International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 8 Issue: 2
DOI: https://doi.org/10.17762/ijfrcsce.v8i2.2081
***Article Received**: 15 March 2022 **Revised**: 18 May 2022 **Accepted**: 25 May 2022 **Publication**: 30 June 2022*

A Fussy Based Neural Genetic Algorithm for Securing Data in Cyber Security

S.R. Rahman
Professor,
Computer Science and Engineering,
State University Mexico
ekkatya1975@mail.ru

Abstract :- Businesses are using cyber security technologies more and more to upgrade their operations. These businesses are prone to hazards and cyber security breaches because to the very specialized characteristics of such settings, including their sensitive exchange of cyber security data and the weak design of connected devices. Our main goal is to develop a cyber security system that can take into account all potential forms of assaults while staying within the allocated budget. To achieve this, a financial strategy based on portfolio management is utilized by enabling the selection of a portfolio of security controls that maximizes security level control while minimizing direct expenses. To solve this problem we proposed Fussy Based Neural Genetic Algorithm for authenticity, reliability and confidentiality of cyber security data and it decreases the danger of cyber security data integrity. Using a complex key, the plaintext is first transformed into a complex cipher text. The key is created using logical operators and is randomly chosen from the cyber security data. By applying principles of proposed algorithm, the cipher text acquired in the first step is rendered even more unreadable in the second phase. Feature Extraction of cyber security data is done by Principle Component Analysis (PCA).The data is encrypted by using Data Encryption Standard (DES). The data is decrypted using the proposed Fussy Based Neural Genetic Algorithm with Particle Swarm Optimization (FNGA-PSO).The suggested model's metrics are examined and compared to various traditional algorithms. This model solves the lack of difference in the authenticity of cyber security information, as well as it will give real and effective information to the organizational companies.

Keywords: *cyber security, Fussy Based Neural Genetic Algorithm, Principle Component Analysis, Data Encryption Standard, Particle Swarm Optimization****.***

I. INTRODUCTION

The tendency toward integrating Cyber-Physical Systems (CPS) into a fully integrated information society, rather than merely a digital Internet, is becoming more and more apparent with the advancement of information technology. Data is an asset of its owner in such an information society, and while that is not often the case, its use should be completely within that owner's control [1]. The built-in sensors within the devices from those large firms are secretly gathering a growing quantity of personal data, including location data, online browsing habits, user calls, and user preferences, which poses a significant danger of data owners' privacy being compromised. Additionally, the use of such data is beyond the control of its owners since there is presently no reliable means to track how the data is used and by whom, and there are few ways to find or penalise offenders who misuse those data [2, 3].

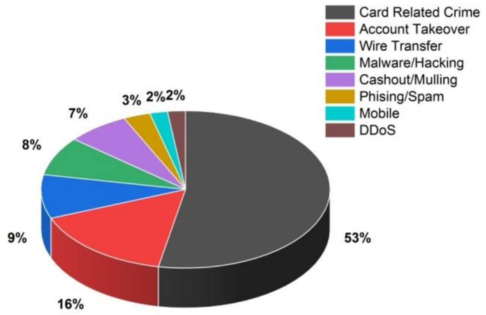

Figure 1: Analysis of cybercrime

Figure 1 depicts the analysis of cybercrime. Every internet user must take steps to protect their personal information against cybercrime, which has become a need for everyone who connects and uses the internet. The internet has become a necessity in almost every aspect of modern life. Security of data is especially critical for online banking, e-commerce, online money transactions, sensitive data transmission, web services, and a host of other activities. The contributions of the paper are follows: Normalization is used to prepare information for later processing, PCA turns raw data into

International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 8 Issue: 2
DOI: https://doi.org/10.17762/ijfrcsce.v8i2.2081
***Article Received**: 15 March 2022 **Revised**: 18 May 2022 **Accepted**: 25 May 2022 **Publication**: 30 June 2022*

numerical characteristics while maintaining original data, and DES converts plaintext data to ciphertext. FNGA-PSO decrypts and restores data. This article's sections: Section II provides a literature review. Shown in section III is proposed technique. Section IV contains the results and discussion. Section V includes the proposed work's conclusion.

II. LITERATURE REVIEW

In this section, we review several studies about securing data in cyber security. Study [4] discussed the relevance of cyber security in Indian enterprises. Surveys of Indian organisations' cyber security measures are done to evaluate approaches and difficulties. This thorough examination includes insights on safeguarding data using cyber security frameworks, risk assessment methods, and government public initiatives. With this knowledge, this article helps overcome cyber risks and assaults, developed a pre cautionary idea, and built a pre vision for lessening data theft among workers and monitoring hacker's actions before assaulting enterprises. Study [6] suggested SecNet, a new network architecture centred on safe data, uses AI and blockchain to tackle data misuse and allow AI to reliably handle data in an unsecure environment. Don't exchange data; store, share, and calculate. SecNet is a blockchain- and AI-based secure computing platform to assure data ownership, give a framework and incentives for data convergence, and strengthen AI for better networking [5]. For cloud and non-cloud systems, the authors have developed a Data Colouring approach for safeguarding data. Digital watermarking, Public Key Infrastructure (PKI), and concatenated fingerprints are used in the process. For example, data may be protected during its generation or while it is being stored. It can also be secured while processing . Study [7] suggest a blockchain-based strategy for CPS in healthcare. The presented method collects data from sensors and detects intrusion using a DBN model. Multiple share creation (MSC) ensures privacy and security using the given approach. Blockchain technology secures data flow to a cloud server that runs a ResNet-based classification algorithm to detect illness. Study [8] describe selective cybersecurity has been considered. The HEVC framework makes use of a strong hybrid approach based on selective encryption and watermarking to ensure secrecy and achieve copyright protection of the transmitted HEVC information. Study [9] presents a quantum-inspired authentication and encryption scheme (QIQW). The proposed protocol builds a blockchain for secure IoT data transfer. Quantum hash algorithms based on QIQW are used to join chain blocks. The described architecture helps IoT nodes communicate and regulate their data. Their protocol can guard against message and impersonation threats, providing secure IoT data transfer. Study [10] describe about database security plan in place for the current communication system in order to protect the data from any threats. Securing a database is not a simple task, and there is no one-size-fits-all methodology for doing so. The authors reviewed some of the particular system attacks and suggested various preventative ways to secure data on the database system. To avoid attacks on both individuals and organisations, they recommend implementing an effective security strategy. Study [11] suggested a project aimed at improving security by modifying key expansion and shiftrow transformation. The goal was to safeguard sensitive data. The experiment produced quicker image encryption and a better overall result than AES. Bandwidth efficiency was improved. This paper proposes a paradigm for safe cyber incident analysis using big data. Our matching method uses repository-based data.To overcome this issue we propose Fussy Based Neural Genetic Algorithm with Particle Swarm Optimization (FNGA-PSO).

III. METHODOLOGY USED

In this research, we investigate how a fussy-based neural genetic algorithm may secure data in cyber security. Figure 2 depicts the overall methodology used. The dataset is normalised and preprocessed. Principle Component Analysis extracts cybersecurity data (PCA). DES encrypts data. Fussy Neural Genetic Algorithm with Particle Swarm Optimization decrypts data (FNGA-PSO).

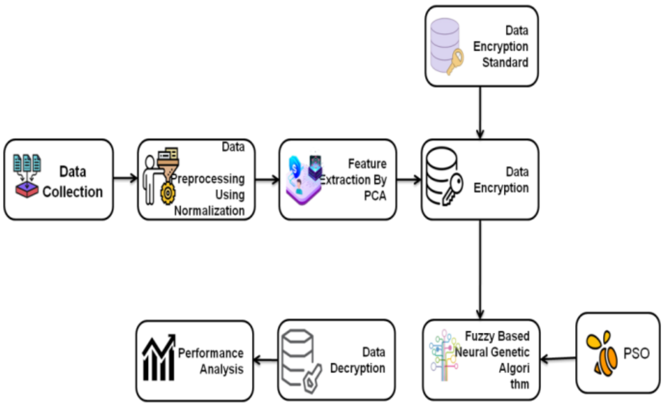
Data Encryption Standard
Data Collection
Data Preprocessing Using Normalization
Feature Extraction By PCA
Data Encryption
Performance Analysis
Data Decryption
Fuzzy Based Neural Genetic Algori thm
PSO

Figure 2: Overall methodology used

A. Data collection

We gathered Sherlock data for this study. Every table has uu id, user id, and version. Unix millisecond timestamp of record collection. The record's volunteer's user id is distinct.

Versions are the agent software release code. Table1 lists Sherlock's 7 data tables.

Table 1: Sherlock dataset [12]

PUSH	**Data**	**No. of. records**
	SMS Log	245,694
	App Packages	108,613
	Screen Status	2,608,765
	Call Log	443,176
	User Presence	685,911
	Moriarty	650,624
	Broadcast Intents	95,471,167

B. Data preprocessing using Normalization

Preprocessing converts raw data into a usable format. Normalization scales or alters data to ensure each characteristic contributes evenly to the total. Normalization creates a new range from an existing one. Several approaches to normalise data within a specific range have been created based on statistical measures from raw (unnormalized) data. Min-Max normalised our data. These strategies are categorised by how they normalise raw data statistical features. Min-Max normalisation uses a linear data at the range's start. This technique preserves data relationships. Pre-defined borders help fit information accurately. In accordance with this approach to normalisation,

$$P' = \left(\frac{P - minvalue\ of\ P}{maxvalue\ of\ P - minvalue\ of\ P}\right) * (S - J) + J \qquad (1)$$

Min-Max data is included in P', and one of the boundaries is [J, S].

The range of the real data is denoted by P, while the mapped one data is denoted by P.

C. Feature extraction using PCA

From the perspective of reducing the number of dimensions, principal component analysis (PCA) can be understood as a collection of orthogonal linear transformations of the original variables, with the goal of the dynamic process being to keep as much of the information contained in the original factors as is practically possible. Let N be an n × u data matrix, where n and u represent the number of factors and observations, accordingly. Assume the entire Y column means are zero for the sake of presenting convenience. $V_1 = \sum_z^u = \alpha 1z\ N_z$, where $\alpha_1 = (\alpha_{11},...,\alpha_1{}^q)$ Q, is the definition of the first principal component. Q is selected to maximize V_1's variance, i.e.

$$\propto_1 = arg \max_{\propto} \propto^Q \widehat{\Sigma} \propto$$
$$subject\ to\ \|\propto_1\| = 1 \qquad (2)$$

with $\Sigma = (N^Q\ N\ )/n$ Sequential definitions for the remaining primary components are as follows:

$$\propto_{h+1} = arg \max_{\propto} \propto^Q \widehat{\Sigma} \propto \qquad (3)$$

depending on

$$\| \propto \| = 1\ \ and\ \ \propto \hat{}Q\ \ \propto \_i = 0, \forall 1 \leq i \leq h \qquad (4)$$

According to this definition, the first g eigenvectors are the first g loading vectors. The singular value decomposition (SVD) of N is connected to PCA by its Eigen decomposition formulation. Assume N denotes SVD.

$$N\ =\ AEL^P \qquad (5)$$

where V and L are orthonormal matrices of n × u and u × u rows and columns, respectively, and E is a diagonal matrix with diagonal components $t1$, ..., tu in descending order. L is the loading matrix of the main components because the columns of L are the eigenvectors. We can see that $V_h=A_h e_h$ since $NL=AE$, A_h is the h^{th} column of A. Recognize that the SVD is a good low-rank estimate of the data matrix. An alternative geometric interpretation of PCA yields a linear manifold as the closest approximation to the observed data. This concept aligns with how PCA is built. Make jy the y^{th} row in Y. Take the first g main components together, which equals $L_h = [L_1|\cdot\cdot\cdot|L_h]$. L_h is a u×h orthonormal matrix by definition. Each observation should be projected to the linear region covered by $\{L_1,..., L_h\}$. The projected data are $U_h N_y$, $1 \leq y \leq n$ and the projection operator is $T_h = L_h L^Q$. By reducing the overall i_2 approximation error, one may determine the optimal projection.

$$\min_{C_h} \sum_{y=1}^m \|j_y - C_h C_h^Q j_j\|^2 \qquad (6)$$

First-generation solution components are easy to describe. Parameters might have different scales and unit types. Each parameter is standardised such that its marginal variance is 1. Using this approach for PCA, you'll get the sample correlation matrix of raw data and the covariance matrix of standardised variables. The correlation matrix's eigenvalues may vary from the covariance matrixes.

D. Data Encryption Standard

The Data Encryption Standard (DES) was created as "Federal Information Processing Standard 46 (FIPS PUB

International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 8 Issue: 2
DOI: https://doi.org/10.17762/ijfrcsce.v8i2.2081
***Article Received**: 15 March 2022 **Revised**: 18 May 2022 **Accepted**: 25 May 2022 **Publication**: 30 June 2022*

46) by the National Bureau of Standards, now the National Institute of Standards and Technology (NIST), in 1977". DES encrypts sixty four-bit blocks using fifty six-bit keys. Method creates 64-bit output from 64-bit input in stages. Encryption uses 16 Feistel rounds and 2 P-boxes. Figure 3 demonstrates DES encryption. Plaintext and key are encryption's two inputs. This requires 64-bit plaintext and 56-bit key.

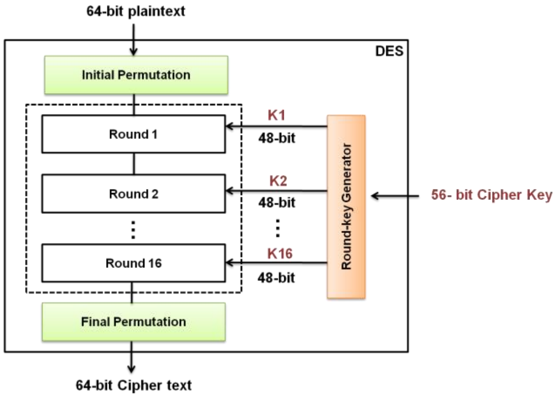

Figure 3: General Representation of DES

E. Data decryption using Fussy Based Neural Genetic Algorithm with Particle Swarm Optimization

Decrypting data returns it to its original state. It's usually a reverse encryption. Only an authorised user with a secret key or password may decode encrypted data. For decrypt the data by using FNGA-PSO. Utilizing a genetic algorithm has the goal of avoiding local minima. As a result, the genetic algorithm is used first to provide a "rough" result. The FNN is then used to refine the outcomes. This research, which combines GA with FNN, shows that GA may provide the initial weights for the FNN. This avoids the local minimum in addition to cutting down on training time. The following are the GA techniques used in this study:

Stage 1: Create n structures for the population at random, and then configure the generational and fitness functions.
Stage 2: For every chromosome, determine the fitness function value.
Stage 3: Execute the crossovers, mutations, and selection of chromosome operators.
Stage 4: For each new chromosome, analyze its fitness function.
Stage 5: Eliminate the chromosomes with lower fitness function values and insert the new chromosomes with higher-fitness function.
Stage 6: End if the end condition is satisfied; otherwise, return to Step 3.
The fitness function is described below:

$$G = \frac{N}{\sum_{j=1}^{N}(U_j - Z_j)^2} \qquad (7)$$

U_j stands for the jth intended output, Z_j is the jth actual output, and N stands for the number of populations. Since binary coding is the most common, that is the coding technique employed. For instance, an 8-digit representation of 12 using the basis of 2 is 00001100. In this research, 50 populations will be included. To reduce the time of decryption process, we use particle swarm optimization. An algorithm for population-based stochastic optimization is particle swarm optimization. PSO is considered to preserve two populations: the particle's present location (rbest) and its best position (ibest) thus far. These two sorts of solutions are used to create the other. As each particle has two properties (velocity and location), its velocity changes dependent on its own and its companion's experience. Formula updates particle velocity and position

$$x_{kf}(v+1) = \omega \times x_{kf}(v) + e_1 \times t_1 \times [r_{kf}(v) - z_{kf}(v)] + e_2 \times t_2 \times [r_{if}(v) - z_{kf}(v)] \qquad (8)$$

$$x_{kf}(v+1) = z_{kf}(v) + x_{kf}(v+1) \qquad (9)$$

Each particle is accelerated toward the best possible position by the stochastic acceleration parameters e_1 and e_2, which are acceleration coefficients. Both t_1 and t_2 signify two random integers that are evenly dispersed within this range (0,1). It resembles the temperature parameter in the simulated annealing process in many ways (SA).Weighted inertia ω is used to balance global and local search. As a general rule, a high inertia weight aids in global exploration, whereas a low inertia weight aids in local exploitation. $z_k = [z_{j1}, z_{j2}, \dots, z_{jk}, \dots, z_{jF}]$ represents the position of the kth particle. jth particle's location in the kth dimension is represented by $z_{kl} \in [z_{min,} z_{max}]$ and its velocity is $X_k = [x_{k1}, x_{k2}, \dots, x_{kl}, \dots x_{kF}]$. It is used to lower the probability of particles exiting the search area, where $x_{kl} \in [x_{min,} x_{max}]$ .The best prior location of the kth particle is stored as rbest and indicated by $R_k = [r_{k1}, r_{k2}, \dots, r_{kl}, \dots r_{kF}]$ and is referred to as $R_i = [r_{i1}, r_{i2}, \dots, r_{il}, \dots r_{iF}]$ represents the best position acquired by the whole swarm thus far.

IV. RESULT AND DISCUSSION

In this paper, we analyze the secure data in cyber security based on fussy based neural genetic algorithm. The parameters are execution time, encryption time, decryption time, throughput, security level. The existing methods are blowfish algorithm [BA (13)], Rivest-Shamir-Adleman encryption [RSA (14)], two fish algorithm [TA (15)] and Advanced Encryption Standard [AES (16)].

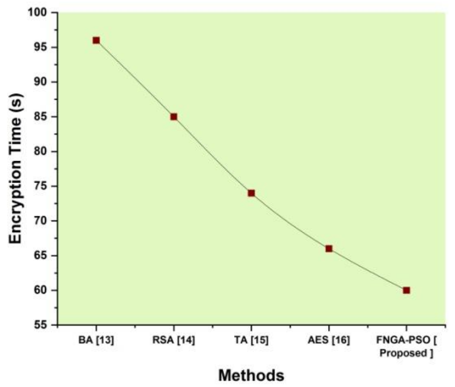

Figure 4: Comparative analysis of encryption time in Suggested and Traditional Methods

Encryption time analyses and illustrates the average amount of time required to encrypt media content files as input. The duration is measured in seconds (s). Figure 4 depicts the encryption time. According to the comparison evaluation, the suggested method's encryption process takes less time than the other four techniques.

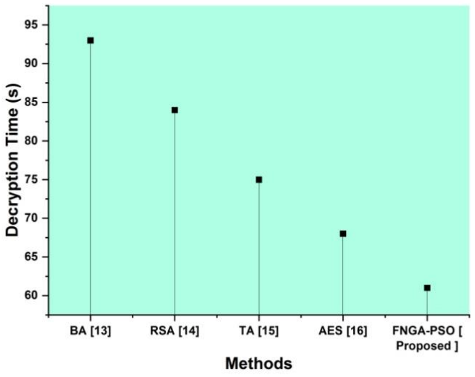

Figure 5: Comparative analysis of decryption time in Suggested and Traditional Methods

Decryption describes the process of restoring encrypted data to its original form. It's common to use reverse encryption. The duration is measured in seconds. Figure 5 depicts the decryption time. From the comparative evaluation, decryption process of the suggested method takes less time than the other four existing methods.

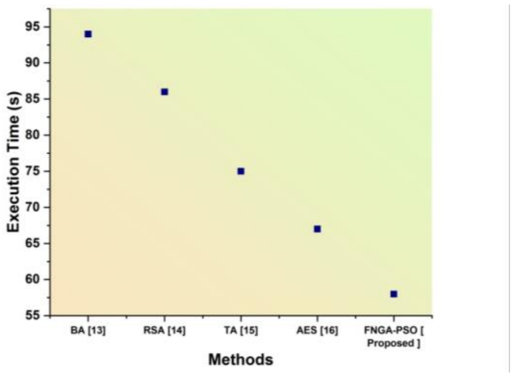

Figure 6: Comparative analysis of execution time in Suggested and Traditional Methods

When estimating the execution time of a task, the amount of time the system spends performing run-time or system actions on its behalf is taken into consideration. It is measured in seconds(s). Figure 7 depicts the execution time. The evaluation showed that the suggested technique has a faster time than the other four methods.

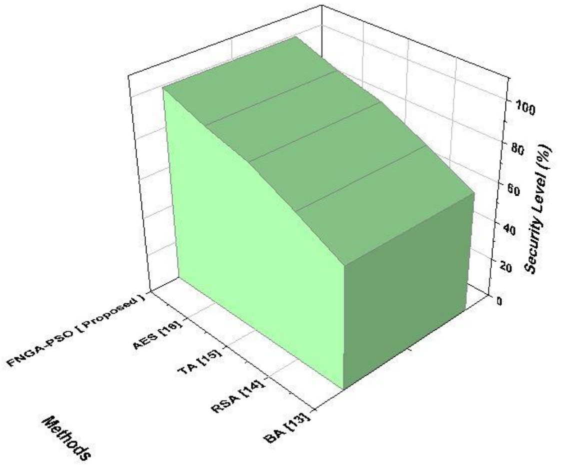

Figure 7: Comparative analysis of security level in Suggested and Traditional Methods

The calculation of the risk that a security event will be attempted or occur is known as the security level. Figure 7 depicts the security level. Based on the evaluation, the suggested method provides a greater degree of security than the other four approaches.

International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 8 Issue: 2
DOI: https://doi.org/10.17762/ijfrcsce.v8i2.2081
***Article Received**: 15 March 2022 **Revised**: 18 May 2022 **Accepted**: 25 May 2022 **Publication**: 30 June 2022*

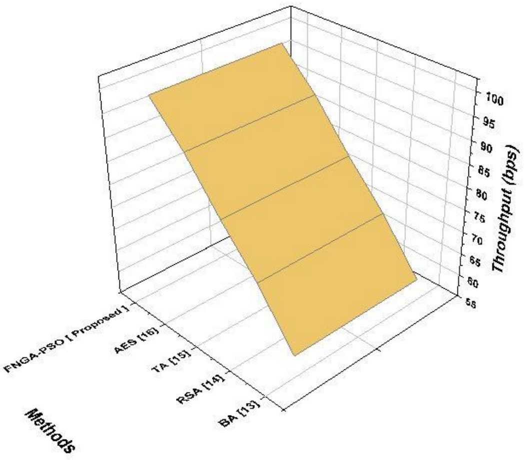

Figure 8: Comparative analysis of throughput in Suggested and Traditional Methods

The quantity of information a system can process or transmit in a given length of time is known as Throughput. The quantity of data that the users get from the server at any given second is measured in bytes per second (bps). Figure 8 depicts the throughput. According to the results of the comparative results, the suggested method has a higher throughput than the other four current approaches.

Blowfish algorithm is that the key must be sent to the receiver outside the band, especially over an unprotected transmission channel [13]. RSA only employs symmetric encryption and full encryption requires the use of both symmetric and asymmetric encryption, it may sometimes fail [14]. Larger encrypted data makes two fish safe. This big size may slow down the application if it's applied to significant amounts of unencrypted data [15]. AES is an Algebraic structure is very simplistic [16]. Hence, our suggested FNGA-PSO outperforms the existing techniques about the securing data in cyber security by overcoming such issues.

V. CONCLUSION

In this paper, we examine that securing data in cyber security by using fuzzy based neural genetic algorithm. In order to avoid insecurity in financial plan, portfolio management is used to increase security level control while lowering direct expenditures. We propose FNGA with PSO for cyber security data authenticity, dependability, and secrecy reduces data integrity risk. Values of Performance measures include Encryption time (60s), decryption time (61s), execution time (58s), and security level (99 percent), throughput (98 bps). The suggested method’s performance was calculated and compared with the current techniques. Data confidentiality, data authentication, and data access control are provided by the suggested security methods. DES encrypts data using symmetric keys. Its 56-bit key is too short to safeguard most encryption-based applications. So, future security studies should incorporate optimization.

REFERENCE

[1]. H. Yin, D. Guo, K. Wang, Z. Jiang, Y. Lyu, and J. Xing, ‘‘Hyperconnected network: A decentralized trusted computing and networking paradigm,’’ IEEE Netw., vol. 32, no. 1, pp. 112–117, Jan./Feb. 2018.

[2]. X. Zheng, Z. Cai, and Y. Li, ‘‘Data linkage in smart Internet of Things systems: A consideration from a privacy perspective,’’ IEEE Commun. Mag., vol. 56, no. 9, pp. 55–61, Sep. 2018.

[3]. Odumesi John Olayemi, “A socio-technological analysis of cybercrime and cyber security in Nigeria”, Academic Journals International Journal of Sociology and Anthropology Vol. 6(3), Odumesi John Olayemi, March, 2014, pp. 116-125

[4]. Bhatia, D., 2022. A Comprehensive Review on the Cyber Security Methods in Indian Organisation. Int. J. Advance Soft Compu. Appl, 14(1).

[5]. Wang, K., Dong, J., Wang, Y. and Yin, H., 2019. Securing data with blockchain and AI. Ieee Access, 7, pp.77981-77989.

[6]. Sule, M.J., Zennaro, M. and Thomas, G., 2021. Cybersecurity through the lens of digital identity and data protection: issues and trends. Technology in Society, 67, p.101734.

[7]. Nguyen, G.N., Le Viet, N.H., Elhoseny, M., Shankar, K., Gupta, B.B. and Abd El-Latif, A.A., 2021. Secure blockchain enabled Cyber–physical systems in healthcare using deep belief network with ResNet model. Journal of parallel and distributed computing, 153, pp.150-160.

[8]. Faragallah, O.S., El-Shafai, W., Sallam, A.I., Elashry, I., EL-Rabaie, E.S.M., Afifi, A., AlZain, M.A., Al-Amri, J.F., El-Samie, F.E.A. and El-sayed, H.S., 2022. Cybersecurity framework of hybrid watermarking and selective encryption for secure HEVC communication. Journal of Ambient Intelligence and Humanized Computing, 13(2), pp.1215-1239.

[9]. Abd El-Latif, A.A., Abd-El-Atty, B., Mehmood, I., Muhammad, K., Venegas-Andraca, S.E. and Peng, J., 2021. Quantum-inspired blockchain-based cybersecurity: securing smart edge utilities in IoT-based smart cities. Information Processing & Management, 58(4), p.102549.

[10]. Mubina Malik, Trisha Patel, “Database security –attacks and control methods”, International Journal of Information Sciences and Techniques (IJIST) Vol.6, No.1/2, March 2016.

[11]. R. Mehla and H. Kaur, “Different reviews and variants of advance encryption standard,” International Journal of

Science and Research (IJSR), ISSN (Online), pp. 2319–7064, 2014.

[12]. Mirsky, Y., Shabtai, A., Rokach, L., Shapira, B. and Elovici, Y., 2016, October. Sherlock vs moriarty: A smartphone dataset for cybersecurity research. In Proceedings of the 2016 ACM workshop on Artificial intelligence and security (pp. 1-12).

[13]. Vengatesan, K., Kumar, A., Subandh, T.S., Vincent, R., Sayyad, S., Singhal, A. and Wani, S.M., 2019, March. Secure Data Transmission Through Steganography with Blowfish Algorithm. In International Conference on Emerging Current Trends in Computing and Expert Technology (pp. 568-575). Springer, Cham.

[14]. Mojisola, F.O., Misra, S., Febisola, C.F., Abayomi-Alli, O. and Sengul, G., 2022. An improved random bit-stuffing technique with a modified RSA algorithm for resisting attacks in information security (RBMRSA). Egyptian Informatics Journal.

[15]. Dhinakaran, D. and Prathap, P.M., 2022. Protection of data privacy from vulnerability using two-fish technique with Apriori algorithm in data mining. The Journal of Supercomputing, pp.1-35.

[16]. Pancholi, V.R. and Patel, B.P., 2016. Enhancement of cloud computing security with secure data storage using AES. International Journal for Innovative Research in Science and Technology, 2(9), pp.18-21.