

A Secure Encryption through Gray Codes and BigIntegers for IoT Devices

Hirendra Singh Sengar, Dr. D.N.Goswami, Dr. Anshu Chaturvedi

Abstract—Cryptography is essential because it allows protection of data securely so that unauthorized person cannot have access to it which ensures the protection of corporate secrets. In this paper, Binary code conversions based cryptography technique has been developed which provides security through binary codes like gray codes. Furthermore, security has been enhanced by the utility of prime numbers and BigInteger values. The designed technique protects the alphanumeric data against various cryptanalytical attacks. Proposed work includes symmetric key technique. The benefit of using symmetric key algorithm is faster execution time as compare to asymmetric key algorithm. It also work on stream ciphers those are faster when compared to block ciphers. Performance and security analysis when compared to other schemes shows that the proposed scheme is more powerful, efficient and secure than other related schemes.

Index Terms— BigInteger, Cryptanalysis, Cryptanalytical attacks, Encryption, Gray codes, Prime numbers, Randomization

1 INTRODUCTION

The internet of things (IoT) is an ecosystem of connected physical devices and objects that are accessible through the internet. It is a giant network of connected digital machines, embedded devices, things and objects. IoT devices are constrained devices such as sensors and smart devices; these have limited memory capacity and limited battery power. The programs run on these devices must be very efficient and less time consuming so that devices may save battery power. While exploiting vulnerabilities in IoTs, brute force attack is very common and compromises the security of the device. Brute forcing is the act of guessing out every possible username and password combination until a successful one is found. Hence, it's important that IoTs are always secured by these attacks. Encryption process ensures the security and privacy of the data stored on IoT devices. Encryption guarantees data confidentiality, integrity and authenticity. Various encryption algorithms were proposed by researchers time to time but these have some limitations associated with them like they employed many time-consuming operations which make its speed down. The bit shifting operations, circular shift operations, XOR operations and many other operations were used in encryption and decryption process of existing proposals which makes both of these processes slower. At present time, IoT devices need cryptographic algorithms for security which provides more security and don't run out of battery power. Cryptanalysis is a way to measure the level of security in IoT environment. Cryptanalysis is the art of breaking cryptographic algorithms using analytical reasoning, pattern locating, guessing and statistical analysis [1]. There are many types of cryptanalytical attacks on alphanumeric data like brute force attack, chosen cipher text attack, known cipher text attack, chosen plain text attack, known plain text attack. A cipher text only attack is one

of the cryptanalytical attacks where attacker does not have any part of plain text message. He only has the set of cipher text messages. He might know the language used during encryption and analysis the frequency distribution of some characters. Based on these activities, he might able to guess the plain text message. In known plain text attack, attacker not only having the cipher text but also has plain text. He discovers the key after performing some analysis on cipher text, plaintext pairs. In chosen plain text attack, attacker chooses some pieces of plain text and compares it with cipher text to obtain the key while in chosen cipher text attack, attacker chooses some different cipher texts[2]. Various encryption schemes have been proposed by researchers. Recently developed, Saurabh Chandra's scheme [3] found vulnerable to these attacks during cryptanalysis process. For providing higher security, the encryption schemes must be free from these attacks. Data travelled among various devices in IoT environment which must be immune to these attacks. Cryptanalysis of our proposed work shows that our proposed scheme is free from these attacks and achieves various security goals.

In cryptographic algorithm, number of bits contained by the key defines its key size. Key size ensures the strength of the key. Key with the smaller sizes are found in existing schemes which is vulnerable to various known attacks but all primitives types are unable to store large key values. Big integers are the only way to store a large key sized value. Proposed work employed the power of BigInteger to enhance the security. As it is known that the RSA and elliptic curve asymmetric algorithms are based on prime numbers. These numbers have interesting properties that make them well suited to cryptography. A prime number is a number that has no factors other than one and itself. That means, to get a prime, two smaller whole numbers cannot be multiplied. Two large primes can be multiplied to get an even larger composite, but other people will have a hard time factoring that composite back into the original two primes. In digital electronics, the digital data can be represented, stored and transmitted as group of binary bits. This group is also called as binary codes. There are many types of binary codes weighted codes, non weighted codes, binary coded decimal, alphanumeric codes. BCD is a weighted code. It is known as 8421 code. It is used for representing decimal numbers. In

- Hirendra Singh Sengar is currently pursuing PhD degree program in Computer Science in Jiwaji University, India, PH-8839913112. E-mail: hirendra.sengar@gmail.com
- D. N. Goswami is currently working as professor in SOS in Computer Science and Application department in Jiwaji University, India, PH-9406586343. E-mail:goswamidn@yahoo.com
- Anshu Chaturvedi is currently working as associate professor in CSE & IT department in M.I.T.S college, India, PH-8839551661. E-mail: anshu_chaturvedi@yahoo.com

weighted codes, each successive digit from right to left represents weights equal to some specified value and to get the equivalent decimal number system we sum the products of these weights by the corresponding binary digit. Excess 3 is a non weighted code. For converting decimal number in excess 3 codes we add three to each decimal digit before converting it into equivalent binary. In gray codes as one advance from one number to next only one bit is changed. Not only change in one bit takes place every time decimal number is also incremented by one from 0 through 9 but even for the change from 9 to 0 also has only one bit in change. One code can be changed into another by conversion process. The power of prime numbers was used with gray codes & BigIntegers and an innovative idea implemented in proposed work to enhance the level of security. Our paper is organized as follows: section2 describes the related work done in the same field. Then in section3, security analysis of the existing work has been done. In section 4, our proposed work has been presented in simulated environment. Furthermore, in section 5, cryptanalysis and performance analysis of the proposed work has been done. Finally, in section 6 we provided conclusion of our research work.

2 BACKGROUND AND RELATED WORK

Sourabh Chandra et al. [3] proposed content based algorithm that performs some logical operations like binary addition and circular bit shifting on binary data. For generating the secured cipher text, they performed encryption process two times. Folding method was used for generating the secret key. Laiphrakpam et al. [4] cryptanalysed and proposed the improved version of the scheme developed by Mrinal et al. [5]. Ammar et al. [6] suryed the security of the main IoT frameworks, a total of 8 frameworks are considered. They clarified the proposed architecture. They highlighted on the security measures of each framework. Boruchinkin et al. [7] proposed a cryptographic device which provides a secure transmission of data. It alerts the user if the crypto headset at the opposite end of the link is not trusted. Muhammed J. et al. [8] developed the innovative function works on the random based operations. The explicit mapping knowledge which correlates the random number with key and plaintext were used in their proposed work. Ajay kushwaha et al. [9] developed the encryption algorithm working on the concept of selection of significant data from the whole message. They applied the blowfish algorithm as encryption algorithm to encrypt the subset of data. They reduced the encryption time overhead and enhanced the performance. Rizky riyaldhi [10] proposed some techniques to improve the performance of AES algorithm. Modifications have been done in S.Box.They also reduced the shifting operations for efficiency. Vania Beatrice Liwandouw et al. [11] studied and analyzed several cryptographic applications running on android platforms, to provide recommendations for users to select the best cryptographic application that can be used on IM. Andrey Starikovskiy [12] studied the performance evaluation of various encryption algorithms based on key size and analyzed that key generation, encoding and decoding time increases with the size of the key. Furthermore they proposed for the protection of text messages. Dalila Slimani et al. [13] proposed

a speech encryption technique based on permutation and substitution processes. Permutation of speech segments has been done by using chaotic baker map which maximizes the benefits of permutation in encryption process. Substitution has been done using masks for destroying the pitch information and filling the silent periods within speech conversation. The encryption system also uses Discrete Cosine Transform to remove the signal intelligibility. Dimas nataneal et al. [14] developed a technique for ensuring the privacy of text messages sent over android chat applications by implementing the ECC algorithm equipped end to end encryption. Their experimental results show that better performance of system in terms of received messages, average encryption time and decryption time. Sreenath thangarajan et al. [15] enhanced the power dissipation of the circuit is enhanced by trading off area and throughput. Said Hraoui et al. [16] proposed an improvement of the Hill cipher algorithm. They reduced the computational complexity by avoiding the inverse matrix search process at the time of decryption. Rawya Rizk [17] proposed an algorithm for higher security by combining the strength of ECC and AES algorithms with minimized key maintenance. Integrity, confidentiality and authentication are the primitive achieved by their proposed approach. Mina Mishra et al. [18] used non linear functions and deterministic random bit generator to develop encryption and decryption algorithms. The developed algorithm was given name based on PRNG. PRNG's state becomes the secret key. The developed encryption scheme undergoes various cryptanalysis test and attacks to ensure its security. Several random keys were selected to perform the analysis. Their proposed algorithm has strength against linear, differential and statistical attacks. Rajni Tiwari et al. [19] They proposed an algorithm that sends the block of cipher text into image format encrypted by RC4 mechanism. At receiving end, receiver applies the no of keys depending on the number of blocks to decrypt the cipher text message. Block division mechanism and number of keys enhanced the security of this approach. Sarita kumari [20] studied the cryptography and data compression techniques and described how the cryptography and data compression techniques are useful to provide the security of data while saving storage. A Vijayan et al. [21] proposed a new algorithm called AVB algorithm which is used to enhance the security of data. This algorithm converts the plain text into cipher text by performing mathematical calculations on the ASCII values of the characters of these texts. The cipher texts also converted into plain text back by performing the same method so the main focus in entire algorithm on ASCII values of characters (data). Their proposed algorithm is efficient in two ways it difficult for the intruders to predict the data as each character follows different form of encryption based on the key. Mohammed Elhoseny et al. [22] proposed method reduced the energy consumption and improved network lifetime by using elliptic curve cryptography. Their approach forms unique 176 bit keys by combining the generated binary strings with node ID, index of transmission round and distance to cluster head. They overcame many attacks like brute force attack, cluster head attack, HELLO flood attack. Md hussain ahmad et al. [23] developed a modified RSA approach where the speed of mutual authentication is enhanced with the help of modified

RSA algorithm and a strong key is used to provide better security.

3 SECURITY ANALYSIS OF EXISTING PROPOSALS

The strength of key decides the level of security. Encryption schemes with the small sized keys are generally vulnerable to different guessing attacks. In Sourabh Chandra et al. [4] method, random number has been given as input to folding method for generating the encryption key. Let any user give the random number 724. The key is calculated as below-

Round 1: $7+2+4=13$

Round 2: $1+3=4$

Encryption key: 4

After doing the cryptanalysis it is found that the value of generated key each time lies between 1 and 9 digits so the key can be easily guessed by attacker in only nine rounds which shows the existing proposal is vulnerable to brute force attack. Once the attacker has the decryption key, he is able to find the number of spaces between strings in cipher text message. Once he finds the spaces in the message, he can easily determine the lengths of all words of the same message. Sourabh Chandra et al. [4] performed two subtraction operations in the decryption process. In first subtraction operation they subtracted all ASCII values by the decryption key and later they subtracted newly ASCII values by the length of words. The whole decryption process with the character table [4] shown in the table 1. The above cryptanalysis shows that both the decryption key and length of all words have been determined by the attacker, thus he easily generates corresponding ASCII values of plain text after performing only two subtraction operations. The whole plain text message can be easily determined after converting the ASCII values to their corresponding character values.

3.1 Ciphertext only Attack (Brute Force Attack)

In this analysis the key 'k' consisting of 1 decimal number only, where this number can be represented in form of 4 binary bits. Hence, the length of the key is 4 bits and size of the key space is $2^4=16$ keys. If the time required for the determination of plaintext for one value of the key in the key space is taken as $1 \text{ ms} = 10^{-3} \text{ s}$, then the time required for obtaining the plaintext by considering all the possible keys in the key space is given as follows which is very short time to break the cipher.

$$(16 \times 10^{-3}) / (24 * 60 * 60) = 1.85185185 \text{ e-7 days}$$

3.2 Known Plaintext Attack

A known plain text attack always allows a brute force attack on a cipher- simply try all keys, decrypt the ciphertext and see if matches the plaintext. In existing proposal the cipher text is transferred in the same order as it was generated. Each letter in the ciphertext has the association with each other in the plaintext which makes this method vulnerable to known plaintext attack. We have taken a pair of plaintext for our cryptanalysis process as follows. After performing the ciphertext only attack on the ciphertext "Qnnuu" we got the plaintext "Hello" which matches to the plaintext given in the pair hence the method is vulnerable to known plain text

TABLE 1
STRING CHARACTER TABLE FOR DECRYPTION PROCESS

Fetched character	ASCII value	ASCII after subtraction with the decryption key [including spaces]	1 st decrypted string	Length of word	ASCII after subtraction with the word length [excluding spaces]	Deciphered text
Q	81	78	N		72	H
N	110	107	K		101	E
U	117	114	R		108	L
U	117	114	R		108	L
X	120	117	U	6	111	O
*	42	39	.		33	!
#	35	32			32	

attack.

(plaintext, ciphertext) = ("Hello", "Qnnuu")

4 PROPOSED SCHEME

4.1 Encryption Process

Encryption is a process that encodes a message so that only intended recipient can read it. An encryption algorithm is used for scrambling the information. Sender inputs the plain text and a prime no to the encryption algorithm. Encryption technique automatically generates encryption key value by using random number generator. The whole plain text is then stored into an array and converted to cipher text after performing some binary code conversions and also performing some arithmetic operations as multiplication of decimal values with key and prime number. The resultant values stored into BigIntegers and then sent to receiver side as cipher text value.

4.2 Decryption Process

Decryption is the process of converting unreadable cipher text to readable information. Receiver gets the cipher text as BigInteger values and further inputs the key and prime no to the decryption algorithm. Decryption process then converts the cipher text into plain text after performing some arithmetic operations like division of BigInteger values with key and prime no and doing some binary code conversions like decimal to binary, binary to gray code, binary to UNICODE. For papers accepted for publication, it is essential that the electronic version of the manuscript and artwork match the hardcopy exactly! The quality and accuracy of the content of the electronic material submitted is crucial since the content is not recreated, but rather converted into the final published version.

4.3 Pseudo Code for Algorithms

Algorithm1- Algorithm for encryption process

Input: plain text, prime no

Output: cipher text

BEGIN

Store plain text message in an array

Input the prime no

Perform key generation using randomization process

FOR each character value in an array

Calculate Unicode value of character

Perform Unicode to binary conversion

Perform binary to gray conversion

```

    Perform gray to decimal conversion
    Multiply decimal value with prime no
    Multiply resultant number with key
    Store number in BigIntegers
END FOR
Send Cipher text to receiver
END

```

Algorithm2- Algorithm for decryption process

Input: cipher text, prime no, key

Output: plain text

BEGIN

Store cipher text message in BigIntegers array

Input the prime no

FOR each char value in array

Divide the number by key

Divide the resultant number by prime no.

Perform decimal to binary conversion

Perform binary to Unicode conversion

Convert Unicode to equivalent character

Store char value in array of characters

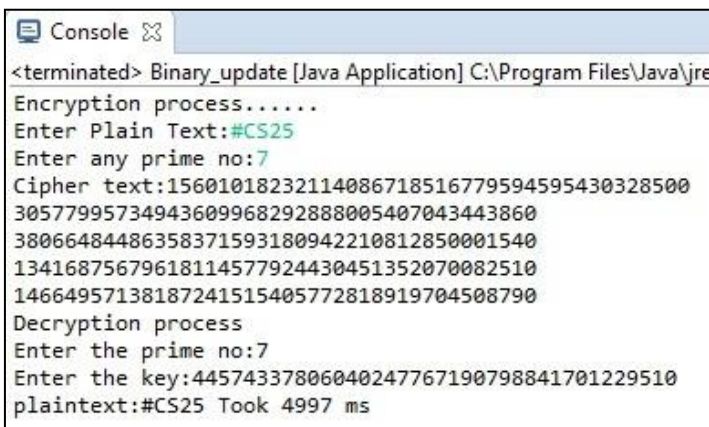
END FOR

Receive the plain text.

END

4.4 Results

The implementation of proposed work was done using Eclipse mars and JAVA 8 on Lenovo G570 with the system configuration of Intel core i3 processor and 2 GB RAM using 128 bit key length. Every run of application generates a different key. BigInteger was used for storing key value. The simulation of text encryption and decryption is shown in fig 1.



```

Console
<terminated> Binary_update [Java Application] C:\Program Files\Java\jre
Encryption process.....
Enter Plain Text:#CS25
Enter any prime no:7
Cipher text:15601018232114086718516779594595430328500
30577995734943609968292888005407043443860
38066484486358371593180942210812850001540
13416875679618114577924430451352070082510
14664957138187241515405772818919704508790
Decryption process
Enter the prime no:7
Enter the key:44574337806040247767190798841701229510
plaintext:#CS25 Took 4997 ms

```

Fig. 1 Output of encryption and decryption

5 PERFORMANCE ANALYSIS

In cryptography, randomness must be supplied in the plain text message to remove the structure of the plaintext message. Higher randomness decreases the correlation between messages. Entropy is a measure of how unpredictable, something is, so high entropy in keys increases security. In Sourabh Chandra's scheme, they used one digit as an encryption key so the calculated entropy of the encryption key in their technique is $\log_2(1)=0$ while in the proposed technique, key having 32 digits so the calculated entropy is $\log_2(32)=5$.

The entropy of the proposed technique is higher than the Sourabh Chandra's technique which makes proposed technique more powerful and secure than Sourabh Chandra's scheme. In Sourabh Chandra's scheme, circular shift operations and other time-consuming operations were used. These operations make encryption process slower. Fig 2, 3 shows the time taken by the encryption and decryption process over the file sizes. It is shown that the proposed algorithm takes less time to encrypt the text as well as to decrypt the text. Fig 4 shows total time which depicts how the proposed algorithm is more efficient than Sourabh Chandra's scheme.

5.1 Time Complexity and Cryptanalysis

The proposed technique provides two level of security. The attacker would not be able to decrypt the message until he has both the prime no and the key at the same time. Guessing the prime number does not ensures breaking of security because the length of the key is 128 bits and size of the key space is $2^{128}=3.40282367e38$ keys. If the one value of key takes the time as $1\text{ ms} = 10^{-3}\text{ s}$ in the key space to determine the plaintext. Then all the possible keys used to determine the plain text will take the following time

$$(3.40282367e38 \times 10^{-3}) / (24 \times 60 \times 60) = 3.40282367e30 \text{ days}$$

This proves that the technique is secured against brute force attack (guessing attack). In proposed technique, each time a new key is generated through randomization process so different-different cipher text generated every time for the same plaintext. Randomization decreases the correlation between plaintext and cipher text and increases the confusion which makes technique secure against various cryptanalytical attacks like known cipher text attack, known plain text attack, chosen cipher text, chosen plain text attack etc.

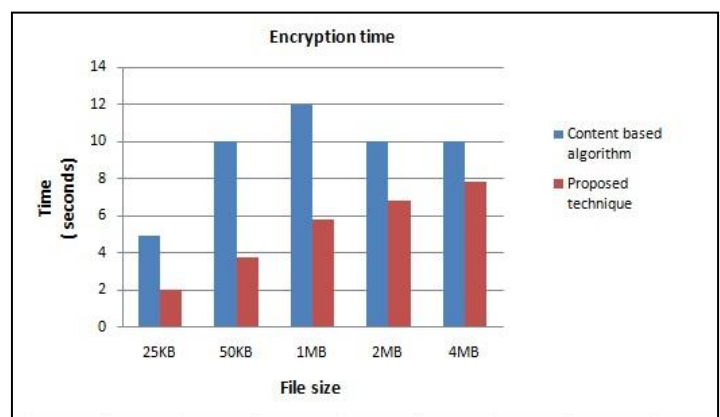


Fig.2 Encryption Time Vs File Size

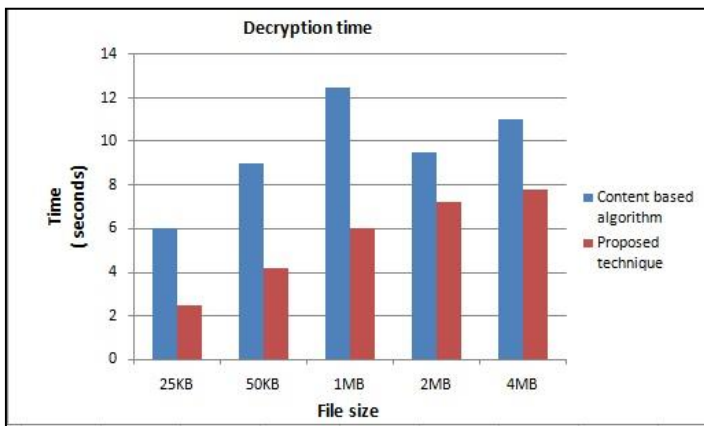


Fig.3 Decryption Time Vs File Size

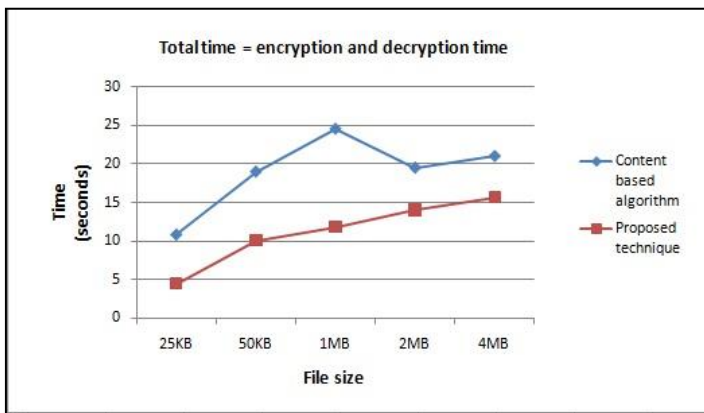


Fig.4 Total Time Vs File Size

6 CONCLUSIONS

After reviewing Sourabh Chandra's scheme and carrying out the security analysis, many attacks have been presented in different circumstances. The aim of our proposed work is to enhance the security through big integers with prime numbers and to provide immunity against attacks. Our proposed work also focused on digital code conversions and randomization process. Results shows that our proposed technique takes less time to encrypt and decrypt of alphanumeric data which makes it more efficient over Sourabh Chandra's scheme. Cryptanalysis process shows that our proposed technique is also robust against various cryptanalytical attacks. Our proposed technique is more secure and less time engrossing. Proposed technique used UNICODE standards so the message written in any language can also be encrypted by this. It is thus concluded that the proposed cryptosystem guarantees the confidentiality of messages and provide better performance.

7 REFERENCES

- [1] Patel, P., Patel, R. & Patel, N 2015, 'Integrated ECC and Blowfish for Smartphone Security', *Procedia Computer Science*, ELSEVIER, pp.210-216.
- [2] <https://www.expertsexchange.com/articles/12460/Cryptanalysis-and-Attacks.html>
- [3] Chandra, S., Mandal, B., Alam, Sk. & Bhattacharyya, S 2015, 'Content based double encryption algorithm using symmetric key cryptography', *Procedia Computer Science*, ELSEVIER, pp.1228-1234.
- [4] Laiphrakpam, D. & Khumanthem M 2016, 'Cryptanalysis of symmetric key image encryption using chaotic Rossler system', *Optik*, vol 7, issue 11, pp. 200-209.
- [5] Mandal K.M., Kar M., Singh K.S. & Varnwal K.V. 2014, 'Symmetric key image encryption using chaotic Rossler system', *Security and Communication Networks*, vol 7, pp. 2145-2152.
- [6] Ammar, M. & Rusello G 2018, 'Internet of Things: A survey on the security of IoT frameworks', *Journal of information security and applications*, ELSEVIER, pp. 8-27.
- [7] Boruchinkin, A., Tolstaya, A & Zhgilev A 2018, 'Cryptographic Wireless Communication Device', *Proc. 8th Annual International Conference on Biologically Inspired Cognitive Architectures (BICA)*, pp. 110-115.
- [8] J., M., Al-Muhammed & Zitar, R 2017, 'k-Lookback random-based text encryption technique', *Journal of King Saud University - Computer and Information Sciences*, vol 31, pp. 92-104.
- [9] Kushwaha, A., Sharma, H. & Ambhaikar, A 2016, 'A Novel Selective Encryption Method for Securing Text over Mobile Ad hoc Network', *Proc. 7th International Conference on Communication, Computing and Virtualization*, 2016, 79, pp. 16-23.
- [10] Riyaldhi, R., Rojali & Kurniawan, A 2017, 'Improvement of Advanced Encryption Standard Algorithm with Shift Row and S.BOX modification mapping in mix column', *Proc. International Conference on Computer Science and Computational Intelligence (ICCS)*, pp. 401-407.
- [11] Liwandouw, V. & Wowor, A 2017, 'The Existence Of Cryptography: A Study On Instant Messaging', *Proc. 4th Information Systems International Conference (ISICO)*, pp. 721-727.
- [12] Starikovskiy, A., Zhgilev, A. & Shevchenko, N 2018, 'Text Messages Protection System', *Proc. 8th Annual International Conference on Biologically Inspired Cognitive Architectures (BICA)*, 2018, pp. 457-466.
- [13] Sliming, D. & Melaka, F 2018, 'Encryption of speech signal with multiple secret keys', *Proc. International Conference Natural Language and Speech Processing (ICNLSP)*, pp. 79-88.
- [14] Nathanael, D., Faisal & Soriano, D 2018, 'Text Encryption in Android Chat Applications using elliptical Curve Cryptography (ECC)', *Proc. 3rd International Conference on Computer Science and Computational Intelligence*, pp. 283-291.
- [15] Thangarajan, S. & Bhaaskaran, V 2018, 'High Speed and Low Power Implementation of AES for Wireless Sensor Networks', *Proc. 8th International Conference on Advances in Computing and Communication (ICACC)*, pp. 736-743.
- [16] Hraoui, S., Gmira, F., Abbou, M., Oulidi A. & Jarjar A 2018, 'A New Cryptosystem of Color Image Using a Dynamic-Chaos Hill Cipher Algorithm', *Proc. Second*

- International Conference on Intelligent Computing in Data Sciences (ICDS), pp. 399-408.
- [17] Rizk. R. & Alkady, Y 2015, 'Two-phase hybrid cryptography algorithm for wireless sensor networks', Journal of Electrical Systems and Information Technology, vol 2, pp. 296-313.
- [18] Mishra M. & Mankar V 2015, 'Text encryption algorithms based on Pseudo Random Number Generator', International Journal of Computer Applications, vol 111, pp. 1-6.
- [19] Tiwari R. & Sinhal A 2016, 'Block Based text data partition with RC4 encryption for text data security', International Journal of Advanced Computer Research, vol 6, pp. 107-113.
- [20] Kumari S 2017, 'A research paper on cryptography encryption and compression techniques', International journal of engineering and computer science, vol 6, pp. 20915-20919.
- [21] Vijayan A., Gobinath T. & Saravanakarthykeyan M. 2016, 'International journal of engineering research and applications', ASCII value based encryption system (AVB), vol 6, pp. 08-11.
- [22] Elhoseny M., Yuan X., El Minir. H. & Riad A 2016, 'An energy efficient encryption method for secure dynamic WSN', Security and communication networks, vol 9, pp. 2024-2031
- [23] Ahmad M. & Tipathi M 2018, 'Development of encryption and decryption technique to secure the confidential data', International journal of advanced research in computer science, vol 9, pp. 60-63