parallel Distributed Comput*. 2017; **103**: 22-31. Special Issue on Scalable Cyber-Physical Systems.

View | [Web of Science®](#) | [Google Scholar](#)

---

31 Damshenas M, Dehghantanha A, Choo K-KR, Mahmud R. M0droid: an android behavioral-based malware detection model. *J Inf Priv Secur*. 2015; **11**(3): 141-157.

[Google Scholar](#)

---

32 Xiao X, Wang Z, Li Q, Xia S, Jiang Y. Back-propagation neural network on Markov chains from system call sequences: a new approach for detecting Android malware with system call sequences. *IET Inf Secur*. 2016; **11**(1): 8-15.

View | [Web of Science®](#) | [Google Scholar](#)

---

33 Canfora G, Medvet E, Mercaldo F, Visaggio CA. Detecting Android malware using sequences of system calls. Paper presented at: 3rd International Workshop on Software Development Lifecycle for Mobile; 2015; Bergamo, Italy.

[Google Scholar](#)

---

34 Xin Su, Chuah M, Tan G. Smartphone dual defense protection framework: Detecting malicious applications in Android markets. Paper presented at: 8th International Conference on Mobile Ad-hoc and Sensor Networks; 2012; Chengdu, China.

[Google Scholar](#)

---

35 Canfora G, Mercaldo F, Visaggio CA. A classifier of malicious Android applications. Paper presented at: 8th International Conference on Availability, Reliability and Security; 2013; Regensburg, Germany.

[Google Scholar](#)

---

36 Rocha BPS, Conti M, Etalle S, Crispo B. Hybrid static-runtime information flow and declassification enforcement. *IEEE Trans Inf Forensics Secur*. 2013; **8**(8): 1294-1305.

View | [Web of Science®](#) | [Google Scholar](#)

---

37 Feldman S, Stadther D, Wang B. Manalyzer: Automated Android malware detection through manifest analysis. Paper presented at: IEEE 11th International Conference on Mobile Ad Hoc and Sensor Systems; 2014; Philadelphia, PA.

[Google Scholar](#)

---

38 Lin Y-D, Lai Y-C, Lu C-N, Hsu P-K, Lee C-Y. Three-phase behavior-based detection and classification of known and unknown malware. *Secur Commun Netw*. 2015; **8**(11): 2004-2015.

View | [Web of Science®](#) | [Google Scholar](#)

---

39 Google Play Store. <http://play.google.com/store?hl=en>. Accessed March 2019.

[Google Scholar](#)

---

40 AppInChina. <http://www.appinchina.co/market/>. Accessed March 2019.

[Google Scholar](#)

---

41 Koodous. <http://koodous.com/>. Accessed March 2019.

[Google Scholar](#)

---

42 1Mobile Market. <http://m.1mobile.com/me.onemobile.android.html>. Accessed March 2019.

[Google Scholar](#)

---

43 9apps. <http://www.9apps.com/>. Accessed March 2019.



44 VirusTotal. <http://www.virustotal.com/>. Accessed March 2019.

[Google Scholar](#)

---

45 Ransomware. <http://ransom.mobi/>. Accessed March 2019.

[Google Scholar](#)

---

46 strace. <http://linux.die.net/man/1/strace>. Accessed March 2019.

[Google Scholar](#)

---

47 Ramos J. Using TF-IDF to determine word relevance in document queries. Paper presented at: 1st Instructional Conference on Machine Learning; 2003; Banff, Canada.

[Google Scholar](#)

---

48 Hu X. Knowledge Discovery in Databases: An Attribute-Oriented Rough Set Approach [dissertation]. Regina, Canada: University of Regina; 1995.

[Google Scholar](#)

---

49 Jensen R, Shen Q. Rough set based feature selection: A review. In: AE Hassanien, Z Suraj, D Slezak, P Lingras, eds. *Rough Computing: Theories, Technologies and Applications*. Hershey, PA: Information Science Reference; 2007: 70-107.

View | [Google Scholar](#)

---

50 Hall M, Frank E, Holmes G, Pfahringer B, Reutemann P, Witten IH. The WEKA data mining software: an update. *ACM SIGKDD Explor. Newsl.* 2009; **11**(1): 10-18.

View | [Google Scholar](#)

---

51 AV-Test. <http://goo.gl/Rg6NDN>. Accessed March 2019.

[Google Scholar](#)

---

52 WEKA. <http://www.cs.waikato.ac.nz/ml/weka/>. Accessed March 2019.

[Google Scholar](#)

---

53 Idrees F, Rajarajan M, Conti M, Chen TM, Rahulamathavan Y. Plndroid: a novel Android malware detection system using ensemble learning methods. *Comput Secur.* 2017; **68**: 36-46.

View | [Web of Science®](#) | [Google Scholar](#)

---

54 Bhandari S, Panihar R, Naval S, Laxmi V, Zemmari A, Gaur MS. SWORD: Semantic aWare andRoid malwaRe Detector. *J Inf Secur Appl.* 2018; **42**: 46-56.

View | [Web of Science®](#) | [Google Scholar](#)

---

55 Alam Mohammed S, Vuong Son T. Random forest classification for detecting Android malware. Paper presented at: 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing; 2013; Beijing, China.

[Google Scholar](#)

---

56 Bhatia T, Kaushal R. Malware detection in Android based on dynamic analysis. Paper presented at: 2017 International Conference on Cyber Security and Protection of Digital Services; 2017; London, United Kingdom.

[Google Scholar](#)

---

57 Goyal R, Spognardi A, Dragoni N, Argyriou M. Safedroid: A distributed malware detection service for Android. Paper presented at: 2016 IEEE 9th International Conference on Service-Oriented Computing and Applications (SOCA); 2016; Macau, China.

[Google Scholar](#)

---

58 Moonsamy V, Batten L. Zero permission Android applications-attacks and defenses. Paper presented at: 3rd International Conference on Applications and Techniques for Information Security; 2012; Melbourne, Australia.

[Google Scholar](#)

---

59 Narain S, Vo-Huu TD, Block K, Noubir G. Inferring user routes and locations using zero-permission mobile sensors. Paper presented at: 2016 IEEE Symposium on IEEE Security and Privacy; 2016; San Jose, CA.

[Google Scholar](#)

---

60 Google TCP Dump. <https://sites.google.com/site/christians310/tcpdump>. Accessed March 2019.



[Google Scholar](#)

61 Ruta D, Gabrys B. An overview of classifier fusion methods. *Comput Inf Syst.* 2000; 7(1): 1-10.

[Google Scholar](#)

62 Goodfellow I, Pouget-Abadie J, Mirza M, et al. Generative adversarial nets. Paper presented at: 27th International Conference on Neural Information Processing Systems; 2014; Montreal, Canada.

[Google Scholar](#)

63 Felt AP, Chin E, Hanna S, Song D, Wagner D. Android permissions demystified. Paper presented at: 18th ACM conference on Computer and Communications Security; 2011; Chicago, IL.

[Google Scholar](#)

64 Rastogi V, Chen Y, Jiang X. Droidchameleon: Evaluating Android anti-malware against transformation attacks. Paper presented at: 8th ACM SIGSAC Symposium on Information, Computer and Communications Security; 2013; Hangzhou, China.

[Google Scholar](#)

65 Rastogi V, Chen Y, Jiang X. Catch me if you can: evaluating android anti-malware against transformation attacks. *IEEE Trans Inf Forensics Secur.* 2014; 9(1): 99-108.

View | [Web of Science®](#) | [Google Scholar](#)

66 Dong S, Li M, Diao W, et al. Understanding Android obfuscation techniques: A large-scale investigation in the wild. Paper presented at: International Conference on Security and Privacy in Communication Systems; 2018; Singapore.

[Google Scholar](#)

67 Proguard. <http://developer.android.com/tools/help/proguard.html>. Accessed March 2019.

[Google Scholar](#)

68 Dasho. <http://www.preemptive.com/solutions/android-obfuscation/>. Accessed March 2019.

[Google Scholar](#)

69 Du P, Samat A, Waske B, Liu S, Li Z. Random forest and rotation forest for fully polarized SAR image classification using polarimetric and spatial features. *ISPRS J Photogramm Remote Sens.* 2015; 105: 38-53.

View | [Web of Science®](#) | [Google Scholar](#)

## Citing Literature

### Number of times cited according to CrossRef: 2

Ke Shao, Qiang Xiong, Zhiming Cai, FB2Droid: A Novel Malware Family-Based Bagging Algorithm for Android Malware Detection, Security and Communication Networks, 10.1155/2021/6642252, 2021, (1-13), (2021).

[View](#)

Xin Su, Lijun Xiao, Wenjia Li, Xuchong Liu, Kuan-Ching Li, Wei Liang, DroidPortrait: Android Malware Portrait Construction Based on Multidimensional Behavior Analysis, Applied Sciences, 10.3390/app10113978, 10, 11, (3978), (2020).

[View](#)

[Download PDF](#)

### ABOUT WILEY ONLINE LIBRARY

[Privacy Policy](#)  
[Terms of Use](#)  
[About Cookies](#)  
[Manage Cookies](#)  
[Accessibility](#)

[Wiley Research DE&I Statement and Publishing Policies](#)  
[Developing World Access](#)

### HELP & SUPPORT

Contact Us  
Training and Support  
DMCA & Reporting Piracy  
**OPPORTUNITIES**

Subscription Agents  
Advertisers & Corporate Partners

**CONNECT WITH WILEY**

The Wiley Network  
Wiley Press Room

Received August 17, 2019, accepted September 7, 2019, date of publication September 16, 2019,  
date of current version September 26, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2941491

# Artificial Muscle Intelligence System With Deep Learning for Post-Stroke Assistance and Rehabilitation

SUNIL JACOB<sup>1,2</sup>, VARUN G. MENON<sup>1,2,3</sup>, FADI AL-TURJMAN<sup>1,4</sup>, (Member, IEEE), VINOJ P. G.<sup>2,5</sup>,  
AND LEONARDO MOSTARDA<sup>1,6</sup>

<sup>1</sup>Center for Robotics, SCMS School of Engineering and Technology, Ernakulam 683576, India

<sup>2</sup>Department of Electronics and Communication Engineering, SCMS School of Engineering and Technology, Ernakulam 683576, India

<sup>3</sup>Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Ernakulam 683576, India

<sup>4</sup>Computer Engineering Department, Antalya Bilim University, 07190 Antalya, Turkey

<sup>5</sup>Department of Electronics and Communication Engineering, APJ Abdul Kalam Technological University, Thiruvananthapuram 695016, India

<sup>6</sup>Computer Science Division, University of Camerino, 62032 Camerino, Italy

Corresponding author: Varun G. Menon (varunmenon@scmsgroup.org)

This work was supported by The Institute of Electrical and Electronics Engineers (IEEE) EPICS, USA, under Grant 2016-12.

**ABSTRACT** Stroke is one of the prime reasons for paralysis throughout the world caused due to impaired nervous system and resulting in disability to move the affected body parts. Rehabilitation is the natural remedy for recovering from paralysis and enhancing the quality of life. Brain Computer Interface (BCI) controlled assistive technology is the new paradigm, providing assistance and rehabilitation for the paralysed. But, most of these devices are error prone and also hard to get continuous control because of the dynamic nature of the brain signals. Moreover, existing devices like exoskeletons brings additional burden on the patient and the caregivers and also results in mental fatigue and frustration. To solve these issues Artificial Muscle Intelligence with Deep Learning (AMIDL) system is proposed in this paper. AMIDL integrates user intentions with artificial muscle movements in an efficient way to improve the performance. Human thoughts captured using Electroencephalogram (EEG) sensors are transformed into body movements, by utilising microcontroller and Transcutaneous Electrical Nerve Stimulation (TENS) device. EEG signals are subjected to pre-processing, feature extraction and classification, before being passed on to the affected body part. The received EEG signal is correlated with the recorded artificial muscle movements. If the captured EEG signal falls below the desired level, the affected body part will be stimulated by the recorded artificial muscle movements. The system also provides a feature for communicating human intentions as alert message to caregivers, in case of emergency situations. This is achieved by offline training of specific gesture and online gesture recognition algorithm. The recognised gesture is transformed into speech, thus enabling the paralysed to express their feelings to the relatives or friends. Experiments were carried out with the aid of healthy and paralysed subjects. The AMIDL system helped to reduce mental fatigue, miss-operation, frustration and provided continuous control. The thrust of lifting the exoskeleton is also reduced by using light weight wireless electrodes. The proposed system will be a great communication aid for paralysed to express their thoughts and feelings with dear and near ones, thereby enhancing the quality of life.

**INDEX TERMS** Artificial muscle intelligence, assistivetechologies, BCI, EEG, exoskeleton, healthcare, intelligent solutions, deep learning system, paralyzed, stroke.

## I. INTRODUCTION

The recent survey by reeve foundation revealed the impact of paralysis on world population, affecting approximately 5.4 million people [1], [2]. The survey also identified stroke (33.7%) as the major cause for paralysis. Paralysis is the deficiency of brain to activate muscle function of any body

The associate editor coordinating the review of this manuscript and approving it for publication was Shadi Aljawarneh.

part. Paralyzed persons find it difficult to perform their routine activities without assistance. Rehabilitation is one of the natural ways of healing paralysis. Because of this there is increasing interest and involvement in the field of post stroke rehabilitation. Exoskeleton-assisted technologies have emerged as a reliable means for rehabilitation of the affected upper and lower limbs [3]. Exoskeleton movements were controlled using sensors like gyroscopes, accelerometers, and potentiometers. Recently the focus is on controlling

exoskeleton using Brain Computer Interface (BCI) [4]. Antelis *et al.* demonstrated upper limb movement of the paralyzed using EEG signals [5]. A closed loop is established between human thought and movement of paralyzed limb using non-invasive BCI [6]. Android feedback based BCI training is employed to enhance brain rhythms during motor imagery task. The realistic feedback is realized in training session using humanoid robot [7]. Humanoid robot is navigated in real-time indoor environment based on human intentions. The asynchronous BCI system was designed using two level classifiers [8]. Co-operation and co-ordination of dual robotic arm is demonstrated using EEG based system. SSVEP (Steady-State Visual Evoked Potentials) are utilized to improve the user concentration level [9]. Electromyography (EMG) sensors are also used to control exoskeleton movements, EMG returns the information regarding human muscular activity [10]. The motor adaptability of upper limb is predicted using resting state functional connectivity. The system could identify effectiveness of robotic upper limb rehabilitation in different patients [11]. However, the system does not investigate real time human behaviors and thoughts. The clinical trials to investigate the effectiveness of BCI training sessions on stroke patients with upper limb paralysis are carried out. The results of the trial indicate that BCI based assistive devices are effective for post stroke rehabilitation [12]. Human intentions measured through cortical potentials were used to control upper-limb exoskeleton movements. The BMI system eliminated the need for recalibration but resulted in large false positive rates [13]. Grasping feature is incorporated into the assistive device for amputees using non-invasive EEG control. The participants were able to grasp the objects, but resulted in low success rate without sufficient training [14]. Brain activity is modulated to control robotic arm with multiple degrees of freedom. The system demonstrated the effective control of robotic arm with few training sessions, but increased the latency periods during certain operations [15]. Hybrid BMI system based on sensorimotor cortical desynchronization (ERD) and electromyography (EMG) activity was designed to control upper limb movements. The integration of BMI, NMES and exoskeleton improved the system accuracy, but increased the system complexity [16]. The linear control of upper limb is demonstrated using motor imagery based BCI and Functional Electrical Stimulation (FES), support is provided to the arm using passive exoskeleton. The generated limb movement is evaluated to identify the precise positioning [17]. The self-induced EEG variations based on ERD/ERS is utilized for controlling upper limb movements. Distinguishable patterns are obtained for left and right-hand movements in both motor imagery and motor execution experiments [18]. Online robot control using motor imagery based BCI is designed with high classification accuracy. The mental imagination of hand movement is detected for controlling the robot movements [19]. An integrated platform consisting of BCI controlled exoskeleton, functional electric stimulation (FES) with proprioceptive feedback is developed. Goal directed

motor task is used for training and subjects could complete the task with minimum latency period [20].

In our previous works [21]–[23], we have demonstrated an alternative technology to exoskeletons using non-invasive brain signals. Also, exoskeletons with feedback mechanism has also been implemented by us [22]. The paralyzed body part is stimulated using Transcutaneous Electrical Nerve Stimulation (TENS) device and Microcontroller [24]. Because of the dynamic and uncertain nature of brain signals, most of the BCI systems result in miss-operation, mental fatigue and it is hard to produce continuous control. The proposed system is designed to address the above gaps in research.

AMIDL is designed to reduce miss-operation, user fatigue and to enhance user capabilities. In the proposed work, human intentions are monitored in real-time employing 16 channel EEG sensors. TENS machine is integrated with Muscle Inspired Algorithm (MIA) to produce movements on the upper limb. Subjects are relieved from the task of carrying exoskeleton structure. The system is designed to perform six different movements on the affected upper limb. The different hand postures used to trigger the rehabilitation process are Release, Grasp, Rollup, Roll down, Rollup Release and Rollup grab. In the offline phase, Artificial Muscle movements corresponding to each posture are recorded to create the database. The decoded EEG signals are transformed into muscle activation signals in real-time environment. The captured EEG signal is converted into frequency domain using Walsh Hadamard Transform (WHT) for feature extraction. The extracted features along with WHT coefficients are utilized for the classification of different limb movements. The activation signal is then correlated with the recorded muscle movements. The signal with superior characteristics is passed on to the upper limb electrodes for inducing motion. In case of ambiguity or inadequate EEG signal, the periodic activation of the affected body part will be taken care by the artificial muscle movements. If the activation is executed by brain signal, the produced gesture is recognized and passed on to the care giver as voice command. Thus, AMIDL transforms human thoughts into different movements on the unique upper limb structure. The EEG activated movements are utilized for communicating paralyzed person's emergency need to the caregivers.

The contributions of our research are,

- An Artificial Muscle Intelligence with Deep Learning (AMIDL) system without exoskeleton structure, in which movements of paralyzed body part is controlled based on user intentions.
- An adaptive mechanism based on recorded muscle movements is integrated with the system to enhance continuous control and facilitate rehabilitation.
- Designed flexible assembly, which can be customized according to the degree of disability.
- Communication aid is incorporated in the system using gesture recognition

- The subject concentration is improved by using multi-media feed back

The rest of the paper is organized into four sections in which section 2 describes different existing methods used in BCI controlled upper limb movements.

## II. RELATED WORKS

In this section, we discuss few existing devices controlled by Brain-Computer Interface designed specifically for paralyzed people. But the problem with most of them is that the users are unable to get continuous control over the device. The users are required to have high level of concentration to get sufficient control on the device, which results in mental fatigue and frustration. Additionally, there is no arrangement to take care of the miss-operations. The subjects are also burdened with the task of carrying the load of exoskeleton on the affected body parts. Our research focus on overcoming these major problems and provides an efficient and flexible solution, which can enhance the post stroke recovery process. Our system also provides a communication aid for the paralyzed to express their feelings.

The assistive rehabilitation devices and its EEG control techniques are systematically reviewed and the major gaps are identified [25]. Three-dimensional robotic assistance using motor imagery task for upper limb rehabilitation is demonstrated with multi-joint exoskeleton. Desynchronization of sensorimotor oscillations in the  $\beta$ -band is measured to control the different robotic hand movements [26]. Different upper limb exoskeletons like Track hold [27] and Armeospring [28] are employed to track upper limb movements. Both these devices have integrated passive robots with virtual reality environment to help patients carry out their daily routine activities. Control of assistive robots are improved by integrating electroencephalography (EEG) and electrooculography (EOG). This hybrid approach called as brain/neural-computer interaction (BNCI) is adopted to control grasping movements of a hand exoskeleton [29]. Multimodal signal approach is further used to enhance control system for external device connected to the upper limb. EEG and EMG signals are integrated to improve the classification accuracy and to reduce the false positive rate [30]. Upper limb robotic orthosis, FES, and wireless BCI are combined in an efficient way on account of EEG signals. EMOTIV EEG device is employed to measure EEG signal, which is used to control grasp/release of an object [31]. An integrated passive robotic system is developed for assisting the paralyzed. The system employs a robotic device which compensates gravitational effects to allow exercise, virtual engines to facilitate interaction and EEG to monitor brain activities. The three components are coordinated in real-time to enhance the rehabilitation process [32]. The effects of BCI therapy on post stroke rehabilitation is analyzed based on motor imagery tasks. The analysis is performed by measuring coherence of EEG in different regions of the brain and the best result for motor recovery is obtained for the activation of lesion hemisphere [33]. The online BCI coupled with hand exoskeleton

is employed to address the issues related to proprioceptive feedback on the regulation of cortical oscillations. The results show an enhancement in SMR desynchronization with proprioceptive feedback during flexing and extending fingers of the exoskeleton [34]. Multimodal architecture based on BCI, exoskeleton and an active vision system is proposed to enhance BCI control and rehabilitation process. The VR environment coupled with bio feedback help to reduce mental fatigue and improve user interactions [35]. Few studies have also been conducted in related areas recently [36]–[42] Al-Turjman *et al.* proposed another interesting system using optimal haptic communications [43]. Xu *et al.* [44] proposed a three-dimensional animation to guide upper limb movements using EEG signals. Feature extraction is carried out by Harmonic Wavelet Transform (HWT) and linear discriminant analysis (LDA) classifier was utilized to classify the patterns for controlling the upper limb movements. MR-compatible robotic glove operates pneumatically and doesn't cause any disturbance to functional Magnetic Resonance imaging (fMRI) images during rehabilitation process [45]. The resistance to mechanically actuated movements in exoskeleton robot is measured based on spasticity. The relevant guidelines for practical neuro-rehabilitation robot design based on degree of spasticity and resistance is established [46]. In most of the design it is hard to get continuous control on the exoskeleton due to the non-stationary nature of the EEG signal. Moreover, the subjects experience metal fatigue and frustration due to lack of superior control. None of the device in the literature focused on providing communication aid for the paralyzed. Our research focus on solving these issues in an efficient manner using AMIDL system proposed in this paper. Table 1 shows the comparisons between AMIDL and existing systems in the literature.

## III. MATHEMATICAL MODEL

This section presents and discusses the mathematical modelling of the proposed system. The system is designed to perform six different movements on the affected upper limb. The different hand postures used to trigger the rehabilitation process are Release, Grasp, Rollup, Roll down, Rollup Release and Rollup grab. In the offline phase, Artificial Muscle movements corresponding to each posture are recorded to create the database. The decoded EEG signals are transformed into muscle activation signals in real-time environment.

In Hand Posture Release operation, the voltage and current applied to electrodes are assumed as  $V_{H-P-R}$  &  $I_{H-P-R}$ . Similarly, the voltage and current applied to electrodes in the other postures are defined as,

$$\text{Hand Posture Release} \rightarrow V_{H-P-R} I_{H-P-R}$$

$$\text{Hand Posture Grasp} \rightarrow V_{H-P-G} I_{H-P-G}$$

$$\text{Hand Posture Roll up} \rightarrow V_{H-P-Ru} I_{H-P-Ru}$$

$$\text{Hand Posture Roll down} \rightarrow V_{H-P-Rd} I_{H-P-Rd}$$

$$\text{Hand Posture Role up Release} \rightarrow V_{H-P-R-R} I_{H-P-R-R}$$

$$\text{Hand Posture Roll up Grasp} \rightarrow V_{H-P-R-G} I_{H-P-R-G}$$

The voltage for Hand Posture Release,  $V_{H-P-R} \neq$  Hand Posture Grasp,  $V_{H-P-G}$ . If they are same the hand posture



**TABLE 1. AMIDL comparisons with existing system (Sorted by success rate).**

| METHOD REFERENCE NO., YEAR | NO. OF SUBJECTS           | TYPE OF CONTROL           | TYPE OF EEG SIGNAL                              | DEVICE ASSIGNED                 | TASK   | ACCURACY/SUCCESS RATE |
|----------------------------|---------------------------|---------------------------|---|---------------------------------|--|-----------------------|
| Ref [14], 2016             | 2 amputees                | EEG -based control        | Motor imagery Low frequency-time domain feature | Prosthetic hand                 | Grasping objects                               | 63.6%                 |
| Ref [15], 2016             | 13 healthy subjects       | EEG-based control         | ERD/ERS   | Arm exoskeleton                 | Reach and grasp tasks                          | 77.8%                 |
| Ref [12], 2017             | 64 stroke patients        | EEG-based control         | Motor imagery 5–30 Hz EEG signal                | Hand exoskeleton                | Hand open/closed                               | 79.4%                 |
| Ref [17], 2016             | 7 healthy subjects        | EEG-based control         | 7–30 Hz EEG signal                              | ArmeoSpring and FES             | left hand, right hand, and feet                | 79.6%                 |
| Ref [16], 2016             | 7 stroke patients         | EEG-based control         | ERD   | ArmeoSpring exoskeleton         | Wrist extensor/flexor                          | 80.7%                 |
| Ref [13], 2016             | 3 chronic stroke patients | EEG-based control         | MRCPs   | MAHI exoskeleton                | Elbow flexion/extension                        | 81.3%                 |
| Ref [11], 2018             | 19 healthy subjects       | EEG-based control         | 15–25 Hz EEG signals                            | Robotic Arm                     | Upper limb movement/reaching                   | 83.5%                 |
| Ref [18], 2016             | 4 healthy subjects        | EEG-based control         | ERD/ERS   | Custom upper limb exoskeleton   | Left/right hand and left hand versus both feet | 84.29%                |
| Proposed System, AMIDL     | 20 subjects               | EEG and EMG based control | Motor Imagery ERD/ERS with multimedia feed back | TENS device with EMG Electrodes | left or right hand movements                   | 87%                   |

will be stable. If  $V_{H-P-R} > V_{H-P-G}$ , then Hand Posture Release will be activated compared to Hand Posture Grasp.

The other parameters in the system is defined as follows. The diameter of EEG electrode is  $D_E$ . The scalp resistance is  $S_R$ . The conductivity of the EEG electrodes depends upon the multiplying factor is assumed as ‘T’.

When the multiplying factor ‘T’ is more, the conductivity will be more & vice versa. The multiplying factor depends on the positioning of EEG electrodes, the diameter of EEG electrodes and scalp resistance.

The  $V_{H-P-T}$  denotes the Hand Posture Threshold. The threshold varies depending on the different types of postures.

**A. THE POSTER ACTIVATION REGION**

The Hand Posture Current in the system is given by,

$$I_{H-P} = \frac{D_E}{S_R} \int_{V_{H-P-initial}}^{V_{H-P-final}} T(E_Q) dV_{initial-final} \quad (1)$$

For the condition from Hand Posture Grasp to Hand Posture Release with the Hand Posture Threshold acting as an intermediate, the Hand Posture Release current is given by,

$$I_{H-P-R} = \frac{D_E}{S_R} \int_{V_{H-P-G}}^{V_{H-P-R}} T(E_Q) dV_{R-G} \quad (2)$$

where  $E_Q$  is the net potential to EEG electrodes. Also, we have,

$$E_Q = V_{H-P-R} - V_{H-P-T} - V_{H-P-G} \quad (3)$$

If  $E_Q$  is positive then,  $V_{H-P-R}$  is dominating  $V_{H-P-T}$  &  $V_{H-P-G}$ . The required potential to EEG electrodes will be analyzed and the Hand Posture Release operations will be performed.

For  $V_{H-P-G} < V_{H-P-T} \leq V_{H-P-R}$ , neglecting the surrounding areas of EEG electrodes and conductive loss. The hand posture for release will be activated as,

$$I_{H-P-R} = V_{H-P}(V_{H-P-G}, V_{H-P-R}) \quad (4)$$

Similar relation can be developed for the remaining postures.

If the movement is a combination of different postures, say Roll up and Release, then,

Let say the initial posture is in grasp stage,

$$I_{H-P-R-R} = \frac{D_E T}{S_R} \left\{ \int_{V_{H-P-G}}^{V_{H-P-Ru}} (V_{H-P-Ru} - V_{H-P-T} - V_{H-P-G}) dV_{G-Ru} + \int_{V_{H-P-Ru}}^{V_{H-P-R}} (V_{H-P-R} - V_{H-P-T} - V_{H-P-Ru}) dV_{Ru-R} \right\} \quad (5)$$

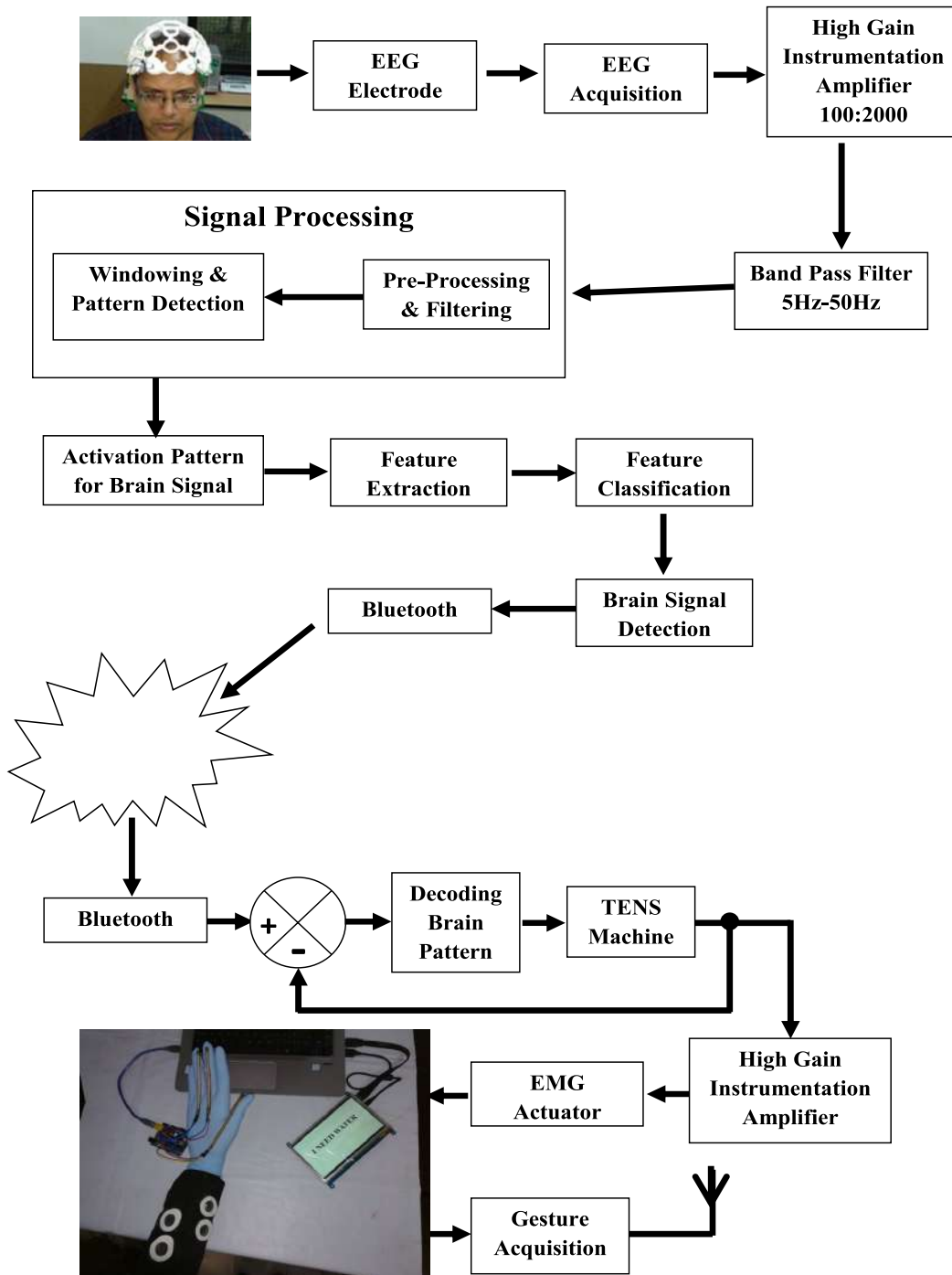


FIGURE 1. System architecture: AMIDL EEG acquisition and muscle stimulation modules.

Using the current value in the first integral and in the second integral we will have,

$$I_{H-P-R-R} = I_{H-P-G-Ru} (V_{H-P-G}, V_{H-P-G-Ru}) + I_{H-P-Ru-R} (V_{H-P-Ru}, V_{H-P-R}) \quad (6)$$

The mathematical model of the system can be summarized as  $I_{H-P}$ , as shown at bottom of the next page.

#### IV. SYSTEM ARCHITECTURE

The architecture of the proposed system is presented in figure 1.

##### A. AMIDL EEG ACQUISITION MODULE

The system architecture is designed using modular approach, it consists of three main modules. They are 1) EEG Acquisition Module, 2) Muscle Stimulation Module and

3) Gesture to Voice Conversion Module. Figure 1 indicates the two main modules of the system. The system captures brain signal using EEG sensor module, which has 14 electrodes to make measurement and two acts as reference. The acquired signal undergoes pre-processing, feature extraction and classification. The low amplitude EEG signal is amplified using high gain instrumentation amplifier with a gain of approximately 1000-2000 db. The signal is band limited by employing band pass filter having a pass band frequency of 5-50Hz. Windowing and pattern selection is utilized for getting finite response. Feature coefficients of the signal are extracted using Walsh Hadamard Transform (WHT). These extracted features are used to classify the thoughts into six different movements. The actual brain pattern is reconstructed using the transmitter Hadamard coefficients. The decoded brain pattern is given to the TENS device, which transforms the thought into muscular actions. The muscle inspired algorithm stored in the controller facilitates the process of conversion. In the offline phase, muscle movements correspond to the six different pre-defined hand postures are recorded to create the database. The hand postures are recorded using 7 Electromyography (EMG) sensors on the different hand muscles. Five EMG electrodes are placed on the finger muscles to record finger activity. Two electrodes are placed on either side of the elbow to identify roll movements. In the online phase, brain signal based on the human thought is acquired and transformed into muscle movement. This transformed muscle movement is then correlated with the recorded muscle movements. The signal with superior characteristics is selected by the controller for producing movements on the affected body part. If the brain signal fails to provide sufficient activation, periodic movements in the upper limb will be triggered by artificial muscle.

**B. AMIDL GESTURE TO VOICE CONVERSION MODULE**

If the brain signal with superior features activate the upper limb, the created gesture will be captured. Flex sensors placed on each finger is used for acquiring the gesture. The captured gesture will be recognized by the algorithm and transforms it into voice commands for the care givers. Figure 2 depicts the AMIDL gesture to voice conversion module. This module is used to give emergency alert messages to the caregivers or relatives.

The main hardware designed for the system has two parts 1) Acquisition module and 2) Muscle stimulation module. The brain signals of the user are acquired by using the EEG sensor. The non-invasive EEG sensor employed captures human intentions using 16 electrodes placed in the structure. 14 electrodes are used for capturing the signal and two electrodes act as reference. Figure 3 depicts the capturing of

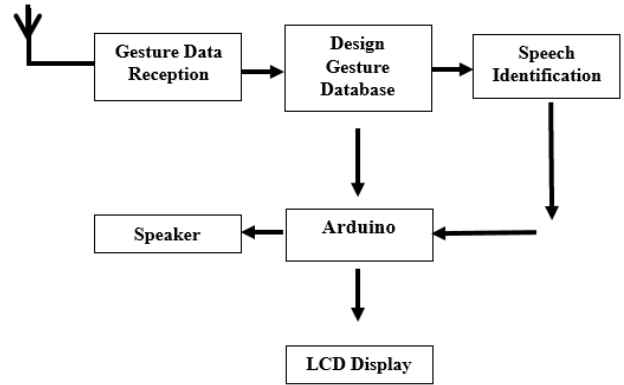


FIGURE 2. AMIDL gesture to voice conversion.



FIGURE 3. Signal acquisition using EEG sensor [21].

EEG signal using sensor from a human subject. The acquired signal is amplified using high gain instrumentation amplifier. The signal is band limited by employing band pass filter with pass band frequency in range of 5-50Hz

Signal undergoes further pre-processing and filtering to reduce the high frequency noise. Frequency domain conversion of the signal is done by using WHT transform and finite sample is selected using window technique. The design uses microcontroller in the acquisition and muscle stimulation module. The microcontrollers communicate with each other using Bluetooth technology. Bluetooth is selected because of short distance between modules and data rate required is less than 1mbps. EEG sensor and other electronic circuits are interfaced to the microcontroller to design the PCB. Figure 4 shows the electronic assembly used in our experimentation.

The muscle stimulation module receives the data using wireless module. The received data is converted into muscle movements or stimulation using muscle inspired algorithm stored in Arduino along with the TENS device interfaced to it. The output of the TENS is connected to the EMG electrode through EMG shield to activate the affected upper

$$I_{H-P} = \begin{cases} I_{H-P-R} (V_{H-P-G}, V_{H-P-R}) & \text{for } V_{H-P-G} < V_{H-P-T} \leq V_{H-P-R} \\ I_{H-P-G-Ru} (V_{H-P-G}, V_{H-P-Ru}) & \text{for } V_{H-P-G} < V_{H-P-T} \leq V_{H-P-Ru} \\ I_{H-P-Ru-R} (V_{H-P-Ru}, V_{H-P-R}) & \text{for } V_{H-P-Ru} < V_{H-P-T} \leq V_{H-P-R} \end{cases}$$

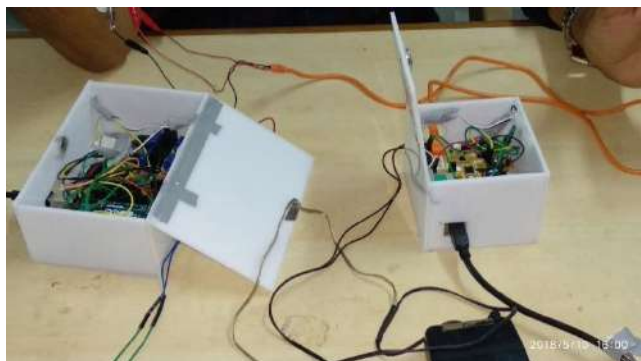


FIGURE 4. PCB designed for the experimentation.



FIGURE 5. Acquisition and stimulation process.

limb movements. The EMG shield helps to customize the stimuli produced by the TENS device. The entire assembly used for acquisition and stimulation is depicted in figure 5.

**V. RESULTS AND DISCUSSION**

Experimentation is carried out in two phases, offline training phase and online recognition phase. Experimentation and validation are done on 10 healthy and 10 paralyzed subjects. In offline phase EEG activity of the paralyzed and EMG activity of the healthy subjects were recorded. In the training phase, subjects were given the familiarization of six different intended actions like, Grasp, Release, Rollup, Rolldown, Rollup Release etc. Multimedia feedback is given to the subjects to enhance the brain patterns. The subjects are enlightened by using encourages messages and appreciation speeches in the feedback, rather than simple live streaming the actions. Rollup-grasp, Rolldown-Release movements of the upper limb are used for communicating the need to the caregivers. In the online phase, user thoughts are recognized and converted into muscular action. The generated muscular action is correlated with the EMG activity of the healthy subjects. Based on the correlation result microcontroller selects the superior signal, which is used for stimulating the affected body part.

**A. RESULTS COMPARISON OF EEG ACTIVATED AND POSTURE ACTUATED MOVEMENTS**

Figure 6 shows the correlation of brain actuated real time EMG and posture actuated EMG for the subject intention to

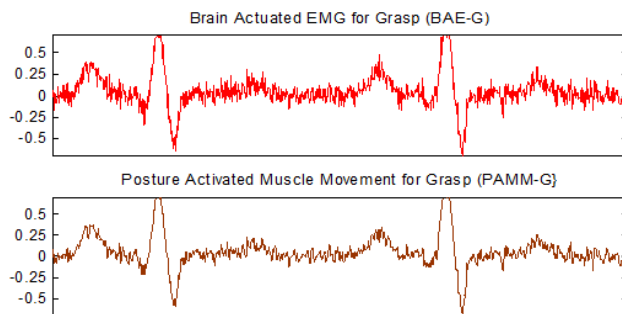


FIGURE 6. EMG activity for attempting grasp movements.

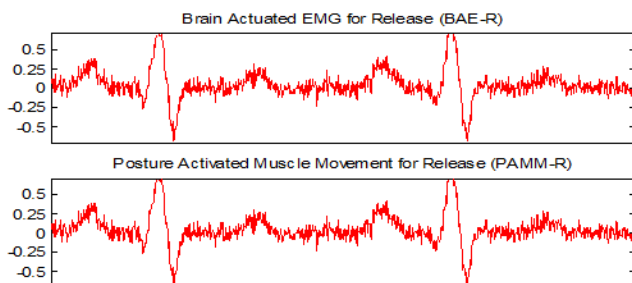


FIGURE 7. EMG variations corresponding to release movement.

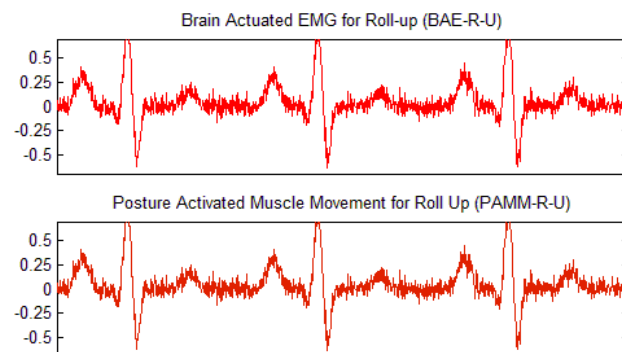


FIGURE 8. EMG activity based on ROLL up upper limb movement.

grasp the object. The EMG activity is recorded using EMG electrodes and measurement is done using Digital Storage Oscilloscope (DSO). The graph shows the amplitude variations of EMG signal with respect to frequency. The amplitude is normalized between  $\pm 0.5$ mv and frequency range used is 0-500Hz.

Figure 7 indicates the EMG variations observed in brain actuated and posture actuated movements corresponding to human intention of “Release”. Based on the correlation result brain actuated signal is selected for the stimulation of upper limb. Figure 8 shows the real time and recorded EMG activity for “Roll up” movement. Roll up movement is recorded using two electrodes placed on the either side of the Elbow. The rollup movement requires high intensity stimulation. In most of the time brain actuated EMG fallen below the desired level, so the stimulation of affected part is initiated in this case by artificial muscle movements. Figure 9 shows the EMG actuated by real time human Intention and the EMG activity produced using the training of “roll down” hand

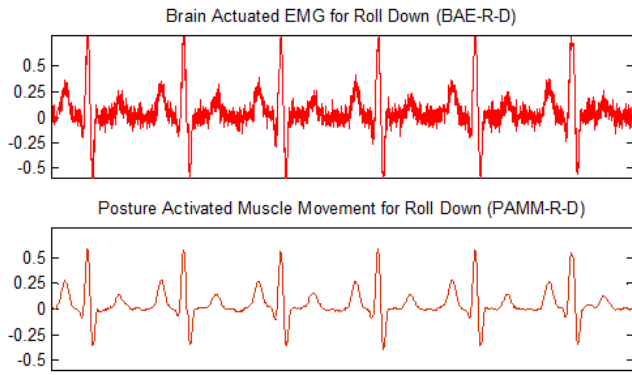


FIGURE 9. EMG activity based on ROLL down upper limb movement.

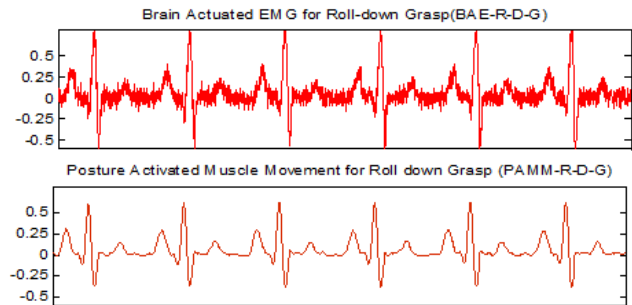
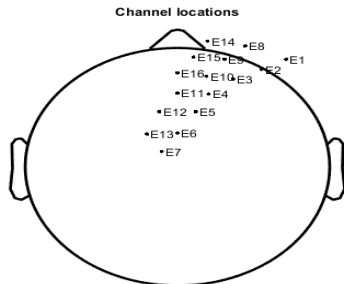


FIGURE 10. EMG activity for the gesture roll down-grasp.



16 of 16 electrode locations shown

FIGURE 11. Electrode placement on the brain [21].

Posture. Roll down ideally requires low intensity signals, so in this movement selection priority is given to signal with low signal strength in the correlation. Figure 10 shows the EMG data acquired for the gesture “Roll down-grasp”. This EMG activity is used for communicating the paralyzed subject’s need to the caregivers.

**B. RESULT OF EEG PATTERNS ON THE REALISTIC HEAD MODELS**

Realistic head models are used for the analysis of EEG signals. EEG sensors with 16 electrodes are used for the capturing the brain signals. The unique electrode placement scheme used in this experimentation is shown in figure 11. The placement scheme mainly concentrated on the frontal and parietal regions of the brain.

The variations of brain patterns with different frequencies are analyzed to facilitate the feature extraction and classification process.

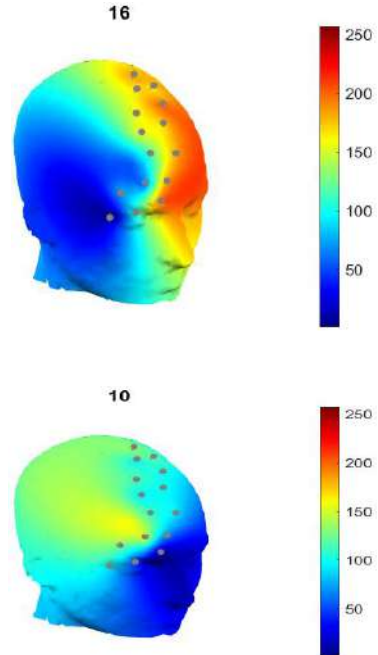


FIGURE 12. Brain pattern comparisons with and without multimedia feedback [21].

TABLE 2. Data statistics for brain actuated Rollup signal.

| STATISTICAL PARAMETERS | X COEFFICIENT VALUES | Y COEFFICIENT VALUES |
|------------------------|----------------------|----------------------|
| Min                    | 1                    | 0                    |
| Max                    | 64                   | 9                    |
| Mean                   | 32.5                 | 4.734                |
| Median                 | 32.5                 | 5                    |

In figure 12 red indicated the maximum interaction of neuron and blue indicates minimum interaction of neurons. The neuron connectivity in the head model on the left is improved when multimedia feedback is used, compared to the figure on right which does not use feedback.

**C. STATISTICAL ANALYSIS OF GENERATED EMG SIGNAL**

Statistical analysis is carried out to determine the correlation between Brain actuated EMG signal and posture actuated EMG signal. The data obtained during Rollup and Rolldown movement of the upper limb are utilized for the analysis.

Correlation matrix help to identify whether the human intentions match the recorded muscle movements. This matrix acts as a second level of classifier before the final actuation of the body part is made.

Correlation Matrix obtained  
[1.0000 0.0867 0.0867 1.0000]

Correlation matrix obtained  
[1.0000 -0.0640 -0.0640 1.0000]

Correlation matrix help to identify whether the human intentions match the recorded muscle movements.



**TABLE 3. Data statistics for posture actuated Rollup signal.**

| Statistical parameters | X coefficient values | Y coefficient values |
|------------------------|----------------------|----------------------|
| Min                    | 1                    | -9.392               |
| Max                    | 64                   | 8.982                |
| Mean                   | 32.5                 | -0.1296              |
| Median                 | 32.5                 | -0.09542             |
| Mode                   | 1                    | -9.392               |
| Standard deviation     | 18.52                | 5.665                |

**TABLE 4. Data statistics for brain actuated Rolldown signal.**

| Statistical parameters | X coefficient values | Y coefficient values |
|------------------------|----------------------|----------------------|
| Min                    | 1                    | 0                    |
| Max                    | 64                   | 9                    |
| Mean                   | 32.5                 | 4.719                |
| Median                 | 32.5                 | 4.5                  |
| Mode                   | 1                    | 0                    |
| Standard deviation     | 18.52                | 3.16                 |

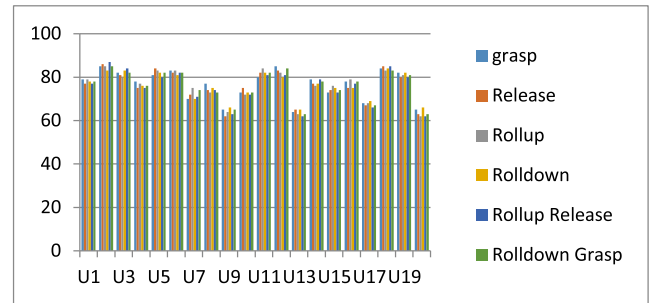
**TABLE 5. Data statistics for posture actuated Rollup signal.**

| Statistical parameters | X coefficient values | Y coefficient values |
|------------------------|----------------------|----------------------|
| Min                    | 1                    | -9.392               |
| Max                    | 64                   | 8.982                |
| Mean                   | 32.5                 | -0.1496              |
| Median                 | 32.5                 | -0.07542             |
| Mode                   | 1                    | -7.392               |
| Standard deviation     | 18.52                | 4.665                |

This matrix acts as a second level of classifier before the final actuation of the body part is made.

#### D. RESULTS OF CLASSIFICATION ACCURACY OF DIFFERENT SUBJECTS

The classification accuracy of the system is verified by performing the test on 10 healthy subjects and 10 paralyzed persons. Maximum obtained 88% efficiency and on an average 80.45% classification accuracy based on the six different human intentions for upper limb movements. The experimentation result shown in figure 13 is the summary of results on 20 participants. U1-U10 are represent healthy subjects, U11-U20 represents paralyzed persons. The reason for improved accuracy for classification among subjects is

**FIGURE 13. Classification accuracy of six different movements on 20 subjects.**

due to systematic training undertaken and usage of feedback. The healthy subject U2 is an experienced user and is more familiar with similar interfaces, obtained high accuracy. However, the unhealthy subjects U11 and U12 also obtained high accuracy through their dedication and passion. Visual feedback and voice encouragement are also given to paralyzed during training. The participants U9 and U13 has shown similar low classification accuracy due to their age and unfamiliarity with the system

The authors used EEG signal to identify the human Intentions and to control upper limb movements of the paralyzed person. Artificial muscle movements are integrated into the system to get continuous movement of the affected body part. Recorded muscle movements help to enhance the rehabilitation process. The burden of carrying exoskeleton is avoided by incorporating by using innovative assembly. The communication aid for the paralyzed is provided by implementing gesture recognition module. AMIDL obtained better classification accuracy compared to many existing methods mentioned in the literature. The two-level classification employed in the system help to reduce false operations. The future research should focus on reducing human workload by incorporating efficient controllers. Accuracy of mapping human intentions with muscle movements has to be increased. Machine learning algorithms that can effectively map human intentions to the desired muscle movements are the way forward.

#### VI. CONCLUSION

AMIDL system with 3 different modular units is designed and implemented. The system validation is carried out by performing online and offline testing on 10 healthy and 10 paralyzed subjects. AMIDL is designed to perform six different movements like Grasp, Release, Rollup, Rolldown, Rollup Release, Rolldown Grasp on the paralyzed upper limb. WHT transform is utilized for feature extraction and classification of EEG signals. The EMG activity of the healthy subjects are correlated with the real-time EMG signals generated by the paralyzed. Selection criteria for the ideal signal is finalized based on the EMG analysis carried out on all six hand postures. The two-level classification method improved the accuracy of the system. The system produced continuous response even in the presence of uncertain real-time inputs.

Results indicate that mental fatigue and miss-operations are reduced. The burden of carrying exoskeleton is minimized by an innovative assembly having array of sensors and control units. Periodic stimulation in the absence of ideal brain signal enhance the rehabilitation process. Gesture Recognition method is utilized for providing communication aid for the paralyzed. In our future work, we are trying to incorporate closed loop controller with haptic feedback. Deep learning algorithms will be used to effectively map EEG signals with recorded EMG signals. The user experience can be enhanced by measuring the user emotions while performing the different activities.

## ACKNOWLEDGMENT

Authors would like to thank Ms. Asha Jacob, SCMS Center for Robotics for providing assistance and guidance in testing and conducting the experiments.

## REFERENCES

- [1] Christopher and Dana Reeve Foundation. *Paralysis statistics*. Accessed: Aug. 5, 2018. [Online]. Available: <https://www.christopherreeve.org/living-with-paralysis/stats-about-paralysis>
- [2] C. Watson, G. Paxinos, and G. Kayalioglu, Eds., *The Spinal Cord: A Christopher and Dana Reeve Foundation Text and Atlas*. New York, NY, USA: Academic, 2009.
- [3] P. Langhorne, J. Bernhardt, and G. Kwakkel, "Stroke rehabilitation," *Lancet*, vol. 377, no. 9778, pp. 1693–1702, 2011.
- [4] C. Wang, X. Wu, Z. Wang, and Y. Ma, "Implementation of a brain-computer interface on a lower-limb exoskeleton," *IEEE Access*, vol. 6, pp. 38524–38534, 2018.
- [5] J. M. Antelis, L. Montesano, A. Ramos-Murguialday, N. Birbaumer, and J. Minguez, "Decoding upper limb movement attempt from EEG measurements of the contralesional motor cortex in chronic stroke patients," *IEEE Trans. Biomed. Eng.*, vol. 64, no. 1, pp. 99–111, Jan. 2017.
- [6] E. Buch, C. Weber, L. G. Cohen, C. Braun, M. A. Dimyan, T. Ard, J. Mellinger, A. Caria, S. Soekadar, A. Fourkas, and N. Birbaumer, "Think to move: A neuromagnetic brain-computer interface (BCI) system for chronic stroke," *Stroke*, vol. 39, no. 3, pp. 910–917, 2008.
- [7] C. I. Penalzoa, M. Alimardani, and S. Nishio, "Android feedback-based training modulates sensorimotor rhythms during motor imagery," *IEEE Trans. Neural Syst. Rehabil. Eng.*, vol. 26, no. 3, pp. 666–674, Mar. 2018.
- [8] Y. Chae, J. Jeong, and S. Jo, "Toward brain-actuated humanoid robots: Asynchronous direct control using an EEG-based BCI," *IEEE Trans. Robot.*, vol. 28, no. 5, pp. 1131–1144, Oct. 2012.
- [9] Z. Li, W. Yuan, S. Zhao, Z. Yu, Y. Kang, and C. L. P. Chen, "Brain-actuated control of dual-arm robot manipulation with relative motion," *IEEE Trans. Cogn. Devel. Syst.*, vol. 11, no. 1, pp. 51–62, Mar. 2019.
- [10] T. D. Lalitharatne, K. Teramoto, Y. Hayashi, K. Tamura, and K. Kiguchi, "EEG-based evaluation for perception-assist in upper-limb power-assist exoskeletons," in *Proc. World Automat. Congr. (WAC)*, Aug. 2014, pp. 307–312.
- [11] I. Faiman, S. Pizzamiglio, and D. L. Turner, "Resting-state functional connectivity predicts the ability to adapt arm reaching in a robot-mediated force field," *NeuroImage*, vol. 174, pp. 494–503, Jul. 2018.
- [12] A. A. Frolov, O. Mokienko, R. Lyukmanov, E. Biryukova, S. Kotov, L. Turbina, G. Nadareyshivily, and Y. Bushkova, "Post-stroke rehabilitation training with a motor-imagery-based brain-computer interface (BCI)-controlled hand exoskeleton: A randomized controlled multicenter trial," *Frontiers Neurosci.*, vol. 11, p. 400, Jul. 2017.
- [13] N. A. Bhagat, A. Venkatakrishnan, B. Abibullaev, E. J. Artz, N. Yozbatiran, A. A. Blank, J. French, C. Karmonik, R. G. Grossman, M. K. O'Malley, J. L. Contreras-Vidal, and G. E. Francisco, "Design and optimization of an EEG-based brain machine interface (BMI) to an upper-limb exoskeleton for stroke survivors," *Frontiers Neurosci.*, vol. 10, p. 122, Mar. 2016.
- [14] H. A. Agashe, A. Y. Paek, and J. L. Contreras-Vidal, "Multisession, noninvasive closed-loop neuroprosthetic control of grasping by upper limb amputees," in *Progress in Brain Research*, vol. 228, 2016, ch. 4, pp. 107–128. doi: [10.1016/bs.pbr.2016.04.016](https://doi.org/10.1016/bs.pbr.2016.04.016).
- [15] J. Meng, S. Zhang, A. Bekyo, J. Olsoe, B. Baxter, and B. He, "Noninvasive electroencephalogram based control of a robotic arm for reach and grasp tasks," *Sci. Rep.*, vol. 6, Dec. 2016, Art. no. 38565.
- [16] F. Grimm, A. Walter, M. Spüler, G. Naros, W. Rosenstiel, and A. Gharabaghi, "Hybrid neuroprosthesis for the upper limb: Combining brain-controlled neuromuscular stimulation with a multi-joint arm exoskeleton," *Frontiers Neurosci.*, vol. 10, p. 367, Aug. 2016.
- [17] C. Vidaurre, C. Klauer, T. Schauer, A. Ramos-Murguialday, and K.-R. Müller, "EEG-based BCI for the linear control of an upper-limb neuroprosthesis," *Med. Eng. Phys.*, vol. 38, no. 11, pp. 1195–1204, Nov. 2016.
- [18] Z. Tang, S. Sun, S. Zhang, Y. Chen, C. Li, and S. Chen, "A brain-machine interface based on ERD/ERS for an upper-limb exoskeleton control," *Sensors*, vol. 16, no. 12, p. 2050, 2016.
- [19] B. Xu, A. Song, G. Zhao, G. Xu, L. Pan, R. Yang, H. Li, and J. Cui, "Design and evaluation of a motor imagery electroencephalogram-controlled robot system," *Adv. Mech. Eng.*, vol. 7, no. 3, 2015, Art. no. 1687814015573607.
- [20] A. M. Elnady, X. Zhang, Z. G. Xiao, X. Yong, B. K. Randhawa, L. Boyd, and C. Menon, "A single-session preliminary evaluation of an affordable BCI-controlled arm exoskeleton and motor-proprioception platform," *Frontiers Hum. Neurosci.*, vol. 9, p. 168, Mar. 2015.
- [21] V. P. G. S. Jacob, V. G. Menon, S. Rajesh, and M. R. Khosravi, "Brain-controlled adaptive lower limb exoskeleton for rehabilitation of post-stroke paralyzed," *IEEE Access*, to be published.
- [22] S. Jacob, "A review of technology advances for assisting paralyzed people [leading edge]," *IEEE Technol. Soc. Mag.*, vol. 36, no. 2, pp. 36–37, Jun. 2017.
- [23] S. Rajesh, V. Paul, V. G. Menon, and M. R. Khosravi, "A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices," *Symmetry*, vol. 11, no. 2, p. 293, 2019.
- [24] P. G. Vinoj, S. Jacob, and V. G. Menon, "Hybrid brainactuated muscle interface for the physically disabled," *Basic Clin. Pharmacol. Toxicol.*, vol. 123, pp. 8–9, Sep. 2018.
- [25] M. Al-Quraishi, I. Elamvazuthi, S. Daud, S. Parasuraman, and A. Borboni, "EEG-based control for upper and lower limb exoskeletons and prostheses: A systematic review," *Sensors*, vol. 18, no. 10, p. 3342, Oct. 2018.
- [26] D. Brauchle, M. Vukelić, R. Bauer, and A. Gharabaghi, "Brain state-dependent robotic reaching movement with a multi-joint arm exoskeleton: Combining brain-machine interfacing and robotic rehabilitation," *Frontiers Hum. Neurosci.*, vol. 9, p. 564, Oct. 2015.
- [27] S. Comani, L. Velluto, L. Schinaia, G. Cerroni, A. Serio, S. Buzzelli, B. Guarnieri, and S. Sorbi, "Monitoring neuro-motor recovery from stroke with high-resolution EEG, robotics and virtual reality: A proof of concept," *IEEE Trans. Neural Syst. Rehabil. Eng.*, vol. 23, no. 6, pp. 1106–1116, Nov. 2015.
- [28] F. Grimm, A. Walter, M. Spüler, G. Naros, W. Rosenstiel, and A. Gharabaghi, "Hybrid neuroprosthesis for the upper limb: Combining brain-controlled neuromuscular stimulation with a multi-joint arm exoskeleton," *Frontiers Neurosci.*, vol. 10, p. 367, Aug. 2016.
- [29] S. R. Soekadar, M. Witkowski, N. Vitiello, and N. Birbaumer, "An EEG/EOG-based hybrid brain-neural computer interaction (BNCI) system to control an exoskeleton for the paralyzed hand," *Biomed. Eng./Biomedizinische Technik*, vol. 60, no. 3, pp. 199–205, 2015.
- [30] E. A. Kirchner, M. Tabie, and A. Seeland, "Multimodal movement prediction—Towards an individual assistance of patients," *PLoS ONE*, vol. 9, no. 1, 2014, Art. no. e85060.
- [31] R. Looned, J. Webb, Z. G. Xiao, and C. Menon, "Assisting drinking with an affordable BCI-controlled wearable robot and electrical stimulation: A preliminary investigation," *J. Neuroeng. Rehabil.*, vol. 11, no. 1, p. 51, 2014.
- [32] M. Steinisch, M. G. Tana, and S. Comani, "A post-stroke rehabilitation system integrating robotics, VR and high-resolution EEG imaging," *IEEE Trans. Neural Syst. Rehabil. Eng.*, vol. 21, no. 5, pp. 849–859, Sep. 2013.
- [33] S. W. Tung, C. Guan, K. K. Ang, K. S. Phua, C. Wang, L. Zhao, W. P. Teo, and E. Chew, "Motor imagery BCI for upper limb stroke rehabilitation: An evaluation of the EEG recordings using coherence analysis," in *Proc. 35th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, Jul. 2013, pp. 261–264.
- [34] A. Ramos-Murguialday, M. Schürholz, V. Caggiano, M. Wildgruber, A. Caria, E. M. Hammer, S. Halder, and N. Birbaumer, "Proprioceptive feedback and brain computer interface (BCI) based neuroprostheses," *PLoS ONE*, vol. 7, no. 10, 2012, Art. no. e47048.

- [35] A. Frisoli, C. Loconsole, D. Leonardi, F. Banno, C. Chisari, M. Bergamasco, and M. Barsotti, "A New Gaze-BCI-Driven Control of an Upper Limb Exoskeleton for Rehabilitation in Real-World Tasks," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 42, no. 6, pp. 1169–1179, Nov. 2012.
- [36] F. Al-Turjman, H. Zahmatkesh, and R. Shahroze, "An overview of security and privacy in smart cities' IoT communications," *Trans. Emerg. Telecommun. Technol.*, Jul. 2019, Art. no. e3677. doi: 10.1002/ett.3677.
- [37] S. Kutia, S. H. Chauhdary, C. Iwendu, L. Liu, W. Yong, and A. K. Bashir, "Socio-Technological factors affecting user's adoption of eHealth functionalities: A case study of China and Ukraine eHealth systems," *IEEE Access*, vol. 7, pp. 90777–90788, 2019.
- [38] F. Al-Turjman and I. Baali, "Machine learning for wearable IoT-based applications: A survey," *Trans. Emerg. Telecommun. Technol.*, May 2019, Art. no. e3635. doi: 10.1002/ett.3635.
- [39] V. Anavangot, V. G. Menon, and A. Nayyar, "Distributed big data analytics in the Internet of signals," in *Proc. Int. Conf. Syst. Modeling Advancement Res. Trends (SMART)*, Nov. 2018, pp. 73–77.
- [40] D. K. Jain, S. Jacob, V. Menon, and J. Alzubi, "An efficient and adaptable multimedia system for converting PAL to VGA in real-time video processing," *J. Real-Time Image Process.*, pp. 1–13, Jun. 2019. doi: 10.1007/s11554-019-00889-4.
- [41] F. Al-Turjman, H. Zahmatkesh, and L. Mostarda, "Quantifying uncertainty in Internet of medical things and big-data services using intelligence and deep learning," *IEEE Access*, vol. 7, pp. 115749–115759, 2019.
- [42] F. Al-Turjman, "Intelligence and security in big 5G-oriented IoT: An overview," *Future Gener. Comput. Syst.*, vol. 102, pp. 357–368, Jan. 2020.
- [43] L. Feng, A. Ali, M. Iqbal, A. K. Bashir, S. A. Hussain, and S. Pack, "Optimal haptic communications over nanonetworks for E-health systems," *IEEE Trans. Ind. Informat.*, vol. 15, no. 5, pp. 3016–3027, 2019.
- [44] B. Xu, S. Peng, A. Song, R. Yang, and L. Pan, "Robot-aided upper-limb rehabilitation based on motor imagery EEG," *Int. J. Adv. Robotic Syst.*, vol. 8, no. 4, p. 40, 2011.
- [45] H. K. Yap, N. Kamaludin, J. H. Lim, F. A. Nasrallah, J. C. H. Goh, and C.-H. Yeow, "A magnetic resonance compatible soft wearable robotic glove for hand rehabilitation and brain imaging," *IEEE Trans. Neural Syst. Rehabil. Eng.*, vol. 25, no. 6, pp. 782–793, Jun. 2017.
- [46] H. S. Nam, S. Koh, Y. J. Kim, J. Beom, W. H. Lee, S.-U. Lee, and S. Kim, "Biomechanical reactions of exoskeleton neurorehabilitation robots in spastic elbows and wrists," *IEEE Trans. Neural Syst. Rehabil. Eng.*, vol. 25, no. 11, pp. 2196–2203, Nov. 2017.



**SUNIL JACOB** is currently the Director with the Centre for Robotics, SCMS School of Engineering and Technology, and also a Professor with the Department of Electronics and Communication Engineering. He was a recipient of the AICTE ChathraVishvakarma Award, in electronics, in 2017, and the Young Gandhian Technological Innovation Appreciation Award, in 2018. His project Muscles to Machine Interface for Paralyzed has been funded by IEEE EPICS USA, and

other funded projects include bionic haptic arm, rejuvenating the cells of human body, de-addiction coil for drug addicts, smart keyboard for disabled person, low cost 3D printer, and wearable device for detection and prevention of heart failure.



**VARUN G. MENON** is currently an Associate Professor with the Department of Computer Science and Engineering, SCMS School of Engineering and Technology and the Head of International Partnerships with the SCMS Group of Educational Institutions, India. His current research interests include the Internet of Things, brain-computer interface, mobile ad-hoc networks, wireless communication, opportunistic routing, wireless sensor networks, fog computing and networking, and

underwater acoustic sensor networks. He is also Distinguished Speaker with the Association of Computing Machinery (ACM). He is currently serving as a Guest Editor of the *Journal of Supercomputing*. He is currently serving on the Review Boards of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE TRANSACTIONS ON COMMUNICATIONS, and the *IEEE Communications Magazine*.



**FADI AL-TURJMAN** (M'07) received the Ph.D. degree in computer science from Queen's University, Canada, in 2011. He is currently a Professor with Antalya Bilim University, Turkey. He is also a leading authority in smart/cognitive, wireless and mobile networks' architectures, protocols, deployments, and performance evaluation. His record spans more than 200 publications in journals, conferences, patents, books, and book chapters, in addition to numerous keynotes and plenary talks at flagship venues. He has authored or edited more than 12 published books about cognition, security, and wireless sensor networks' deployments in smart environments with Taylor & Francis and Springer (Top tier publishers in the area). He was a recipient of several recognitions and best papers' awards at top international conferences. He also received the prestigious Best Research Paper Award from Elsevier COMCOM Journal for the last three years, prior to 2018, in addition to the Top Researcher Award for 2018 at Antalya Bilim University, Turkey. He led a number of international symposia and workshops in flag-ship IEEE ComSoc conferences. He is serving as the Lead Guest Editor in several journals, including the *IET Wireless Sensor Systems*, Springer, EURASIP, *MDPI Sensors*, Wiley&Hindawi WCM, and the Elsevier COMCOM and *Internet of Things*.



**VINOJ P. G.** received the B.Tech. degree in electronics and communication from the Cochin University of Science and Technology, Cochin, India, in 2004, and the M.Tech. degree in embedded system from the National Institute of Electronics and Information Technology, Calicut, India, in 2008. He is currently pursuing the Ph.D. degree in electronics and communication engineering with APJ Abdul Kalam Technological University, Kerala, India. He was a Researcher with Robhatah Robotic Solution, Bangalore. He is currently an Assistant Professor with the Department of Electronics and Communication, SCMS School of Engineering and Technology and an Associate Member of the Center for Robotics.



**LEONARDO MOSTARDA** received the Ph.D. degree from the Computer Science Department, University of L'Aquila, in 2006. He cooperated with the European Space Agency (ESA) on the CUSPIS FP6 Project to design and implement novel security protocols and secure geo tags for works of art authentication. To this end, he was combining traditional security mechanisms and satellite data. In 2007, he was a Research Associate with the Distributed System and Policy Group, Computing Department, Imperial College London, where he was involved in the UBIVAL EPRC Project in cooperation with Cambridge, Oxford, Birmingham, and UCL for building a novel middleware to support the programming of body sensor networks. In 2010, he was a Senior Lecturer with the Distributed Systems and Networking Department, Middlesex University, where he founded the Senso LAB, an innovative research laboratory for building energy efficient wireless sensor networks. He is currently an Associate Professor and the Head of Computer Science Department, University of Camerino, Italy.

...

# Review of IS 1893-1(2002): Effect of Unreinforced Masonry Infill Walls on Seismic Response of Framed Structures



Gayathri Krishna Kumar and **M. G. Airin**

**Abstract** Earthquake, its occurrence and effects, its impact and structural response have been studied for many years in earthquake history and is well documented. The structural engineers have tried to examine the various method, with an aim to determine the complex dynamic effect of seismically induced forces in structures, for designing of earthquake resistant structures in a advanced and easy manner. From the study conducted it was found that more precise results are found from nonlinear static analysis method. An overview of the past researches conducted on the modelling of masonry infilled frame issues, it was found that macro model which consider the effect of masonry weak links is used for modelling the infill panels. Different factors governing the period of vibration was checked, and the result shows the effect of stiffness of the building is the most important factor influencing the period of vibration. Parametric study was conducted to determine the most influential factor that affects the period of vibration of a structure. From the observations it was clear that the effect of stiffness is the most important factor influencing the period of vibration. Therefore a curve with dimensionless height and lateral displacement were plotted using nonlinear static analysis obtained from SAP2000. From the above mentioned curve, the effective stiffness of the building under consideration is calculated, which route to find the period of vibration of the structure that is considered for the seismic analysis [1].

**Keywords** Dynamic · Infill · Vibration · Parametric

---

G. Krishna Kumar (✉)

Federal Institute of Science and Technology, Angamaly, India

e-mail: [gaya3krishnakumar92@gmail.com](mailto:gaya3krishnakumar92@gmail.com)

M. G. Airin

**SCMS School of Engineering and Technology, Karukutty, India**

e-mail: [airinmg@scmsgroup.org](mailto:airinmg@scmsgroup.org)

© Springer Nature Switzerland AG **2020**

K. Dasgupta et al. (eds.), *Proceedings of SECON'19*,

**Lecture Notes in Civil Engineering** 46,

[https://doi.org/10.1007/978-3-030-26365-2\\_60](https://doi.org/10.1007/978-3-030-26365-2_60)





Contents lists available at ScienceDirect

# Groundwater for Sustainable Development

journal homepage: <http://www.elsevier.com/locate/gsd>

Research paper

## Development of a novel groundwater iron removal system using adsorptive Fe(II) process

Nitha Abraham<sup>a</sup>, Jency James<sup>a</sup>, Tuhin Banerji<sup>b</sup>, Ratish Menon<sup>a,\*</sup><sup>a</sup> SCMS Water Institute, SCMS School of Engineering and Technology Campus, Karukutty, Ernakulam, India<sup>b</sup> National Environmental Engineering Research Institute, Mumbai Zonal Centre, 89/B, Dr. A.B. Road, Worli, Mumbai, 400018, India

## ARTICLE INFO

## Keywords:

Adsorptive process  
 Ferric hydroxide flocs  
 Groundwater treatment  
 Iron removal

## ABSTRACT

Potential of Ferric Hydroxide[Fe(OH)<sub>3</sub>] flocs to be used as a media for the adsorptive removal of Fe(II) in water was explored in detail. It was found that this removal mechanism created new adsorption sites as the adsorption process continued. Batch experiment studies were conducted to determine the effect of contact time, adsorbent dosage, pH and competitive ions on the removal mechanism. Contact time and adsorbent dosage emerged as the dominating factors in the adsorption process, and the adsorption occurred effectively in the pH range 6.5–7. The Fe(II) adsorption was slightly hindered by calcium and manganese ions present in the groundwater, while the effects of other competitive ions such as sulphate, chloride and fluoride on the adsorptive removal mechanism were less pronounced. The kinetic process of the Fe(II) adsorption on Fe(OH)<sub>3</sub> was indicated to be a pseudo second order reaction that relied on the assumption of chemisorption as the rate limiting step. Based on the kinetic study, a new batch mode adsorption unit was recommended for domestic and industrial applications.

### 1. Introduction

Groundwater is the major source of drinking water in most parts of the world. In India, 50% of urban water requirement and 85% of rural domestic water requirement are met by ground water use (World Bank, 2010). Groundwater is considered as the primary source of drinking water because of its convenient availability, naturally good quality and its relatively low capital cost. However, it is also vulnerable to all sorts of contaminations due to natural causes or various anthropogenic activities such as agricultural, domestic and industrial (Sharma, 2001). One of the major concerns regarding the contamination of groundwater is the precipitation and accumulation of heavy metals. Natural sources of heavy metals may include weathering and erosion of bed rocks and ore deposits (Chakraborti et al., 2010). Due to the rich availability of laterite soil, iron content in Indian states such as Kerala is high (DMG, 2016). When leaching occurs, the iron enters the aquifer affecting the water quality of the aquifer. As per the Central Groundwater Board status, about 13 districts of Kerala have iron content in the aquifers at a concentration exceeding the permissible limit of 1.0 mg/l (CPCB, 2007a, b). The presence of iron results in a reddish colour and undesirable odour (Kulkarni, 2016). Fe(II) is colourless in the dissolved form, but in contact with air it is converted into the insoluble Fe(III) form, precipitates of

which cause the reddish colour, metallic taste and unpleasant odour of the water. This impairs the organo-leptix properties of water and may promote the growth of certain types of chlorine-tolerant microorganisms (Vidovic et al., 2014). A dose of 1500 mg/l iron can damage blood tissues in children while among adults, it can cause digestive disorders, skin diseases and dental problems (Khurana and Sen, 2008). As per the drinking water standards in India, desirable limit of iron is 0.3 mg/l (IS 10500:2012). High levels of iron make large volumes of water unavailable for drinking, and water scarcity ensues.

In ground water, iron exists mainly as Fe(II) due to lack of oxygen (Redman et al., 2002; Buschmann et al., 2006; Palmer et al., 2006; Benner and Fendorf, 2010). The water solubility of Fe(II) make its removal from groundwater a key concern for most water supply companies who use groundwater as their source. Researchers have attempted to develop advanced technologies for the treatment of water, more effective and economic than the prevailing ones (Sheng et al., 2017; Sharma et al., 2005; Tekerlekopoulou et al., 2006, 2013). Though many technologies currently exist, they are either expensive to maintain or require high energy for their operation, thereby reducing their affordability for low income households (Chaturvedi and Dave, 2012). Adsorptive filtration has been considered a promising alternative to different conventional iron removal mechanisms (Sharma et al., 2001).

\* Corresponding author.

E-mail address: [ratishmenon@scmsgroup.org](mailto:ratishmenon@scmsgroup.org) (R. Menon).

<https://doi.org/10.1016/j.gsd.2019.100318>

Received 3 March 2019; Received in revised form 25 November 2019; Accepted 13 December 2019

Available online 19 December 2019

2352-801X/© 2020 Elsevier B.V. All rights reserved.