Atlantis Highlights in Computer Sciences, volume 4
Proceedings of the 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021)

A Review on Challenges and Latest Trends on Cyber Security Using Text Cryptography

Anjali[1,*] Kshiteesh R Bharadwaj[1] Rohan Koundinya UH[1] Varun RK[1] A. Ajina[1]
Prathima G[1]

[1]*Information Science of Engineering, RV Institute of Technology and Management, Bengaluru, Karnataka, India*
[*]*Corresponding author. Email: anjali_is19.rvitm@rvei.edu.in*

ABSTRACT

In the IT sector, an important role is played by Cyber Security. Securing information has become one of the biggest challenges even today. The cybercrimes are growing enormously bit by bit and many measures are taken to prevent cyber-crimes. Despite these dealings, cybersecurity is still a tremendous apprehension to many. So, this paper emphasizes encounters met by cybersecurity and the modern cyber security performances using text cryptography. The secured way of transmission of data over the network from security attacks is using cryptography. This paper explores different cryptographic approaches to improve data security and performance evaluation metrics. The notable ones among them like Playfair, BCD encoded key management and Blowfish operate on discrete techniques of their own. Unlike the conventional encryption schemes which focus on improving algorithms for the text message, the BCD method aims at enriching the algorithm for key generation. The Blowfish functions on subkey generation and permutation for data encryption.

Keywords: *Blowfish Approach, Cyber Security, Performance Evaluation Metrics, Playfair technique, Text Cryptography, Vigenère meth.*

1. INTRODUCTION

Now, in the era of digitization, people are getting fond of the internet and hackers are getting quick-witted every day, thereby making it hard to secure privacy [1]. Every day news about phishing, vulnerability exploit, IoT-based attacks, etc. is heard [2-3]. The hackers reputedly target companies and then steal the details of clients (name, number, email, personal correspondence, etc.), which leads to massive financial and reputational losses for a business [4]. As the internet has grasped a position that meets this era, expanding exponentially over the past few periods, data security has developed a major apprehension for everyone linked to the network [5]. Data security guarantees that data is merely available to the proposed recipient and avoids any modification of the information [6-7]. To reach this position of security, several algorithms and approaches have been established. Cryptography scripts can be precise as encrypted data tactics, liable on certain algorithms that convert the data scribbled to the human eye unless expressed by algorithms and the sender [8-10]. Cryptography further branches out to Text encryption, Image encryption, Audio Encryption, and Video encryption. Text encryption forms the base for any cryptographic method. It mainly deals with the conversion of plain text into secure ciphertext [11-13]. This can be done with the help of a key. Key can be classified into two types, symmetric and asymmetric. The ciphers mentioned in this paper deal with the symmetric key where the same private key is to be shared with both sender and receiver [14] as shown in Fig. 1.

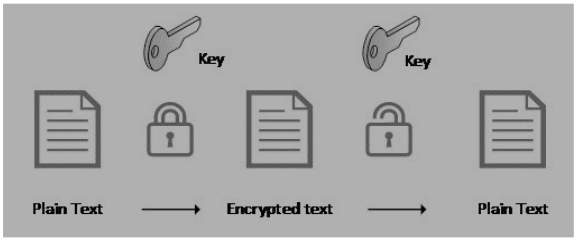

Figure 1 Text Cryptography

2. RELATED WORK

Data Security is one of the principal and continuing concerns and this paper aims to explore the perception of security in cryptography. Here important approaches like BCD, Blowfish, Vigenère, Playfair are discussed.

2.1 Technique - 1

Marzan and Sison [15] proposed an algorithm that handles plaintext containing alphabets, numbers, and special characters. This study heightened the Playfair cipher by key encryption and decryption process that will direct the key security difficulty without negotiating its runtime functioning. The runtime performance of this system outclassed the study of Amalia *et al.* in relation to encryption and decryption methods. Similarly, in this technique, the key security algorithm demonstrates a robust avalanche effect. Limitation in accommodation of character is the weakness of Playfair cipher. By eliminating the letter j from ciphertext it roots uncertainty and makes the ciphertext easy to break by the frequent occurrence of attacks. Thus, the Playfair cipher algorithm should be made into a 5x19 key matrix that can hold any type of 95 characters. By modifying the Playfair cipher into a 5x19 matrix, it can overcome its weakness and be strongly encrypted [16].

2.2 Technique - 2

Ranjan *et al.* [17] have presented a new algorithm according to the idea of poly alphabet cipher an improved version of the mono alphabet, uses BCD coded parity bits checker. The key sequence is generated with the help of the BCD converter and a 4-bit even parity checker which leads to the creation of a substitution technique model. It is observed that small key variations produce maximum avalanche effect which in turn boosts the strength and security of the algorithm.

2.3 Technique - 3

Vigenère cipher is an advanced method of encryption using a serial disclosure of a variety of Caesar ciphers created based on letters of a specific keyword making it much harder to crack. The different encryptions applied depends on the length of the keyword. This algorithm uses a table called the Vigenère table. The user inputs are plain text and the keyword, if the keyword is not equal to plain text, then it is repeated to match the length of plain text. There are some defects in this cipher which is hidden by using the Hill cipher. The defects of this cipher are that it is easy to detect the size of the key to start a statistical attack and two same letters are located at the same place at different blocks which makes the cipher weak. So, by combining these two algorithms an unfailing hybrid algorithm will be obtained, which will help in resisting the attacks including statistical attacks [18].

2.4 Technique - 4

Nie and Zhang [19], combined two widespread encryption algorithms, Blowfish and DES. DES algorithm was advanced by the IBM team [20]. Blowfish, the algorithm developed by Bruce Schneider remains uncracked till date. Being a symmetric encryption algorithm, it has a varying key size from 32 to 448 bits and uses block cipher. Through various analyses and tests, it has proved to be a fast encryption algorithm. In the Enhanced blowfish algorithm (ebf), by dropping the number of rounds and enlarging the block size, using a variable key span with further revolution and shifting method on selected rounds, the accomplishment of blowfish can be expanded. So, the outcome demonstrates that the swiftness of encryption and decryption get upgraded by 11.3653% and 9.8028% respectively [21]. The AES algorithm and Blowfish algorithm both utilize the same power but while generating ciphertext, blowfish displays quicker results [22].

3. TAXONOMY

The taxonomy is pictorially represented in Fig. 2.

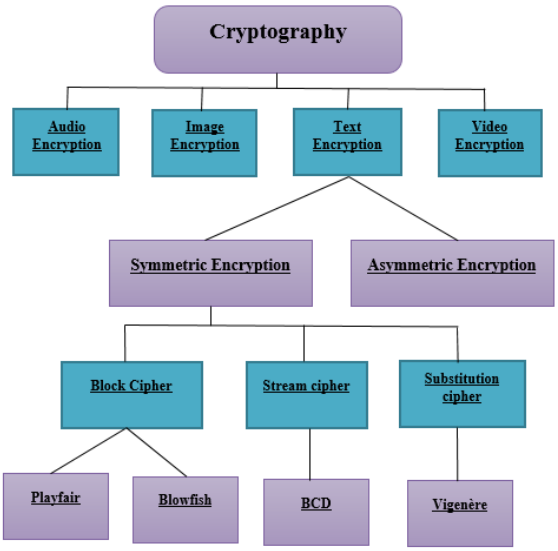

Figure 2 Taxonomy of Cryptography

4. SCHEMATIC ANALYSIS

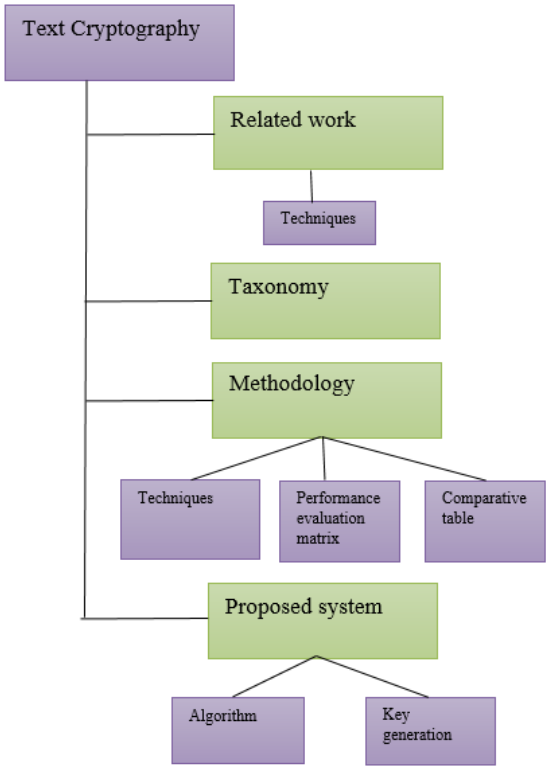

Figure 3 Schematic analysis

The schematic analysis is shown in fig.3.

Section 1 contains an outline of cryptography which plays a chief role in fighting the rising cybercrimes and also deals with types of encryptions. Section 2 contains a briefing over the chosen techniques for this survey which is followed by the taxonomy in the next section. Section 5 contains a thorough description of the ciphers picked for this survey starting from Playfair, it follows symmetric encryption which uses the block cipher matrix method. The next cipher has an algorithm for efficient key management using binary coded decimal and parity checkers. The Vigenère cipher which is a modification of the Caesar cipher uses a table for its encryption scheme. Finally, the Blowfish has the division of keys into smaller segments for secure encryption. In the same section, this paper also discusses the metrics used for performance evaluation which are needed in knowing the efficiency of each algorithm. The latter half comes to the comparative study of each of the techniques based on applications, features, advantages and all of them have proven to be efficient. In section 6 the proposed idea has been given which can be implemented in the future.

5. METHODOLOGY

The procedure of encryption and decryption is as shown in Figure 4.

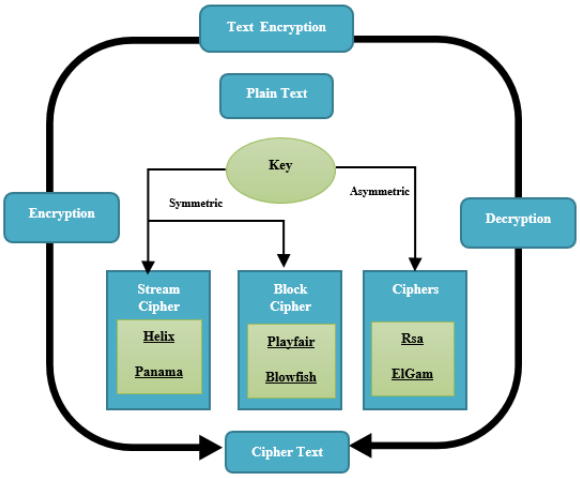

Figure 4 Process of encryption and decryption

5.1 Techniques

5.1.1. An Enhanced Key Security of Playfair Approach

It is a manual symmetric polyalphabetic encryption system that uses a block substitution cipher. Based on the symmetric approach, Playfair cipher uses only a particular key for encryption and decryption. This cipher has a great advantage over the monoalphabetic cipher. Because Playfair cipher uses matrix method (Fig. 5) in which letters are arranged in N X N form (N rows and N column), so the attacker gets confused and won't be able to break it.

Playfair cipher with 16x16 matrix

In this paper, the plain text contains alphabets, integers, and different characters.

i. The process of repetition of plaintext letterings in the identical duo includes replacing the initial letter by the letter to the right, with the initial component of the row circularly succeeding the last one and then the next letter to the left, with the last element of a row circularly following the initial.
ii. If an expression does not have an even number of letters, then add Z there to make it even. And by adding Z, it will not affect decryption.

Playfair Cipher Algorithm

Initially, the dispatcher will enter the plaintext (P1) collectively with its key (K1). Then the same key is used to encode the plaintext and arrange the key into a Playfair matrix of 16x16. The improved algorithm on K1 will be put on to construct Cypher Text (C1). To achieve this, convert ASCII letters into binary form, then the resultant will be renewed into a binary number.

Next is to get the two's complement of the binary number and Exclusive OR the outcome to the key size of the plaintext key. Follow the Bit Swapping method, the first position will be the last bit l, the second position will be the first- bit f, the third position will be the l-1, and then so on. The resultant of the bit swapping method will be changed into decimal and then that decimal number changed into their equivalent ASCII character. To decrypt the coded text C1, the enhanced key algorithm will be applied again. The decryption process will begin with the bit swapping method till the adaptation of the ASCII character is complete. Now at the recipient side, the recipient will decode the encoded key and use that key to retrieve the plaintext. So basically, the dispatcher and recipient will be knowing the key as it comes under symmetric encryption.

Figure 5 Letters arranged in N X N form

5.1.2. Efficient key management and ciphertext generation using BCD coded parity bits

This encryption algorithm uses a stream cipher and is constructed on the concept which is an upgraded version over a mono alphabet known as the poly alphabet cipher. This method is based on symmetric encryption and uses a key that can either be a numeral, a string, or a word. The generation of cipher keys of 256 characters is done with the aid of a BCD converter and a 4-bit even parity checker. Poly alphabet cipher is utilized for encryption and establishes a prototype for substitution technique. The steps for generating the key sequence are shown in Fig. 6.

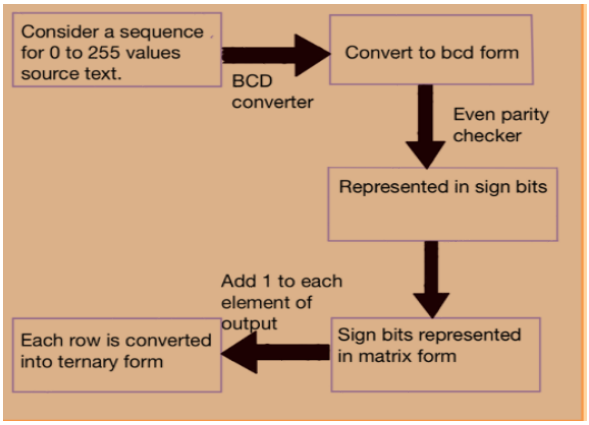

Figure 6 Steps for generating the key sequence

5.1.3 Vigenère Cipher Approach

Vigenère cipher was first used in 1585 in a book by Blaise de Vigenère and hence the name. In this method, this paper makes use of a table called Vigenère table or Vigenère square. This Vigenère square is a 26X26 matrix filled with all the alphabets ranging from A up to the letter Z in sequential order. Starting from the next successive rows each letter is transferred one position to its left in a cyclical manner. In this method two inputs are required from the user 1) a plain text and 2) a repetitive keyword, matching the overall size of the plaintext.

Illustration, Visvesvaraya Technological University be a plain text and RVITM be a keyword, then remove all the punctuations and spaces, changing all letters to capital letters, and distributing the output into a 5-letter set as shown below:

Visvesvaraya Technological University

Rvitmrvitmrv itmrvitmrvitm rvitmrvitm

5.1.4 Blowfish technique

The Blowfish algorithm is a 64-bit block cipher with a flexible key length that was pioneered by the foremost cryptologist Bruce Schneider. Being unbroken till date finds its enhancement in hardware applications owing to its compactness. The algorithm comprises two major parts of which the key expansion part leads to the creation of several sub-key arrays computing to 4168 bytes from a key of max 448 bits.

The data encryption part entails going through a round network of key reliant permutation, and a key and data reliant substitution for 16 rounds.

All functions on the Blowfish are XORs and adding up to 32-bit words.

5.2 Performance Evaluation Metrics

5.2.1. Run-Time Performance

The runtime performance of the intended key security algorithm will be achieved by acquiring the finishing time of the algorithm and is evaluated in milliseconds through a time complexity of O(n), with n as the number of computations.

5.2.2. Avalanche Effect

A minor shift in either the key or the plain text resulting in a substantial change in the cipher-text leads to the property termed the avalanche effect.

The avalanche effect taken into account as one of the worthiest properties is a word linked with a

particular behaviour of mathematical functions used for encryption.

This effect is typically satisfied when changing of bits in a text is harmonized with an avalanche effect including a probability of more than 50%.

Formula:

AE (%) = # of changed bits in ciphertext x 100 / total # of bits in ciphertext.

5.2.3. Brute-force attack

Brute force attacks remain straightforward and dependable as the computer is let to perform all possible permutations of usernames and passwords and don't stop until they uncover the right one. The best possible way in stopping a brute force attack is to break it as the process is carried on.

Formula:

Estimated time = (number of character set key length) / ((encryption/second) (EPS))

5.2.4. Execution Time Analysis

The key factor in estimating the working of all algorithms is the summation of time taken for both encryption and decryption processes and this is distinguished as execution time.

5.2.5. Throughput Analysis

Throughput acts as a key factor of power management as it possesses inverse proportionality to the expended power of the algorithm.

Throughput of a specific algorithm is computed by, division of complete data size in kilobytes and execution time in seconds as throughput is put across in terms of kilobytes per second.

5.2.6. Entropy

Randomness holds its position as a significant property by preventing the hacker from guessing the key. Entropy is the degree of randomness in the information which quantifies ambiguity in the information. The relationship between key and ciphertext grows complex as the degree of randomness is higher and is known as the confusion property [23].

5.2.7. An Optimal number of bits required for encoding

It is fundamental for the encrypted text to maintain its optimality which is achieved by reducing the number of characters. After encoding is done there is a transmission of ciphertext over a network which measures the bandwidth requirement. [24] For less consumption of storage and bandwidth, encoding is expected to be done with fewer bits.

5.3 Comparative table

Sl. No.	Techniques	Features	Advantages	Disadvantages	Applications
1.	**Playfair**	It is a manual symmetric polyalphabetic encryption system that uses a block substitution cipher. Based on the symmetric approach, the Playfair cipher has the same key for both processes.	It is a rigid cipher as the frequency analysis method used to disrupt simple substitution ciphers is tough.	The matrix format of this cipher always needs to neglect one letter as it can accommodate just 25 and cannot be reconstructed after decryption.	The British forces in the Second Boer war and world war I have seen a greater application of this cipher.
2.	**BCD Code**	It uses stream cipher and the concept of poly alphabet cipher. Ciphertext depends on the generation of key sequences.	BCD follows conversion to binary for arithmetic processing, hardware to work directly on BCD can be built. There exists no boundary to the extent of a number which can be followed by just adding a new 4-bit sequence.	BCD arithmetic in hardware takes a large portion of electronics thereby making it time-consuming. There is a wastage of space as it accommodated 16 bits whereas a single-digit just requires 4 bits.	Binary-Coded Decimal is used for doing arithmetic in decimal, usually to satisfy the requirements of human-written contracts that are expressed in decimal figures and subject to given rules of rounding that do not give the same results as rounding in binary.

3.	**Vigenère**	It uses a simple form of polyalphabetic substitution using multiple substitution alphabets.	The rotation of cipher through different shifts makes it invulnerable to frequency analysis and makes sure the same letter will not continually be encrypted to the same ciphertext letter.	The occurrence of the histogram can be seen in this cipher by which the key will be in repetition until its length matches the plain text.	Securing of digital images follows the application of the Vigenère cipher.
4.	**Blowfish**	The algorithm features key expansion of 448bits into several subkey arrays up to 4168 bits. Data encryption goes on for 16 rounds based on XOR operation.	Blowfish uses only XOR and addition on 32-bit words making it easy to implement in a short time. It uses memory up to or lesser than 4KB while running.	The initialization of s boxes and subkeys consumes a large space for memory.	Blowfish stipulates a 2pc protocol and superior data security for protected data transactions.

6. PROPOSED METHODS

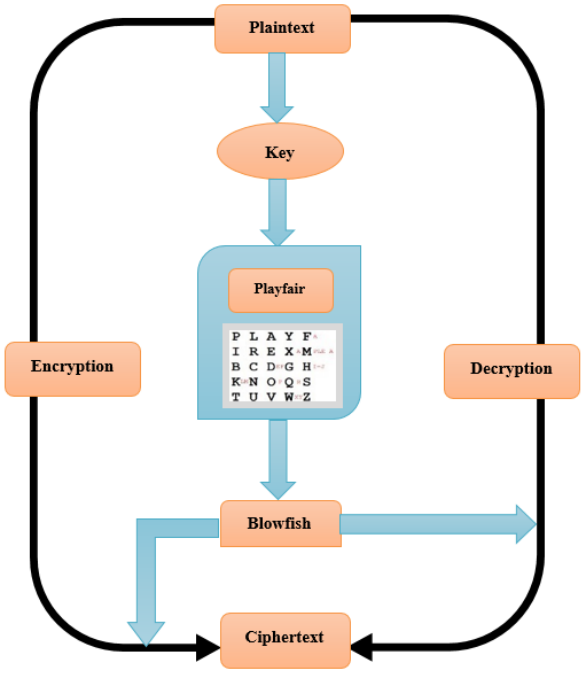

Figure 7 Proposed System Architecture

The proposed system architecture is as shown in Fig. 7. The key factors that led to this model are improvised with the BCD method and the complexity of the F function is replaced by the Playfair cipher making it harder to crack (Fig. 7). In this proposed method, a symmetric encryption algorithm using a block cipher and a modified Blowfish algorithm will be used [25-30]. Then the key sequence of 256 bits using a BCD code converter is generated and a 4-bit parity checker is used (Fig. 8).

6.1 Algorithm

This algorithm follows a unique passing accompanied by the XORed operation [31]. The initial step has a partition of 64-bit plain text into left and right parts of 32bits each [32]. There is a V-array whose first element gets XORed with the left part to create a value called 'Ro'. 'Ro' is next run past the Playfair cipher and XORed with the right part containing 32 bits to yield a new value called 'Li'. Now 'Li' switches the left part and 'Ro' switches the right part and the process is reiterated 15 more times with consecutive members of the V-array. The resulting 'Ro' and 'Li' are lastly XORed with the last two entries (17 and 18) in the V-array and recombined to generate the 64-bit cipher [33].

6.2 Key generation

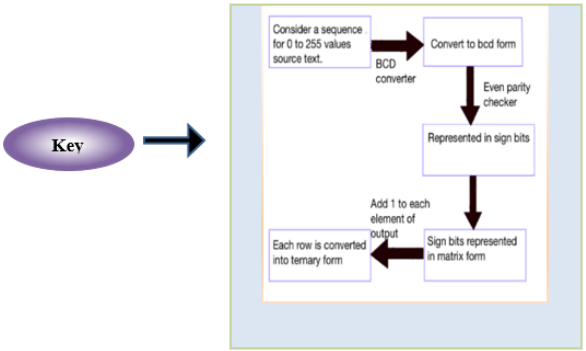

Figure 8 Key generation technique

Here the V-array consists of the key sequence divided into sub-arrays by the key expansion method [34]. The decryption will have the following processes in the reverse order and the plain text will be generated

back [35]. This technique has good chances of procuring a fine result as it will be the hybrid of other ciphers.

7. CONCLUSION

In the era of rising data breaches, distinct encryption algorithms have made it to the forefront, the most capable among them have been recorded in this paper which grants scope for the researchers to work on their advancement. Both stream and block cipher encryption techniques have been listed and elucidated in brief with different key sequences. Results of various parameters that comprise the Avalanche effect, Throughput analysis, and execution time have been considered as performance evaluation metrics. In the new proposed architecture, plan to build a strong model using the Blowfish as the base upon which minor modifications will be done with the help of the Playfair approach. And an efficient key is generated with the help of a BCD converter and an even parity checker which will provide better results.

REFERENCES

[1] Prabu, S., Balamurugan Velan, F. V. Jayasudha, P. Visu, and K. Janarthanan. "Mobile technologies for contact tracing and prevention of COVID-19 positive cases: a cross-sectional study." International Journal of Pervasive Computing and Communications (2020).

[2] Do, Dinh-Thuan, Tu Anh Le, Tu N. Nguyen, Xingwang Li, and Khaled M. Rabie. "Joint impacts of imperfect CSI and imperfect SIC in cognitive radio-assisted NOMA-V2X communications." IEEE Access 8 (2020): 128629-128645.

[3] Subramani, Prabu, K. Srinivas, R. Sujatha, and B. D. Parameshachari. "Prediction of muscular paralysis disease based on hybrid feature extraction with machine learning technique for COVID-19 and post-COVID-19 patients." Personal and Ubiquitous Computing (2021): 1-14.

[4] Z. Guo, L. Tang, T. Guo, K. Yu, M. Alazab, A. Shalaginov, “Deep Graph Neural Network-based Spammer Detection Under the Perspective of Heterogeneous Cyberspace”, Future Generation Computer Systems, https://doi.org/10.1016/j.future.2020.11.028.

[5] Bhuvaneswary, N., S. Prabu, S. Karthikeyan, R. Kathirvel, and T. Saraswathi. "Low Power Reversible Parallel and Serial Binary Adder/Subtractor." Further Advances in Internet of Things in Biomedical and Cyber Physical Systems (2021): 151.

[6] Naeem, Muhammad Ali, Tu N. Nguyen, Rashid Ali, Korhan Cengiz, Yahui Meng, and Tahir Khurshaid. "Hybrid Cache Management in IoT-based Named Data Networking." IEEE Internet of Things Journal (2021).

[7] Puttamadappa, C., and B. D. Parameshachari. "Demand side management of small scale loads in a smart grid using glow-worm swarm optimization technique." Microprocessors and Microsystems 71 (2019): 102886.

[8] L. Tan, H. Xiao, K. Yu, M. Aloqaily, Y. Jararweh, “A Blockchain-empowered Crowdsourcing System for 5G-enabled Smart Cities”, Computer Standards & Interfaces, https://doi.org/10.1016/j.csi.2021.103517

[9] Subramani, Prabu, Ganesh Babu Rajendran, Jewel Sengupta, Rocío Pérez de Prado, and Parameshachari Bidare Divakarachari. "A block bi-diagonalization-based pre-coding for indoor multiple-input-multiple-output-visible light communication system." Energies 13, no. 13 (2020): 3466.

[10] Hu, Liwen, Ngoc-Tu Nguyen, Wenjin Tao, Ming C. Leu, Xiaoqing Frank Liu, Md Rakib Shahriar, and SM Nahian Al Sunny. "Modeling of cloud-based digital twins for smart manufacturing with MT connect." Procedia manufacturing 26 (2018): 1193-1203.

[11] Monitoring for COVID-19 Patients by 5G-Enabled Wearable Medical Devices: A Deep Learning Approach”, Neural Computing and Applications, 2021, https://doi.org/10.1007/s00521-021-06219-9

[12] L. Tan, K. Yu, F. Ming, X. Cheng, G. Srivastava, “Secure and Resilient Artificial Intelligence of Things: a HoneyNet Approach for Threat Detection and Situational Awareness”, IEEE Consumer Electronics Magazine, 2021, doi: 10.1109/MCE.2021.3081874.

[13] L. Tan, N. Shi, K. Yu, M. Aloqaily, Y. Jararweh, “A Blockchain-Empowered Access Control Framework for Smart Devices in Green Internet of Things”, ACM Transactions on Internet Technology, vol. 21, no. 3, pp. 1-20, 2021,https://doi.org/10.1145/3433542.

[14] Z. Guo, A. K. Bashir, K. Yu, J. C. Lin, Y. Shen, “Graph Embedding-based Intelligent Industrial Decision for Complex Sewage Treatment Processes”, International Journal of Intelligent Systems，2021, doi: 10.1002/int.22540.

[15] Richard M. Marzan, Ariel M. Sison "An Enhanced Key Security of Playfair Cipher Algorithm", ICSCA, February 19-21, 2019.

[16] Sumarsono, Muhammad Anshari, Amiroh Mujahidah "Expending Technique Cryptography for Plaintext Messages by Modifying Playfair Cipher Algorithm with Matrix 5 x 19", International Conference on Electrical Engineering and Computer Science (ICECOS) 2019.

[17] Rahul Ranjana, Debabala Swainb, Bijay Paikaray, "Efficient key management and ciphertext generation using BCD coded parity bits", Elsevier, Procedia Computer Science, Vol.57, pp.703-709,2015.

[18] Hamza Touil, Nabil EL Akkad Khalid Satori "Text Encryption: Hybrid cryptographic method using Vigenère and Hill Ciphers", 2020 International Conference on Intelligent Systems and Computer Vision (ISCV).

[19] Tangyuan Nie, Teng Zhang, "A Study of DES and Blowfish Encryption Algorithm", TENCON, IEEE, Jan 2009

[20] Priyadarshini Patil, Prashant Narayankar, Narayan D G, Meena S Md, "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish", Elsevier, Procedia Computer Science, 2016

[21] Gurjeevan Singh, Ashwani Kumar, K. S. Sandha, "A Study of New Trends in Blowfish Algorithm", IJERA ISSN: 2248-9622 www.ijera.com Vol. 1, Issue 2, pp.321-326, March 2016

[22] Usha Kumari, T. Pavani, A.Sampath Dakshina Murthy, B. Lakshmi Prasanna, M. Pala Prasad Reddy. "Generating Cipher Text using BLOWFISH Algorithm for Secured Data Communications", IJITEE (International Journal of Innovative Technology and Exploring Engineering) December 2019.

[23] Nitya Khare and Dhari, S. Veena, "A survey on Playfair cipher encryption technique." Journal for Scientific Research & Development| Vol. 5, Issue 10, 2017.

[24] Aakash, Jitendra Kumar Soni, Bharti Sharma," A.J. CIPHER", 2017 2nd International Conference on Telecommunication and Networks (TEL-NET), Aug 2017.

[25] J. John Raybin Jose, E. George, Dharma, Prakash Raj, M. Rajapandian, "AIDEA – A Processing Capacity Based Cryptographic Approach", ICETECT 2011

[26] Happy Niti Noor Muchsin, Dina Evita Sari, De Rosal Ignatius Moses Setiadi "Text Encryption using Extended Bit Circular Shift Cipher", IEEE 2019

[27] Beth T. and Gollmann D. "Algorithm Engineering for Public Key Algorithms". IEEE Journal on Selected Areas in Communications; Vol. 7, No 4, PP. 458-466

[28] A Ramesh, A Suruliandi, "Performance Analysis of Encryption Algorithms for Information Security", 2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT-2013), pp 840-844.

[29] Godfrey L. Dulla, Bobby D Gerardo, Ruji P. Medina, "An enhanced BlowFish (eBf) Algorithm for securing x64 File message content", 2018 IEEE 10th International Conference on (HNICEM)

[30] Adam Hyder, Manoj Dhande, Kush Dharod, Mahesh Lohar, Keyur Makan "Text to Image Encryption Using 16*16 Playfair Cipher and Dynamic Color Channel Selection Technique", 2018 3rd International Conference for Convergence in Technology(I2CT)

[31] Saloni Goyal, Balie Shalomi Pancholi, B. Ashwath Rao, Shwetha Rai, N. Gopalakrishna Kini "Parallel Message Encryption Through Playfair Cipher Using CUDA" 2020 Evolution in Computational Intelligence pp 519-526 Advances in Intelligent Systems and Computing, vol 1176. Springer, Singapore

[32] Deepanshu Gautam, Chandan Agrawal, Parth Sharma, Munish Mehta, Poonam Saini, "An Enhanced Cipher Technique Using Vigenère and Modified Caesar Cipher"; 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI).

[33] Jamaluddin, Romindo, "Hybrid Cryptosystem Analysis by Using the Combination of Vigenere Cipher and RSA for Text Security", International Journal of Advanced Technology & Engineering Research (IJATER), Vol 3 Issue 1 pp141-147. 2013

[34] Apri Siswanto, Sri Wahyuni, and Yudhi Arta, "Combination Playfair Cipher Algorithm and LSB Steganography for Data Text Protection", In Proceedings of the Second International Conference on Science, Engineering and Technology ICoSET,125-129,2019, Riau, Indonesia

[35] Sheena Hussain, "Cyber Security in Cloud Using Blowfish Encryption", International Journal of Information Technology (IJIT) – Volume 6 Issue 5, Sep-Oct 2020