Received on May 2020

Journal of Soft Computing and Engineering Applications

https://srkpublication.org/

A Proficient Chaos integrated Multi-Layer Perceptron Neural network (Chaos-MLPNN) model based Secured encryption and data Transmission Scheme in IoT

C. Raju[1*], A.P. Sherine[2]

[1]*Assistant Professor, Department of Electronics and Communication Engineering, Bannari Amman Institute of Technology, Sathyamangalam, Tamil Nadu, India*

[2]*Assistant Professor, Department of Electronics and Communication, CSI Institute of Technology, Thovalai, India*

[*]Corresponding author email: raju@bitsathy.ac.in

Abstract: Nowadays the life of people has been changed by the Information developers to improve the quality of living. On the contrary the diverse IoT devices and its classified data transferred over networks, origin grave security and confidentiality disputes. Hence, the rapid development of IoT in smart data processing and transmission comprehend us the necessity in developing a secured data transmission model. In this paper, we aimed to introduce a Chaos integrated Multi-Layer Perceptron Neural network (Chaos-MLPNN) model based Secured encryption and data Transmission Scheme in IoT. The conventional encryption and transmission scheme have the problem of key length, less reliability, computation complexity etc. Hence the parallel and dynamic characteristics of our proposed method will come up with encryption speed, security and overall efficiency with its non-periodic characteristics. Here, the recital flaws of Multi-Layer Perceptron Neural network encryption are optimised by the chaotic Multi Verse Optimization Algorithm. Finally, the experimental test analysis will ensure the reliability and efficiency of our approach in encrypting and securing the transmitted data through IoT.

Keywords: Internet of Things (IoT), Encryption, Multi-Layer Perceptron Neural network (MLPNN), Optimization Algorithm, Secured data Transmission

1. INTRODUCTION

At present, the usage of Internet of Things (IoT) devices has become a trend among researchers and corporate. Due its impact in human society by adopting lot of applications, over 26 billion IoT devices will be in use at the end of 2020 in varies sectors like government, business, medical applications, transportations, personnel gadgets etc [1].These IoTs allows all the things around us to interconnect over the internet without any human interventions either by using the wired or wireless networks based on the unique addressing scheme [2]. The communal acquaintance of IoT applications sturdily depends on its reliability and security of the data transmitted by the user [3]. But the data collected by these heterogeneous IoT applications are in greater risk by the hackers. Henceforth, many researchers have come up several solutions for this crisis but still the privacy and security of those resource limited IoT application has become an emerging challenge for all time [4, 5].

Encryption, Biometrics and Anonymity are the generally used approaches in securing the IoT information's in many applications. However, the techniques or algorithms used in this above (Encryption, Biometrics and Anonymity) process will also play a foremost part in the efficiency and reliability of the smart IoT devices [6].Cui et.al in [7] says that the simple cryptographic algorithms are used in the sensors and IoT devices with less computational power, pose serious threat to the heterogenic, scalable and dynamic IoT application systems. The security threat in IoT originates from the channels to which the IoT components are connected and then through protocols and then through network attacks, applications and Software's [8]. However, the technology advancement in mining and machine learning methods makes the attackers to think even smarter to surpass our security mechanism [9, 10].

All these above challenges motivated us to develop an efficient chaos integrated machine learning model for a secured encryption and data transmission in IoT in this paper. Here, the enactment blemishes of Multi-Layer Perceptron Neural network are optimized by the chaotic Multi Verse Optimization Algorithm by Sayed et al. in [11]. Encryption is carried out by introducing a new key and our proposed model's will be tested and analysed to delineate its potential in a secured data transmission. The rest of the paper is portrayed as follows: Section 2 describes the most recent research works related to IoT Security in short. Section 3 describes the process of our proposed Chaos-MLPNN model inlasting. Section 4 delineates the experimental test results and finally, the paper ends with the brief conclusion of our exertion.

2. RELATED WORK

Numerous research works interrelated to encrypting and securing the IoT data are proposed by varies research scholars, among them some of the most recent research works were reviewed here in this section.

Guan (2017) et al. in [12] has presented a parallel processing scheme of ciphertext and attribute-based encryption and data acquisition in this paper. To begin with, they have partitioned the data blocks and encrypted by its access subtree nilsequence, in order to have a parallel processing scheme.In addition, a secret sharing of threshold is followed to protect the access tree info's and finally the experimental analysis proves its efficiency in satisfying the security demands in a cloud-IoT grid system with less time and cost.

Elhoseny (2018) et al. in [13] has built a hybrid model to secure the medical image text data by integrating 2D-DWT-1L and 2D-DWT-2L with the encryption stratagem. The base of the hybrid model is from the conventional encryption standards and entire process starts with the encryption of secret data and the output was hidden based on the above discrete wavelet transforms. Finally, the experimental analysis was carried out based on six standard statistical parameters and its comparison with the state of art methods depicts its ability in securing the confidential medical data.

Luo (2020) et al. in [14] has proposed a communication protocol with a symmetric key to assist the resource consumption minimization with a light weight encryption for a secured data transmission process. The device which generates the symmetric keys and detects attack are deputized based on a logistic map chaotic system. Finally, the experimentation was done to analyze the security assets and to cross check the run time efficacy in comparison with the states of art methods.

Tahsien (2020) et al. in [15] has presented a survey on exploiting the machine learning technology to detect the miscellaneous behaviour of IoT smart devices. Here they have discussed the IoT architecture, possible attacks, State of art ML techniques and its part in IoT application. Finally, the survey paper concludes with the challenges present in enacting the ML techniques in securing the IoT applications.

Deebak (2020) et.al in [16] has proposed a routing and monitoring Authentication and Encryption (ATE) protocol Model to provide a flexible secured network. In this work, the adversaries in the sensor network are discovered by means of a multi-variant tuple using Two-Fish (TF) symmetric keys. Here, a hybrid routing protocol is developed by inheriting the properties of Multipath OLSR and AOMDV protocols. From the result analysis, it is evident that the proposed protocol model can outperform the other routing schemes.

Bu (2019) et al. in [17] has designed a model to securely share the sensitive info's through IoT. By using their scheme, they ensure the security of the sensitive information's based on the Threshold Secret Sharing (TSS) strategy by dividing the information's into multiple parts and warehoused among the diverse system devices. Hence, the data here can be retrieved, only with the presence of all devices only and still even after the identification of all the devices, the secret will be unidentifiable to the attackers.

Medileh (2020) et al. in [18] has presented a scalable Flexible encryption Technique (FlexenTech) to have a secured storage and data transmission in IoT. This suggested approach is apt for the resource constrained devices and networks and has the ability to defend common attacks with less encryption time. Finally, the performance is analyzed based on the confidentiality level for varies key sizes and achieves a computation time of about 9.7% when compared it with the literature rivals.

Received on May 2020

3. PROPOSED METHODOLOGY

3.1. Internet of Things (IoT)

The eminence of human life with more tactic can be accomplished barely with the aid of IoT in varies sectors for frequency identification, data transformation, management and identification process. The network Architecture of IoT is built up with seven layers and each layer has its own obligation to do during the transmission process. Mainly, here the identification of the physical world through data acquisition is performed by the sensing layer. Furthermore, the exchange of data in between the sender and receiver is carried out through the network layer and then the algorithm implementation, computation and its evaluation are done through the application layer.

In IoT, the data related to particular individual or a sector can be under threat all through the management platform. The data security in IoT is in need of cryptographic hardware device and authentication trot for timely feedback about the system status. In this paper, we aimed to introducing a Chaos integrated Multi-Layer Perceptron Neural network (Chaos-MLPNN) model based Secured encryption and data Transmission Scheme in IoT. Here, the encryption of data is done during the transmission and its major issue is the generation of key for every transaction, which plays a major part in the speed and the efficiency of the entire transmission process. Hence our proposed secured transmission scheme will offer a wide range practical sustenance, together with software appliance trial routines, system instatement, and troubleshoot all through the progressions of system maneuvers and system overhauls.

3.2. Chaos integrated Multi-Layer Perceptron Neural network (Chaos-MLPNN*)*

Chaos in the MLPNN is achieved by integrating the degrees of freedom and by the exchange of archives in between them. Figure 1 shows the chaotic MLPNN model, the foremost layer feeds the input to the network and then with multiple hidden neurons connected mutually to each other with inner $I_{j,i}$ neurons and retrieves the output from the other chaotic neurons. In this work the role of MLPNN is to simulate the chaotic Multi Verse Algorithm optimized weight-based origination of key in between the transmitter and the receiver by selecting the analogous hidden layer among all the available layers in MLPNN for every transmission. During this process all the other hidden layers will be inactive except the chosen one and the corresponding end product from the output layer will be the key for the particular transmission process. The hidden neurons in the MLPNN can be expressed as follows in equation (1).

$$Hl_j = 1/\sqrt{n}[\textstyle\sum_{i=1}^{n} w_{j,i} y_{j,i}] \tag{1}$$

where, Hl_j represents the hidden layer with 'n' number of neurons with $j = 1, \dots \dots . m$ and $i = 1, \dots \dots . n$. The output of the MLPNN hidden layer is expressed as follows in equation (2).

$$\partial_j = sgn\left(Hl_j\right) \tag{2}$$

The output of ∂_j will be +1 (Positive) for active layers and -1(negative) for the inactive layers correspondingly, hence the output of MLPNN will be the multiplicities of all the available hidden layers and it is expressed as follows in equation (3).

$$\delta = \textstyle\prod_{j=1}^{k} \partial_j \tag{3}$$

The output of the sender and the receiver MLPNN should be identical, only then their weight values should be updated for upcoming transmissions. i.e at the start of the MLPNN synchronization process, the weight vector is generated randomly by the Chaotic Multi verse optimization algorithm and after the exchange of communication bits (Optimal weight) by the sender and the receiver, the check of equivalence is done, if the bit value is not identical then we go for a learning rule as in equation (4).

$$w_{j,i}^{+} = p\left(w_{j,i} + x_{j,i}\tau\left(\delta_j \tau\right).\left(\tau^1\tau^2\right)\right) \tag{4}$$

To share a common structure, the synchronising rule is described as follows in equation (5).

$$w_{j,i}^{+} = p\left(w_{j,i} + g\left(\delta_j, \tau^1, \tau^2\right). x_{j,i}\right) \tag{5}$$

We assume that the weight distribution among the MLPNN layer will be $\delta_j x_{j,i} = +1$or $\delta_j x_{j,i} = -1$ or inequal based on the optimal weights obtained. During the synchronization process, the correlation among the MLPNN's can be defined by (2L+1) variables, the probability of determining the weights can be expressed as follows in equation (6).

$$Pb_{1,2}^{j} = Pb(w_{j,i}^{1} = a \wedge \ w_{j,i}^{2} = b \tag{6}$$

$$Pb_j^{1,2} = w_j^1 w_j^2 / \sqrt{w_j^1} w_j^1 \sqrt{w_j^2 w_j^2} = {r_j^{12}} \Big/ {\sqrt{q_j^1 q_j^2}} \tag{7}$$

After the synchronization process, the weight vector at both the sending and receiver side MLPNN will be identical and the active hidden layer output is utilized to generate the secret key. The hidden layer unit will be evaluated by using the following equation (8) and (9).

Received on May 2020

$$\delta_j = sgn\left[\sum_{i=1}^{n} w_{ji}\, x_{ji}\right] \qquad (8)$$

$$sgn(x) = \begin{cases} -1\ if\ x < 0, \\ 0\ if\ x = 0, \\ 1\ if\ x > 0, \end{cases} \qquad (9)$$

Generally, the layers of MLPNN are mathematically described as in equation (10).

$$L_j^{\rho} = \omega\left[\sum_{i=1}^{n} L_i^{(1)} w_{i,j}^{1} + w_{0,i}^{0}\right]; 1 \leq 0 \leq -1 \qquad (10)$$

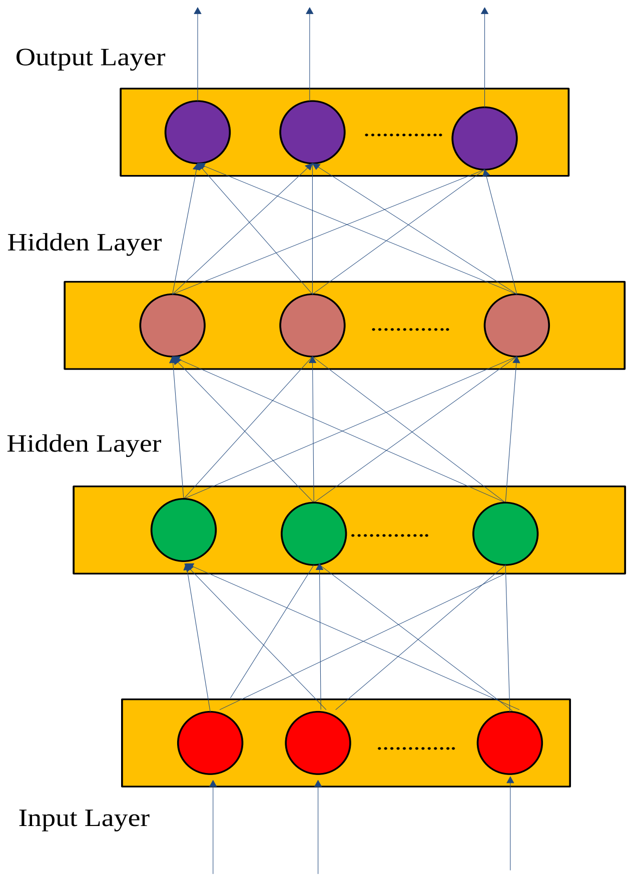

Figure 1 : Basic MLPNN

3.2.1. Chaotic Multiverse Optimization Algorithm (Chaotic-MVO)

The multiverse optimization algorithm (MVO) is a stochastic approach, in which the chaotic variables are presiding over computing the Travelling Distance Rate (TDR). The AC parameters here are fine-tuned by ten chaotic maps to enhance the convergence rate as well as the performance efficiency. The equation of TDR with Chaos is described in the following equation (11).

$$TDR_i = 1 - \left[{iter^{c_i}}\Big/{max_{iter}^{c_i}}\right]; c_i - value\ obtained\ by\ the\ chaotic\ map\ at\ ith\ iteration \qquad (11)$$

here, the feasible mechanism is employed to the standard MVO algorithm by generating four set of rules to achieve the best solution bybalancing the feasible and infeasible individuals.

1. Feasible solution is chosen even for infeasible solutions.
2. Violation of constraints by the infeasible solutions from 0.01-0.001 is considered as the feasible one.
3. More than one feasible solution means, then the solution with best objective will be chosen.
4. Among the infeasible solutions, the solution with fewer sums of violation constraints is considered as infeasible.

Henceforth , here maily based on the rule number 2 global optimization of the problem with high probability can be attained.

3.2.1.1.Steps followed by the Chaotic-MVO

- **Initialization:**The search space, position boundary, agents and number of iterations where initialized.
- **Fitness Evaluation:** For each iteration the position of search agent will be evaluated by using the fitness function and the solution with optimal position can only satisfy all the 4 rules.
- **Updation:** The position is updated by using the equations (11) and (12).

$$y_i^j = \left\{ y_i^j \begin{cases} y_j + TDR \times \left[\left(ub_j - lb_j\right) \times r_4 + lb_j\right) r_3 < 0.5;\ r_2 < WEP \\ y_j - TDR \times \left[\left(ub_j - lb_j\right) \times r_4 + lb_j\right) r_3 \geq 0.5\ ;r_2 \geq WEP \end{cases} \right. \qquad (12)$$

here, $r_2, r_3 and\ r_4$ are the random parameters (0-1) and constant parameter WEP represents the wormhole existence probability

- **Termination Criteria:**When the optimization process reaches its final iteration, then it reaches the stopping criteria.

3.3. Chaos-MLPNN based IoT Secured encryption and data Transmission Model

The frame work of the Secured encryption and data Transmission model is shown in the figure 2.Here the standard MVO is improved my means of the chaotic variables and utilized to determine the MLPNN weights. The Chaos integrated MLPNN encryption and transmission model starts by initializing the random solutions and search spaces and each will represents the weight bias of the MLPNN. The optimal solution obtained by equation (11) is utilized as thesecrect ket for the data transmission through the MLPNN network.

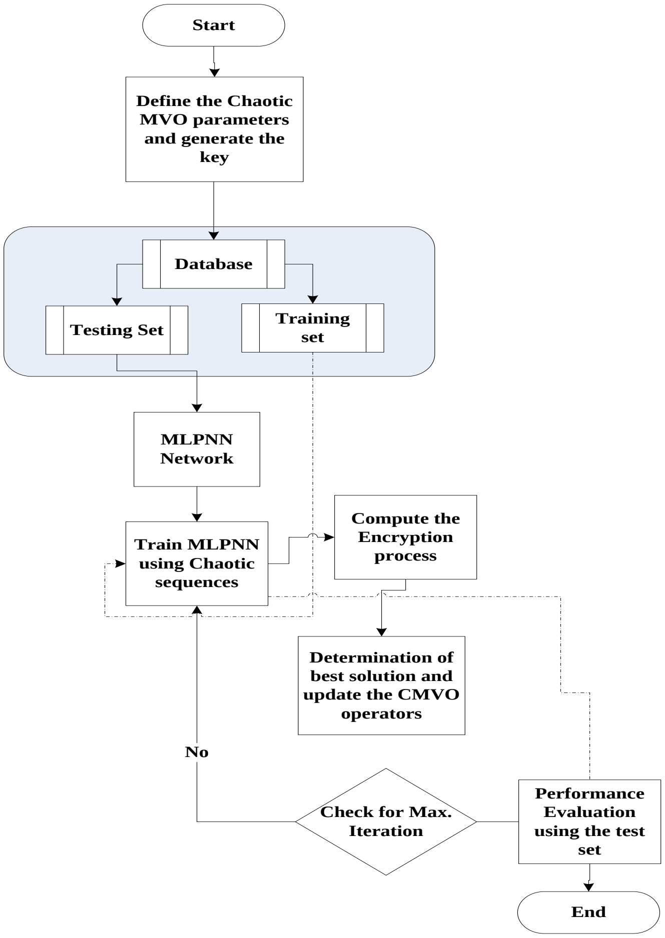
Start
Define the Chaotic MVO parameters and generate the key
Database
Testing Set
Training set
MLPNN Network
Train MLPNN using Chaotic sequences
Compute the Encryption process
Determination of best solution and update the CMVO operators
No
Check for Max. Iteration
Performance Evaluation using the test set
End

Figure 2: Proposed Flow Chart

The updation using equation (12) is done until it reaches the final termination criteria.In IoT, the network layer ensures the security by means of a secured encryption and reliable data transmission process. Here, the data to be transmitted is passed by the sensor to the chip of encryption to get the protocol based encrypted data and then return back right through the chip to the sensor. Then the data centre will collect those encrypted data and transfer it to the decryption server. The user will be having a unique secret key and it should be submitted for server authentication, if not the user cannot enter into the particular platform. The random Value generated by the network will be subdivided into two and our chaos integrated MLP neural network will go through these ranges with no repetition. So that the global search, the problem of local minima will get evaded. During the encryption process, the phases are considered as a set of blocks with n bits, $S = S_0S_1S_2 \ldots\ldots.S_{n-2}S_{n-1}$; $0 \leq i \leq n-1$ and the sub streams where XORed and generated correspondingly. Multiple blocks are preceded by 8 bits $(2^8 = 256\, blocks)$ to form interceded subkeys. These keys will be tiptoed into the encrypted data. The Key generated by the Chaos integrated MLPNN is XORed repeatedly with the cipher text until it reaches the termination criteria. The chaotic MLPNN model is a dynamic system with sensitive nervous system, so that the memory mock-ups can be identified with less differences is named as dynamic memory.

5. RESULT AND DISCUSSION

In this section, we evaluate the parallelly implemented performance of our proposed Chaos integrated Multi-Layer Perceptron Neural network (Chaos-MLPNN) model in securing the transmission process and about its computational and communication overheads. During the synchronization process, The MLPNN at the sender and the receiver side will be interrelated by means of the weight vectors. For every iteration, corresponding vectors are generated randomly and then later the output bits were communicated by both the sender and the receiver, if the bits are not matched then the authentication process will get failed. For analyzing our suggested strategy, we have considered 10 files of dissimilar sizes from 2546 bytes - 3658475 bytes. In figure 3, the encryption time achieved by our proposed approach in comparison with the others is illustrated. It is clearly deliberated that the time taken to encrypt the data by the proposed approach is lesser than the other encryption techniques. The security analysis of our proposed approach in comparison with the others is shown in table 1.

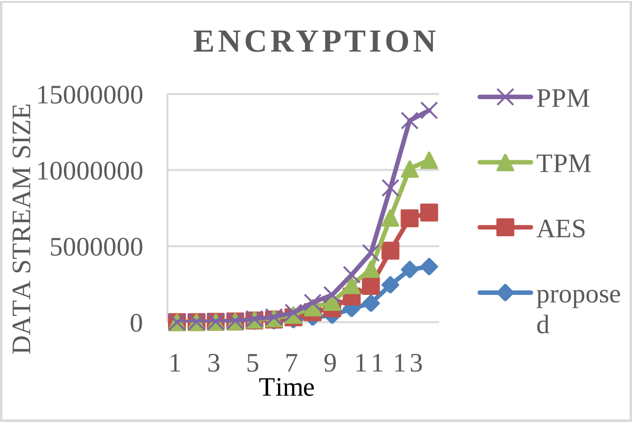

Figure 3: Encryption Time Analysis

Table 2: Secured Transmission Comparison

Method of	Mutual Authentication	Privacy	Data Integrity	Security	End-to End Security
Saeed et.al in [23]	Y	N	Y	Y	Y
Liu et.al in [19]	Y	N	Y	N	Y
Xiong et.al in [20]	Y	N	Y	Y	Y
Wang et.al in [25]	Y	N	Y	Y	Y
Proposed	Y	Y	Y	Y	Y

In Figure 4 and 5, the communication overhead analysis with respect to the Number of IoT devices is represented. From the analysis, it is clear that our proposed approach outperforms the conventional encryption and security strategies. Increase in IoT devices increases the computation overhead. The security problems of the conventional neural networks will be overcome by our proposed Chaos integrated MLPNN and it has low significant overhead for IoT devices. The overheads for 90%, 60% and 40% of IoT devices are shown in figure 5 has better performance for a greater number of IoT devices.

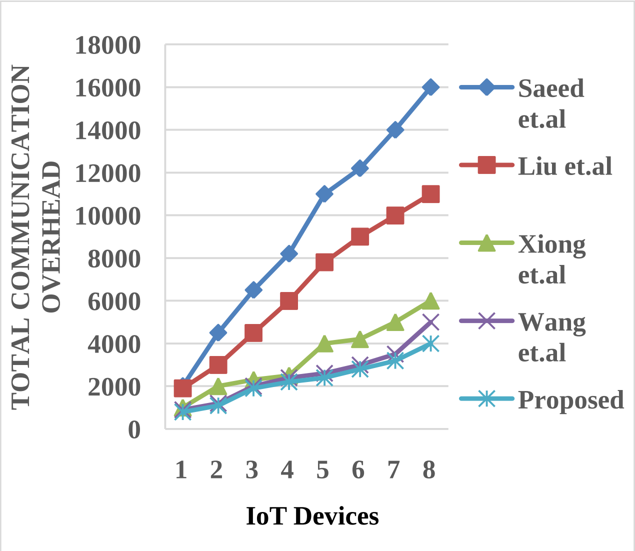

Figure 4: Communication Overhead Vs IoT Devices

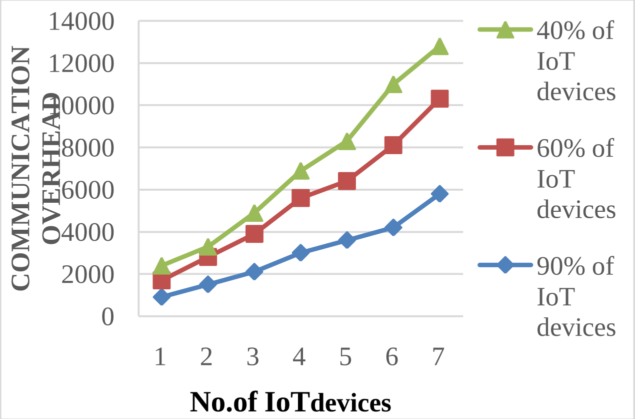

Figure 5: Communication Overhead analysis over diverse number of IoT devices

6. CONCLUSION

In this paper we present a Chaos integrated Multi-Layer Perceptron Neural network (Chaos-MLPNN) model based Secured encryption and data Transmission Scheme in IoT. The security here is improved by means of a Chaotic MVO-MLPNN based secret key exchange strategy and by its parallel diligence. The weights of the MLPNN are the secret key used here for encryption and the chaotic MVO algorithm integrated with the MLPNN is utilized here to get an Optimal weight vector. The performance of our approach is evaluated based on the its encryption time and communication overheads and the authentication model here ensures the flexible and efficient secured data transmission than that of the conventional scheme in [19-22].

7. REFERENCES

[1] O. Arias, J. Wurm, K. Hoang, and Y. Jin. **Privacy and security in internet of things and wearable devices**. *IEEE Transactions on Multi-Scale Computing Systems* Vol. 1, no. 2, 99-109, 2015.

[2] H. Atlam, W. Robert, and G. Wills. **Internet of Things: state-of-the-art, challenges, applications, and open issues.** *International Journal of Intelligent Computing Research (IJICR)* Vol.9, no. 3, 928-938, 2018.

[3] M. Al Ameen, J. Liu, and K. Kwak. **Security and privacy issues in wireless sensor networks for healthcare applications.** *Journal of medical systems* Vol. 36, no. 1, 93-101, 2012.

[4] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao. **A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications.** *IEEE Internet of Things Journal*,Vol. 4, no. 5, 1125-1142, 2017.

[5] S. Sicari, R. Alessandra, L. Alfredo Grieco, and A. Coen-Porisini. **Security, privacy and trust in**

Internet of Things: The road ahead. *Computer networks* Vol.76 , 146-164, 2015.

[6] M.C. Chuang, and M. C. Chen. **An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics.** *Expert Systems with Applications* Vol. 41, no. 4 ,1411-1418, 2014.

[7] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang. **Security and privacy in smart cities: Challenges and opportunities**. *IEEE access* Vol. 6 ,46134-46145, 2018.

[8] N. Chaabouni, M. Mohamed , A. Zemmari, C. Sauvignac, and P. Faruki. **Network intrusion detection for IoT security based on learning techniques**. *IEEE Communications Surveys & Tutorials* Vol.21, no. 3 , 2671-2701, 2019.

[9] Y. He, Y. Gihan, J. Mendis, and J. Wei. **Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism**. *IEEE Transactions on Smart Grid* Vol.8, no. 5 , 2505-2516, 2017.

[10] I. Corona, G. Giorgio, and F. Roli. **Adversarial attacks against intrusion detection systems: Taxonomy, solutions and open issues.** *Information Sciences* Vol.239 ,201-225, 2013.

[11] G. Sayed Ismail, A. Darwish, and A. Ella Hassanien. **A new chaotic multi-verse optimization algorithm for solving engineering optimization problems.** *Journal of Experimental & Theoretical Artificial Intelligence* Vol. 30, no. 2 ,293-317, 2018.

[12] Z. Guan, J. Li, L. Wu, Y. Zhang, J. Wu, and X. Du. **Achieving efficient and secure data acquisition for cloud-supported internet of things in smart grid**. *IEEE Internet of Things Journal* Vol. 4, no. 6 , 1934-1944, 2017.

[13] M. Elhoseny, G. Ramírez-González, M. Osama, A. Elnasr, A. Shihab, N. Arunkumar, and A. Farouk. **Secure medical data transmission model for IoT-based healthcare systems**. *Ieee Access* Vol. 6 ,20596-20608, 2018.

[14] X. Luo, L. Yin, C. Li, C. Wang, F. Fang, C. Zhu, and Z. Tian. **A Lightweight Privacy-Preserving Communication Protocol for Heterogeneous IoT Environment.** *IEEE Access* Vol. 8 ,67192-67204, 2020.

[15] M. Tahsien Syeda, H. Karimipour, and P. Spachos. **Machine learning based solutions for security of Internet of Things (IoT): A survey**. *Journal of Network and Computer Applications* ,102630, 2020.

[16] D.. Deebak, and F. Al-Turjman. **A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks**. *Ad Hoc Networks* Vol.97 ,102022, 2020.

[17] L. Bu, M. Isakov, and M. A. Kinsy. **A secure and robust scheme for sharing confidential information in IoT systems.** *Ad Hoc Networks* Vol. 92 , 101762, 2019.

[18] S. Medileh, A. Laouid, E. B. Nagoudi, R. Euler, A. Bounceur, M. Hammoudeh, M. AlShaikh, A. Eleyan, and O. A. Khashan. **A Flexible Encryption Technique for the Internet of Things Environment**. *Ad Hoc Networks* ,102240, 2020.

[19] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, **Certificateless remoteanonymous authentication schemes for wirelessbody area networks**,*IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 332–342, 2014.

[20] M. E. S. Saeed, Q. Liu, G. Tian, B. Gao, and F. Li, **Remote authentication schemes for wireless body area networks based on the Internetof Things**, *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4926–4944, 2018.

[21] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, **Certificateless remoteanonymous authentication schemes for wirelessbody area networks**, *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 332–342, 2014.

[22] C. Wang and Y. Zhang, **New authentication scheme for wireless bodyarea networks using the bilinear pairing**, *J. Med. Syst.*, vol. 39, no. 11,p. 136, 2015.