International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Novel Intelligent AI-based Security to Enhance the Data Communication

Amjan Shaik[1], Bui Thanh Hung[2], Prasun Chakrabarti[3], Dr.Siva Shankar S.[4]

Submitted: 24/01/2023 **Revised:** 13/03/2023 **Accepted:** 09/04/2023

Abstract: In this work, we propose a novel known as matrix translation and Elliptic curve cryptography (MT-ECC) approach for secured data communication in IoT network systems. The proposed approach includes phases such as the key generation stage, encryption stage; cluster-based secure routing stage, and decryption stage. Moreover, we introduced two types of tables such as string location relying on ASCII value and Prime number generation table and space reference table. Meanwhile, after the completion of key generation on the transmitter side, the data is transmitted to the receiver side and authorized users can access the data without any loss. Besides, if any attacks happen means it is necessary to detect the intrusion and normal data, and for that purpose we propose a novel Deep Neural Network (DNN) based Gazella optimization (GO) algorithm which effectively detects the intrusion and separates the normal data traffic from the available datasets. For the experimental purpose, we have taken the Kaggle dataset and implemented it in MATLAB and the comparative results show that the proposed approach is effectively used for secured communication and detects intrusion efficiently in case attacks happen.

Keywords: *Internet of things, Deep Neural network, ASCII, string value, prime numbers, MT-ECC, and secure communication.*

1. Introduction:

The communication system [1] from the Internet of Things (IoT) devices transfer and unite without any connected wires to communicate. The information server unites and interchanges with some physical objects. The organization [2] links the devices with each other to generate multiple functions such as thermostats, refrigerators, and sensors. The IoT devices [3] have several applications: wearable technology, industrial automation, smartphones, homes, watches, healthcare, and buildings. It is an electronic device [4] that we wear in many gadgets such as smart jackets, medicines, jewelry, and Fitbit. The messages are quickly delivered, analyze the fitness of our body, and GPS can track the location through the phone whenever necessary.

The device is free-standing and compact without activating any devices. Nowadays wearables are used by everyone common and the sales are hiked by 25 million units. In this world, 53% and 43% of women and men are attracted to using wearables. The most popular wearable devices [5] are smart glasses, rings, earphones, helmets, and clothes. It is very useful, restricted, suitable, and prohibitive. The forthcoming technology uses these smart devices for communication without using mobile phones with the help of smartwatches and trackers. Human intrusion is decreased by the automation in industries by advanced software and robots[28].

Machines and robots help humans in all the ways in industries with technology. The four different phases of automation [6] are flexible, integrated, fixed, and programmable automation. The supplement automation is programmable for a product. The production cost and time are more for reprogramming any changes. It is differentiated into fixed, flexible, and programmable automation. The software applications are web browsing and operating system that have the ability to unsegregated systems. Smartphones [7] are

[1]*Professor & HoD-CSE, St.Peter's Engineering College, Hyderabad, TS, INDIA, amjansrs@gmail.com and Post Doctoral Scholar, Industrial University of Ho Chi Minh city, VIETNAM.*

[2]*Data Science Department, Faculty of Information Technology,*
Industrial University of Ho Chi Minh city, VIETNAM, buithanhhung@iuh.edu.vn

[3]*Deputy Provost, ITM SLS Baroda University, Vadodara Gujarat, India*
Drprasun.cse@gmail.com

[4]*Department of Computer Science and Engineering, KG Reddy College of Engineering and Technology (Autonomous) R R District,Telangana, India.*
drsivashankars@gmail.com

designed to send calls and messages and play games on the computer.

Communication is a wide area to explore our skills through the internet, transfer messages, and receive them within a second also able to travel the whole world with the communication of smartphones. Home appliances are linked with the latest technology to access the lights, fans, television, refrigerator, and other devices in our home. Wink Hub, smart things, and google home. The authority of the entire cycle is given to the smart devices to manipulate the product with one touch. The ability to access communication devices is with consolation, accessibility, and ease. The Internet of Things unites the patients in healthcare to access and generate the proper treatment for the best end product. Healthcare [8] is observed in many ways by connected inhalers, glucose, heart rate, and ingestible sensors are the observers of healthcare.

The interrelated connectors interchange and transfer data with multimedia files, images, and text. The modules of data communication are transmission medium, sender, protocol, and receiver. The messages are transmitted anywhere in the world without any support. The exporter can export any type of element and import the element in the correct manner. Data communication [9] plays a most important part in our day-to-day lives through the internet with smart devices. The components are half-duplex, full-duplex, and simplex data communication.

It can accept and convey instruction on both sides referred to as half-duplex. The instruction conveyed in a single mode is referred to as simplex. The instruction is conveyed by both the sides of data but at one time the instructions are conveyed or accepted. It can be easily accessed, is flexible, safe, and efficient the cost is low and fast. For the transmission of data without any loss, it is ineluctable to design a secured communication hence many approaches have been stated still date and many fail to achieve the detection of attacks some of the works show less secured data communication and in context with these we propose, a novel MT-ECC based secured communication and DNN-GO approach for the detection of intrusion in the IoT nodes [28]. The main contributions of the works are listed below,

- The proposed work is based on M-ECC for the secured communication and the key generations stages are based on the tables introduced in our work and the matrix translation phase stated in our approach.
- The traffics are collected from each node and if any intrusions happen means they are detected using the DNN and MLP which effectively detects the intrusion further the overfitting issues are overcome by using the adopted GO approach.
- The proposed work is effectively used for secured communication in the IoT platform.

The rest of the work is organized as follows: in section 2 the relevant works are analyzed and highlighted the merits and demerits. The system model is stated in section 3. The proposed work is elucidated in section 4. Experimental analyses are stated in section 5 with the dataset description and the work is concluded in section 6.

2. Literature Survey:

Lin et al. [10] have presented federated learning based on a deep anomaly framework for sensing time-series data. The device is efficient for new communication in the Industrial Internet of Things. In time series data the features are identified and detected with the convolutional neural network. The framework is enhanced to compress the K selection gradient in the proposed system. The accuracy is more in identifying the time series data. meanwhile, the security of the data is a big challenging issue as per this work.

Nie et al. [11] have described a machine learning framework that establishes two-phase data driven for reconstructing the trajectory vessels. There are two phases of bidirectional long short-term memory and the clustering method based on density. The main contributions are high performance, numerous experiments, and automatic detection. The timestamped points are recognized and restored the outliers are necessary for various degraded points. It is efficient and reliable, and the cost is effective. However, mitigating the traffic will enhance the performance of the stated model.

Singh et al. [12] have demonstrated a deep learning-based blockchain framework for the secured industrial framework. The framework is prevented by a distributed denial of service attacks with three phase validation scheme, identity generation phase, and scheme verification phase. The planes are validated and generated by a deep Boltzmann machine from the switches. The computation time and cost of communication are less. It is also efficient and scalable, however, there is a loss in data due to low security.

Yin et al. [13] highlighted a secure data collaboration framework (FDC) based on deep learning technology. The data center blockchains are blockchain, private, and public. For the transmission and usage of data, the blockchain manages the system. The registration, administration, and management of data are managed by the private data center. It organizes security for several organizations through the public data center. The performance is feasible, secure, sensitive, and efficient. Moreover, optimal security is the demerit of the stated work.

Makkar et al. [14] suggested a machine learning framework for the Internet of Things to detect spam. The proposed method is used for the decision-making of each model for different purposes. The framework is divided into three different models reduction, selection, and engineering of features. It enhances accuracy, security, and usage, however, the optimal security level is not obtained by the stated work.

For cyber-physical systems, Li et al. [15] have presented a new deep learning-based intrusion detection model. The recurrent unit and convolutional neural network represent the proposed method to be used. Many cyber-physical systems are developed by federated learning by identifying in a privately training process is retained by the position to retain the private and secure model. The effectiveness is more to detect the identical model. However, from different areas, cyber security problems have to be resolved for better communication.

Mothukuri et al. [16] have described Federated Learning (FL) to identify different IoT networks. The different layers classify the attacks of the Gated Recurrent unit to implement the proposed method. The various models are identified to combine with groups to increase performance. It is secure and reliable for detecting intrusion algorithms. Analyzing large datasets is a complicated process.

Zolanvari et al. [17] have demonstrated the Industrial Internet of Things (IIoT) protocols based on communication networks. Command injection, SQL injection, and backdoor are the types of attacks to identify machine learning. The normal traffic is detected to vary multiple attacks by ranking for the features. The performance is increased in security to detect various attacks. However, the false negatives are higher, and are difficult to achieve better communication.

To improve reliability Garg et al. [18] have introduced a hybrid deep learning-based detection scheme in multimedia. There are two parts end-to-end and detection module. Irregular activities are detected by the anomaly detection module. The latency and bandwidth are satisfied by the end-to-end module. It is efficient and effective in identifying the data delivery of multimedia. However, it is difficult to analyze the state work for multiple domains.

3. System Model

The system model of the stated work is illustrated in figure 1. It includes a user interface and data gathering module, sensor nodes, key generation module with the third part auditor, encryption and decryption stages, cluster-based routing, end user module, and cloud at the destination.

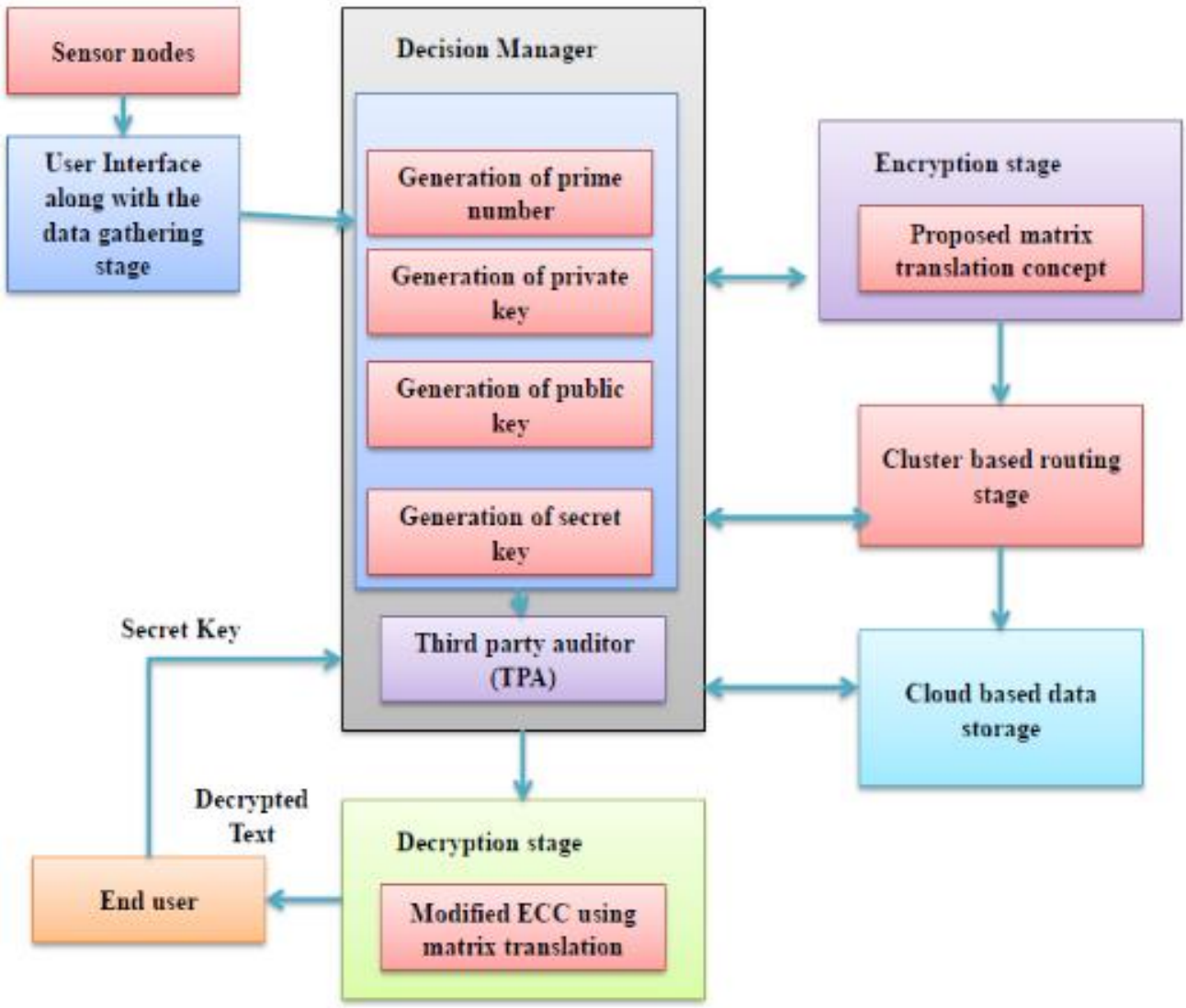

Fig 1: System model of the proposed system

4 Proposed Matrix Translation and Elliptic Curve Based Cryptosystem (MT-ECC) for secured data communication in IoT

The secured data communication in the IoT-based approach utilizes a secured routing algorithm and hence the new approach is used to combine the key generation, encryption, and decryption stages of our work. For secured communication, we have used two various tables such as (i) space reference table and (ii) string position-based ASCII value and prime number generation table for the generation of the key. The former one is used to allot values for the spaces that are used in the sentences prior to the encryption and decryption stages. The latter one is used to convert the strings into numerical digits and assigns the nearest prime value [19]. The space reference table is listed in table 1.

Table 1: Space reference table

Space location (SL)	Symbols used to replace the space	Respective ASCII values of space	SL*ASCII=TA
1	#	32	32
2	!	34	68
3	&	36	108
4	%	37	148

The values for the spaces are assigned in a sentence using the space reference table and after the completion of the fourth space it will start from the first space and the Text to ASCII value can be evaluated by the location value and the respective ASCII value.

Prime Generation table with the String location-based ASCII value generation

Table 2: Prime number selection tabular column

String	String Location	ASCII value of the string	SL*ASCII=TA	Nearest prime value p
T	1	85	85	89

The ASCII value of every single bit of string from the input sentence is evaluated and considered as key values. the location of the string is responsible for the SL value and respective prime values are evaluated. An illustration to evaluate the TA and prime value is shown in table 2. The prime number is chosen from the nearest value as shown in table 2.

- **Matrices Translation**

The organization of generated number in rows and columns is called a matrix and each number are denoted as elements and the numbers must be real. The row of the matrix is denoted as *a* and column is denoted as *b* and the order is denoted as M [19]. the matrix transformation is achieved by reflection, translation, rotation, and dilation. The shape of the graph is retained in these four ways. Translation means moving the plane from one location to another on the coordinate plane without varying the orientation.

With the key generated from the key generation stage of encryption and the decryption, the location of points is varied and formulates the matrix and translation approach.

- **Translation standard form**

Consider the points u and v from the plane shifted in a particular distance based on the orientation given and can be formulated as

$$\begin{pmatrix} U' \\ V' \end{pmatrix} = \begin{pmatrix} m+|u| \\ |n|+|v| \end{pmatrix} = \begin{pmatrix} U \\ V \end{pmatrix} \quad (1)$$

The translation points are indicated as m and n and are completely responsible for the transformation process.

- **Key Generation stage**

This section presents the key generation stage of the proposed approach which is responsible for secured data communication.

- **Public key generation**: The public keys are generated with the help of Matrix Translation methodology and generated by the PM and PN. The estimation of PA is with the help of two point's uG and vG and udM, vdMand similarly the PN is evaluated with the help of uG, vG and udN, vdN. In general, it can be termed as, $PM = G = dM,\ PN = G + dN$.
- **Private key generation**: With the help of random numbers from the elliptic curve (udM, vdM) and (udN, vdN) the private keys are generated as (dM, dB). It can be expressed as, $dM = (udM, vdM),\ dN = (udN, vdN)$.

Thus, with the generation of keys, the transmission of data is secured and only the authorized user can access the data with the apt keys that are generated on the transmitter side. The next stage is to secure the data transmission it is necessary to detect the intrusion from the traffic that is generated by all nodes in the network. For this, we proposed a novel approach known as DNN based GO approach which can be used to detect normal and intrusion traffic and therein significantly reduce the intrusion and secured the data communication[28].

4.1 Proposed DNN-based intrusion detection

This section reveals the proposed DNN-based Gazella optimization (GO) approach for the detection of intrusion while conducting a secured MT-ECC data communication in an IoT network. The detailed study is explained below and the schematic overlay is illustrated in figure 2.

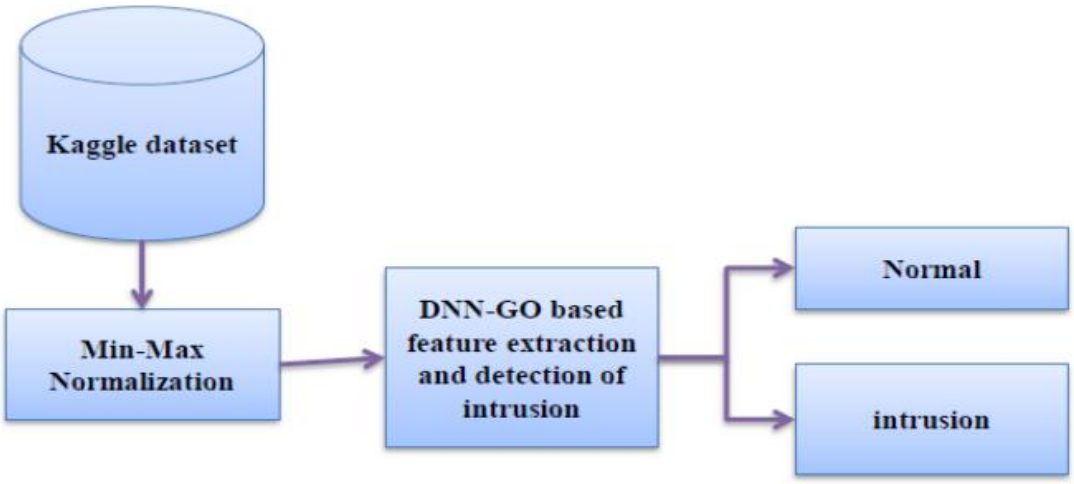

Fig 2: Schematic overlay of the proposed approach

- **Min-Max based Normalization**

It is the first step [19, 20] of our proposed work, and the normalization of the images is represented by,

$$I_{Norm}(a,b) = \begin{cases} 2^x - 1 & for \;\; N(a,b) > 2^x - 1 \\ N(a,b) & for \;\; 0 \le N(a,b) \le 2^x - 1 \\ 0 & for \;\; 0 < N(a,b) \end{cases} \quad (2)$$

Here,

$$N(a,b) = round\left(\frac{I(a,b) - \min_{Norm}}{\max_{Norm} - \min_{Norm}} \left(2^x - 1\right) \right)$$

The minimum normalized value is denoted as $\min_{Norm}$ and the value of maximum normalized can be given as $\max_{Norm}$ and after normalization the number of image pixels is estimated as *x*. The minimum and maximum intensities are taken from the image histogram are taken as $\min_{Norm}$ and $\max_{Norm}$.

4.2 DNN

The DNN [20] is used to detect the network traffic from the node which is affected. It has three processes that are (i) the neural network platform can be used to detect normal traffic and intrusion traffic, (ii) Multilayer perceptron (MLP) can be used to enhance the detection of intrusion accurately and it includes hidden layers that are used for computation and synapses connected with the weights of the arcs. Let us assume that the activation function H_i of the ith unit is a nonlinear function and hidden input values are estimated as

$$H_i = f(x_i) \quad (3)$$

Here, $x_i = \sum s_{ij} H_i + g_i$ (4)

The weight linear sum of the output can be determined x_i and the amplitude value from the unit I to unit j can be denoted as s_{ij} and the bias among the nodes is denoted as g_i. The classification of intrusion and normal traffics are achieved by the DN and the MLP uses a single hidden layer and multiple usages of hidden layers might have led to overfitting problems. Hence backpropagation learning algorithm is used to sustain the popular learning algorithm of neural networks which is simple and swifter while computing the simple concept. This exploits the stochastic gradient descent (SGD) approach. Moreover, the random selections of weights are used for the activation of linear region and learning becomes slow when the gradients weights are involved.

The standard logistic function is taken from the MLP for the activation of weights and can be denoted as, $s(i) \in \{0,1\}$. The classes are handled with the standard logistic function and classes are taken as L. the labels are assumed as w(i) and z(i) for the training set. Then the standard logistic function is expressed as,

$$J\phi(x) = \frac{1}{1+e^{-\phi^T x}} \tag{5}$$

The cost function is denoted as ϕ and according to ***(i)*** Xavier and Yoshua that the cross-entropy cost function can be used for the classification than the quadratic cost for the training neural network. Further, the falling local optima can be avoided using the GO algorithm which effectively overcomes the overfitting issues and averts the falling for the local optima which is explained below.

4.3 Gazelle Optimization Algorithm:

In the predator-dominated environment, the gazelles' survival ability of the metaheuristics algorithm inspires the gazelle optimization (GO) algorithm. Equation (6) represents the gazelles (X) candidate population initialization in the GO algorithm [22]. Generate the population based on both lower and upper-bounds issues.

$$Y == \begin{bmatrix} y_{1,1} & y_{1,k} & \cdots & y_{1,D-1} & y_{1,D} \\ y_{2,1} & y_{2,2} & \cdots & y_{2,D-1} & y_{2,D} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ y_{m,1} & y_{m,k} & \cdots & y_{m,D-1} & y_{m,D} \end{bmatrix} \tag{6}$$

Equation (2) randomly generates the current candidate population set as *Y*. In the j^{th} dimension of k^{th} population, the position is $y_{j,k}$. Th problem dimension is *D* and the total number of candidate population *m*.

$$y_{j,k} = Random \times \left(BU_k - BL_k\right) + BL_k \tag{7}$$

The lower and upper bound variables are BU_k and BL_k. In each iteration, determine the optimal solution if the best-obtained solution. The below equation expresses the elite matrix [23].

$$Elite = \begin{bmatrix} \grave{y}_{1,1} & \grave{y}_{1,k} & \cdots & \grave{y}_{1,D-1} & \grave{y}_{1,D} \\ \grave{y}_{2,1} & \grave{y}_{2,2} & \cdots & \grave{y}_{2,D-1} & \grave{y}_{2,D} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ \grave{y}_{m,1} & \grave{y}_{m,k} & \cdots & \grave{y}_{m,D-1} & \grave{y}_{m,D} \end{bmatrix} \tag{8}$$

The gazelle vector is $\grave{y}_{1,1}$. If the better gazelle substitute the top gazelle, update the elite at the end of each iteration. The exploitation and exploration phases are the two major parts of the GO algorithm.

Exploitation:

In the absence of a predator, graze the gazelles in this stage. Uniformly characterize the Brownian motion. The domains of neighborhood areas are covered.

$$\overrightarrow{Gazelle}_{L+1} = \overrightarrow{Gazelle}_L + SP \cdot \vec{B} * \vec{B}_R * \cdot \left(\overrightarrow{Elite}_L - \vec{B}_R * \cdot \overrightarrow{Gazelle}_L\right) \tag{9}$$

The next iteration solution is $\overrightarrow{Gazelle}_{L+1}$ and the current iteration solution is $\overrightarrow{Gazelle}_L$. The speed of grazing gazelles is *SP*. The random vectors $\vec{B}_R$ with respect to the Brownian motion tend to the interval [0, 1].

(ii) Exploration:

The gazelle flees when the predator spots it, and the latter pursues. Both runs exhibit a sharp turn in direction, which is indicated by the region [23]. This direction progress occurs each iteration; when the iteration number is odd, the gazelle moves in one direction, while when the number of iterations is even, it moves in the opposite direction[28].

$$\overrightarrow{Gazelle}_{L+1} = \overrightarrow{Gazelle}_L + SP \cdot \vartheta \cdot \vec{B} * \vec{B}_R * \cdot \left(\overrightarrow{Elite}_L - \overrightarrow{B_{RV}} * \cdot \overrightarrow{Gazelle}_L\right) \tag{10}$$

Based on the Levy distributions, the random vector $\vec{B}_{RV}$ reached the gazelle and the top speed is SP. The algorithm avoids being trapped in a local minimum because the effect influences the gazelle's ability to flee, which is determined by the predator's success rates. The algorithm avoids being trapped in a local minimum because the effect influences the gazelle's ability to flee, which is determined by the predator's success rates.

$$\overrightarrow{Gazelle}_{L+1} = \overrightarrow{Gazelle}_L + SP \cdot \vartheta \cdot FC * \vec{B} * \vec{B}_R * \cdot \left(\overrightarrow{Elite}_L - \overrightarrow{B_{RV}} * \cdot \overrightarrow{Gazelle}_L\right) \tag{11}$$

Hence,

$$FC = \left(1 - \frac{Itr}{Max_{Itr}}\right)^{\left(2\frac{Itr}{Max_{Itr}}\right)} \tag{12}$$

$$\overrightarrow{Gazelle}_{L+1} = \begin{cases} \overrightarrow{Gazelle_L} + FC\left[\overrightarrow{B_U} + \vec{B} * \left(\overrightarrow{B_U} - \overrightarrow{B_L}\right)\right] * \vec{A} & if \quad S \le SR \\ \overrightarrow{Gazelle_L} + \left[SR(1-S) + S\right]\left(\overrightarrow{Gazelle_{S1}} - \overrightarrow{Gazelle_{S2}}\right), & Otherwise \end{cases} \tag{13}$$

The binary vector is $\vec{A}$ and it is defined as,

$$\vec{A} = \begin{cases} 0, & S < 0.2 \\ 1, & Otherwise \end{cases} \tag{14}$$

The gazelle matrix indexes are S_1 and S_2. Figure 3 flowchart of GO algorithm.

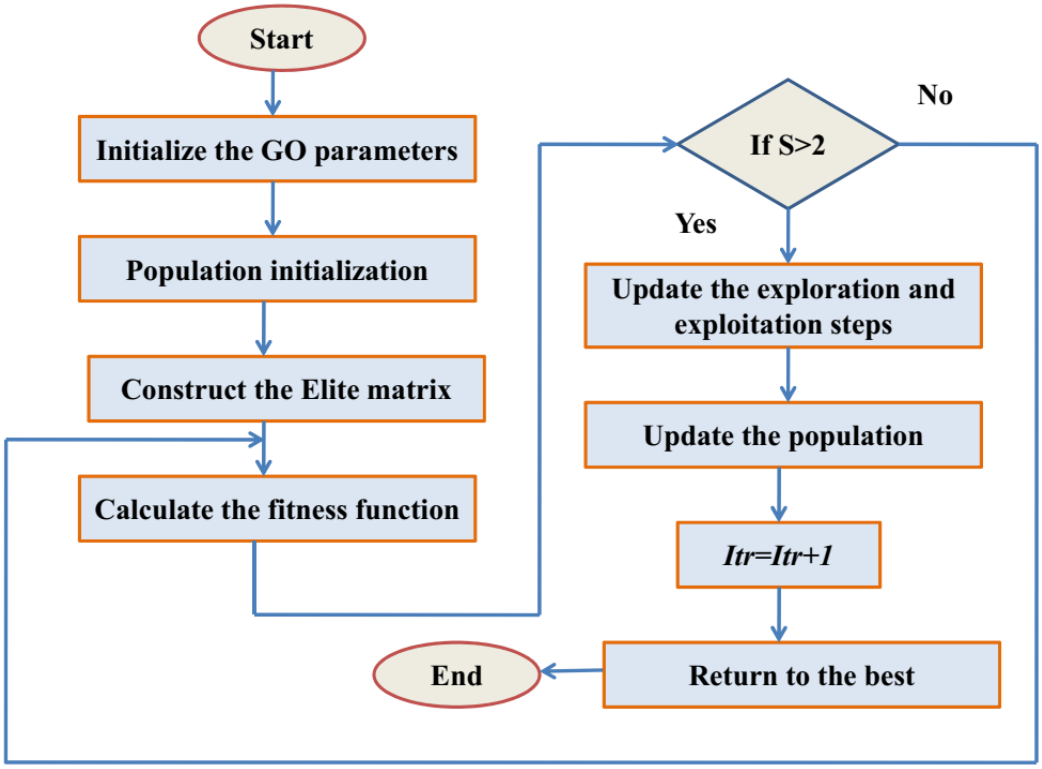

Fig 3: Flowchart model of GO algorithm

5 Result and Discussion:

This section discusses the experimental outcomes of the proposed methodology using various investigation analyses. MATLAB tool is used for the implementation model. The dataset details were collected from https://www.kaggle.com/datasets/therohk/million-headlines for the investigation. The detailed description of experimental outcomes is delineated in the following section.

5.1 Performance metrics:

The performance measures like packet delivery ratio, accuracy, security level, detection rate, computational time and etc to analyze the performance of the proposed framework.

$$Accuracy = \frac{(TN + TP)}{(FN + FP + TN + TP)} \tag{15}$$

The proportion of data packets received at the receiver end to those that were initially sent by the sender is known as the packet delivery ratio (PDR).

$$PDR = \frac{Number \quad of \quad packet \quad received}{Total \quad packets \quad sent} \tag{16}$$

The delay was brought on by the link's data rate.

$$Delay = Packet \quad departure \quad time - Packet \quad arrival \quad time \tag{17}$$

The true positive and negative classes are TP and TN. Further, FP and FN are the false positive and negative classes.

The performance of the packet delivery ratio with respect to the number of packets is delineated in Figure 4. Methods like ECC, MECC, KDP, RSA and proposed are used to analyze the packet delivery ratio. Based on the existing related algorithms, the

proposed method offers a superior packet delivery ratio. While sending the packets in encrypted form, the security attacks drop an efficient prevention of pack and it achieves improved packet delivery ratio performances.

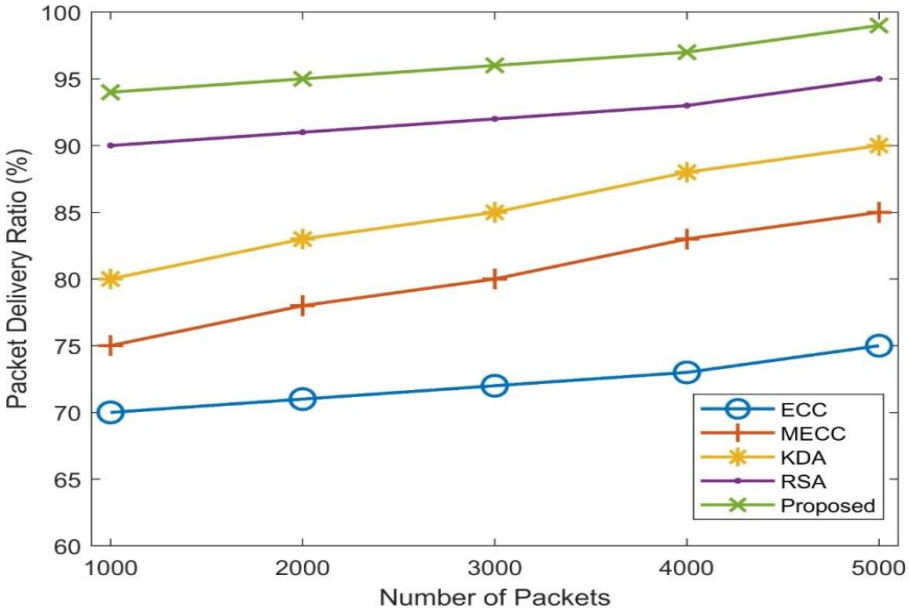

Fig 4: Performance of packet delivery ratio

The performance of the packet delivery ratio with respect to the energy consumption results is delineated in Figure 5. Method like ECC, MECC, KDP, RSA and proposed is used to analyze the energy consumption results. By varying the nodes in one round, the proposed method consumes less energy than other existing methods like ECC, MECC, KDP and RSA. Because the proposed secure routing algorithm prevents attackers from "feeding" the proposed method it uses less energy for routing than ECC, MECC, KDP, and RSA.

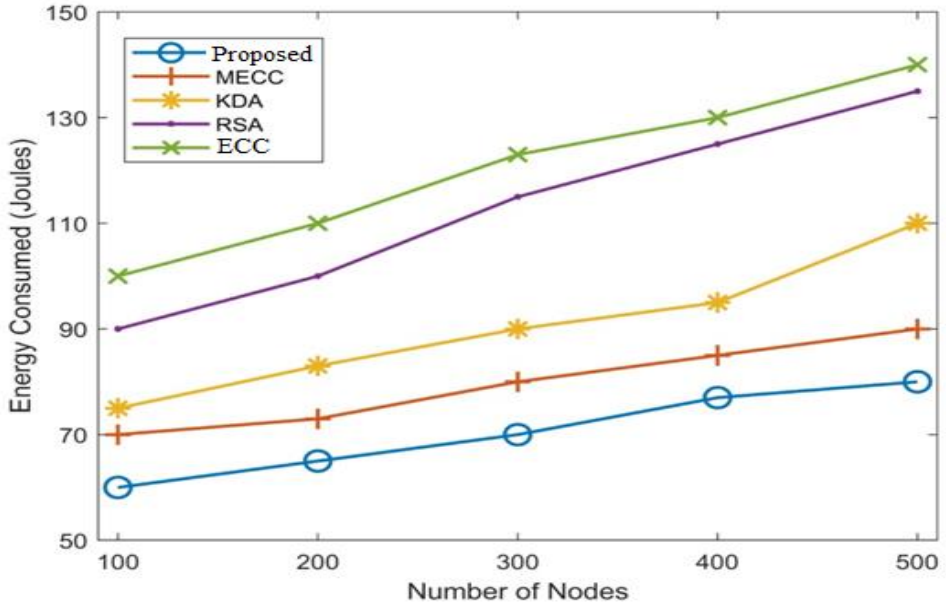

Fig 5: Performance of energy consumption

Figure 6 explains the percentage of accuracy and detection rate performance. The comparative analysis is investigated by using the proposed method with the existing approaches like DL-IDS, DRL, HNS, and DLTD respectively. The proposed method offers above 90% of results in terms of both accuracy and the detection rate in which the proposed method result is higher than that of other

previous methods like ECC, MECC, KDP, and RSA.

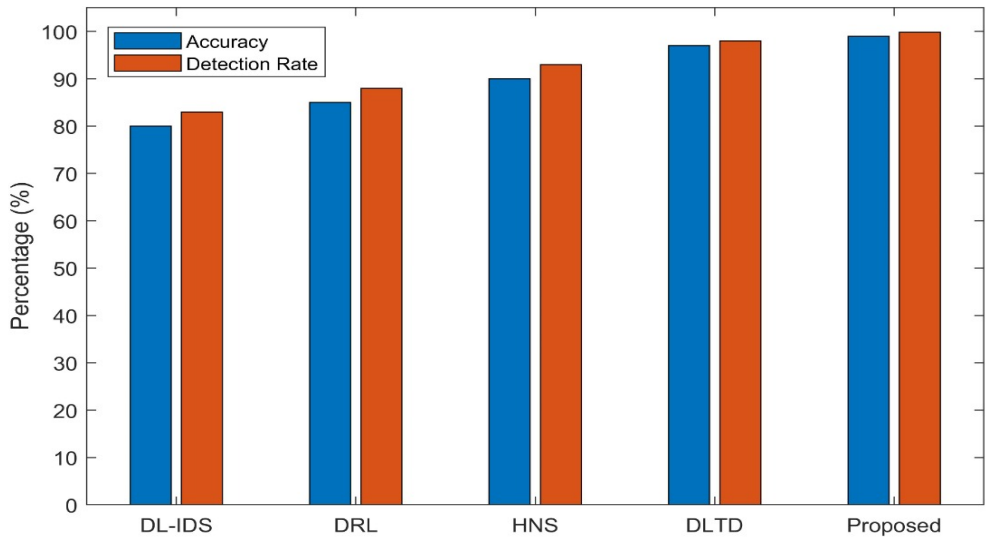

Fig 6: Performance of accuracy and detection rate

Figure 7 explains the performance of delay with respect to the previous methods. While comparing delay, the methods such as DL-IDS [24], DRL [25], HNS [26], and DLTD [27] and the proposed method are used for this investigation. The avoidance of passive attacks, such as packet flooding and packet copying by hostile nodes, is what causes the decrease in delay. Due to the proposed work, hostile nodes were prevented from making their efforts.

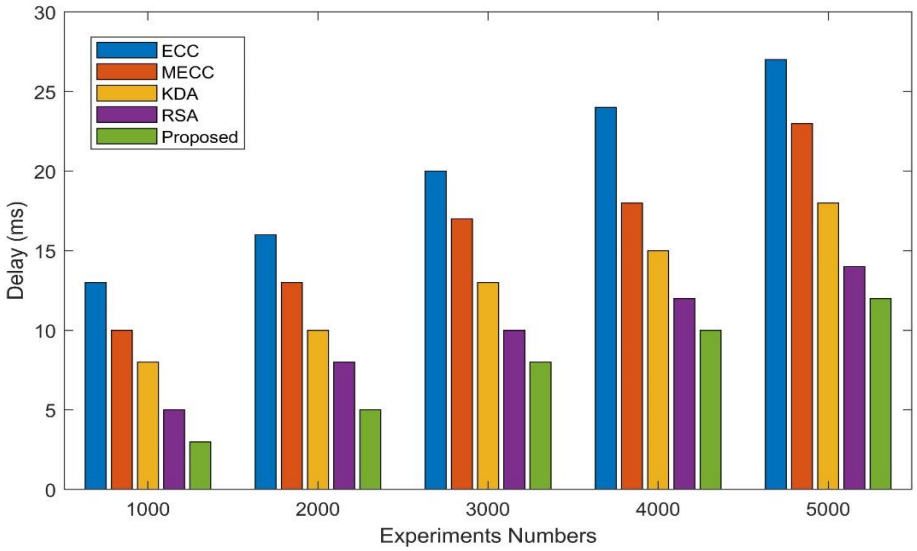

Fig 7: Performance of delay

Figure 8 plot the performance of key computational time. For this examination of computing time, the methods DL-IDS, DRL, HNS, DLTD, and the proposed method are employed. The proposed method offers minimum computational time. When compared to the previous methods such as DL-IDS, DRL, HNS, and DLTD, the minimum computational time is achieved by the proposed approach.

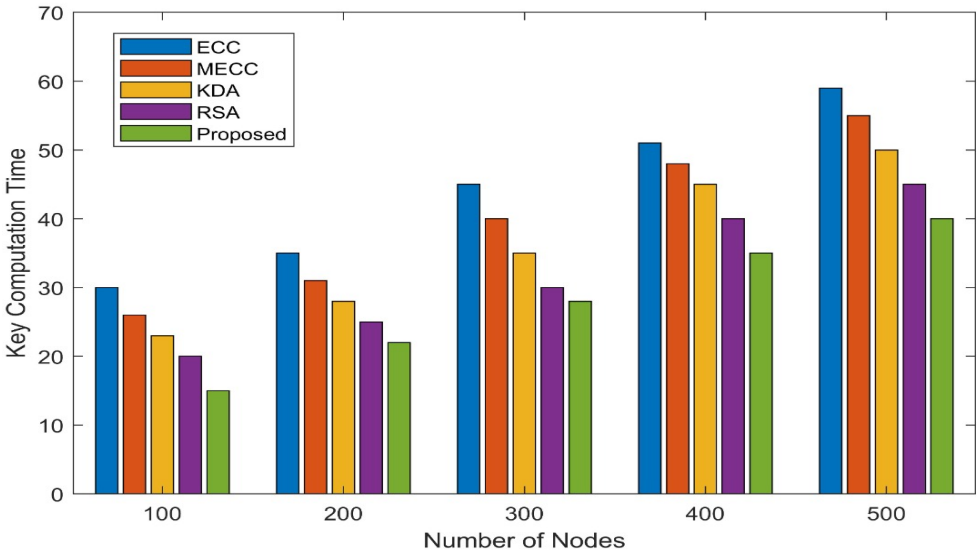

Fig 8: Performance of key computational time

Table 3 explains the performance of the security level with respect to the previous methods. While comparing security levels, the methods such as DL-IDS, DRL, HNS, DLTD, and the proposed method are used for this investigation DL-IDS, DRL, HNS, DLTD, and the proposed method offer 70%, 84%, 85%, 88% and 96% of security levels. When compared to the previous methods, the proposed method offers superior security level percentages.

Table3: Performance of security level of security level

Techniques	Percentage of security level
DL-IDS	70%
DRL	84%
HNS	85%
DLTD	88%
Proposed	96%

6. Conclusion:

This study presents a novel matrix-based matrix translation and elliptical curve cryptosystem for secured communication. Further, the gazelle optimization algorithm with the DNN model accurately detects the intrusion. The implementation model is created using the MATLAB tool. For the investigation, the dataset information was gathered from https://www.kaggle.com/datasets/therohk/million-headlines. The proposed method offers superior results based on security level, packet delivery ratio, accuracy, and detection rate when compared to the ECC, MECC, KDP, and RSA methods. While compared to the previous studies, the proposed method offers minimum delay, computational time, and energy consumption. ECC, MECC, KDP, RSA, and the proposed approach provide security levels of 70%, 84%, 85%, 88%, and 96%, respectively. The proposed method provides higher security level benefits as compared to the previous methods.

References:

[1] Niu, Z., Zhang, B., Wang, J., Liu, K., Chen, Z., Yang, K., Zhou, Z., Fan, Y., Zhang, Y., Ji, D. and Feng, Y., 2020. The research on 220GHz multicarrier high-speed communication system. *China Communications*, *17*(3), pp.131-139.

[2] Fortino, G., Fotia, L., Messina, F., Rosaci, D. and Sarné, G.M., 2020. Trust and reputation in the internet of things: State-of-the-art and research challenges. *IEEE Access*, *8*, pp.60117-60125.

[3] Shafique, K., Khawaja, B.A., Sabir, F., Qazi, S. and Mustaqim, M., 2020. Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and

prospects for emerging 5G-IoT scenarios. *Ieee Access*, *8*, pp.23022-23040.

[4] Do, D.T., Van Nguyen, M.S., Nguyen, T.N., Li, X. and Choi, K., 2020. Enabling multiple power beacons for uplink of NOMA-enabled mobile edge computing in wirelessly powered IoT. *IEEE Access*, *8*, pp.148892-148905.

[5] Dian, F.J., Vahidnia, R. and Rahmati, A., 2020. Wearables and the Internet of Things (IoT), applications, opportunities, and challenges: A Survey. *IEEE Access*, *8*, pp.69200-69211.

[6] Sekaran, R., Patan, R., Raveendran, A., Al-Turjman, F., Ramachandran, M. and Mostarda, L., 2020. Survival study on blockchain-based 6G-enabled mobile edge computation for IoT automation. *IEEE access*, *8*, pp.143453-143463.

[7] Liao, B., Ali, Y., Nazir, S., He, L. and Khan, H.U., 2020. Security analysis of IoT devices by using mobile computing: a systematic literature review. *IEEE Access*, *8*, pp.120331-120350.

[8] Azghadi, M.R., Lammie, C., Eshraghian, J.K., Payvand, M., Donati, E., Linares-Barranco, B. and Indiveri, G., 2020. Hardware implementation of deep network accelerators towards healthcare and biomedical applications. *IEEE Transactions on Biomedical Circuits and Systems*, *14*(6), pp.1138-1159.

[9] Du, Z., Wu, C., Yoshinaga, T., Yau, K.L.A., Ji, Y. and Li, J., 2020. Federated learning for vehicular internet of things: Recent advances and open issues. *IEEE Open Journal of the Computer Society*, *1*, pp.45-61.

[10] Liu, Y., Garg, S., Nie, J., Zhang, Y., Xiong, Z., Kang, J. and Hossain, M.S., 2020. Deep anomaly detection for time-series data in industrial IoT: A communication-efficient on-device federated learning approach. *IEEE Internet of Things Journal*, *8*(8), pp.6348-6358.

[11] Liu, R.W., Nie, J., Garg, S., Xiong, Z., Zhang, Y. and Hossain, M.S., 2020. Data-driven trajectory quality improvement for promoting intelligent vessel traffic services in 6G-enabled maritime IoT systems. *IEEE Internet of Things Journal*, *8*(7), pp.5374-5385.

[12] Singh, M., Aujla, G.S., Singh, A., Kumar, N. and Garg, S., 2020. Deep-learning-based blockchain framework for secure software-defined industrial networks. *IEEE Transactions on Industrial Informatics*, *17*(1), pp.606-616.

[13] Yin, B., Yin, H., Wu, Y. and Jiang, Z., 2020. FDC: A secure federated deep learning mechanism for data collaborations in the Internet of Things. *IEEE Internet of Things Journal*, *7*(7), pp.6348-6359.

[14] Makkar, A., Garg, S., Kumar, N., Hossain, M.S., Ghoneim, A. and Alrashoud, M., 2020. An efficient spam detection technique for IoT devices using machine learning. *IEEE Transactions on Industrial Informatics*, *17*(2), pp.903-912.

[15] Li, B., Wu, Y., Song, J., Lu, R., Li, T. and Zhao, L., 2020. DeepFed: Federated deep learning for intrusion detection in industrial cyber–physical systems. *IEEE Transactions on Industrial Informatics*, *17*(8), pp.5615-5624.

[16] Mothukuri, V., Khare, P., Parizi, R.M., Pouriyeh, S., Dehghantanha, A. and Srivastava, G., 2021. Federated-Learning-Based Anomaly Detection for IoT Security Attacks. *IEEE Internet of Things Journal*, *9*(4), pp.2545-2554.

[17] Zolanvari, M., Teixeira, M.A., Gupta, L., Khan, K.M. and Jain, R., 2019. Machine learning-based network vulnerability analysis of industrial Internet of Things. *IEEE Internet of Things Journal*, *6*(4), pp.6822-6834.

[18] Garg, S., Kaur, K., Kumar, N. and Rodrigues, J.J., 2019. Hybrid deep-learning-based anomaly detection scheme for suspicious flow detection in SDN: A social multimedia perspective. *IEEE Transactions on Multimedia*, *21*(3), pp.566-578.

[19] Pradeep, S., Muthurajkumar, S., Ganapathy, S. and Kannan, A., 2021. A matrix translation and elliptic curve based cryptosystem for secured data communications in WSNs. *Wireless Personal Communications*, *119*(1), pp.489-508.

[20] Ramesh, S., Yaashuwanth, C., Prathibanandhi, K., Basha, A.R. and Jayasankar, T., 2021. An optimized deep neural network based DoS attack detection in wireless video sensor network. *Journal of Ambient Intelligence and Humanized Computing*, pp.1-14.

[21] Goldberg, S.N., Stein, M.C., Gazelle, G.S., Sheiman, R.G., Kruskal, J.B. and Clouse, M.E., 1999. Percutaneous radiofrequency tissue ablation: optimization of pulsed-radiofrequency technique to increase coagulation necrosis. Journal of vascular and interventional radiology, 10(7), pp.907-916.

[22] Juvekar, C., Vaikuntanathan, V. and Chandrakasan, A., 2018. {GAZELLE}: A low latency framework for secure neural network

inference. In 27th USENIX Security Symposium (USENIX Security 18) (pp. 1651-1669).

[23] Agushaka, J.O., Ezugwu, A.E. and Abualigah, L., Gazelle Optimization Algorithm: A novel nature-inspired metaheuristic optimizer for mechanical engineering applications.

[24] Otoum, Yazan, Dandan Liu, and Amiya Nayak. "DL-IDS: a deep learning–based intrusion detection framework for securing IoT." *Transactions on Emerging Telecommunications Technologies* 33, no. 3 (2022): e3803.

[25] Qiu, Han, Qinkai Zheng, Gerard Memmi, Jialiang Lu, Meikang Qiu, and Bhavani Thuraisingham. "Deep residual learning-based enhanced JPEG compression in the Internet of Things." *IEEE Transactions on Industrial Informatics* 17, no. 3 (2020): 2124-2133.

[26] Alzubi, Jafar A., Ramachandran Manikandan, Omar A. Alzubi, Issa Qiqieh, Robbi Rahim, Deepak Gupta, and Ashish Khanna. "Hashed Needham Schroeder industrial IoT based cost optimized deep secured data transmission in cloud." *Measurement* 150 (2020): 107077.

[27] Yu, K., Tan, L., Mumtaz, S., Al-Rubaye, S., Al-Dulaimi, A., Bashir, A.K. and Khan, F.A., 2021. Securing critical infrastructures: deep-learning-based threat detection in IIoT. *IEEE Communications Magazine*, *59*(10), pp.76-82.

[28] Amjan Shaik, Bui Thanh Hung, Prasun Chakrabarti, Siva Shankar S and Nikhat Parveen,"A Novel Intelligent AI-based Security to Enhance the Data Communication: An Empirical Review", 2nd International Conference on Intelligent Systems & Sustainable Computing (ICISSC -2022), Malla Reddy University, Hyderabad, India.