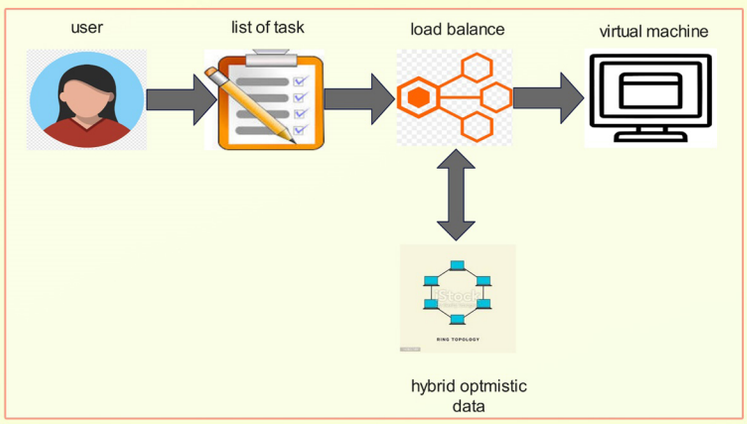
Volume 01, Number 01, 2023

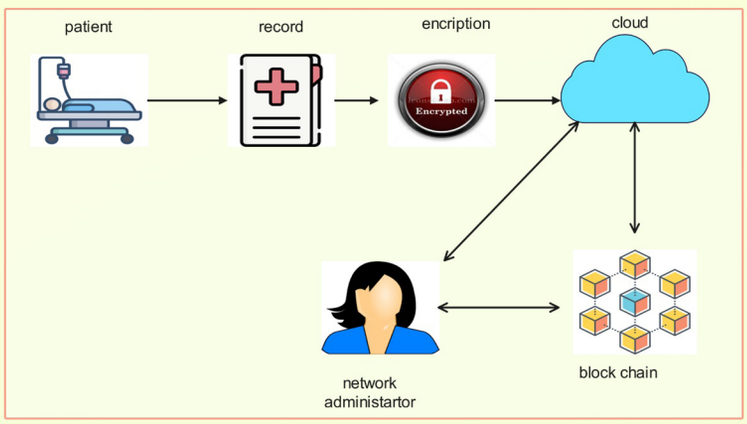
KITS PRESS
For the Research

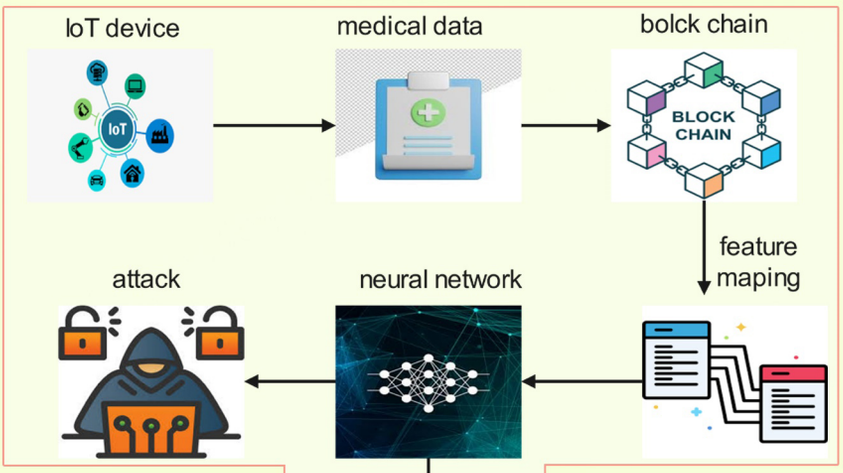
IJCEO

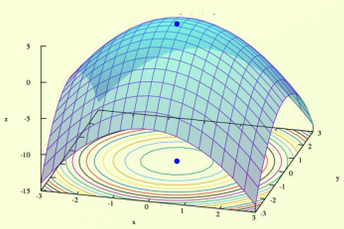
ISSN : XXXX-XXXX

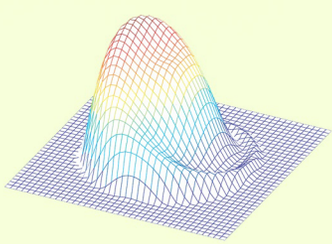
International Journal of Computer and Engineering Optimization

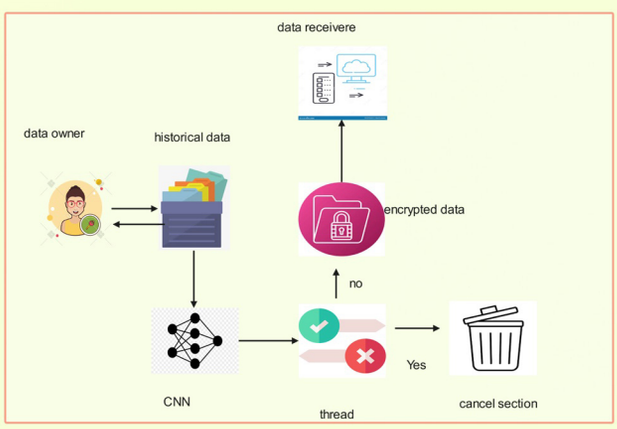


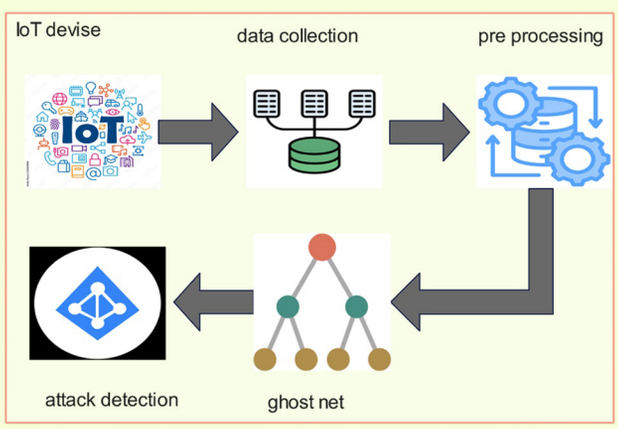












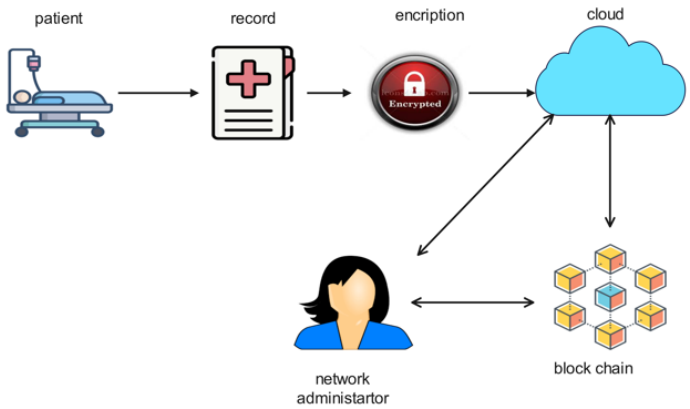
International Journal of Computer and Engineering Optimization

(IJCEO)

1. BLOCK CHAIN ASSISTED CLOUD BASED MEDICAL DATA STORAGE VIA QUANTUM DIFFIE-HELLMAN KEY EXCHANGE

G. Sreetha, T. V. Chitra

Abstract – Electronic Health Records (EHR) security ensures the confidentiality of patients' information and guarantees healthcare providers' accountability. Sharing such medical records with third party through an unsecure channel may be abused or disclosed to other unauthorized parties. Therefore, there is a rising need for a novel technology, which allows for outsourcing the data through an unsecure channel while preserving the privacy of EHR. In this paper, a novel Block chain Assisted Cloud based Key exchange (BACK) technique has been introduced, that uses blockchain technology for secure data transmission. The proposed method uses the novel secure Quantum Diffie Hellman key exchange (QDHKE) system for sharing the key in an unsecure environment. The BACK methodology helps in sharing the medical data through unsecure channel while maintaining the confidentiality and privacy of health information. The proposed method has been evaluated using CloudSim simulator. The efficiency of the technique has been assessed in terms of particulars like the time it takes to encrypt, decode, and execute and computational cost. According to the experimental results, the proposed BACK method achieves less encryption time of 12.5%, 7.4%, and 4.65% than existing techniques such as Healthchain, Blockchain integrated with IPFS, and Blockchain-based FL respectively.

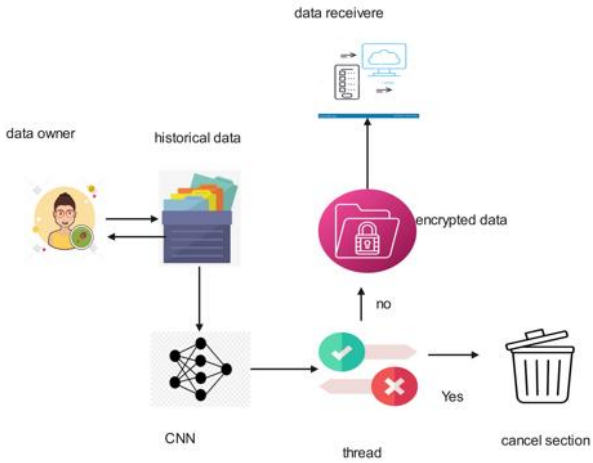


Keywords – *Medical data security, blockchain, Key exchange, Quantum Diffie-Hellman.*

2. DEEP LEARNING BASED AUTHENTICATION SECURE DATA STORING IN CLOUD COMPUTING

M. Prabhu, G. Revathy, R. Raja Kumar

Abstract – To communicate organizationally important data among working units in a federated cloud environment, secure mutual authentication is a crucial necessity. The administration of data while preserving its usefulness and security system is a worry for the cloud owner. Cloud data sharing is becoming more and more popular as a viable way to give people simple access to data. supported by positive advances in cloud technology. Yet, as more businesses and customers store their data on cloud servers, it poses a growing threat to user privacy and data security. People are inclined to encrypt information before sending it to the cloud in order to ensure its confidentiality. Yet the data processing has gotten challenging due to broad encryption methods. In order This paper provides a novel mutual authentication mechanism that combines deep learning-based recognition and control of security breaches to enable secure communication between participating entities. Convolutional Neural Networks (CNN) for online threat detection with RSA Cryptography and Schnarr's signature scheme-based public-key encryption technologies. A network intrusion dataset from the Canadian Institute for UNSW-NB15 is used to measure performance, and the AVISPA security analysis tool confirms its effectiveness in comparison to other methods in terms of security features and communication costs.

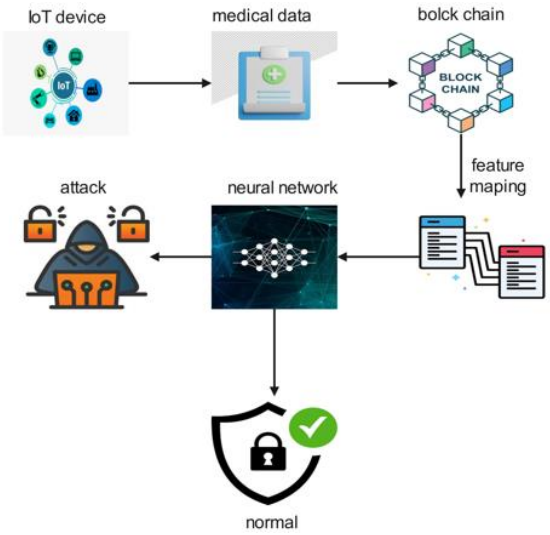


Keywords – RSA cryptography; mutual authentication; AVISPA security analysis, Schnorr signature; Convolutional neural networks (CNN), threat, encrypted data

3. SECURE BLOCKCHAIN BASED DEEP LEARNING APPROACH FOR DATA TRANSMISSION IN IOT-ENABLED HEALTHCARE SYSTEM

R.R. Sathiya, S. Rajakumar, J. Sathiamoorthy

Abstract – Healthcare service quality has been improved by integrating the Internet of Things (IoT) with conventional medical networks. In contrast, device-mounted sensors and wearables employed in Healthcare Systems (HS) monitoring and data transmission ongoing over unprotected open channels to adjacent devices. The effectiveness of operations is being improved by the link among IoT devices and computers, yet it allows attackers to commit a variety of cyber-attacks that could jeopardize patients under vital observation. Using Deep-BiLSTM in a healthcare IoT system for Secure Data Transmission is presented in this paper. In particular, the first unique there is a suggested blockchain design that assure data security and reliability transfer through the use of the Zero Knowledge Proof (ZKP) mechanism. The validated data is then utilized to create a deep learning framework for identification of intrusions in the HS network. A Bidirectional Long Short-Term Memory (BiLSTM) and Deep Convolutional Neural Network (DCNN) are integrated to create a highly efficient intrusion detection method. experiments using two sources of open data (CICIDS-2017 and ToN-IoT) has been used to compare the proposed method with 96% better performance. The suggested BD-BiLSTM methodology has 98% precision, accuracy, recall, and F1 score, which is pretty high when compared to other approaches. of BDL-SMDTA, PBDL and GWMNN.

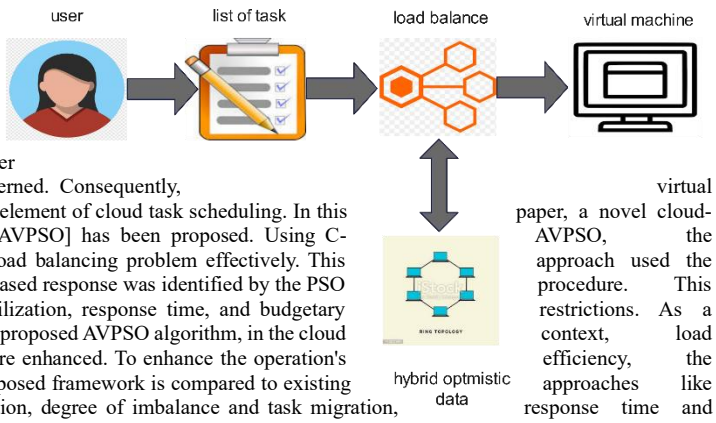


Keywords– Internet of things, health care system, cyber-attack, deep-BILSTM, Zero knowledge proof mechanism (ZKP), deep convolutional neural network

4. C-AVPSO: DYNAMIC LOAD BALANCING USING AFRICAN VULTURE PARTICLE SWARM OPTIMIZATION

Dharavath Champla, V. Ramkumar, P. Ajay

Abstract – A new technology called cloud computing enables users to access services from anywhere, at any time, under different conditions, and is controlled through an outside cloud service provider. Cloud task scheduling is a complicated optimisation problem. However, both under- and over-loading conditions cause a range of system problems as far as power consumption, machine failures, and so forth are concerned. Consequently, virtual machine (VM) work-load balancing is regarded as a key element of cloud task scheduling. In this paper, a novel cloud-based African vulture particle swarm optimisation [C-AVPSO] has been proposed. Using C-AVPSO, the developed optimization algorithm solves the dynamic load balancing problem effectively. This approach used the AVO process to get the exploration space, while the increased response was identified by the PSO procedure. This algorithm successfully addresses the task's resource utilization, response time, and budgetary restrictions. As a result of combining the AVO and PSO algorithms into the proposed AVPSO algorithm, in the cloud context, load balancing performance measures and convergence rate are enhanced. To enhance the operation's efficiency, the proposed method balances VM loads efficiently. The proposed framework is compared to existing approaches like QMPSO, FIMPSO and ACSO Based on energy utilization, degree of imbalance and task migration, response time and resource utilization. The proposed C-AVPSO technique reduces resource utilization of 19.1%, 31%, and 54% than, QMPSO, FIMPSO and ACSO existing techniques.

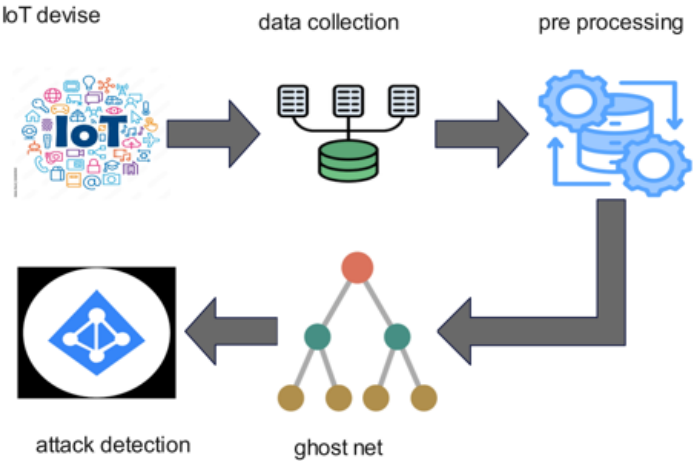


Keywords –DYNAMIC Load Balancing, swarm optimization, PSO algorithm, Virtual machine, Cloud computing.

5. INTRUSION DETECTION ARCHITECTURE (IDA) IN IOT BASED SECURITY SYSTEM

M. Amanullakhan, M. Usha, S. Ramesh

Abstract – Through the use of billions of data points, the internet of things (IOT) links billions of objects to the internet, all of which require security. A major issue for cyber security is the expanded attack surface of IOT. To overcome these challenges, Intrusion Detection Architecture (IDA) has been proposed in this paper, which helps to trace the Intrusion Data in IOT. The proposed Intrusion Detection Architecture (IDA) is performed in three stages namely, Data Collection, Pre-processing in Data encoding and Classification block. Initially, the request from the IOT devices is sent to the Data collection (DC) and pre-processing stage there it could find the amount of data. The collected data traces and filter through the Normalization Technique (NT). Then the filtered data goes to the data encoding block. After the encoded data goes to classification block here it classifies the data by Ghost Net technique and finally the attack can be classified and detected. The effectiveness of the suggested IDA strategy has been assessed using assessment measures such as configuration latency, detection rate, accuracy, precision, recall rate, false detection rate. The proposed method reduces the communication overhead of 75%, 50% and 38% than SSTS, ANT and FPDS existing techniques.



Keywords – IoT, Intrusion detection, Cyber security, Data encoding, Ghost Net technique.

International Journal of Computer and Engineering Optimization (IJCEO)
Volume 1, Issue 1, September – October (2023)

RESEARCH ARTICLE

BLOCK CHAIN ASSISTED CLOUD BASED MEDICAL DATA STORAGE VIA QUANTUM DIFFIE-HELLMAN KEY EXCHANGE

G. Sreetha[1, *] and T. V. Chitra[2]

[1]Department of Computer Science and Engineering, Arunachala College of Engineering for Women, Manavilai, Tamilnadu, India.

[2]Department of Computer Science and Engineering, Arunachala College of Engineering for women, Manavilai, Tamilnadu, India.

[*]*Corresponding e-mail: sreethasree2000@gmail.com*

Abstract – Electronic Health Records (EHR) security ensures the confidentiality of patients' information and guarantees healthcare providers' accountability. Sharing such medical records with third party through an unsecure channel may be abused or disclosed to other unauthorized parties. Therefore, there is a rising need for a novel technology, which allows for outsourcing the data through an unsecure channel while preserving the privacy of EHR. In this paper, a novel Block chain Assisted Cloud based Key exchange (BACK) technique has been introduced, that uses blockchain technology for secure data transmission. The proposed method uses the novel secure Quantum Diffie Hellman key exchange (QDHKE) system for sharing the key in an unsecure environment. The BACK methodology helps in sharing the medical data through unsecure channel while maintaining the confidentiality and privacy of health information. The proposed method has been evaluated using CloudSim simulator. The efficiency of the technique has been assessed in terms of particulars like the time it takes to encrypt, decode, and execute and computational cost. According to the experimental results, the proposed BACK method achieves less encryption time of 12.5%, 7.4%, and 4.65% than existing techniques such as Healthchain, Blockchain integrated with IPFS, and Blockchain-based FL respectively.

Keywords *– Medical data security, blockchain, Key exchange, Quantum Diffie-Hellman.*

1. INTRODUCTION

The vast volume of medical data must be shared in order to increase medical knowledge and is a crucial tool for documenting patient information for therapy [1]. However, under the previous approach, each healthcare system had its own set of medical servers where it kept all of the data linked to health. Traditional Electronic Health Records (EHR) systems sometimes have a single point of failure since they are centralized [2-6]. The emergence of block chain technology has led to the creation of a creative solution to this issue, because it has the properties like anonymity, decentralization, and immutability [7-12]. All EHRs must be maintained on a blockchain, which is difficult because of the expenditure and size [13]. The most practical option for obtaining this kind of data and resolving these problems is cloud computing [14-17].

Cloud computing provides various services where, data outsourcing is one of those important services. This service enables users to outsource their data to one or more database service providers and grant authorized clients getting into the data. The security of outsourced data is one of the primary issues in outsourcing [18-20]. If EHR security has been compromised, patient personal information may be exposed, resulting in major issues.

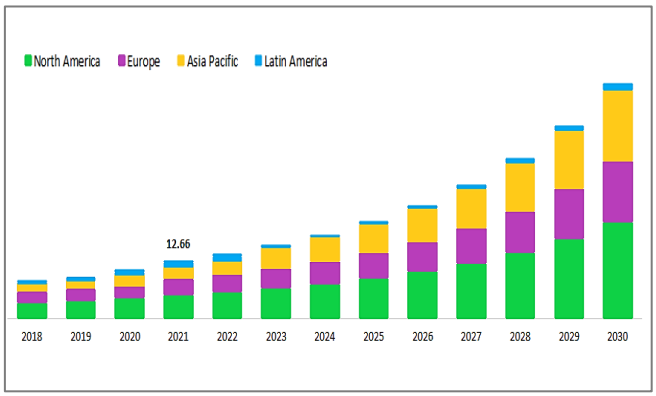


Figure 1. Statistics of medical data cyberattacks

According to the Centre for Strategic and foreign Studies, the US Cybersecurity and Infrastructure Security Agency (CISA) recognized Conti ransomware in over 400 assaults against US and foreign organizations in September 2021, as indicated in Figure 1. Therefore, to address the privacy concerns, a novel Block chain Assisted Cloud based Key exchange (BACK) technique has been introduced in this paper, which allows for data outsourcing through unsecure channel and also enhances privacy and security of medical data. The main objectives of the suggested BACK technique are given as below.

- Initially, the sensor data will be gathered from the victim in the form of EHR and provided to the medical center (MC) for diagnosis.
- For outsourcing the data to other MC's, the MC and patients will register themselves in the cloud as an authorized user by providing their identities with the help of network administrator (NA).
- For uploading the data, the MC will encrypt the data using homomorphic encryption and stored it in the cloud and a transaction data log will be created in the blockchain.
- For accessing the data, the user connects with the network administrator and the medical centre over public channels, and his or her identification is verified. After verification, the key will be exchanged using QDHKE, which preserves the security of the data in an unsecure environment.
- The effectiveness of the suggested method has been assessed based on certain metrics, including the execution, decryption, and encryption times.

This corresponds to the manner in which the remainder of the paper was written. Section 2 provides an overview of the literature review for secure medical data sharing. Section 3 describes the BACK methodology in detail. Section 4 describes the particulars of the experiment's execution and outcomes. The planned work's conclusion and future directions are covered in Section 5.

2. LITERATURE REVIEW

Medical EHR data sharing has been considered as the crucial thing during data outsourcing, because the privacy of medical data is necessary. Therefore, many researchers have concentrated on secure data sharing and provided many solutions for data security. This section discusses several works that use cloud and blockchain technology to share EHR.

In 2019, Niu, J., et al [21] suggested a blockchain-based attribute cryptosystem-based medical data exchange system. The analysis outcomes demonstrated that the suggested technique provides better computing performance than other similar techniques and meets the confidentiality and falsifiability requirements of the random Oracle model. This is a negative because the steps for mutual authentication and session key negotiation are not covered.

In 2020, Chenthara, et al [22] proposed a completely new clinical chain model that guarantees the integrity, scalability, and security of electronic health records. founded on the blockchain. According to the experimental results, the proposed methodology provides higher data security and data integrity amidst permitting all parties involved in the medical chain system to share and access medical records The main flaw is that once implemented, many customers who register for verification will share their information with other parties in an unreliable manner.

In 2021, Zaabar, B., et al [23] offered a novel architecture that gets around the issue of centralized storage by using a distributed database. Results of performance evaluation and comparative analysis of Hyperledger Caliper have demonstrated the superiority of various throughput and latency metrics, blockchain-based healthcare systems must be robust with regards to privacy and security requirements. This system's drawback is that it is unable to ensure perfect forward secrecy.

In 2022, Jayabalan, J. and Jeyanthi, N., [24] introduced a blockchain-oriented model connected to IPFS for electronic medical databases in health care. According to the experimental results, the suggested off-chain healthcare information storage approach using IPFS shields the blockchain architecture from scalability problems. The disadvantages were that they could not ensure data integrity or provide fine-grained access control to medical information.

In 2022, Singh, M.B. and Pratap, A., [25] proposed a secure privacy-preserving architecture in smart healthcare using a blockchain-based IoT cloud platform and federated learning (FL). Using this technique, customers can obtain fully built machine learning models without storing private data on cloud servers. The drawback is that the proposed work is not suitable for real-world environments.

In 2023, Adeniyi, A.E. et al. [26] created a altered AES algorithm to protect patient health information by changing the final cycle of AES. In terms of encryption time, modified AES exceeds the AES algorithm, with regards to decryption time; AES performs better than modified AES. However, this cannot minimize the amount of computation any further.

In 2023, Gupta, I. et al. [27] created a safe, efficient, and privacy-preserving communication model (SeCoM) for the preservation of medical data Experiments demonstrate that it enhances privacy protection, detection efficiency, and data utilization by up to 9.49%, 83%, and 43.25%, respectively. The temporal complexity of this procedure is its downside.

The above reviewed methods were helpful in sharing the data securely. However, these methods possess some drawbacks that were discussed above. In order to overcome these drawbacks, a novel Block chain Assisted Cloud based Key exchange (BACK) technique has been introduced in this paper, which is discussed in section 3.

3. BLOCK CHAIN ASSISTED CLOUD BASED KEY EXCHANGE MECHANISM

In this section a novel Block chain Assisted Cloud based Key exchange (BACK) technique has been introduced which allows for data outsourcing through an unsecure channel and also enhances privacy and security of medical data. Registration phase, authentication phase, and storage phase are the three phases of the proposed BACK technique. Initially, the sensor data will be obtained from the patient's electronic health record and provided to the medical center (MC) for diagnosis. For outsourcing the data to other MC's, the MC and patients will register themselves in the cloud as an authorized user by providing their identities with the help of network administrator (NA). For uploading the data, the MC will encrypt the data using homomorphic encryption and stored it in the cloud and a transaction data log will be created in the blockchain. For

accessing the data, the user connects with the network administrator and the medical centre over public channels, and his or her identification is verified. After verification, the key will be exchanged using QDHKE, which preserves the security of the data in an unsecure environment. The architecture of the proposed BACK technique is given in figure 2.

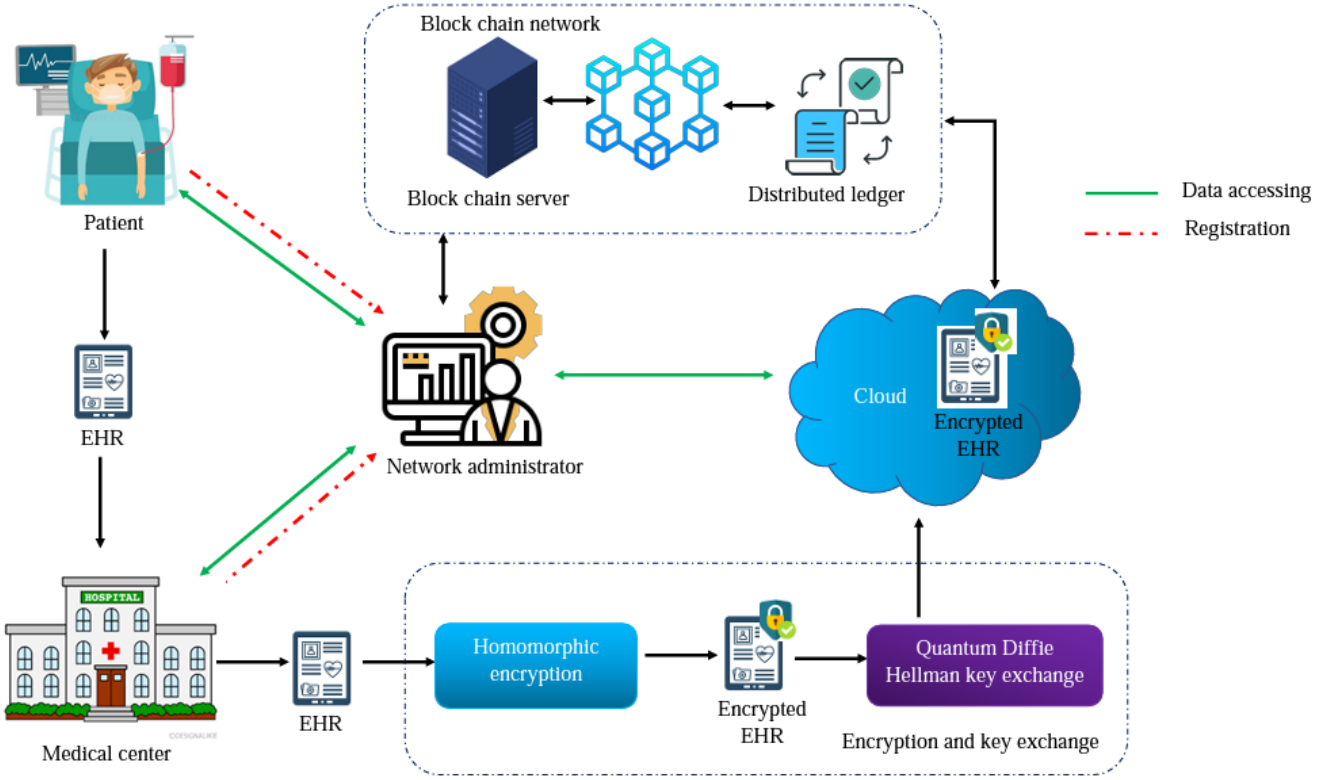


Figure 2. BACK architecture

3.1. Registration Phase

Initially, the patient will come to MC and the medical devices such as ECG, EEG will be connected to the person and the data will be collected by the doctor in the form of EHR. After acquisition, for uploading and accessing the data from the cloud needs registration. Therefore, the patient and MC should register themselves as the authorised users in the cloud with the help of network administrator.

3.1.1 Patient Registration

The patient (p_a) must register his or her identify with the network administrator in order to receive the medical diagnostic. The NA will assist the patient in registering his or her public and private keys, which will be done via a secure connection. The registration for patient has been shown in figure 3.

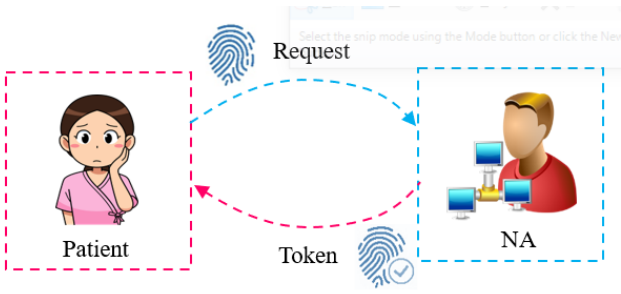


Figure 3. Patient registration

Step 1: p_a request NA for registration and send their biometrics for storage

Step 2: NA computes their biometrics and send a token p_t to p_a for future reference.

3.1.2. Medical centre registration phase

To communicate data from various healthcare centres, medical centres must first register with the network administrator, and the process is shown in figure 4.

Step 1: MC selects ID and transmits the unique identify to NA through protected medium.

Step 2:NA computes ID and stores ID in database. The NA sends token M_t to MC viva secure channel.

Step 3: MC save M_t in his database for future communication system.

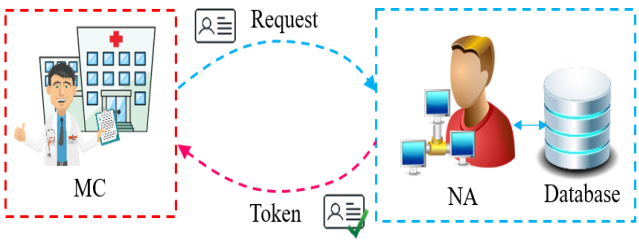


Figure 4. MC registration

3.2 Storage Phase

After registration, the medical centre generates encrypted EHR using homomorphic encryption for preserving privacy of the data and stores EHR in Cloud Storage.

3.2.1. Homomorphic encryption

The algorithms that make up the public-key, homomorphic encryption method that we employ are as follows:

- KeyGen (parms) produces a public evaluation key (evk) and a public/private key pair (pk, sk). When the parms system parameter is supplied, both of them are used in homomorphic multiplication.
- Encryption algorithm Enc(pk,m). Plaintext m should be encrypted with public key pk.
- Dec(sk,c) is a decryption algorithm that uses private key sk to decode ciphertext c.
- Given the input encryptions c1 and c2 of m1 and m2, the homomorphic addition operation Add (c1, c2) generates a cipher text that encrypts the total of m1 and m2.
- • Mult (c1, c2) is a homomorphic multiplication function that, assuming the encryptions c1 and c2 of m1 and m2, generates cipher text which encrypts the m1 + m2 result.

3.2.2. Quantum Diffie-Hellman key exchange

For exchanging the key for decrypting the EHR, a revolutionary physics-based quantum DH protocol (abbreviated as qDH) has been used which will be thoroughly explained. A quantum state in the qDH protocol will be the equivalent of the final key in the traditional DH protocol. In the lines that follow, the qDH protocol's requirements are detailed.

Suppose there are two communication parties, X and Y, that can exchange qubits. Each of the parties X and Y has a set of secret values that are designated by the letters SX and SY, respectively. These fixed secrets will be used to create shared, secret states for X and Y during the key exchange mechanism.

The initial secrets contained in SX and SY are retained stored by X and Y, respectively, while these created secret states are considered to be ephemeral ones.

Both sides must have agreed on a predetermined SP of shared, publically available information prior to the qDH communication. Since qDH takes into account quantum states and their two operations, SP contains state information of an initial, common state. |0i will be used to indicate it.

Thus, SP = |0i,..., where "..." denotes the presence of additional, shared, and publicly available information, which is optional. Given that the initial state |0i is shared or known to the public, X and Y must be able to prepare such a precise state.

Any operation for X and Y must therefore have a mutually known state as its starting point. In addition, the sets SX, SY, and SP result in the respective individual unitary operators U(SX), U(SY), and U(SP). Later, concrete illustrations of SX, SY, SP and their respective unitary operations will be shown. It is first demonstrated how the general qDH scheme is composed of:

- Party X creates a qubit state |0i according to the information supplied and made accessible to the public by SP. Then, depending on the secrets of set SX, X transmits a qubit |Xi=U(SX)|0i to Y, where U(SX) is a unitary operator.Depending on the secrets of set SY.
- Party Y receives |Ai and alters it using its own unitary operator U(SY). This leads to the equation |YAi=U(SY)|Xi.Y now follows the same procedures that X did in the first two steps.
- A qubit state |0i is created by Y according to the shared, accessible information SP. A qubit |Yi= U(SY)|0i is sent from Y to X.
- Party X receives $|\psi Yi$ and modifies that state by with U(SX), and unitary U(SP). This results in $|\psi XYi := U(SP)U(SX)|\psi Yi.$ Both communication parties are now in possession of the following states: $|\psi XYi$ (for X at the end of step 4) and $|\psi YXi$ (for Y at the end of step 2).

We now require, that $U(SP)U(SX)U(SY) = U(SY)U(SX)$. (1) Given that constraint for U(SX), U(SY), and U(SP), one has $|\psi XYi = |\psi YXi$, (2) and as a result, despite never having sent these final states and without being aware of each other's set of secrets, both X and Y are in possession of identical quantum states. Figure 5 illustrates such idea.

Actions taken on the side of X are represented, X. similar to the Y as the heading. The quantum states sent and their direction of transmission are shown in the "quantum channel" column. The following gives a straightforward illustration of SX, SY, SP, and their corresponding unitary operators.

3.3 Authentication Phase

When a new user wants to access to the EHR, he will be authenticated. Patient and MC communicate with NA and, he will start the authentication process in the public channel. After authorization, the key will be exchanged. The process for authorization has been given as follows.

Step 1: p_t and MC login with their token, ID and biometric.

Step 2: NA verifies the token T and biometric by comparing it with their data and aborts if not the authenticated one.

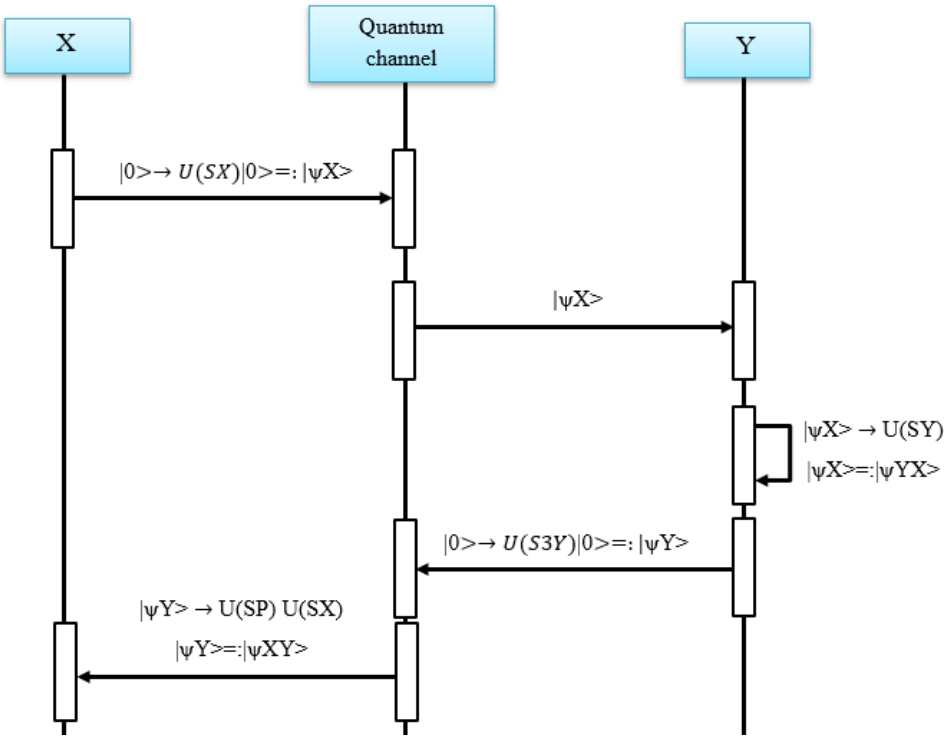


Figure 5. Working of Quantum Diffie Hellman key exchange

3.4 *Uploading data-log in blockchain*

The cloud server computes access rate of the user, transaction histories, and creates a data log, and uploads it to the blockchain. The data is finally stored in the cloud server's database. Each blocks contain the details of previous value, hash function and the data, which is represented in figure 6. Blockchain makes the proposed BACK system secure, because it is immutable and it is transparent. So, there will be no cheating among the users and the data will be more secure.

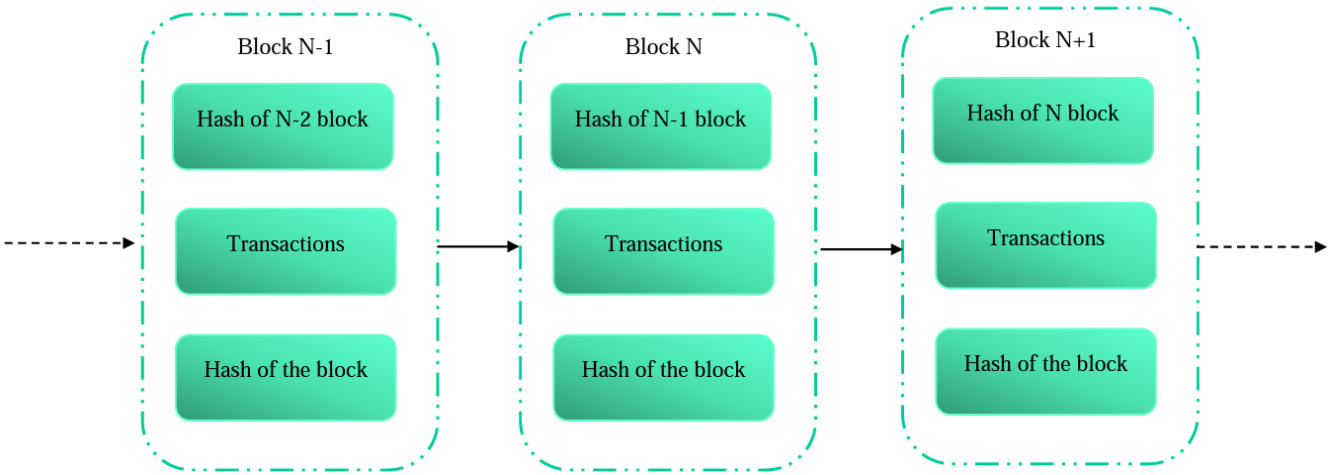


Figure 6. Blockchain mechanism of data storing

4. RESULTS AND DISCUSSION

The data upload procedure, access control mechanism, and encryption technology discussed in the previous part are all included in the method suggested in this article. This paper conducts Histogram analysis, and comparison analysis in terms of encryption time, decryption time, execution cost and security strength with previous work. Aiming to evaluate and validate the proposed novel BACK technique, the proposed scheme has been implemented on cloudsim platform and performance has been assessed.

4.1. BraTS 2020 dataset

The Segmentation of Brain Tumors The dataset, known as BraTS 2020, consists of multimodal 3D brain MR pictures and ground truth brain tumour segmentation annotated by medical professionals, with four T1, T1-c, T2, and FLAIR MRI modalities. 335 photos make up the BraTS 2020 dataset, 230 of which are used for training and 105 for testing. Edoema, enhancing tumour, necrosis, and non-enhancing tumour are all described as tumour subregions. Based on the description, three nested subregions were

created: total tumour (WT), tumour core (TC), and enhancing tumour (ET). The implications of the suggested and present techniques for encrypted images will be discussed in this section.

Figure 7 (a) shows the medical center homepage where they can access the data and update the data. Figure 7(b) represents the patient registration page, where the patient details need to be entered for their registration. Figure 7(c) represents the medical record updation page where we can update the medical records and also enter new medical data records. Figure 7(d) represents the patient detail access page in where we can view patient details and medical records.

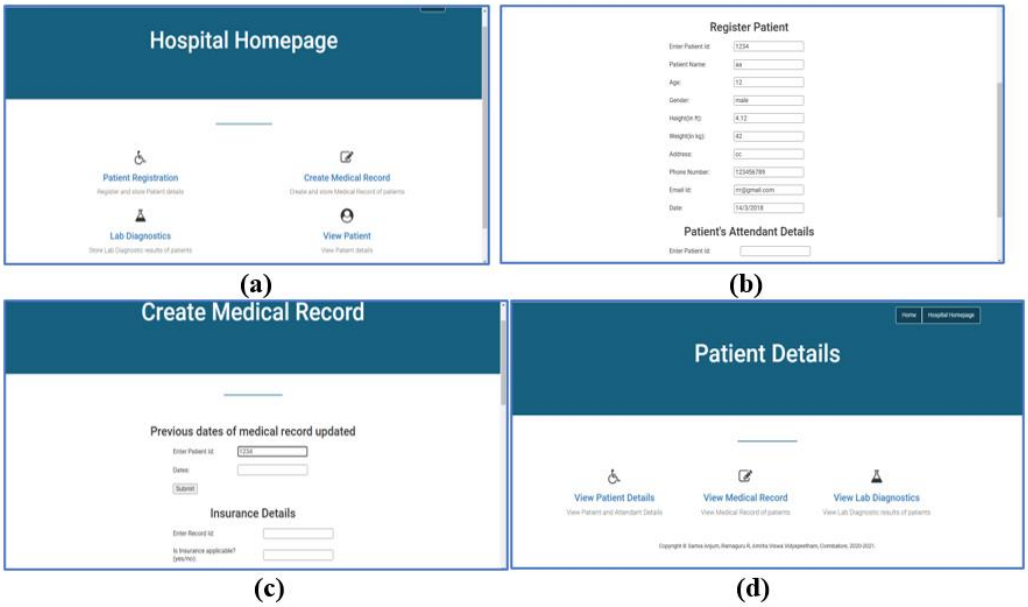


Figure 7. Real-time implementation (a) medical center Homepage (b) Patient registration page (c) Medical record updation (d) Patient detail access page

4.2. Performance Analysis

The medical images are saved in the cloud in encrypted form to provide security. Accessing the medical images by the authorized user is very simple on the other hand unauthorized users cannot access the medical image. The procedure for encryption of medical images is shown in Figure. 8.

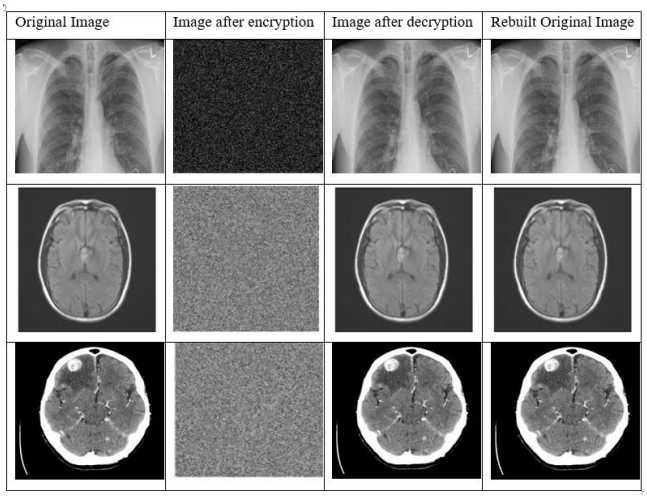


Figure 8. Performance analysis for BACK technique

The above figure describes the performance analysis of the BACK technique. Encryption is done to securely store the input medical data. Medical images that are kept in the cloud are encrypted and only accessible by the user. The images are not accessible to unauthorized users. The original image that has been rebuilt is also decrypted with the same technique. The images are transformed into an encrypted form using homomorphic encryption.

4.3. Histogram analysis

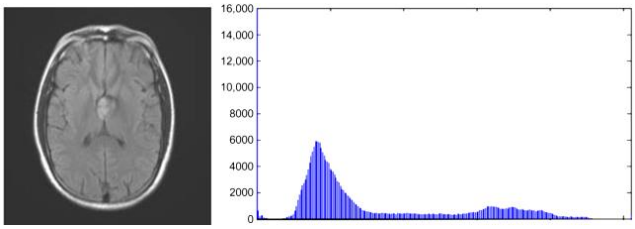


Figure 9. Histogram of original image

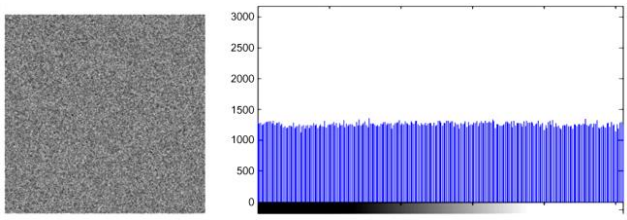


Figure 10. Histogram of encrypted image

The scatter plots of medical images throughout the encryption process are shown in Figures 9 and 10, which largely suggest that the scatter plots of the actual and encrypted picture may be distinguished from one another.

After encryption, the histogram's coherence demonstrates that the suggested model provides protection against attackers.

4.4 Comparison analysis

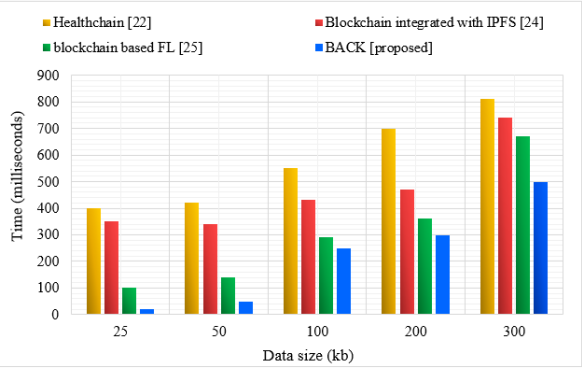


Figure 11. Encryption time comparison

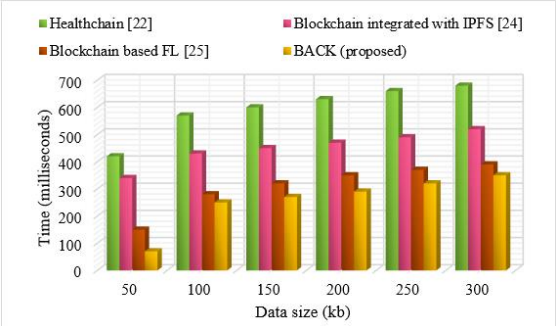


Figure 12. Decryption time comparison

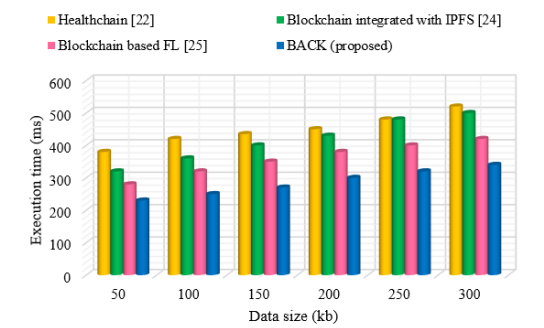


Figure 13. Comparative analysis of execution time

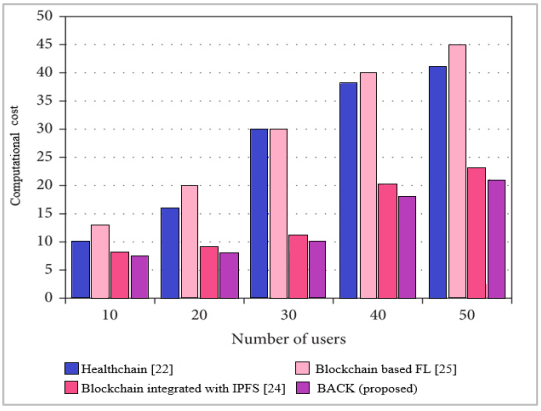


Figure 14. Comparative analysis of computational time

Figure 11 shows the encryption times of the existing Healthchain [22], Blockchain integrated with IPFS [24], Blockchain based FL [25] and proposed BACK algorithms. An increase in key size (bits) can enhance encryption time, according to this study. According to the experimental results, the proposed BACK method achieves less encryption time of 12.5%, 7.4%, and 4.65% than existing techniques such as Healthchain, Blockchain integrated with IPFS, and Blockchain based FL.

The proposed system and the existing approach are compared in Figure. 12 at the time of implementation. The proposed BACK method implementation time is quicker than the existing techniques. From the figure 13, it is clear that the proposed method achieves less execution time than existing techniques such as Healthchain [22], Blockchain integrated with IPFS [24], Blockchain based FL [25].

Figure 14 represents the computational time contrasting the suggested approach with the methods already in use. From the figure, it is clear that the proposed method achieves less computational cost than other existing techniques.

5. CONCLUSION

In this paper, an efficient BACK technique has been proposed for protecting the health records of patients while outsourcing the data through cloud storage. The proposed system ensured data and device security by implementing information security measures. The proposed method has been evaluated using CloudSim simulator. An evaluation of the effectiveness of the suggested strategy is based on several metrics, including execution time, encryption time, computational cost and decryption time. The suggested BACK technique is compared to state-of-the-art techniques such as Healthchain, Blockchain integrated with IPFS, Blockchain based FL. According to the experimental results, the proposed BACK method achieves less encryption time of 12.5%, 7.4%, and 4.65% than existing techniques such as Healthchain, Blockchain integrated with IPFS, and Blockchain based FL. E-healthcare data exchanged across multiple networks will be the subject of more data security and privacy assessments in the future.

CONFLICTS OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

FUNDING STATEMENT

No funding was received to assist with the preparation of this manuscript.

ACKNOWLEDGEMENTS

The authors would like to thank the reviewers for all of their careful, constructive and insightful comments in relation to this work.

REFERENCES

[1] Y. Alemami, A.M. Al-Ghonmein, K.G. "Al-Moghrabi, and M.A. Mohamed, Cloud data security and various cryptographic algorithms", *International Journal of Electrical and Computer Engineering*, vol.13, no. 2, pp.1867, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] S. Gadde, J. Amutharaj, and S. Usha. "A security model to protect the isolation of medical data in the cloud using hybrid cryptography", *Journal of Information Security and Applications*, vol. 73, pp.103412, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] M.K. Abdul-Hussein, and H.T. ALRikabi. "Secured Transfer and Storage Image Data for Cloud Communications", *International Journal of Online & Biomedical Engineering*, vol. 19, no. 6, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] N. Santos, B. Ghita, and G. Masala. "Medical Systems Data Security and Biometric Authentication in Public Cloud Servers", *IEEE Transactions on Emerging Topics in Computing*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] G. Sucharitha, V.E.D.U.L.A. Sitharamulu, S.N. Mohanty, A. Matta, and D. Jose, "Enhancing Secure Communication in the Cloud through Blockchain Assisted-CP-DABE", *IEEE Access*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] G. Borghini, S. Caputo, L. Mucchi, A. Rashid, S. Jayousi, M. Hämäläinen, T. Paso, and M. Hernandez. "Security of Wireless Body Area Networks for Healthcare Applications: Comparison between ETSI and IEEE Approaches", *In 2023 IEEE 17th International Symposium on Medical Information and Communication Technology (ISMICT)*, pp. 1-6. IEEE, 2023, May. [CrossRef] [Google Scholar] [Publisher Link]

[7] B. Chen, T. Xiang, D. He, H. Li, and K.K.R. Choo. "BPVSE: Publicly Verifiable Searchable Encryption for Cloud-Assisted Electronic Health Records", *IEEE Transactions on Information Forensics and Security*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] X. Li, H. Zhao, and W. Deng. "BFOD: Blockchain-based privacy protection and security sharing scheme of flight operation data", *IEEE Internet of Things Journal*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] J. Liu, Y. Fan, R. Sun, L. Liu, C. Wu, and S. Mumtaz. "Blockchain-Aided Privacy-Preserving Medical Data Sharing Scheme for E-Healthcare System", *IEEE Internet of Things Journal*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] X. Liu, S. Zhang, H. Huang, W. Wang, and R. Malekian, "A Verifiable and Efficient Secure Sharing Scheme in Multiowner Multiuser Settings", *IEEE Systems Journal*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] B.D. Deebak, and S.O. Hwang. "A Cloud-Assisted Medical Cyber-Physical System Using a Privacy-Preserving Key Agreement Framework and a Chebyshev Chaotic Map", *IEEE Systems Journal*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] M.F. Alomari, M.A. Mahmoud, Y.B. Yusoff, N. Gharaei, R.A. Abdalla, and S.S. Gunasekaran, "Data Encryption-enabled Cloud Cost Optimization and Energy Efficiency-based Border Security Model". *IEEE Access*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] H. Gao, H. Huang, L. Xue, F. Xiao, and Q. Li, "Blockchain-enabled Fine-Grained Searchable Encryption with Cloud-edge Computing for Electronic Health Records Sharing", *IEEE Internet of Things Journal*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] Z. Hua, X. Liu, Y. Zheng, S. Yi, and Y. Zhang, "Reversible data hiding over encrypted images via preprocessing-free matrix secret sharing", *IEEE Transactions on Circuits and Systems for Video Technology*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] A. Ali, M.F. Pasha, A. Guerrieri, A. Guzzo, X. Sun, A. Saeed, A. Hussain, and G. Fortino. "A Novel Homomorphic Encryption and Consortium Blockchain-based Hybrid Deep Learning Model for Industrial Internet of Medical Things", *IEEE Transactions on Network Science and Engineering*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[16] J. Sun, G. Xu, T. Zhang, X. Yang, M. Alazab, and R.H. Deng, "Privacy-Aware and Security-Enhanced Efficient Matchmaking Encryption", *IEEE Transactions on Information Forensics and Security*. 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] P. Tian, C. Guo, K.K.R. Choo, X. Tang, and L. Yao, "A Privacy Preserving Hybrid Range Search Scheme over Encrypted Electronic Medical Data in IoT Systems", *IEEE Internet of Things Journal*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[18] Y. Wang, and D. Papadopoulos. "Multi-User Collusion-Resistant Searchable Encryption for Cloud Storage", *IEEE Transactions on Cloud Computing*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[19] R.R. Irshad, S.S. Sohail, S. Hussain, D.Ø. Madsen, M.A. Ahmed, A.A. Alattab, O.A.S. Alsaiari, K.A.A. Norain, and A.A.A. Ahmed "A Multi-Objective Bee Foraging Learning-based Particle Swarm Optimization Algorithm for Enhancing the Security of healthcare data in cloud system", *IEEE Access*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[20] N. Yang, C. Tang, Q. Zhou, and D. He. "Dynamic Consensus Committee-based for Secure Data Sharing with Authorized Multi-Receiver Searchable Encryption", *IEEE Transactions on Information Forensics and Security*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[21] J. Niu, X. Li, J. Gao, and Y. Han. "Blockchain-based anti-key-leakage key aggregation searchable encryption for IoT", *IEEE Internet of Things Journal*, vol.7, no.2, pp.1502-1518, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[22] S. Chenthara, K. Ahmed, H. Wang, F. Whittaker, and Z. Chen, "Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology", *Plos one*, vol.15, no. 12, pp. e0243043, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[23] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, "HealthBlock: A secure blockchain-based healthcare data management system", *Computer Networks*, vol. 200, p.108500, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[24] J. Jayabalan, and N. Jeyanthi. "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy", *Journal of Parallel and Distributed Computing*, vol.164, pp.152-167, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[25] Singh, M.B. and Pratap, A., "BPFISH: Blockchain and Privacy-preserving FL Inspired Smart Healthcare", arXiv preprint arXiv:2207.11654, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[26] A.E. Adeniyi, K.M. Abiodun, J.B. Awotunde, M. Olagunju, O.S. Ojo and N.P. Edet, "Implementation of a block cipher algorithm for medical information security on

cloud environment: using modified advanced encryption standard approach", *Multimedia Tools and Applications*, pp. 1-15. [CrossRef] [Google Scholar] [Publisher Link]

[27] I. Gupta, D. Saxena, A.K. Singh and C.N. Lee, "SeCoM: An Outsourced Cloud-Based Secure Communication Model for Advanced Privacy Preserving Data Computing and Protection", *IEEE Systems Journal*, pp. 1-12, 2023. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

G. Sreetha, she was born in Kanyakumari District, Tamilnadu, India in 2000. She received her BE degree in computer science and engineering from Arunachala college of engineering, Manavilai, Anna University, India in 2021. Currently she is pursuing her ME degree in computer science and engineering from Arunachala college of Engineering, Manavilai, Anna University, India. Her interested research area is cloud computing, and cryptography.

T. V. Chithra received her B.E. degree in CSE from M.S University, Tirunelveli in 2004, and obtained M.E. degree in CSE from Anna University, Chennai in 2009. She obtained Ph.D. degree from Anna University, Chennai for her research work on Wireless Sensor Network in 2021. She has published 4 papers in international journals, fourteen papers in conferences and four books. Currently she is working as Associate Professor in the Department of CSE Arunachala College of Engineering for Women, India. Her research areas of interest include WSN, BigData, Cloud Computing, Internet of Things.

Arrived: 02.08.2023
Accepted: 29.09.2023

International Journal of Computer and Engineering Optimization (IJCEO)
Volume 1, Issue 1, September – October (2023)

RESEARCH ARTICLE

DEEP LEARNING BASED AUTHENTICATION SECURE DATA STORING IN CLOUD COMPUTING

M. Prabhu[1, *], G. Revathy[2] and R. Raja Kumar[3]

[1]Department of Electronics and Communication Engineering, Saveetha School of Engineering, SIMATS, Chennai India.
[2]Department of Electronics and Instrumentation Engineering, Sengunthar Engineering College, Erode, Tamil Nadu 638057, India
[3]Department of Mathematics, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu 600119 India.

[*]*Corresponding e-mail: prabhu.ece05@gmail.com*

Abstract – To communicate organizationally important data among working units in a federated cloud environment, secure mutual authentication is a crucial necessity. The administration of data while preserving its usefulness and security system is a worry for the cloud owner. Cloud data sharing is becoming more and more popular as a viable way to give people simple access to data. supported by positive advances in cloud technology. Yet, as more businesses and customers store their data on cloud servers, it poses a growing threat to user privacy and data security. People are inclined to encrypt information before sending it to the cloud in order to ensure its confidentiality. Yet the data processing has gotten challenging due to broad encryption methods. In order This paper provides a novel mutual authentication mechanism that combines deep learning-based recognition and control of security breaches to enable secure communication between participating entities. Convolutional Neural Networks (CNN) for online threat detection with RSA Cryptography and Schnarr's signature scheme-based public-key encryption technologies. A network intrusion dataset from the Canadian Institute for UNSW-NB15 is used to measure performance, and the AVISPA security analysis tool confirms its effectiveness in comparison to other methods in terms of security features and communication costs.

Keywords *– RSA cryptography; mutual authentication; AVISPA security analysis, Schnorr signature; Convolutional neural networks (CNN), threat, encrypted data*

1. INTRODUCTION

Securing every online communication between sending and receiving entities has become a requirement in order to guarantee secure and efficient online commerce or data collaboration. As a result, to enable secure key exchange and the development of secure sessions during data sharing, a reliable mutual authentication system is required. In the previous year, 47% of firms suffered security attacks or failed compliance audits, according to Thales Report 2020. In addition, a multi-server environment has added new difficulties and sparked security flaws. Numerous researchers have put forth a variety of security solutions in response to online data exchange security flaws, these include mutually authenticated safe secret key exchange, secure data storage and sharing, safeguarded credential storage, techniques for granting access to data, and safe authentication protocols.

Clients that save their data on the cloud may easily and rapidly retrieve it without needing to be specialists in the setup and upkeep of the equipment or architecture. In comparison with desktop computer, cloud computing offers significantly greater power. But it also introduces additional privacy and security problems because users lose control over their data when it is outsourced and they no longer have physical access to it. Full access to cloud services exposes customers' data to several dangers and hostile attacks, and security breaches are common as a result.

Despite these benefits, keeping personally identifiable information in a cloud environment greatly increases the need for security. As sensitive data is transferred from the federated domain to the distribution domain, this raises questions about regulatory compliance. Big data technologies can be used to their full potential, however, issues with privacy and security must be addressed first. Also, as the cloud is based on the pillars of two fundamental foundations, such as cloud computing and networking, Internet connectivity and infrastructure are crucial. The network can be utilized for cloud computing and other applications for numerous cloud applications.

Digital data is now protected by encryption. The goal of this area of computer science is to transform data into understandable representations for only authorized users. Basic cryptography is demonstrated with an encrypted message where the letters have been replaced with other characters. In the presence of adversaries, or malicious outsiders, cryptography enables a secure route of communication. A key (also referred to as cipher text) and an algorithm are used in encryption to convert a plaintext

input into an encrypted output. The three primary objectives of cryptography are data privacy, data authenticity, and data integrity.

In order to overcome the issues with online data sharing, a mechanism for improved mutual authentication is created in this study. It is based on the trusted cloud server's integration of RSA cryptography and deep learning techniques. It is advised to follow the correct registration procedure, engage in deep learning, and use key agreement and RSA cryptography for threat detection during the session setup and password change stages, respectively. For secure online data sharing. The principal contributions of the planned work are summarized as follows:

- An RSA Cryptography and deep learning-based Authentication Protocol is proposed to facilitate data exchange among users on federated cloud servers.
- At a trusted cloud server, CNN is used to develop an online threat detection system to mitigate denial of service attacks.
- Verification using AVISPA tool for security analysis and state-of-the-art protocol comparison with the suggested protocol.

The remaining portions of this work are arranged as follows: Section 2 reviews the literature on earlier studies; Section 3 provides a detailed analysis of the suggested work; Section 4 offers the findings; and Section 5 concludes.

2. LITERATURE SURVEY

In 2018 Olufemi Olakanmi, O. and Oke, S. [6] proposed a successful mutual authentication system for using diverse MCC services. With the proposed technique, cryptography operations can be integrated with voice signatures to create an effective mutual authentication scheme that eliminates key escrow issues while enabling authorized users to more affordably obtain varied MCC services. The assessments of security and performance indicate that our suggested system outperforms the two most recent state-of-the-art MCC service systems. We will use other penetration tests that are available in the future to investigate the scheme's security in more detail.

In 2019 Gupta, I., et. al.., [4] proposed a layered architecture based on sensitivity is effective for protecting data security and privacy in a cloud environment. Because of the multilayer security in the suggested design, cloud service providers experience less overhead overall. To evaluate the effectiveness of the layer-based strategy, experimental analysis is done. According to the experimental findings, processing 200 papers of 20 MB each took 437, 2239, 3142, and 3900 milliseconds for content that is successively public, private, and top-secret. The outcomes of the experiments demonstrate the accuracy, applicability, dependability, and effectiveness of the suggested strategy.

In 2019 Zhang, L.,[7] proposed a CP-ABE method with effective authority verification that protects privacy. Assuming the decisional linearity assumptions and the decisional BDHE issue, the suggested approach achieves selected security. a CP-ABE approach in the standard model that protects privacy. With constant-size private keys and brief cypher texts, the proposed approach has numerous advantages over the existing ones. Moreover, just four pairing computations are required for decryption. The suggested approach also allows for authority verification without any privacy leakage.

In 2019 Han, S.,[5] proposed to a group exchanging secret key prevents unauthorized access to shared data and the communication process. management protocol (SSGK) is used. Data that is shared is encrypted using a group key in SSGK, and the group key is distributed secretly. According to in-depth security and performance assessments, Cloud storage reduces dangers to privacy and security and frees up around 12% of space.

In 2020 Butt, U.A., [2] proposed an analysis of machine learning (ML) techniques to address CC security risks, issues, and solutions; also, the usefulness of each method is evaluated based on its characteristics, advantages, and disadvantages. Algorithms for semi-supervised, supervised, unsupervised, and reinforcement learning are used to address cloud security issues. Security threats and attacks were examined as the most difficult problems in CC.

In 2021 Nassif, A.B. et al..,[1] proposed Security strategies and techniques for ML and the cloud. The three key research areas covered by the SLR's findings are I the different risks to cloud security, (ii) the ML methods used, and (iii) the performance outcomes. Furthermore, with a use rate of 16% and 14%, respectively, the two most common areas of cloud security are DDoS and data privacy.

In 2022 Reddy, S. et., al..,[3] suggested a state-of-the-art SaaS architecture that makes advantage of attack node mitigation. The Median Fitness-oriented Sea Lion Optimization algorithm (MFSLnO) is used to modify the weight and activation function during the Deep Belief Network (DBN) attack detection phase. The suggested method outperforms traditional approaches, achieving an 89% throughput and a 16% packet loss ratio.

3. PROPOSED METHODOLOGY

In this section a novel deep encrypt technique has been proposed to overcome the security while sharing data in cloud.The identification module and the encryption module are the two steps that make up the suggested technique. Whether it is an attack or not will be determined by the suggested strategy. The session will be stopped or cancelled if it is an attack.

3.1. Identification Module

There will be data theft during transmission when the data owner transmits information to the receiver initially. The historical data will be gathered in this module to discover the live data from the data owner, which will be provided for CNN classification.

3.1.1. CNN

The overall performance and complexity of a CNN structure may be influenced by a variety of hyper-

parameters, including the number and characteristics of hidden layers, pooling schemes, normalization plans, and cost functions. To train a CNN system for visualizing a landscape, additional reference annotations—also called labels or targets—and data from remote sensing were required. Convolution layers are more potent data structures that can be used with CNN-based training; however support vector networks and random forests are two examples of machine learning techniques that utilize relatively simple array-type data structures.

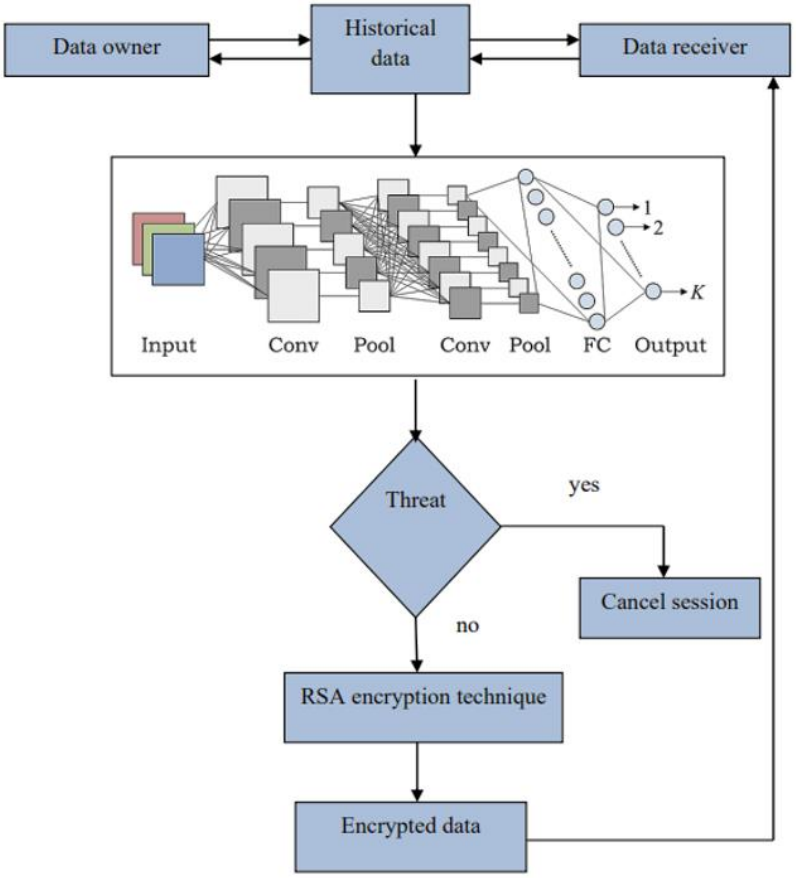


Figure 1. Block diagram of proposed methodology

In order to lower the number of pieces in that stimulus, the pooling method will fully reduce the insight along the spatial representation. The acquired features are typically dynamically down-sampled via additional-level methods within every multiple convolutional layer series. Max-pooling is the most common type of pooling procedure. Max-pooling aims for large activations rather than, say, average pooling. There are numerous distinct sorts of architectures that can be referred to by the term "CNN architecture," which outlines the potential connections between the neuronal or pooling layers of a CNN. As a result, CNNs are able to communicate a variety of opinions, many of which are influenced by their goals.

The convolutional layer will estimate as a scalar product the mass of the neurons whose output is related to certain input volume areas and the strength of the input volume-connected region. The corrected unit, also called ReLu, tries to stimulate the output from activating the previous layers by adding a "definite data" kernel operation (e.g., logarithmic kernel function). The fully connected layers are going to execute operations akin to those in traditional artificial neural networks (ANNs) with the goal of extracting output values of the kernel function which may be utilized for classification in the end. ReLu can also be used to enhance performance in between these layers.

3.2. Encryption Module

The RSA encryption method is used to encrypt the data. The difficulty of dissecting really large numbers determines how secure the RSA method is. The procedure using two enormously big prime numbers acts to create both the private key and the public key. According to estimates, it is just as difficult to decrypt Predicting the plaintext from the signal key and the cipher text is as difficult as calculating the product of two huge prime integers. The ISAKMP/Oakley design has considered using the RSA algorithm as a possible authentication technique. One essential element of the design is the Diffie-Hellman key exchange protocol.

To attain optimal effectiveness, the symmetric cryptographic algorithms and public key cryptography algorithms are always coupled. In other words, the DES key must be transmitted using an asymmetric key cryptosystem, such as RSA, and the confidential data must be supplied encrypted using a symmetric key cryptosystem. This uses two separate types of encryptions, high-speed DES and the practical and secure RSA key management scheme.

RSA is helpful for both authentication and encryption. The generated signature key for public key algorithms is only kept on the user's computer, which increases security compared to hash signatures. In order to provide localized components that are compatible with the end user's local OS, the RSA algorithm is implemented using C++.

Because there is currently no demonstration that breaking RSA would absolutely require factoring large numbers, it is not completely established in principle that RSA is equivalent to integer factorization. Instead, the security of RSA depends on how challenging integer factoring is. Several RSA variations are been shown to be interchangeable with integer factorization techniques. Hence, the data receiver will receive the encrypted data.

4. RESULT & DISCUSSION

The traditional numerical parameters given below have been used to evaluate the suggested model. Equations (1), (2), (3), and (4) were used to calculate accuracy, recall, specificity, and sensitivity, respectively. Equation (1) was used to calculate the accuracy.

4.1. Evaluation metrics

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

$$Specificity = \frac{TN}{TN+FP} \quad (2)$$

$$Recall = \frac{TP}{TP+FP} \quad (3)$$

$$Percision = \frac{TP}{TP+FP} \quad (4)$$

For the provided data, there are four possible outcomes: true positive (TP), false positive (FP), false negative (FN), and true positive (TN). Positive labels are applied to false negative data, whereas positive labels are applied to actual positive data and classified accordingly. While TN data is labeled as negative and labeled as negative, false positive data is considered to be positive. The comparison graph is plotted below.,

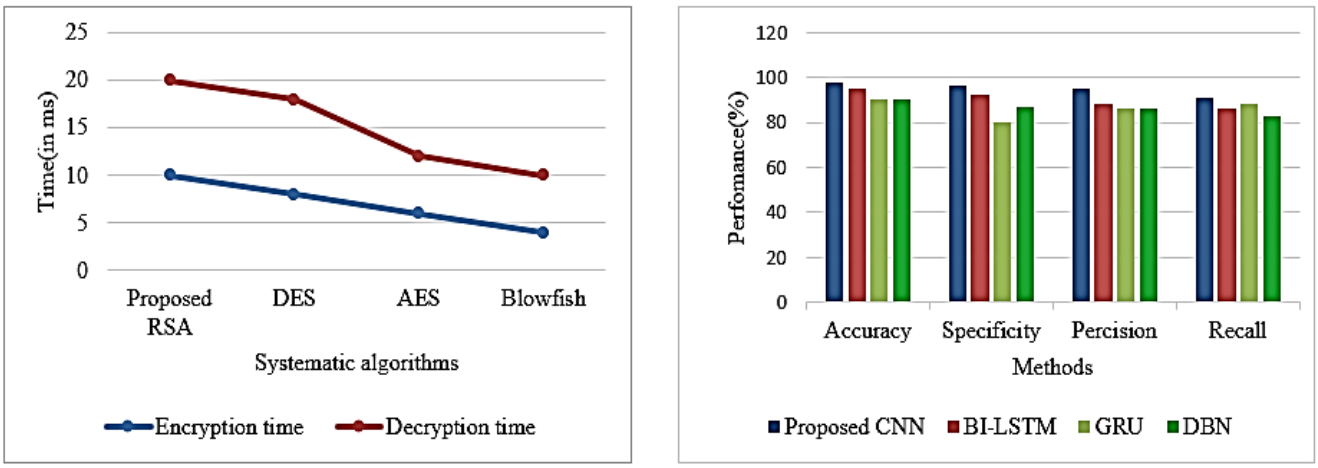


Figure 2. Comparative analysis of proposed methodology

In Figure 2, several metrics, such as recall, accuracy, specificity, and precision rate, are represented graphically as an overview of proposed and existing approaches. Viewing the graphs clearly shows that the proposed approach is appropriate for recognizing assaults and superior to all presently used methods. Sensitivity and specificity of the suggested approaches are 98.01% and 96.02%, respectively. The proposed framework outperformed the current BI-LSTM, GRU, and DBN in terms of sensitivity and specificity when compared to earlier models. A comparison graph for encryption and decryption time also analyzed.

5. CONCLUSION

Introducing a ground-breaking mutual authentication method for secure data transmission since the user's actual identification is frequently utilized session keys are never directly disclosed on the public network, it is founded on cryptography and deep learning. In this study, a unique mutual authentication technique is presented that combines RSA cryptography with deep learning-based convolutional neural networks (CNN) for online threat detection. Also, this mutual authentication system's security has been examined using the AVISPA security analysis tool. The findings show that the suggested protocol is inexpensive to compute with and secure from a wide range of security threats that could arise during online data sharing in a multi-cloud context.

CONFLICTS OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

FUNDING STATEMENT

No funding was received to assist with the preparation of this manuscript.

ACKNOWLEDGEMENTS

The authors would like to thank the reviewers for all of their careful, constructive and insightful comments in relation to this work.

REFERENCES

[1] A.B. Nassif, M.A. Talib, Q. Nasir, H. Albadani, and F.M. Dakalbab, "Machine learning for cloud security: a systematic review", *IEEE Access*, vol. 9, pp. 20717-20735, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] L. H. Merino, & M. Cukier, "An Approach for Preventing and Detecting Attacks in the Cloud", *In 2020 IEEE/ACM 13th International Conference on Utility and Cloud Computing (UCC)*, IEEE, pp. 165-175, 2020, December. [CrossRef] [Google Scholar] [Publisher Link]

[3] S. Reddy, and G.K. Shyam, "A machine learning based attack detection and mitigation using a secure SaaS framework", *Journal of King Saud University-Computer and Information Sciences*, vol.34, no.7, pp. 4047-4061, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] I. Gupta, N. Singh, and A.K. Singh. "Layer-based privacy and security architecture for cloud data sharing", *Journal of Communications Software and Systems*, vol.15, no.2, pp.173-185, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[5] S. Han, K. Han, and S. Zhang, "A data sharing protocol to minimize security and privacy risks of cloud storage in big data era", *IEEE Access*, vol.7, pp. 60290-60298, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[6] O. Olufemi Olakanmi, and S.O. Oke. "MASHED: Security and privacy-aware mutual authentication scheme for heterogeneous and distributed mobile cloud computing services", *Information Security Journal: A Global Perspective*, vol.27, no.5-6, pp.276-291, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[7] L. Zhang, Y. Cui, and Y. Mu. "Improving security and privacy attribute-based data sharing in cloud computing", *IEEE Systems Journal*, vol.14, no.1, pp.387-397, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[8] A.K. Singh, and D. Saxena. "A cryptography and machine learning based authentication for secure data-sharing in federated cloud services environment", *Journal of Applied Security Research*, vol.17, no.3, pp.385-412, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] M. Karuppiah, A.K. Das, X. Li, S. Kumari, F. Wu, S.A. Chaudhry, and R. Niranchana. "Secure remote user mutual authentication scheme with key agreement for cloud environment", *Mobile Networks and Applications*, vol.24, pp.1046-1062, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[10] G. Wang, Q. Liu, and J. Wu. "Achieving fine-grained access control for secure data sharing on cloud servers", *Concurrency and Computation: Practice and Experience*, vol.23, no.12, pp.1443-1464, 2011. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

M. Prabhu, Associate Professor, Department of Electronics and Communication Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences (SIMATS), Chennai, received his BE [ECE] degree from Anna University, Chennai in the year 2005, ME in communication systems from Anna University, Chennai in 2011 and Doctoral degree from Anna University, Chennai in the year 2023. He is having more than 18 years of experience in reputed engineering colleges. He has published 2 peer-reviewed International Journals, many papers at national and international conferences. Also, he has attended 50 FDPs, workshops, and seminars. His research interest lies in the field of wireless communications, Wireless sensor networks, Adhoc and sensor networks and 5G communications

G. Revathy received her M.E. degree from Kongu Engineering College, Anna University, India. She is now actively performing as an Assistant Professor in the Department of Electronics and Instrumentation Engineering at Erode Sengunthar Engineering College, India. Her research areas include Digital Image Processing, Artificial Intelligence, Deep Learning. Also, in addition to this, she had an ISTE membership.

R. Raja Kumar graduated in Mathematics and he completed his doctorate in Chaotic Communications in 2013. He is a Professor of Mathematics in Sathyabama Institute of Science and Technology (Deemed University), Chennai, Tamil Nadu, India. He has 30 years of teaching experience and has 50 reputed publications and 6 International books to his credit. He is a member of Ramanujan Mathematical Society. His research interests include Communication Engineering and Mathematics.

Arrived: 05.08.2023
Accepted: 15.10.2023

International Journal of Computer and Engineering Optimization (IJCEO)
Volume 1, Issue 1, September – October (2023)

RESEARCH ARTICLE

SECURE BLOCKCHAIN BASED DEEP LEARNING APPROACH FOR DATA TRANSMISSION IN IOT-ENABLED HEALTHCARE SYSTEM

R. R. Sathiya[1 *], S. Rajakumar[2] and J. Sathiamoorthy[3]

[1]Department of Computer Science and Engineering, Amrita School of Computing, Amrita Vishwa Vidyapeetham, Coimbatore, India
[2]Department of Electronics and Communication Engineering, Panimalar Engineering College, Chennai, India
[3]Department of Computer Science and Engineering, RMK Engineering College, Tamilnadu, India

[*]*Corresponding e-mail: rajamani3314@gmail.com*

Abstract – Healthcare service quality has been improved by integrating the Internet of Things (IoT) with conventional medical networks. In contrast, device-mounted sensors and wearables employed in Healthcare Systems (HS) monitoring and data transmission ongoing over unprotected open channels to adjacent devices. The effectiveness of operations is being improved by the link among IoT devices and computers, yet it allows attackers to commit a variety of cyber-attacks that could jeopardize patients under vital observation. Using Deep-BiLSTM in a healthcare IoT system for Secure Data Transmission is presented in this paper. In particular, the first unique there is a suggested blockchain design that assure data security and reliability transfer through the use of the Zero Knowledge Proof (ZKP) mechanism. The validated data is then utilized to create a deep learning framework for identification of intrusions in the HS network. A Bidirectional Long Short-Term Memory (BiLSTM) and Deep Convolutional Neural Network (DCNN) are integrated to create a highly efficient intrusion detection method. experiments using two sources of open data (CICIDS-2017 and ToN-IoT) has been used to compare the proposed method with 96% better performance. The suggested BD-BiLSTM methodology has 98% precision, accuracy, recall, and F1 score, which is pretty high when compared to other approaches. of BDL-SMDTA, PBDL and GWMNN.

Keywords *– Internet of things, health care system, cyber-attack, deep-BILSTM, Zero knowledge proof mechanism (ZKP), deep convolutional neural network*

1. INTRODUCTION

Traditional healthcare systems have been transformed into intelligent ones through the Internet of Things (IoT), which allows patient data is continuously monitored and accessible remotely. In medical field, a number of medical devices powered by the Internet of Things (IoT) collect real-time health information of patients, such as their body temperature and other important details.[8] In fact, IoT can help the medical field in diagnosing and treating patients remotely. [9]. It is, however, possible to eavesdrop, manipulate the data, and exploit other security vulnerabilities in an IoT-authorized Healthcare System (HS) when the nodes are related 24/7 over an open, insecure public channel. [10] whereby attackers try to take advantage of the dependability, and security of IoT data and devices.[11]

To address the issues raised above, IoT-enabled healthcare is possible with blockchain and deep learning (DL). To begin, A block and a chain make up a blockchain (a form of public database). It is impossible to modify data once it has been blocking chain of immutable blocks recording data attacks [12]. Furthermore, consensus mechanisms support the reliability of distributed data stored on a blockchain. [13] As a result, while transmission through IoT-enabled HS, it is safe and reliable to consider the patient's medical information. [6] Because of blockchain's immutability and decentralized architecture, smart contracts can boost trust between parties engaged in the data transfer by independently enforcing and carrying out the terms of the contract.

To detect aberrant network behaviors and prevent HS attacks, The majority of intrusion detection systems are DL-based typically utilized over deep learning technologies. However, most with some attack types, IDS developed in the literature perform badly in terms of the rate of false alarms and detections. since they take data directly from the network. [14,15]. Furthermore, one of the key challenges with IoT-authorized HS is scalability. The justification is that, as the number of as the number of IoT device rises, to keep up, more storage space will be required for data generation's exponential expansion. [16]. These attacks not only target hospital network components with malicious

software or malware, but they also target genuine IoT devices with the goal of limiting their operation [17].

This strategy assumes that the communication's endpoints (IoT devices and Edge servers) cannot be completely trusted. Additionally, it is presumed that they speak on a channel that is open, public, and insecure. IoT devices and edge servers, however, are thought of as semi-trusted. A message delivered between two entities can have its contents changed by an attacker [18].

Also, the assailant obtains entry to important data and able in order to carry out a data poisoning assault. As a result, in order to prevent the information from being viewed by unauthorized parties, verifying the involved parties is crucial before initiating secret communication. Therefore, it is crucial to consider this approach while investigating IoT data security. [19].

Prior to secret communication, it is necessary to confirm that the involved parties to stop them from gaining access to the information [20-25]. As a result, it is critical to consider this paradigm while analyzing the security of IoT data [26-27]. Furthermore, scalability is one of the more major challenges in IoT-enabled HS [28,29]. The argument is that additional storage space will be needed as the number of IoT devices rises to support the exponential growth in data generated [31-35].

In this article BD-BILSTM was developed and implemented, as a result of combining blockchain and deep learning approaches, the aforementioned issues can be addressed. There are several main contributions to this paper:

- The BD-BILSTM system combines blockchain technology with deep learning (DL) techniques in order to transmit data securely.
- It is planned to implement a blockchain-authorized security framework. The fundamental technique uses zero knowledge evidence to register and verify IoT devices.
- The above technique validates data records, provides a standardized method for transmitting medical information in the HS network, and protects against data contamination threats.
- A security architecture with DL capabilities is suggested. A Deep convolutional neural network by using the (DCNN) technique, raw data can be encoded into a format that is more suitable for storage.
- The development of an intrusion detection system makes use of the Bidirectional Long Short-Term Memory (BiLSTM) technology.
- ToN-IoT and CICIDS-2017 network he proposed BD-BiLSTM framework is evaluated using datasets.
- Suggested method has been determined by the evaluation metrices of accuracy, precision, F1 score and recall.

Therefore, the remainder of the paper will be organized as follows: A review of the literature is presented in Part 2, followed by an evaluation of the proposed work in Section 3, a discussion of the findings in Section 4, and a conclusion in Section 5.

2. LITERATURE SURVEY

The relevant work in these fields is presented in this section, with a focus on the Deep-BiLSTM technique for Secure Data Transmission and conventional healthcare systems with higher-quality healthcare services. Some of those methods have been discussed in this section.

In 2020, Li, J. et al., [1] proposed a secure architecture for IoT-enabled healthcare system's edge computing on SDN. IoT device authentication is handled employing a straightforward authentication technique via the Edge servers. After authentication, SDN controller manages Resource allocation, network optimization, and load balancing for the healthcare system is connected to the Edge servers. With a reduction in network control overhead, it improves throughput, latency, packet delivery ratio, average reaction time, and overall network performance.

In 2021 Wang, K. et al., [2] proposed an IoT-cloud-authorized healthcare data system with forward privacy and verifiability, as well as Verifying a multi-keyword search method constructed using a pseudo-random function (PRF). This technique overcomes the challenge of scenario for top-K searches with just partial results to evaluate the accuracy of search findings. The trial's findings demonstrate the FEncKV system is appropriate for IoT-authorized healthcare systems.

In 2021 Arul, R. et al., [3] proposed an adaptable service compliance (BASC) effort is based on the blockchain to prevent non-dormant health care services from becoming a liability. Regarding providing and facilitating end users' utilization of medical data, it is trustworthy in overcoming dormancy worries. Verification of affordability is the result of learning, and background checks vouch for the accuracy of the information. This improves the aid's honesty while preventing healthcare service failures and delays.

In 2021 Li, W. et al., [4] proposed a thorough review making use of applying machine learning (ML) techniques to extensive data analysis in healthcare industry. It makes it possible for government agencies and healthcare professionals to keep up with the most recent developments in ML-based large-scale data analysis in healthcare. Additionally, it offers extensive and recent studies on big data analytics techniques for the Internet of Things and smart health based on machine learning. Also, full analysis of their advantages and disadvantages is given.

In 2021 Said, O. and Tolba, A., [5] proposed a significant IoT-authorized to provide a broad spectrum of communication amongst healthcare devices, healthcare architecture uses satellites and high-altitude platforms in addition to Internet coverage technologies. (HAPs). Efficiency of the suggested IoT-authorized healthcare framework is assessed using NS3. The results of the simulation demonstrate that the proposed IoT-enabled healthcare system outperforms the conventional healthcare design.

In 2021 Peneti, S. et al., [6] proposed a modular neural network-based network approach with gray wolf optimization is used to handle security in smart environments. (GWMNN). An optimized neural network is utilized in IoT-enabled smart applications to maintain latency and compute resource usage. In contrast to multi-layer perceptrons and deep learning networks, the system has minimal latency and good security (99.12%), according to simulation findings that are used to analyses the system's effectiveness.

In 2022 Sardar, A. et al., [7] proposed a secure facial recognition solution for the Internet of Things in medical. Cancellable biometrics, BioCrypto-Circuits, and BioCrypto-Protection Schemes are the three stages template protection approaches that have been established to protect biometric data. FERET, CVL, IITK, Casia-Face-v5, and these benchmark face databases were used to evaluate how well the proposed system will operate. Results are provided using suggested system's correct recognition rate and equal error rate.

In 2022 Zhang, L. et al., [8] proposed a federated learning continues even if the quantity of internet users declines. remains above a predetermined level in a dropout-tolerant technique. The security analysis shows that the proposed solution protects data privacy. The costs of computing and communication are theoretically studied as well. The experimental findings show that, in comparison to earlier methods, the suggested scheme provided positive results while preserving anonymity.

In 2022 Neelakandan, S. et al., [9] proposed a new secure medical data transfer and diagnosis model powered by blockchain (BDL-SMDTD). The BDL-SMDTD model's objective is to determine diseases with maximum detection rate while securely transmitting medical images. Using feature extraction based on ResNet-v2, the recommended BDL-SMDTD model's highest classification performance was attained with 96.94% sensitivity, 98.36% specificity, and 95.29 accuracy.

In 2022 Kumar, R. et al., [10] proposed Deep learning (DL) techniques are coupled with smart contracts and permissioned blockchain to produce the PBDL, a special platform for secure and effective data transmission. By the use of a smart contract-based consensus mechanism, PBDL initially uses a blockchain approach communication entity to be registered, checked (using zero-knowledge proof), and validated. The IoT-Botnet and ToN-IoT datasets used in the security analysis and testing results demonstrate the PBDL framework's superiority to other exiting techniques.

It can be seen from the reviews above that these methods have some shortcomings. This research proposes a Deep-BiLSTM technique Enabling Safe Data Transfer in Internet of Things-Approved Medical Systems to address these disadvantages.

3. PROPOSED METHODOLOGY

This part presented BD-BILSTM, which combines block chain and deep learning methods to ensure the accuracy of the data and secure data transmission in order to identify intrusion in the HS network.

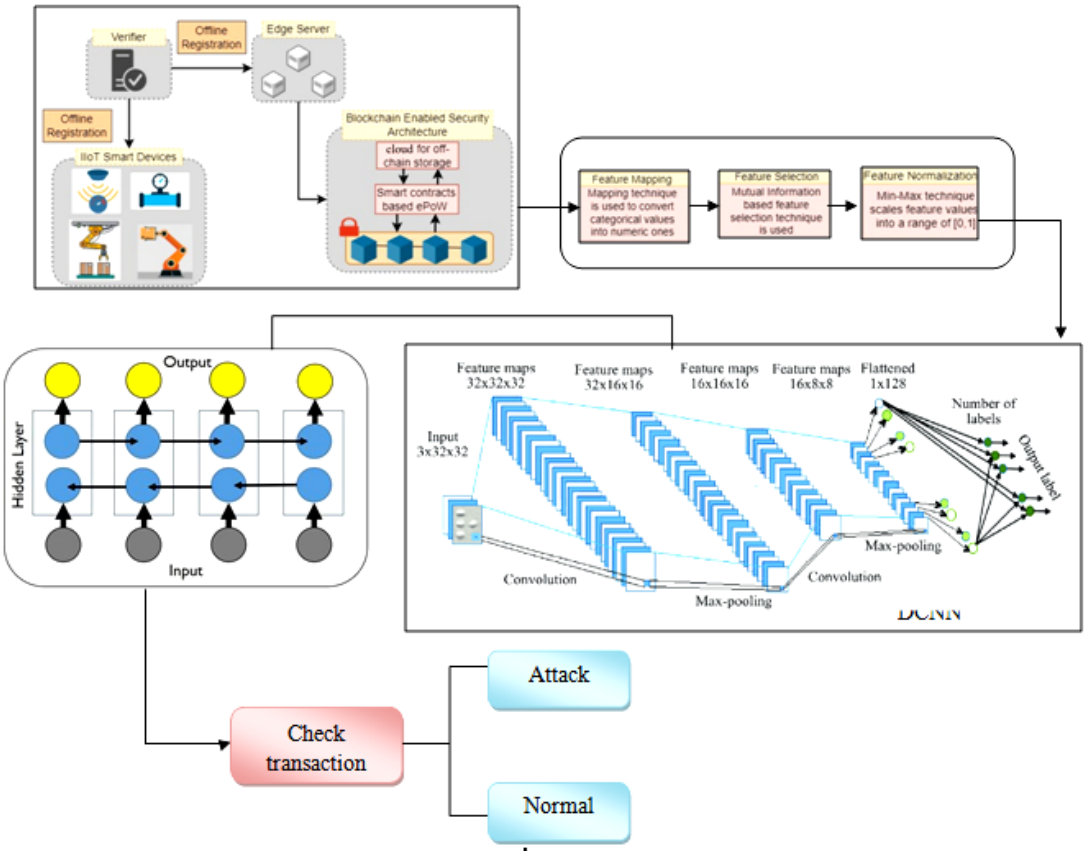


Figure 1. Overall block diagram of proposed method

The proposed BD-BILSTM is summarized in Figure 1, which shows the communication taking place among various parties. IoT devices are just one of the many communication entities included in this architecture. Verification *(V)*, edge servers (*EDGE*). All participating entities must be registered by V before being added to the network. Few resources and computational power are available to the S_{di}. The computing resources and power are constrained. Since each $S_{di}$is connected to the Internet, data can be sent and received online. (*EDGE*) includes data analysis servers, industrial computers, and other like gadgets. To undertake mining activities, one or more S_{di} are connected to EDGE. The BD-BILSTM systematic design consists of two major components: (i) a blockchain-authorized security framework and (ii) a deep learning-authorized security framework, this is illustrated in Figure.2 below and explained below,

To identify IoT device and safe data transfer, blockchain technology is employed. In the deep learning authorized security framework, transforming the original datasets' dimensions into a new structure using a DCCN approach. The way that these structures' function is explained in full below,

3.1. Block chain authorized security framework

The BD-LSTM is divided into six distinct phases in the first level of security: (i) initialization, (ii) registration and verification, (iii) encryption and decryption, (iv) block creation and validation, (v) data generation and block updation, and (vi) consensus. As shown below, all steps must be performed in a detailed manner.

(i) initialization phase

This stage is evaluated by trusted verifier *V* in order to bootstrap the framework settings. *V* adds the IoT sensor node S_d to the suggested framework.,

Step 1: With a Non-singular representation for the elliptic curve E_{P_N}(a, b): $y^2 = x^3 + ax + (b \bmod P_N)$, the verifier V selects the suitable biggest prime number P_N

Step 2: The verifier selects at random PR_{VK}(private key) ∈, Z_{P_N}Rk ∈ {0,1}Z_{P_N} and sets PR_{VK}as private key. Next, PB_{VK}(public key) is generated using $PB_{VK} = PR_{VK}$.

Step 3: Then, the Hash function H(.) based on one-way cryptography is chosen by V, and makes the required elements public.

(ii) Verification and Registration phase

IoT sensor node S_{di} asks the verifier *V* to join the blockchain network during the registration step. Once the *PK* is developed successfully, timestamp TS_i is stored for verification of the Sdi registration. • The PK is made up of ID_{sdi} vand M_{sd_i}which is submitted to verifier V with the time included.

(iii) Encryption and decryption phase:

A public key PB_{sd_i} and a private key PB_{sd_i} are produced once the IoT device S_{d_i} has been successfully registered by the verifying authority V.

$$CP1 = (P_N 1 * P_N) + SKEY_{sd_i} \quad (1)$$

$$CP2 = MSG_{sd_i} + \left(P_N 1 * PB_{sd_i}\right) + SKEY_{sd_i} \quad (2)$$

Here CP1 and CP2 denote the ciphertext. Finally, equation is used to decrypt the message (3)

$$MSG_{sd_i} = \left(\left(CP2 - PB_{sd_i}\right) * CP1\right) - SKEY_{sd_i} \quad (3)$$

(iv) Block generation and testing phase:

Beginning of S_{d_i} the block generation and evaluation procedure, For the Appropriate Recognition, brand-new block $ID_{sd_i}{}^{BLOCK}$ is performed by, which forwards it for inclusion into the blockchain with credentials. $PB_{sd_i}$and IB_{sd_i}. The real data is then preserved by the IPFS storage layer.

(v) Data generation and block updation:

This stage illustrates how S_{d_i} produces data and the corresponding block updates. $ID_{sd_i}{}^{TX}$ and makes updation in block. Furthermore, $ID_{sd_i}{}^{BLOCK}$ Becomes part of the blockchain network after being successfully updated.

(vi) Consensus phase:

Following the satisfactory ZKP verification, the ID_{sd_i} is produced, given to the appropriate Blockchain sensor node update, and IoT sensor node. In order to add transactions to the blockchain network and perform transaction verification, the *ePoW* consensus method is used i.e., I$ID_{sd_i}{}^{NEWIX}$by ID_{sd_i}.

3.2. Deep learning enabled security architecture

3.2.1. Deep convolutional neural network (DCNN)

In-depth learning Cyberattacks are recognized through a convolutional neural network (DCNN). Deep learning has the ability to reveal higher-level features and more abstract concepts that reveal links that are more complicated and interconnected than what is currently known about deep neural network methodologies.

Deep learning is defined by a significantly higher number of sequentially connected neural layers. Moreover, as a result of additional modifications, more data is typically needed for training and computational burdens as complexity increases. These developments provide the ability to quickly calculate repeated non-linear modifications of the crucial input data, which is the main strength of the architecture for deep learning and allows for end-to-end learning.

Three key ideas form the foundation of the CNN topology: temporal or spatial sampling, shared weights, as well as regional receptive domains. Hence, CNNs are often composed of various layers known as convolutional layers, and that small kernels comprise each convolutional layer that enable efficiently extracting high-level data. Layers that are fully connected receive input from the final convolutional layer.

The basic CNN model is composed of an alternating convolutional layer, input layer, non-linear layers and pooling or subsampling layers. In this case, has fewer completely linked layers, however a sofmax classifier is frequently found as the very last layer. Convolutional layers are made up of convolutional stages, detector stages, and pooling stages in accordance with a complex layer terminology.

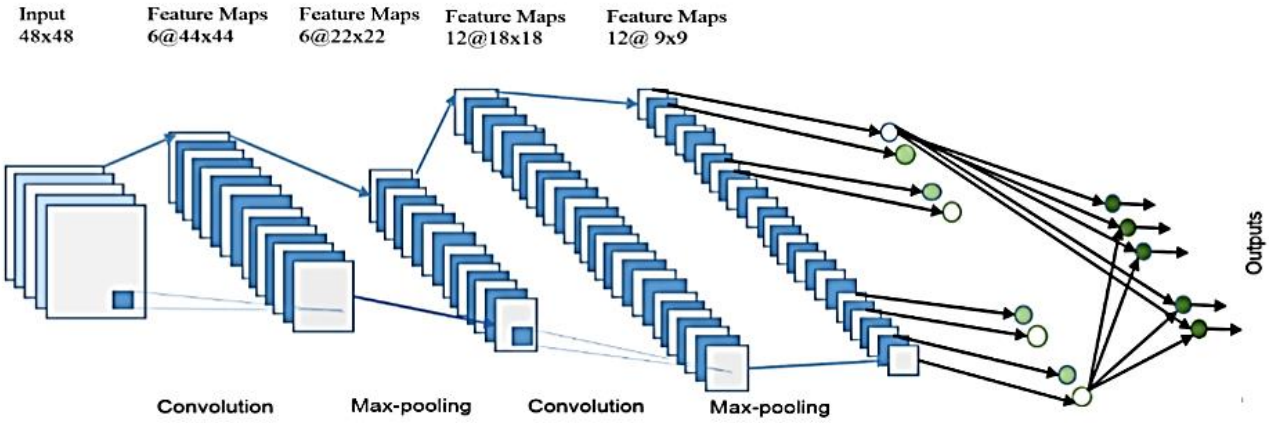


Figure 2. DCNN architecture

This indicates that there are multiple stages in each convolutional layer. Convolutional layers are routinely switched out with sub-sampling layers in order to speed up computation and eventually strengthen spatial and configurational invariance. This is a list of a CNN's fundamental layers.

Input layer:

Typically, a multidimensional array of data serves as the input. Where the network is fed data, Patterns, video signals, time series, or image pixels or their transformations can all be used as input data.

Convolutional layer:

It serves as CNN's main foundation. Convolution's main objective is to separate different characteristics from the input. Edges, corners, textures, and lines are among the low-level significant characteristics from which the first convolutional layer extracts information.

Non-linear layer or detector layer:

Each linear activation is detected by the detector stage using a nonlinear activation function. Many nonlinear activation functions are shown here. A neuron's output f as a function of its input x is typically represented as $f(x) = \tanh(x), sigmoid(x)$ or Rectified Linear Unit (ReLU). ReLU applies the function$y = \max(x, 0)$. The nonlinear properties are increased of the decision function in convolutional layer.

Pooling or down sampling layers:

Typically, a pooling layer decreases the feature maps' size of the feature maps and creates down sampled versions in the input map. Through pooling, the inputs are divided into regions of size $R \times R$with each region producing a single output. If a pooling layer receives an input of size $W \times W$, the output size P is calculated by,

$$P = \left|\frac{W}{R}\right|$$

The maximum output inside a rectangular region is the focus of the max pooling activity. Invariance is introduced using max pooling.

Fully connected layers:

The last level of the CNNs' topology, which is made up of a general multi-layer network, has been attained. In the subsequent layers, every activation from the previous layer will be a fully connected 1D layer. It is feasible to pull features from these layers to train another classifier.

3.2.2 Bidirectional Long Short-Term Memory (BiLSTM)

A model for sequence processing called Bi-LSTM comprises two LSTMs. One processing the information forward and the other processing it backward. The network can access more data with the aid of Bi-LSTMs, which is advantageous for the context of the algorithm. Bidirectional LSTM connects both of the hidden LSTM (Bi-LSTM) layers to the output layer. In the application, using two LSTM as one layer encourages improving the learning long-term dependency, which subsequently will increase model performance. Bi-LSTM architecture shows in Figure 3.

The reversed inputs from time $t-1$ to $t-n$ are used to calculate the backward LSTM layer output sequence $\overleftarrow{h}$ just because the unidirectional and forward LSTM layer output sequences, h and h′, are generated similarly. The function was then applied to these output sequences to create the output vector y_t. Similar to an LSTM layer, a Bi-LSTM layer's final output can be denoted by a vector, $Y_t = y_{t-n}, \ldots, y_{t-1}$ where the final element, y_{t-1}, is the anticipated heart rate for the subsequent iteration.

Given input tasks $X = (x_1 \ldots, x_T)$, the hidden vector tasks $h = (h_1, \ldots, h_T)$ and the output vector tasks $Y = (y_1, \ldots, y_T)$ using the subsequent equations from $t = 1$ to T.

$$h_t = H(W_{xh}x_t + W_{hh}h_{t-1} + b_h) \quad (4)$$

$$y_t = W_{hy}h_t + b_0 \quad (5)$$

Where W and b stand for weight and bias matrices, respectively, and the function for a hidden layer is H. H is often a sigmoid function applied element by element.

$$i_t = \sigma(W_{xi}x_t + W_{hi}h_{t-1} + W_{ci}c_{t-1} + b_i) \quad (6)$$

$$f_t = \sigma(W_{xf}x_t + W_{hf}h_{t-1} + W_{cf}c_{t-1}b_f) \quad (7)$$

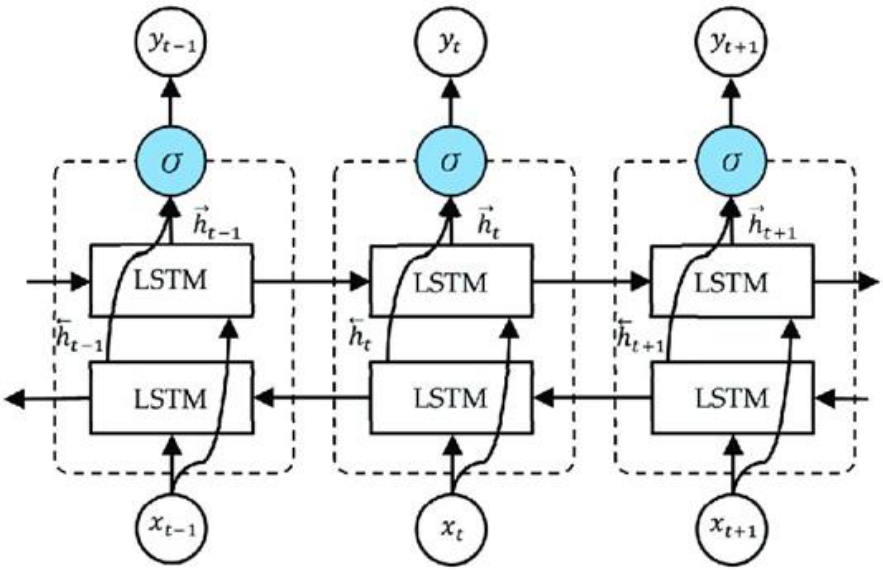


Figure 3. Bi-LSTM architecture

$$c_t = f_t c_{t-1} + i_t \tanh(W_{xc}x_t + W_{hc}h_{t-1} + b_c)$$

$$O_t = \sigma(W_{xo}x_t + W_{ho}h_{t-1} + W_{co}c_t + b_o) \quad (9)$$

$$h_t = O_t \tanh(c_t) \quad (10)$$

The input gate, forget gate, output gate, and cell activation vectors, respectively, are represented by the letters *i f, o* and c, while the logistic sigmoid function is represented by σ. These variables all have the same size as the hidden vector h. Input-output gate matrix W_{x0} and hidden input gate matrix W_{hi} are both used in computers.

The following formula is used to determine the output vector y(t).

$$y(t) = \sigma y(\overrightarrow{h_t}, \overleftarrow{h_t}) \quad (11)$$

where the σy function combines the hidden layer output neuron sequences. and is capable of adding, concatenating, multiplying, and averaging any of the four operations.

4. RESULT & DISCUSSION

This section rates the effectiveness of proposed BD-BiLSTM. The proposed model has been evaluated using the conventional numerical parameters listed below,

4.1 Evaluation Metrics

4.1.1. Accuracy

The accuracy of all correctly predicted categories to the dataset's actual classifications represents the prediction algorithm's accuracy. Equation (12) determines the model's accuracy. Each prediction model typically yields four distinct outcomes: False Negative (FN)., False Positive (FP), True Negative (TN), and True Positive (TP).

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+TN+FN+FP}} \quad (12)$$

4.1.2. Precision

(8) Precision is an exact definition of the frequency of positive abnormalities in a particular picture. The higher proportion of information is highlighted by precision. Equation (13) calculates the precision of the model.

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} = \frac{\text{True position}}{\text{Total predicted position}} \quad (13)$$

4.1.3. Recall

The amount of accurate phishing URL predictions made over all URLs in the dataset is known as the prediction algorithm's recall. Equation (14) determines the model's recall.

$$\text{Recall} = \frac{\text{TP}}{\text{TP+FN}} = \frac{\text{True position}}{\text{Total prediction position}} \quad (14)$$

4.1.4. F1 score

The method of calculating the classifier's harmonic mean for recall and precision. It is possible to turn it into a single metric. Equation (15) determines the model's F1 score.

$$\text{F1 score} = \frac{2\times(\text{precision}\times\text{recall})}{(\text{precision+recall})} \quad (15)$$

4.2 Performance metrics

Figure 4 displays the comparability analysis's accuracy and F1 score for the suggested and existing methods.

The new BD-BiLSTM approach is compared to the existing PBDL, BDL-SMDTD, and GWMNN. The prediction results were examined using measures for precision, F1 score, recall, and accuracy.

The proposed BD-BiLSTM is high in comparison to other existing approaches. The size of the F1 is 0<100 in size, shown in figure 4.

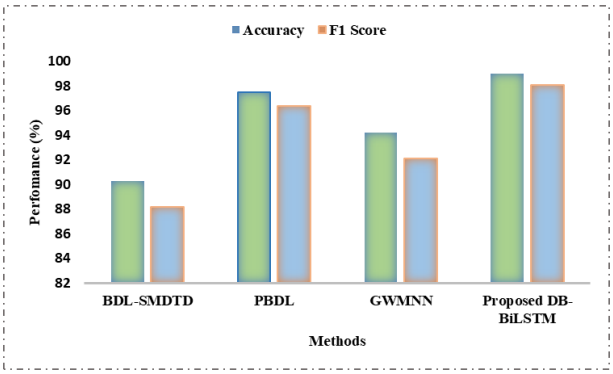


Figure 4. Comparative analysis with existing and Proposed method

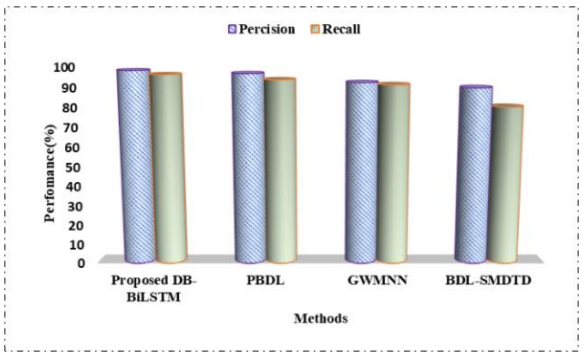


Figure 5. Comparative analysis with existing and Proposed method

Figure 5. Shows the Recall and precision of the analysis in comparison to the suggested and existing methods. The existing PBDL, BDL-SMDTD, GWMNN are compared with proposed BD-BiLSTM method. Performance analysis of existing CICIDS, TON-IOT vs proposed DB-BiLSTM shown in Figure 6.

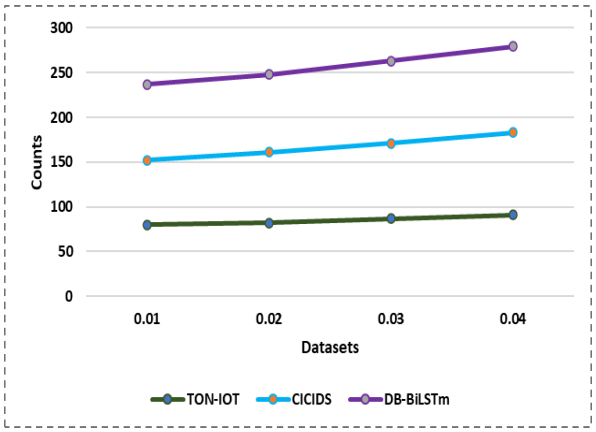


Figure 6. Performance analysis of existing CICIDS, TON-IOT vs proposed DB-BiLSTM

TON-IOT covers nine aberrant observations, the majority of which are encountered in IoT/IoT environments, including backdoors and DDoS., it consists of 43 labelled features. Ransomware, SSH-Patator, and other updated attack observations are included in CICIDS., it consists of 78 labelled features. As a result, the proposed BD-BiLSTM has high performance than CICIDS and TON-IOT.

5. CONCLUSION

In this paper, a new Deep-BiLSTM technique based on Blockchain is created to transmit data securely in IoT-approved healthcare systems. To guarantee security, BD-BiLSTM offers a two-level design. At the initial level, a blockchain architecture was shown in particular, the first unique a scalable blockchain architecture using the Zero Knowledge Proof (ZKP) technique is suggested to guarantee data security and integrity. The bidirectional long short-term memory is used by the deep convolutional neural network on the second level's deep learning architecture to recognize network intrusions. The validated data is then utilized to develop a deep learning framework for identifying HS network breaches. The use of IPFS-based off-chain storage enhances the scalability of BD-BiLSTM. The latter combines Bidirectional Long Short-Term Memory (BiLSTM) and Deep Convolutional Neural Network to create an efficient intrusion detection system. The suggested solution has been compared Using analysis with two public datasets (CICIDS-2017 and ToN-IoT), our proposed Bi-LSTM performs 96% better. According to experimental findings of F1 score, recall precision, and accuracy the proposed BD-BiLSTM technique has 98% in which is relatively high compared to existing methods of BDL-SMDTA, PBDL and GWMNN.

CONFLICTS OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

FUNDING STATEMENT

No funding was received to assist with the preparation of this manuscript.

ACKNOWLEDGEMENTS

The authors would like to thank the reviewers for all of their careful, constructive and insightful comments in relation to this work.

REFERENCES

[1] J. Li, J. Cai, F. Khan, A.U. Rehman, V. Balasubramaniam, J. Sun, and P. Venu. “A secured framework for sdn-based edge computing in IOT-enabled healthcare system”, *IEEE Access*, vol. 8, pp.135479-135490, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] K. Wang, C.M. Chen, Z. Tie, M. Shojafar, S. Kumar, and S. Kumari. “Forward privacy preservation in IoT-enabled healthcare systems”, *IEEE transactions on industrial informatics*, vol.18, no. 3, pp.1991-1999, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] R. Arul, R. Alroobaea, U. Tariq, A.H. Almulihi, F.S. Alharithi, and U. Shoaib. “IoT-enabled healthcare systems using block chain-dependent adaptable services”, *Personal and Ubiquitous Computing*, pp.1-15, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] W. Li, Y. Chai, F. Khan, S.R.U. Jan, S. Verma, V.G. Menon, and X. Li. “A comprehensive survey on machine learning-based big data analytics for IoT-enabled smart healthcare system”,*Mobile networks and applications*, vol.26, pp.234-252, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] O. Said, and A. Tolba, "Design and evaluation of large-scale IoT-Enabled healthcare architecture", *Applied Sciences*, vol.11, no. 8, p.3623, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[6] S. Peneti, M. Sunil Kumar, S. Kallam, R. Patan, V. Bhaskar, and M. Ramachandran. "BDN-GWMNN: internet of things (IoT) enabled secure smart city applications", *Wireless Personal Communications*, vol.119, pp.2469-2485, 2021, [CrossRef] [Google Scholar] [Publisher Link]

[7] A. Sardar, S. Umer, R.K. Rout, S.H. Wang, and M. Tanveer, "A Secure Face Recognition for IoT-Enabled Healthcare System", *ACM Transactions on Sensor Networks (TOSN)*, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] P. Zhang, F. Liu, N. Kumar, and G.S. Aujla, "Information classification strategy for blockchain-based secure sdn in iot scenario", In IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 1081-1086. IEEE, 2020, July. [CrossRef] [Google Scholar] [Publisher Link]

[9] S. Neelakandan, J.R. Beulah, L. Prathiba, G.L.N. Murthy, E.F. Irudaya Raj, and N. Arulkumar. "Blockchain with deep learning-enabled secure healthcare data transmission and diagnostic model", *International Journal of Modeling, Simulation, and Scientific Computing*, vol.13, no. 04, p.2241006, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] R. Kumar, P. Kumar, R. Tripathi, G.P. Gupta, A.N. Islam, and M. Shorfuzzaman, "Permissioned Blockchain and Deep Learning for Secure and Efficient Data Sharing in Industrial Healthcare Systems", *IEEE Transactions on Industrial Informatic*s, vol.18, no. 11, pp.8065-8073, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] S. Aggarwal, R. Chaudhary, G.S. Aujla, N. Kumar, K.K.R. Choo, and A.Y. Zomaya, 2019. "Blockchain for smart communities: Applications, challenges and opportunities", *Journal of Network and Computer Applications*, vol.144, pp.13-48. [CrossRef] [Google Scholar] [Publisher Link]

[12] W. Zhao, C. Jiang, H. Gao, S. Yang, and X. Luo. "Blockchain-enabled cyber–physical systems: A review", *IEEE Internet of Things Journal*, vol.8, no. 6, pp.4023-4034, 2020 [CrossRef] [Google Scholar] [Publisher Link]

[13] M. Zolanvari, M.A. Teixeira, L. Gupta, K.M. Khan, and R. Jain. "Machine learning-based network vulnerability analysis of industrial Internet of Things", *IEEE Internet of Things Journal*, vol.6, no. 4, pp.6822-6834, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[14] O. Alkadi, N. Moustafa, B. Turnbull and K.K.R. Choo. "A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks", *IEEE Internet of Things Journal*, vol.8, no. 12, pp.9463-9472, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[15] S. Rathore, B.W. Kwon, and J.H. Park, "BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network", *Journal of Network and Computer Applications*, vol.143, pp.167-177, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[16] C. Liang, B. Shanmugam, S. Azam, M. Jonkman, F. De Boer, and G. Narayansamy. "Intrusion detection system for Internet of Things based on a machine learning approach", In 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), pp. 1-6. IEEE, 2019, March. [CrossRef] [Google Scholar] [Publisher Link]

[17] M. Hasan, M.M. Islam, M.I.I. Zarif, and M.M.A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches", *Internet of Things*, vol.7, p.100059, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[18] R. Gupta, S. Tanwar, F. Al -Turjman, P. Italiya, A. Nauman, and S.W. Kim. "Smart contract privacy protection using AI in cyber-physical systems: tools, techniques and challenges", *IEEE access*, vol.8, pp.24746-24772, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[19] M. Keshk, B. Turnbull, N. Moustafa, D. Vatsalan, and K.K.R. Choo. "A privacy-preserving-framework-based blockchain and deep learning for protecting smart power networks", *IEEE Transactions on Industrial Informatics*, vol.16, no. 8, pp.5110-5118, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[20] I. Namatēvs, "Deep convolutional neural networks: Structure, feature extraction and training", *Information Technology and Management Science*, vol. 20, no.1, pp.40-47, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[21] J. Xu, P. Vijayakumar, P.K. Sharma, and U. Ghosh, "Homomorphic encryption-based privacy-preserving federated learning in iot-enabled healthcare system", *IEEE Transactions on Network Science and Engineering*, 2022., [CrossRef] [Google Scholar] [Publisher Link]

[22] G.S. Aujla, and A. Jindal, "A decoupled blockchain approach for edge-envisioned IoT-based healthcare monitoring", *IEEE Journal on Selected Areas in Communication*s, vol.39, no. 2, pp.491-499, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[23] A.A. Khan, A.A. Laghari, M. Shafiq, O. Cheikhrouhou, W. Alhakami, H. Hamam, and Z.A. Shaikh, "Healthcare Ledger Management: A Blockchain and Machine Learning-Enabled Novel and Secure Architecture for Medical Industry", *Human-Centric Computing and Information Sciences*, vol.12, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[24] T.R. Gadekallu, M.K. Manoj, N. Kumar, S. Hakak, and S. Bhattacharya, "Blockchain-based attack detection on machine learning algorithms for IoT-based e-health applications", *IEEE Internet of Things Magazine*, vol.4, no. 3, pp.30-33, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[25] N. Al Asad, M.T. Elahi, A. Al Hasan, and M.A. Yousuf, November. "Permission-based blockchain with proof of authority for secured healthcare data sharing", *In 2020 2nd International Conference on Advanced Information and Communication Technology (ICAICT)*, pp. 35-40, IEEE, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[26] H. Babbar, S. Rani, and S.A. AlQahtani. "Intelligent Edge Load Migration in SDN-IIoT for Smart Healthcare", *IEEE Transactions on Industrial Informatics*, vol.18, no. 11, pp.8058-8064, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[27] B.S. Egala, A.K. Pradhan, V. Badarla, and S.P. Mohanty, "Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control", *IEEE Internet of Things Journal*, vol.8, no. 14, pp.11717-11731, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[28] E. Ashraf, N.F. Areed, H., Salem, E.H. Abdelhay, and A. Farouk, "Fidchain: Federated intrusion detection system for blockchain-enabled iot healthcare applications", In Healthcare Vol. 10, No. 6, pp. 1110. MDPI, 2022, June. [CrossRef] [Google Scholar] [Publisher Link]

[29] S.A. ElRahman, and A.S. Alluhaidan, "Blockchain technology and IoT-edge framework for sharing healthcare services". *Soft Computing*, vol.25, no. 21, pp.13753-13777, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[30] P. Bhattacharya, S. Tanwar, U. Bodkhe, S. Tyagi, and N. Kumar. "Bindaas: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications", *IEEE transactions on network science and engineerin*g, vol.8, no. 2, pp.1242-1255, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[31] S. Pal. “Internet of Things and Access Control: Sensing, Monitoring and Controlling Access in IoT-Enabled Healthcare Systems”, vol. 37, 2021. Springer Nature. [CrossRef] [Google Scholar] [Publisher Link]
[32] M. Javaid, and I.H. Khan. “Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic”, *Journal of Oral Biology and Craniofacial Researc*h, vol.11, no. 2, pp.209-214, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[33] S. Rani, M. Chauhan, A. Kataria, and A. Khang. “IoT equipped intelligent distributed framework for smart healthcare systems”, arXiv preprint arXiv:2110.04997, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[34] G. Hameed, Y. Singh, S. Haq, and B. Rana, “Blockchain-based model for secure IoT communication in smart healthcare. In Emerging Technologies for Computing”, *Communication and Smart Cities: Proceedings of ETCCS* 2021, pp. 715-730. Singapore: Springer Nature Singapore, 2022. [CrossRef] [Google Scholar] [Publisher Link]
[35] T. Veeramakali, R. Siva, B. Sivakumar, P.C. Senthil Mahesh, N. Krishnaraj, “An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model”, *The Journal of Supercomputing.* 2021 Sep 1:1-21. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

R.R. Sathiya completed her Bachelor’s Degree in Information Technology from Bharathiar University, Coimbatore, Tamilnadu, India, in the year 2004 and her Master’s Degree in Computer Science and Engineering from Anna University, Coimbatore, Tamilnadu, India, in the year 2010. Her areas of interest include cloud computing, Internet of Things, and Image processing. She has published technical papers in International Conferences and Journals.

S. Rajakumar, is currently working as Professor in the department of Electronics and Communication Engineering, Panimalar Engineering College, affiliated to Anna University, Chennai. He has organized several Conferences and Seminars related to Image Processing and Signal Processing. He completed his B.E., degree in Electronics and Communication Engineering from Sun College of Engineering and Technology, Nagercoil affiliated to Manonmaniam Sundaranar University, Tirunelveli. He obtained his M.E., degree in Applied Electronics and Ph.D in Image Processing from Sathyabama University, Chennai, India in the year 2006 and 2013 respectively. He has published several research articles in National and International Conferences and Journals. His areas of interest include Digital Signal Processing, Image Processing, Pattern Recognition, VLSI and Communication Engineering.

J. Sathiamoorthy is currently working as an Associate Professor, Department of Computer Science and Engineering in RMK Engineering College, Chennai. He has completed M. Tech (CIT) and Ph.D from Manonmaniam Sundaranar University, Tirunelveli Tamilnadu, India. He has over 18 years of teaching experience. He has published papers in Network Security in National and International journals and has presented in International Conferences and Seminars. He has published more than 20 research papers in reputed journals in the area of ad-hoc networks especially MANET, VANET, FANET and Underwater Communication. He has acted as a reviewer in many reputed international journals.

Arrived: 10.08.2023
Accepted: 19.10.2023

International Journal of Computer and Engineering Optimization (IJCEO)
Volume 1, Issue 1, September – October (2023)

RESEARCH ARTICLE

C-AVPSO: DYNAMIC LOAD BALANCING USING AFRICAN VULTURE PARTICLE SWARM OPTIMIZATION

Dharavath Champla[1,*], V. Ramkumar [2] and P. Ajay[3]

[1]Department of Computer Science and Engineering, SRM Easwari Engineering college, Chennai.
[2] Department of Electronics and Communication Engineering, K. Ramakrishnan college of Technology, Samayapuram, Tamil Nadu 621112, India.
[3]Department of Electronics and Communication Engineering, Rathinam Technical Campus, Eachanari, Coimbatore, Tamil Nadu, 641021 India

[*]*Corresponding e-mail: champla.805@gmail.com*

Abstract – A new technology called cloud computing enables users to access services from anywhere, at any time, under different conditions, and is controlled through an outside cloud service provider. Cloud task scheduling is a complicated optimisation problem. However, both under- and over-loading conditions cause a range of system problems as far as power consumption, machine failures, and so forth are concerned. Consequently, virtual machine (VM) work-load balancing is regarded as a key element of cloud task scheduling. In this paper, a novel cloud-based African vulture particle swarm optimisation [C-AVPSO] has been proposed. Using C-AVPSO, the developed optimization algorithm solves the dynamic load balancing problem effectively. This approach used the AVO process to get the exploration space, while the increased response was identified by the PSO procedure. This algorithm successfully addresses the task's resource utilization, response time, and budgetary restrictions. As a result of combining the AVO and PSO algorithms into the proposed AVPSO algorithm, in the cloud context, load balancing performance measures and convergence rate are enhanced. To enhance the operation's efficiency, the proposed method balances VM loads efficiently. The proposed framework is compared to existing approaches like QMPSO, FIMPSO and ACSO Based on energy utilization, degree of imbalance and task migration, response time and resource utilization. The proposed C-AVPSO technique reduces resource utilization of 19.1%, 31%, and 54% than, QMPSO, FIMPSO and ACSO existing techniques.

Keywords *– DYNAMIC Load Balancing, swarm optimization, PSO algorithm, Virtual machine, Cloud computing.*

1. INTRODUCTION

Cloud computing is the most advanced and rapidly evolving technology in computer science today [27]. The cloud is a network of IT resources, and computing is the act of executing work in remote connection to those resources and charging a pay-as-you-go system. A technology based on the internet that offers a variety of cloud-based services that are efficient, dependable, and inexpensive, [29] and these services may be accessed from any device, location, or time. It offers on-demand self-service, which means that when we need a resource, we can use (configure) it without requiring the assistance of a third party. Today, there are other cloud service providers to choose from, such as Google Cloud and Amazon Web Services. A computer model called "cloud computing" gathers resources over the Internet. [28] For example, servers, storage, applications, and services.

By ensuring sufficient cloud resource management, the affordable and scalable benefits of cloud computing may be realized. One of the major elements of the cloud structure is that these cloud resources are virtual. Customers can rent services of Cloud Service Provider (CSP) offerings [30]. With resources for the virtual cloud at hand, the CSP's role in providing services to the user is highly complex. As a result, load balancing has received more attention from researchers. This load balancing improves overall system performance. Cloud Service Providers (CSPs) are left with unbalanced computers that have a wide Resources and tasks gradients of user’s consumption as a result. [11]

No machine is overworked or underpowered thanks to Redistributing workloads in distributed systems like the cloud [12,13]. The technique of load balancing has assisted networks and resources in delivering the highest throughput with the quickest reaction times. [14In load balancing, a number of factors are accelerated to improve the performance of the cloud, such as reaction time, execution time, and system stability. [15,16]. Several academics have discussed load balancing strategies, such as (i)static load balancing and (ii) dynamic load balancing, in both heterogeneous and homogeneous situations. [17]

When the single VM is overloaded with tasks and if there are a lot of empty virtual machines in the cloud network, it would be best to move the workloads from the

overworked to the underworked ones. [26]. Calculating every conceivable task-resource mapping in a cloud context is challenging, and finding the best mapping is not an easy process. [24] Thus, we require an effective task distribution method that can schedule tasks in a way that prevents a large number of virtual computers from being overburdened or underloaded. The cloud task scheduler [25] then begins to perform load balancing operations as soon as it has allocated the task to a virtual machine, so that tasks can be transferred between overloaded and underloaded virtual machines after the task has been allocated to a virtual machine while maintaining the balance of all virtual machines.

This is an overview of this paper's main contributions;

- In this paper, a novel cloud-based African vulture particle swarm optimisation [C-AVPSO] has been proposed.
- The C-AVPSO optimization algorithm efficiently balances load in cloud networks. In this technique, the AVO process was used to acquire the exploration space, and the PSO procedure was used to identify the improved response.
- In the developed algorithm, the constraints related to resource utilization, response time, and cost are successfully resolved.
- In a cloud environment, C-AVPSO improves the convergence rate and performance metrics by combining AVO and PSO algorithms. This method maximizes operation efficiency by efficiently balancing VM loads.
- A comparison of the proposed framework and existing approaches like QMPSO, FIMPSO and ACSO is conducted based on energy consumption, degree of imbalance, migration of tasks, response time, and resource usage.

Therefore, the remainder of this article will be structured as follows: The first part of the paper provides a review of the literature. Following that, the proposed research is evaluated in Section 3, results are discussed in Section 4; finally, a conclusion is presented in Section 5.

2. LITERATURE SURVEY

For load balancing in CC, a variety of heuristics and meta-heuristic methods have been used. This section summarizes the pertinent work in these areas with a particular emphasis on African vulture particle swarm optimization (AVPSO) for dynamic load balancing. In this part, we've talked about a few of those technique.

In 2020 Mishra, S.K. et al. [1] proposed a category of algorithms for cloud load balancing. Additionally, several approaches to load balancing in cloud computing platforms are explained. Finding overloaded and under loaded nodes and balancing the load are the steps in the load balancing process. between them. The simulation is performed in clouds simulator to examine the Heuristic-based performance methods, and the results are detailed.

In 2019 Afzal, S. and Kavitha, G., [2] proposed a comprehensive encyclopaedic analysis about the load balancing techniques. The pros and disadvantages of the current methods are described, and algorithms are addressed. As a result, 80% of works do not analyze how the load balancing algorithm performs while evaluating performance.

In 2018 Volkova, V.N. et al. [3] proposed the cloud analyst analytical tool is used to assess various algorithms. A comparison of algorithm load balancing algorithms is also performed. Load balancing helps the centralized server run better. The load balancing algorithm investigated. Results were compared using Data on total response time, center time, and data center load and processing on an hourly basis cost.

In 2022 Jena, U.K., et al. [4] proposed QMPSO is a revolutionary methodology for dynamic load balancing across virtual machines that uses a mixture of an enhanced Q-learning algorithm and amended Particle Swarm Optimization (MPSO). Hybridization's goal is to improve machine performance through load balancing among the virtual machines. The algorithm's resilience was demonstrated by comparing the QMPSO simulation results to the current load balancing and scheduling technique.

In 2019 Polepally, V. and Shahu Chatrapati, K. [5] proposed a load-balancing technique based on constraint measure. First, the load and capacity of each virtual machine are calculated. The load balancing approach computes and analyses the decision factor for each virtual machine. The suggested load balancing method's performance is compared to those of current load balancing techniques like HDLB, DLB, and HBB-LB for capacity and load estimation parameters.

In 2022 Latchoumi, T.P. and Parthiban, L. [6] proposed to obtain the best resource scheduling in a CC scenario, an innovative Quasi Oppositional Dragonfly Algorithm for Load Balancing (QODA-LB) was developed. The main goal of this strategy is to decrease task execution costs and times while keeping the load distributed evenly across all VMs in the CC system. The simulation results showed superior performance to the leading methods and optimal load balancing efficiency.

In 2020 Devaraj, A.F.S., et al. [7] proposed, Firefly and the Improved Multi-Objective Particle Swarm Optimization (FIMPSO,) as a new load balancing algorithm. According to the simulation results, the FIMPSO algorithm produced the most efficient end with shortest common response time of 13.58ms, surpassing all other comparable techniques with the greatest CPU utilization of 98%, the highest memory utilization of 93%, the highest dependability of 67%, the greatest throughput of 72%, and the maximum make span of 148.

In 2020 Semmoud, A., et al. [8] proposed a fresh method for various cloud computing configurations for load balancing. The suggested method seeks to reduce Makespan and VM idle time while raising system stability.When the VM load surpasses the Starvation Threshold, an adaptive limit, the suggested method restricts task transfer. We compared the STLB algorithm to a load balancing algorithm that was inspired by honey bee behaviour, and we

found that the suggested method outperformed about the amount of migrations and the typical idle time, the HBB-LB algorithm.

In 2021 Balaji, K., et al. [9] proposed, a load balancing system that addresses optimization suggested by using the adaptive cat swarm optimization (ACSO) method. The effectiveness of the suggested method is assessed with a variety of value indicators, and its performance is contrasted with that of competing techniques. Our suggested solution takes the least time and energy in compared to the current algorithm.

In 2017, Kumar, M. and Sharma, S.C. [10] proposed a load-dynamic balancing method that speeds up cloud resource use while decreasing make-span time. a conventional approach using Cloud load balancing through task migration. In comparison to FCFS and SJF approaches, the results of the trial show that the recommended method lowers the manufacture span time and boosts the average resource utilisation ratio.

It can be seen from the reviews above that these methods have some shortcomings. This research proposes a AVPSO technique for dynamic load balancing to address these disadvantages.

3. PROPOSED METHODOLOGY

This article presents a new algorithm for African vulture particle swarm optimization that optimizes dynamic load balancing by considering cost, resource use, and response time. By employing this technique, you may balance job preferences, boost the throughput of the virtual machines, and disperse the load among them by adjusting the waiting times for complicated tasks.

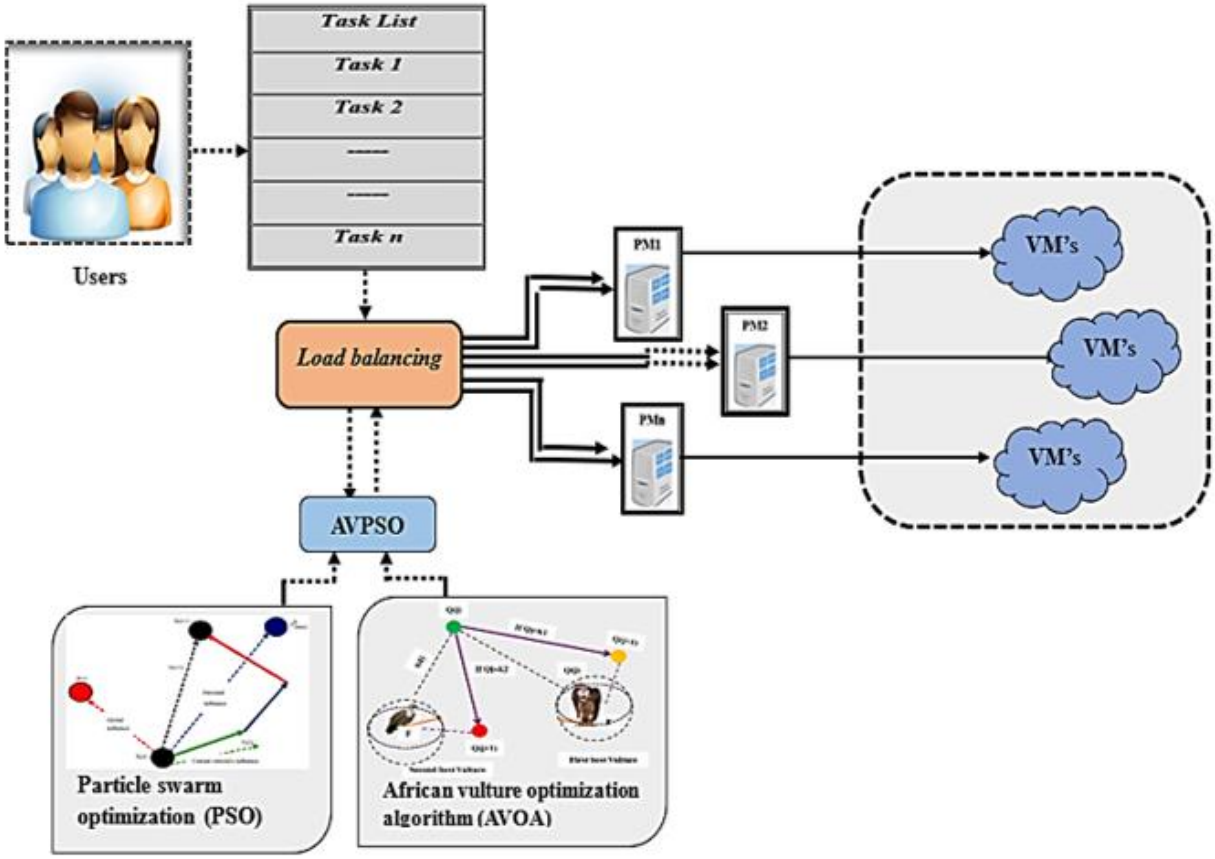


Figure 1. Block diagram of proposed methodology

Figure.1 illustrates the proposed methodology. The primary process in the cloud is workload distribution to virtual machines (VMs). Using node performance data, decisions about load balancing happen in the dynamic load balancing mode. Due to low number of VMs, resource delivery to the task is crucial in cloud systems.

As a result of the VM being overburdened with jobs, the reaction time of the system is lengthened. Thus, a dynamic load-balancing procedure based on AVPSO is suggested to distribute the tasks across the virtual machines (VMs). This strategy involves moving Underloaded VMs take on the VMs' burdened tasks. As a result, both the latent times and the performance are accelerated. The recommended work-based load balancing method distributes the load in the cloud efficiently. The system increases resource utilization while reducing costs and response times. The capacity of each VM is determined after job scheduling. Divide the overflow, underload, and balanced containers according to the VM's remaining capacity. To complete the load balancing procedure, the ideal underload container is found in the proposed task. The tasks are then moved using the migration approach of the best under loaded virtual machines to the worst overloaded

ones. The AVO algorithm is used into PSO to finish the load balancing process and obtain the search space.

3.1. Load balancing in cloud

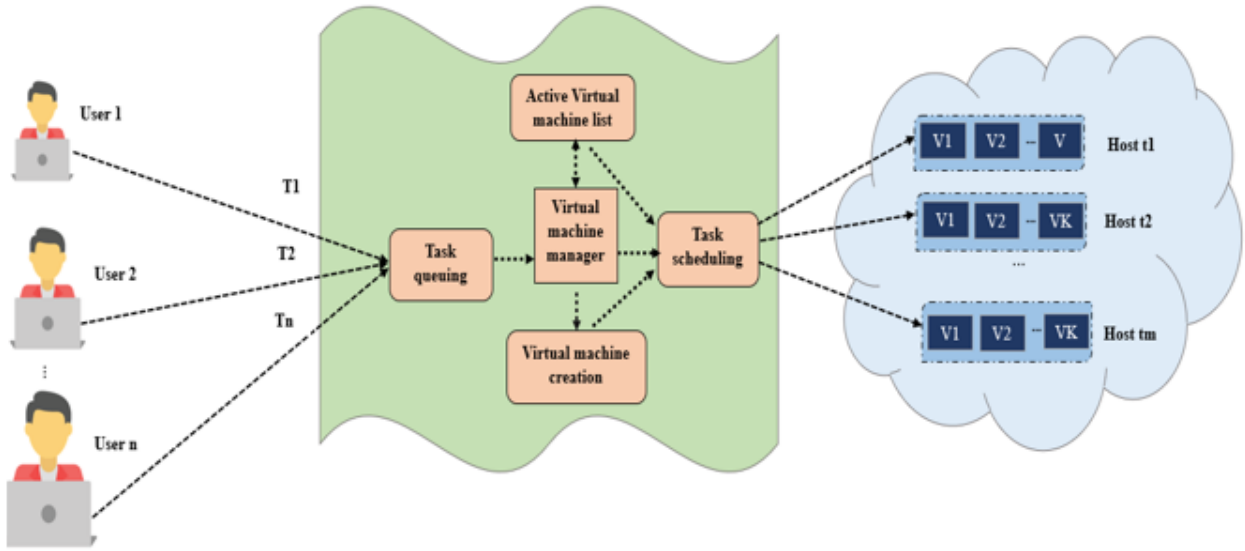


Figure 2. Scheduling cloud tasks for load balancing

Figure 2 depicts the scheduling task in cloud. Owing to cloud computing, that offers cloud services to cloud consumers, every operation is completed in a cloud environment. Due to the enormous volume of diverse input tasks so as to balance the demands of diverse resources, load balancing is necessary. The cloud system's task queue receives the tasks with n inputs $T_1, T_2, \dots T_n$ .The Virtual Machine head then the get input tasks from task queue and have a comprehensive knowledge of the active VM, existing resources across servers, and the length of the local task queue across all hosts. The system's resource availability was confirmed by the VM manager. The VM management submitted the tasks to the task scheduler if the group of tasks could be completed using the active VMs that are now available. If resource availability does not meet requirements, the VM management generate the necessary VMs in the server. Task allotment in cloud computing is therefore quite difficult. The service's QoS degrades when only a small number of VMs are overloaded, only a small number are free, or when there are fewer tasks to complete. Users may switch to another Cloud provider if they are unhappy with their current service as a result. Each cloud server is limited in the amount of virtual machines it can support.

3.2. Particle Swarm Optimization (PSO)

Particle swarm optimisation (PSO), is one of the bio-inspired algorithms, is basic in its quest to find the supreme answer in the area of problems. It is distinct from conventional optimisation methods in that it only uses the objective function itself and does not depend on the gradient or any differential forms of the objective function. The search is impacted by two distinct learning processes carried out by the particles in PSO. Each particle learns from its own movement-related experiences as well as those of other particles. Learning from one's own experiences is referred to as cognitive learning, whereas social learning involves learning from others. Using social learning, each swarm particle visits the best solution, which is then recorded in each particle's memory as *gbest*. The particle stores the best solution it has independently discovered so far, known as *pbest*, in its memory through cognitive learning. In terms of PSO, time is the iteration. The rate at which the position is changing in relation to the iteration can be regarded of as the velocity in PSO. The iteration counter increases by a factor of unity, which leads to equalize velocity V and position X, the dimensions must be the same.

The most efficient response for a D-dimensional search space, with the i^{th} particle of the swarm at the step time t denoted by a D- dimensional vector., $x_i^t = (x_{i1}^t, x_{i2}^t, \dots . x_{iD)}^t{}^T$. Likewise, the velocity at step time t can be represented by another D−dimensional vector $v_i^t = (v_{i1}^t, v_{i2}^t, \dots, v_{iD}^t)^T$.

The earlier position of the i^{th} particle at the step time t is denoted as $p_i^t = (p_{i1}^t, p_{i2}^t, \dots, p_{iD}^t)^T$. $'g'$indicates which particle is the most efficient in swarm. Using velocity update equation, the i^{th} particle's velocity is upgraded in equation (1)

Velocity update equation:

$$v_{id}^{t+1} = v_{id}^t + c_1 r_1 (p_{id}^t - x_{id}^t) + c_2 r_2 (p_{gd}^t - x_{id}^t) \quad (1)$$

As shown in (2), the position is upgraded based on the position update equation;

Position update equation:

$$x_{id}^{t+1} = x_{id}^t + v_{id}^{t+1} \quad (2)$$

Where, $d = 1,2, \dots D$ denotes the dimensions where the values i=1,2,...,s stand for the particle index. Whereas c1 and c2, or the cognitive and social scaling factors, are constants, S is the size of the swarm. It seems from

equations (1) and (2) that each particle's dimensions are changed individually. Through the locations of the top places, *gbest* and *pbest*, so far discovered. Equation (1) and (2) outline the PSO algorithm's fundamental configuration. Algorithm provides a PSO method algorithmic approach.

Algorithm 1

Create a D-dimensional swarm which has been initialized with the velocity vectors associated with it;

for t=1 to the *maximum bound pn the number of iterations* **do**

for i=1 to S **do**

for d=1 to D **do**

Implement equation 1 to update velocity;
Implement equation 2 to position velocity;

end

Evaluate updated location fitness;

Prior data on gbest and pbest be updated on necessity;

end

Stop when the problems solved by gbest;

end

3.3 African Vulture Optimization algorithm (AVOA)

The algorithm, known as the AVOA illustrates how African vultures navigate and forage for food. African vultures are among the rare species of vultures capable of reaching the maximum altitude among the various vulture species. African vultures are continually moving from one place to an additional in pursuit of better food sources due to their circular motions in the sky. They are at odds with one another in order to obtain the food source. The initial vultures used by the AVO algorithm are some random individuals, and after determining their objective value, their ability is calculated. Each time, one of the top two vultures is either moved or eliminated by a new population type. The following is a list of the prerequisites and points for the regular AVOA.

$$R_i = \begin{cases} Best\ volture\ 1, & if\ pi = L_1 \\ Best\ volture\ 1, & if\ pi = L_2 \end{cases} \tag{3}$$

$$L_1 + L_2 = 1 \tag{4}$$

where,

L1 and L2 define two parameters that are attained before optimisation in the range [0, 1]. to decide which group member is the finest,

$$Pi = \frac{F_i}{\sum_{j=1}^{m} F_i} \tag{5}$$

In equation (5) 'F' determines the vultures' level of contentment,

The ratio of vulture starvation has then been determined. As a person runs out of energy, they will engage in combat with nearby, more powerful vultures to obtain food. You can model this as follows:

$$t = k \times \left(sin^w \left(\frac{\pi}{2} \times \frac{iter_i}{max_{iter}} \right) + cos \left(\frac{\pi}{2} \times \frac{iter_i}{max_{iter}} \right) - 1 \right) \tag{6}$$

$$F = (2 \times \delta_1 + 1) \times y \times \left(1 - \frac{iter_i}{max_{iter}} \right) + 1 \tag{7}$$

Equation (6) uses w to denote a constant to represent an optimisation procedure, and $iter_i$ to denote the current iteration. y represents a randomly inserted value among 0 and 1. k specifies the random value in range of [2, 2], and δ_1 denotes a random integer between 0 and 1. max_{iter}defines the total number of iterations. The vulture becomes hungry if y decreases to 0, else, it increases to 1.

After that, a random mechanism with two policies was taken into consideration to execute algorithm exploration. The following are examples of how people in an environment hunt for food sources:

If P_1 is less than $rand_{p1}$,

$$P(i+1) = R_i - F + \delta_2 \times ((ub - lb) \times \delta_3 + lb) \tag{8}$$

If P_1 is above or equal to $rand_{p1}$,

$$P(i+1) = R_i - D(i) \times F \tag{9}$$

Where,

$$D(i) = |X \times R(i) - P(i)| \tag{10}$$

R denotes a supreme vulture, X indicates how the vulture decides whether or not to keep food acquired from another vulture, which is obtained by $X = 2 \times \delta_i$ where $i = 1,2,3$ two numbers that are created randomly in the value of [0, 1], and $ub\ and\ lb$ denote the boundaries for variables at both lower and higher levels.

Additionally, $|H|$ should be less than 1 in order to abuse the algorithm. This consists of two parts with two siege-fight and rotating flight policies, defined by P_2 and P_3 as two parameters ranging from 0 to 1. Based on the strategy described above, the weakest vulture tries to steal the healthiest food in specified manner that follows;

$$P(i+1) = D(i) \times (F + \delta_4) - d(t) \tag{11}$$

$$d(t) = R_i - P(i) \tag{12}$$

Where, δ_4 is a probability number between 0 and 1.

Moreover, the following is the mathematical description of the vulture's spiral motion:

$$S_1 = R(i) \times \left(\frac{\delta_5 \times P(i)}{2\pi} \right) \times \cos(P(i)) \tag{13}$$

$$S_2 = R(i) \times \left(\frac{\delta_6 \times P(i)}{2\pi} \right) \times \sin(P(i)) \tag{14}$$

$$P(i+1) = R_i - (S_1 + S_2) \tag{15}$$

where δ_5 and δ_6 represent two random numbers between "0" and "1." Most vultures will struggle for food in the beginning if δ_{p_3} ,is a random number between 0 and 1, it's bigger than (or equal to) P_3. The harsh siege-fight policy

has been used if δ_{p_3} is less than P_3. When vultures are famished, it can create a huge competition among them to locate food. The following equation accomplishes this:

$$A_1 = BestVilture_1(i) - \frac{BestVilture_1(i)\ (i)\times P(i)}{BestVilture_1(i)\ (i) - P(i)^2} \times F \quad (16)$$

$$A_2 = BestVilture_2(i) - \frac{BestVilture_2(i)\ (i)\times P(i)}{BestVilture_2(i)\ (i) - P(i)^2} \times F \quad (17)$$

where, $BestVilture_1(i)$ *and* $BestVilture_2(i)$ represent the best vultures from both sets, while P(i) represents the vector's position in the moment.

$$P(i+1) = \frac{A_1 + A_2}{2} \quad (18)$$

The once-healthy vultures lose their strength and capacity to speak in front of crowds. They then fly to a different location to acquire food once more,

$$P(i+1) = R(i) - |d(t)| \times F \times LF(d) \quad (19)$$

where, LF denotes Levy flight (LF) and calculated analytically as follows:

$$LF(x) = \frac{u \times \sigma}{100 \times |v|^2} \quad (20)$$

$$\sigma = \left(\frac{\Gamma(1+P) \times \sin\frac{\pi\rho}{2}}{\Gamma(1+\rho_2 \times \rho \times 2\left(\frac{\rho-1}{2}\right)} \right) \quad (21)$$

Where, ρ denotes the fixed value, while u and v are the arbitrary numbers between 0 and 1.

4. RESULTS AND DISCUSSIONS

This algorithm is implemented in Cloud Sim as a load balancing algorithm based on C-AVPSO. Our proposed method is similar to the traditional methods QMPSO, FIMPSO, ACSO in terms of the energy utilization, degree of im-balance, number of tasks migration, response time and resource utilization.

4.1 Evaluation metrics

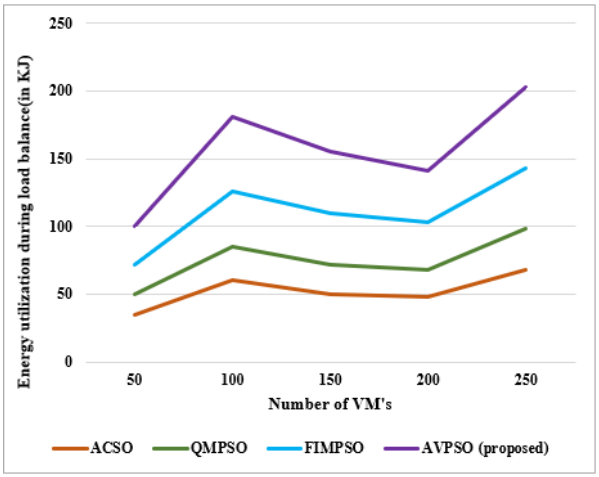


Figure 3. Energy utilization vs number of VM's

4.1.1. Energy utilization

When compared to other algorithms like FIMPSO, ACSO, and QMPSO during load balance, the proposed C-AVOPSO technique used the most energy. Also, the energy utilisation analysis revealed that, when compared to other algorithms, the proposed C-AVPSO approach required the least amount of energy (by altering the number of VMs from 0 to 250).

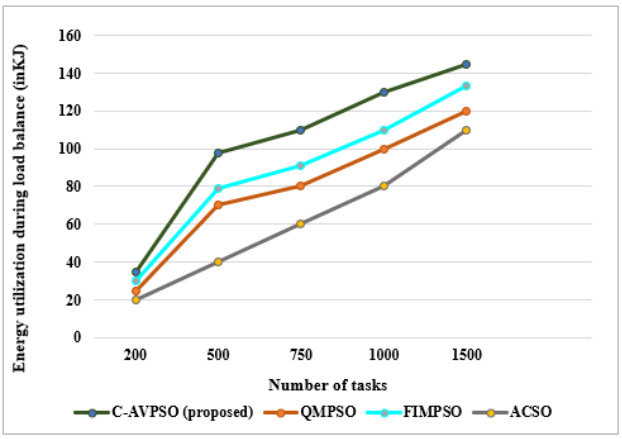


Figure 4. Energy utilization vs number of tasks

By comparing the suggested AVPSO to the various current algorithms, it was discovered that the proposed AVPSO used the most energy within number of Tasks from 100 to 1500.

4.1.2. Migration

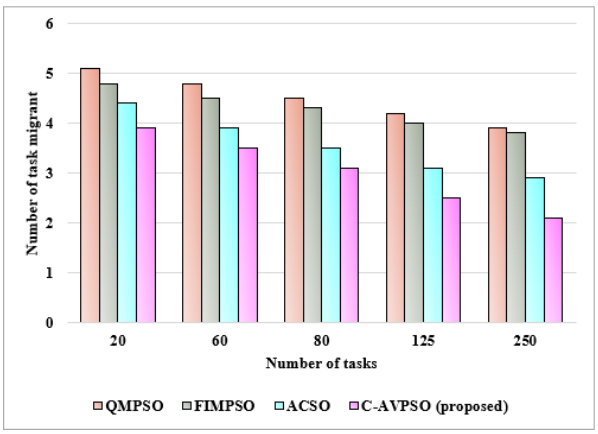


Figure 5. Migration Vs Number of tasks

Figure. 5 illustrates how the number of tasks migrated in relation via total number of tasks. Comparing the C-AVPSO technique to the current QMPSO, FIMPSO, and ACSO algorithms, it was discovered that there was less task migration.

4.1.3. Degree of imbalance

The reduction of imbalance associated with greater load balancing results in the cloud's optimal load balancing. The amount of imbalance determines how long jobs must wait. In general, the load balancing is based on how many jobs the users have requested. The degree of im-balancing after load balancing and before load balancing is depicted in Fig. 7. After the load balancing procedure, it shows that the produced C-AVPSO provide lower degree of imbalance.

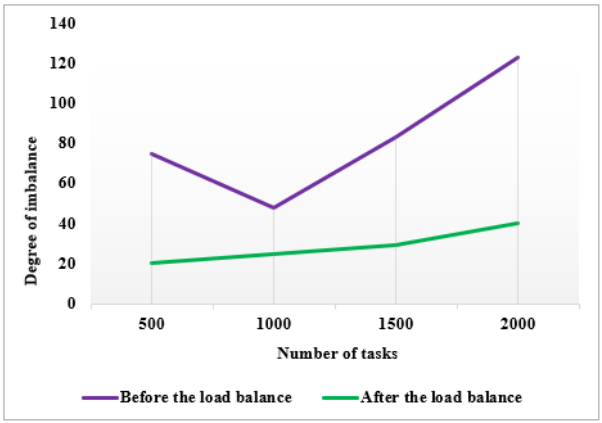


Figure 7. Degree of imbalance Vs Number of tasks

4.1.4. Resource utilization

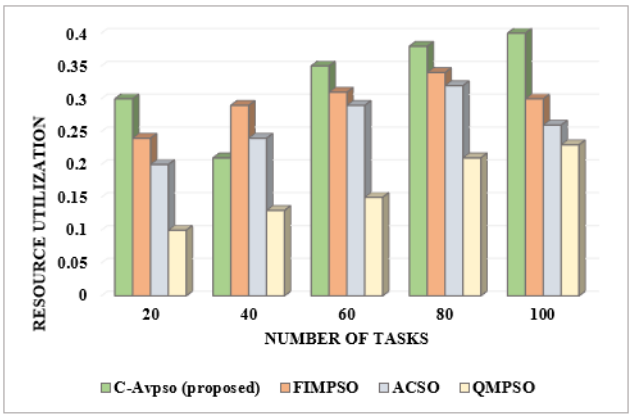


Figure 8: Resource utilization Vs Number of tasks

According to Figure 8, the suggested strategy's average resource utilisation performs admirably in every case when compared to other alternatives. This is because the suggested strategy enables the simultaneous assignment of each individual work to the best processor available. The effectiveness of the suggested strategy can be increased by maximizing resource use.

4.1.5. Response time

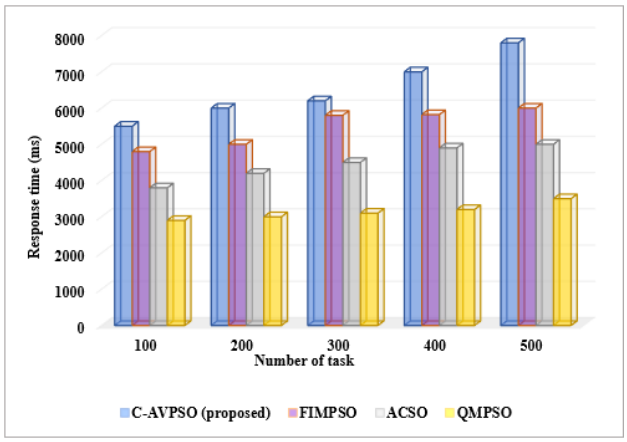


Figure 9. Response time Vs Number of task

Figure 9 shows a comparison of response times for various job counts. Between 100 to 500 jobs can be found in both the proposed and current algorithms. When a load balancing system allocates VMs with lower load conditions in response to user demand, this is known as its response time. Comparing the proposed AVPSO to the current QMPSO, FIMPSO, and ACSO approaches, it has the highest response.

5. CONCLUSION

In this paper, a novel cloud-based African vulture particle swarm optimization [C-AVPSO] has been suggested. Using C-AVPSO, the developed optimization algorithm solves the dynamic load balancing problem effectively. This approach used the AVO process to acquire the exploration space, and the PSO procedure to identify the improved response. The task's cost limitations, reaction time, and resource utilization are all satisfactorily resolved by this approach. As a result of combining the AVO and PSO algorithms into the proposed AVPSO algorithm, in the cloud context, load balancing performance measures and convergence rate are enhanced. To enhance the operation's efficiency, the proposed method balances VM loads efficiently. The suggested method was implemented in cloud sim tool. The proposed framework is compared to existing approaches like QMPSO, FIMPSO and ACSO Based on energy utilization, degree of imbalance and task migration, resource utilization, and response time. The proposed C-AVPSO technique reduces resource utilization of 19.1%, 31%, and 54% than, QMPSO, FIMPSO and ACSO existing techniques.

REFERENCES

[1] S. K. Mishra, B. Sahoo and P. P. Parida, “Load balancing in cloud computing: a big picture”, *Journal of King Saud University-Computer and Information Sciences*, vol. 32, no. 2, pp.149-158, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] S. Afzal and G. Kavitha, “Load balancing in cloud computing–A hierarchical taxonomical classification”, *Journal of Cloud Computing*, vol. 8, no. 1, pp.22, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[3] V. N. Volkova, L. V. Chemenkaya, E. N. Desyatirikova, M. Hajali, A. Khodar and A. Osama, “Load balancing in cloud computing”, *In 2018 IEEE conference of russian young researchers in electrical and electronic engineering (EIConRus)*, pp. 387-390, 2018. IEEE. [CrossRef] [Google Scholar] [Publisher Link]

[4] U. K. Jena, P. K. Das and M. R. Kabat, “Hybridization of meta-heuristic algorithm for load balancing in cloud computing environment”, *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 6, pp.2332-2342, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] V. Polepally and K. Shahu Chatrapati, “Dragonfly optimization and constraint measure-based load balancing in cloud computing”, *Cluster Computing*, vol. 22, no. Suppl 1, pp.1099-1111, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[6] T. P. Latchoumi and L. Parthiban, “Quasi oppositional dragonfly algorithm for load balancing in cloud computing environment”, *Wireless Personal Communications*, vol. 122, no. 3, pp.2639-2656, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] A. F. S. Devaraj, M. Elhoseny, S. Dhanasekaran, E. L. Lydia and K. Shankar, “Hybridization of firefly and improved multi-objective particle swarm optimization algorithm for

energy efficient load balancing in cloud computing environments", *Journal of Parallel and Distributed Computing*, vol. 142, pp.36-45, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[8] A. Semmoud, M. Hakem, B. Benmammar and J. C. Charr, "Load balancing in cloud computing environments based on adaptive starvation threshold". *Concurrency and Computation: Practice and Experience*, vol. 32, no. 11, pp. e5652, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] K. Balaji, P. S. Kiran and M. S. Kumar, WITHDRAWN: An energy efficient load balancing on cloud computing using adaptive cat swarm optimization, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] M. Kumar and S. C. Sharma, "Dynamic load balancing algorithm for balancing the workload among virtual machine in cloud computing", *Procedia computer science*, vol. 115, pp. 322-329, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[11] S. Afzal, G. Kavitha, "Optimization of task migration cost in infrastructure cloud computing using IMDLB algorithm", *In: 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET)*, pp 1–6, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[12] R. Achar, P. S. Thilagam, N. Soans, P. V. Vikyath, S. Rao, A. M. Vijeth, "Load balancing in cloud based on live migration of virtual machines", *In: 2013 annual IEEE India Conference (INDICON)*, pp 1–5, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[13] D. Magalhães, R. N. Calheiros, R. Buyya, D. G. Gomes, Workload modeling for resource usage analysis and simulation in cloud computing. Comp Elect Eng, vol. 47, pp. 69–81, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[14] R. N. Calheiros, R. Ranjan, C. A. De Rose and R. Buyya, "Cloudsim: A novel framework for modeling and simulation of cloud computing infrastructures and services", arXiv preprint arXiv:0903.2525, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[15] S. Dam, G. Mandal, K. Dasgupta, P. Dutta, Genetic algorithm and gravitational. emulation-based hybrid loads balancing strategy in cloud computing, *In: Proceedings of the 2015 third international conference on computer, communication, control and information technology (C3IT)*, pp 1–7, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[16] A. Dave, B. Patel, G. Bhatt, "Load balancing in cloud computing using optimization techniques: a study", *In: International Conference on Communication and Electronics Systems (ICCES)*, pp 1–6, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[17] D. A. Shafiq, N. Z. Jhanjhi and A. Abdullah, "Load balancing techniques in cloud computing environment: A review", *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 7, pp.3910-3933, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[18] J. C. Bansal, "Particle swarm optimization", *Evolutionary and swarm intelligence algorithms*, pp.11-23, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[19] D. Wang, D. Tan and L. Liu, "Particle swarm optimization algorithm: an overview", *Soft computing*, vol. 22, pp.387-408, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[20] M. Farid, R. Latip, M. Hussin and N. A. W. Abdul Hamid, "A survey on QoS requirements based on particle swarm optimization scheduling techniques for workflow scheduling in cloud computing", *Symmetry*, vol. 12, no. 4, pp.551, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[21] D. Wu, "Cloud computing task scheduling policy based on improved particle swarm optimization", *In 2018 International Conference on Virtual Reality and Intelligent Systems (ICVRIS)*, pp. 99-101, 2018. IEEE. [CrossRef] [Google Scholar] [Publisher Link]

[22] Y. Wang, S. Li, H. Sun, C. Huang and N. Youssefi, "The utilization of adaptive African vulture optimizer for optimal parameter identification of SOFC", *Energy Reports*, vol. 8, pp.551-560, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[23] B. Abdollahzadeh, F. S. Gharehchopogh and S. Mirjalili, "African vulture's optimization algorithm: A new nature-inspired metaheuristic algorithm for global optimization problems", *Computers and Industrial Engineering*, vol. 158, pp.107408, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[24] I. M. Ibrahim, "Task scheduling algorithms in cloud computing: A review", *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 4, pp.1041-1053, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[25] E. H. Houssein, A. G. Gad, Y. M. Wazery and P. N. Suganthan, "Task scheduling in cloud computing based on meta-heuristics: review, taxonomy, open challenges, and future trends", *Swarm and Evolutionary Computation*, vol. 62, pp.100841, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[26] M. Masdari and M. Zangakani, "Green cloud computing using proactive virtual machine placement: challenges and issues", *Journal of Grid Computing*, vol. 18, no. 4, pp.727-759, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[27] P. Srivastava and R. Khan, "A review paper on cloud computing", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 8, no. 6, pp.17-20, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[28] M. I. Malik, S. H. Wani and A. Rashid, "CLOUD COMPUTING-TECHNOLOGIES". *International Journal of Advanced Research in Computer Science*, vol. 9, no. 2, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[29] K. D. Patel and T. M. Bhalodi, "An efficient dynamic load balancing algorithm for virtual machine in cloud computing", *In 2019 International conference on intelligent computing and control systems (ICCS)*, IEEE. pp. 145-150, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[30] A. Rashid and A. Chaturvedi, A, "Cloud computing characteristics and services: a brief review", *International Journal of Computer Sciences and Engineering*, vol. 7, no. 2, pp. 421-426, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[31] "Synthetic structure of industrial plastics (Journal Article)", *Plastics*, vol. 3, no. 2, pp. 15–64, 1964. [CrossRef] [Google Scholar] [Publisher Link]

[32] G. O. Young, Synthetic structure of industrial plastics (Book style with paper title and editor), in *Plastics*, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, 15–64. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

Dharavath Champla, currently doing as a Research Scholar, Department of Computer Science and Engineering, Anna University, Chennai, SRM Easwari Engineering college, Chennai. I have experience of over 4 years in the field of engineering, academics, administration and active research. I am an alumnus of JNTU Hyderabad. I was completed my previous Degrees, "B tech" Vidhya Bharathi Institute of Technology in 2011, "M tech" Ashoka Institute of Engineering and Technology in 2014, Affiliated to JNTU Hyderabad.

V. Ramkumar has completed his Ph.D. degree in Information and communication engineering from Anna University, Chennai, Tamilnadu. He has received his M.E degree in VLSI Design from Anna University and B.E degree in Electronics and Communication Engineering. His area of research includes VLSI Design and Optical communication. He has over 8 years of teaching experience in various reputed institutions in Tamil Nadu. Currently he is working as Assistant Professor in K. Ramakrishnan College of Technology, Tiruchirappalli. He has completed various courses on latest technologies in NPTEL, Coursera. He has delivered lectures to institutions on topics like Recent Trends in VLSI, Intern in core field, Career opportunities through GATE, Believe in Yourself, etc. He has organize & conduct various workshop and value-added course like VLSI-Cadence, IOT, PCB Design, Low Power VLSI etc., He has been scientific core committee member for International Conferences conducted in 2021.

P. Ajay is a renowned researcher and academician in the field of Wireless Networks, Artificial Intelligence and Soft Computing. He was born and brought up in India, and his passion for engineering led him to pursue a Master's degree in Electronics and Communication Engineering from Anna University, followed by a PhD degree from Anna University in 2023. Dr. Ajay began his professional journey in 2017 as an Assistant Professor at Karpagam College of Engineering, where he worked tirelessly for 3 years. During his tenure, he held various positions and made significant contributions to the institution. His technical expertise and research interests led him to explore new avenues in the field of Communication Systems and Automation, where he made significant contributions. Dr. Ajay's research work has been recognized and appreciated by the academic community, and he has received several awards and honors throughout his career. Dr. Ajay has also authored or co-authored over 25-refereed publications in journals and conferences, and he has applied for five patents that have been published in the Indian Patent Journal. Dr. Ajay is a member of various professional bodies like IEEE, MAENG, IACSIT, ISTE, and IETE. He is a reviewer for different reputed journals like Elsevier, Wiley, Inderscience, and has been a Guest Editor for a few special issues in Hindawi, Elsevier, Inderscience, Springer, etc. In his current role, Dr. Ajay is a part of the faculty at Rathinam Group of Institutions in Coimbatore, India, where he serves as a guide and mentor to students pursuing their undergraduate and postgraduate studies in the field of Electronics and Communication Engineering. He is known for his dedication, passion, and commitment to teaching and research, and his contributions have helped shape the careers of numerous students.

Arrived: 18.08.2023
Accepted: 23.10.2023

International Journal of Computer and Engineering Optimization (IJCEO)
Volume 1, Issue 1, September – October (2023)

RESEARCH ARTICLE

INTRUSION DETECTION ARCHITECTURE (IDA) IN IOT BASED SECURITY SYSTEM

M. Amanullakhan[1, *], M. Usha[2] and S. Ramesh[3]

[1] Department of Electronics and Communication Engineering, Mohamed Sathak Engineering College, Kilakarai, India.
[2] Department of Masters in Computer Application, MEASI Institute of Information Technology, Tamilnadu, India.
[3] Department of Computer Science Engineering, Krishnasamy College of Engineering Technology, Anand Nagar, Kumarapuram, Cuddalore, India

[*]*Corresponding e-mail: amanulla82@gmail.com*

Abstract – Through the use of billions of data points, the internet of things (IOT) links billions of objects to the internet, all of which require security. A major issue for cyber security is the expanded attack surface of IOT. To overcome these challenges, Intrusion Detection Architecture (IDA) has been proposed in this paper, which helps to trace the Intrusion Data in IOT. The proposed Intrusion Detection Architecture (IDA) is performed in three stages namely, Data Collection, Pre-processing in Data encoding and Classification block. Initially, the request from the IOT devices is sent to the Data collection (DC) and pre-processing stage there it could find the amount of data. The collected data traces and filter through the Normalization Technique (NT). Then the filtered data goes to the data encoding block. After the encoded data goes to classification block here it classifies the data by Ghost Net technique and finally the attack can be classified and detected. The effectiveness of the suggested IDA strategy has been assessed using assessment measures such as configuration latency, detection rate, accuracy, precision, recall rate, false detection rate. The proposed method reduces the communication overhead of 75%, 50% and 38% than SSTS, ANT and FPDS existing techniques.

Keywords *– IoT, Intrusion detection, Cyber security, Data encoding, Ghost Net technique.*

1. INTRODUCTION

An increasing number of sectors are utilising the Internet of Things [1]. Everybody's life is changing as a result of the Internet of Things (IoT), that provides services like monitoring and managing linked smart gadgets. Smart cities [2], homes [3], cars [4], industrial [5], digital health care smart control system [6], commuting [6], wearables [7], farming [8], and many more areas are among the numerous uses for the Internet of Things. The Internet of Things (IoT) is a growingly well-liked technology that allows actual objects, such as cars and home appliances, to interact and even communicate with one another [9]. Autonomous and semi-autonomous smart automobiles make up the Internet of Vehicles (IOV), which may be defined as an Internet of Things (IoT) system having incorporated sensing as well as management capabilities for computerized navigation and enhanced safety [10].

In recent years, IoT technologies and platforms have expanded rapidly. IoT is a relatively new technology, yet it does not always imply that it is simpler than the current system. Otherwise, interactions between the real world and the internet actually make IoT platforms and systems more complex [11]. The Internet of Things (IoT) most crucial characteristic is how widely it is used and how easily it can be adapted to computer networks [12]. Large amounts of data are generated by IoT device sensors, which call for authentication, security, and privacy [13].

Yet, because to the variety, decentralization and due to the IoT network's complexity, certain IoT problems with relation to cyber physical security are emphasized [14]. Cybersecurity is currently the top priority for the Internet of Things (IoT) as one of its core topics. By utilizing solutions like block chain, intelligent logistics, and smart home management, IoT cyber security reduces cyber security risk for individuals and enterprises [15]. It has been observed that IoT devices are vulnerable to numerous cyber dangers when seen as sensors that can be connected to a computer network.

Cyber-physical systems (CPSs) are integrated technologies that include IoT for smart cities, industry, and healthcare [16]. Securing the topology to which the devices are connected as soon as possible against potential cyberattacks is one of the most crucial factors to take into consideration in the IoT [17]. IoT application on the critical infrastructure has called for an explosion of cyber security challenges on the grid [18]. To overcome these challenges, Intrusion Detection Architecture (IDA) has been proposed in this paper, which helps to trace the Intrusion Data in IOT. The following list summarizes the primary contributions of the suggested IDA approach.

- The proposed Intrusion Detection Architecture (IDA) is performed in three stages namely, Data Collection, Pre-processing, Data encoding and Classification block.
- Initially, the request from the IOT devices is sent to the Data collection (DC) stage there it could

find the amount of data in pre-processing technique.

- The collected data traces and filter through the Normalization Technique (NT) by Data cleaning in Deep Learning (DL). Then the filtered data goes to the data encoding block.
- After the encoded data goes to classification block here it classifies the data by Ghost Net technique and finally the attack can be classified and detected.
- Using assessment criteria including configuration delay, detection rate, accuracy, precision, recall rate, and false detection rate, the effectiveness of the suggested IDA technique has been assessed.

This essay's remaining sections are organized as follows: Part II covers the review of the literature. It serves as a stand-in for the method that Section III suggests. Section IV contains the results and discussions. Section V covers the conclusion and future initiatives.

2. LITERATURE SURVEY

Data privacy in IoT network is concerned, especially for IoT devices which used in moreover sensitive industries, such as healthcare and finance. Many studies have been conducted to solve this problem. Among those, some of the techniques have been reviewed in this section.

In 2020, Yan Zhang, B., et al., [19] aimed a security conscious authentication convention for the multiple server CE Internet of Thing (IoT) system by merging PUFs and the block-chain method. An official oracle model and security and privacy features are used to prove the protocol's security. This protocol's formal proof is based on the random predicted theory and the automated verification tool, which provide semantic security.

In 2020, Waseem Iqbal, H., et al.,[20] put forward the idea to risks, security requirement, troubles to assault vectors relevant in IoT networking system. Through Software Defined Networking (SDN) the IOT architecture deployed attention base networks. The main barriers are unified to the entire IoT participants in single platform, which issues are highlighted by the core. And some findings, emphases to IOT paradigm on a network supported security solution.

In 2021, Kwok-Yan Lam,[21] proposed an ActivityNetwork Things (ANT) with three systems those are device, internet and semantic of architectural perspectives in studying IoT systems, these architectures are based by centric security reference of architecture. The approach helps for security risks manager which was focused the critical activities happened in other micro perimeters with an IoT network system.

In 2021, Shikhar Verma, [22] had suggested the RAW mechanism to evaluate the IoT and inspect the output which was on the basis of on mathematical model. By reducing the risk in the final analysis in for every single device towards an optimal scan rate which was to optimize the tradeoff. The admin cannot control the network parameters by this approach which considers the perspective. Thus, the network was unable to utilize successfully for security enhancement.

In 2021, Wei Zhou, C., et al., [23] had proposed the inspecting Internet of Things security through logical flaws in IOT devices and platforms. It provides information on newly found logic defects specific to IOT systems and platforms. The lessons that can be drawn from these kinds of bugs were covered. The approach in IOT systems and platforms will be focused on newly found logic problems.

In 2021, Jun Zhang, Y., et al., [24] approached a smart transportation security system (STSSs). For the security concern the STSS architecture was proposed. Because there were many smart transportation innovations are facing this problem. For the purposes of examining its feasible and applicability the socio technical was assembled. These assemble approach requires legitimate of socio technical and social interventions.

In 2021, Jiyoon kim [25] had put forward a technique to enable safe mobile terminal transitions between hubs by Mobile Terminal Handover (MTH) security protocol. The issue with the current protocols was resolved by utilizing a brand-new entity known as the Backhaul Management Function (BMF). These protocols can safeguard and protect data between the terminals. the exchangeable messages and then it moves across the hub.

In 2021, Fei Zhu, X., et al., [26] had proposed the integrity and source authentication protecting requirements which was satisfied by the first identification based on RSS and chosen exposure controls healthcare data or information sharing ways in IoT. Which provide possible strategy on the side of a beholder to prevent further reduction or random reduction from corrupt signature have been keep.

In 2021, Shuodi Hui, Z., et al., [27] had offered a method that quantifies a large amount of mobile network traffic data sets that include 46.651 Internet of Things devices in order to prevent IoT privacy breaches. It blends empirical measures with methodical analysis. Additionally, there is a greater degree of privacy leaking to users and platforms are present in IOT devices and also does different daily pattern in privacy leakage to follow their working ways.

In 2022, Hua Deng, Z., et al., [28] had proposed IOT cloud-assisted scheme for the Flexible Privacy preserving Data Sharing (FPDS). By this way, users in IOT could share the data's which was outsourced by the cloud FPDS manner. It protects privacy outsourced data in privacy and with identify-based encryption, and it introduced a fine-grained delegation to the flexible data. And for more importantly, to the owners FPDS provides a flexible data sharing mechanism.

From these literature studies, the authors are used IOT to make the work secured and privacy. The Internet of Thing (IOT) security technique that involves protecting data as it is starts transfers from the local devices in order to the clouded one. Here some techniques are used for the security, the granular methodology, a mathematical model are used to evaluate and identify risks, and 5G modeling

based the indications for making key judgments include station coverage and the metro convenience index.

3. IDA TECHNIQUES IN IOT

The Intrusion Detection Architecture (IDA) is proposed in this section is performed in three stages namely, Data Collection, Pre-processing and Data encoding, and Classification block. The request from the IOT devices is sent to the Data collection (DC) way there it could find the amount of data in pre-processing technique. The collected data traces and filter through the Normalization Technique (NT) by data cleaning in Deep Learning (DL). Then the filtered data goes to the data encoding block. After the encoded data goes to classification block there it classifies the data by Ghost Net technique and finally the attack can be classified and detected. The efficiency of the proposed IDA approach has been determined using the evaluation metrics such as configuration latency, detection rate, accuracy, precision, recall rate, false detection rate. Overall proposed system method has shown and detailed in Figure.1.

3.1 Data collection

In data collection it collects all IOT requested data such as, Protocol, IP address, Frame length, File type, Host post, Frame number, etc. The collected data are the traces of Pre-processing. The Internet of Things device filters packets, chooses features from a range of network features, including the duration and frame number, gives them labels, and stores these details in a database. The gathered data are then taken as traces. The traces from the IOT devices are then pre-processed with data cleaning in Deep Learning (DL) process.

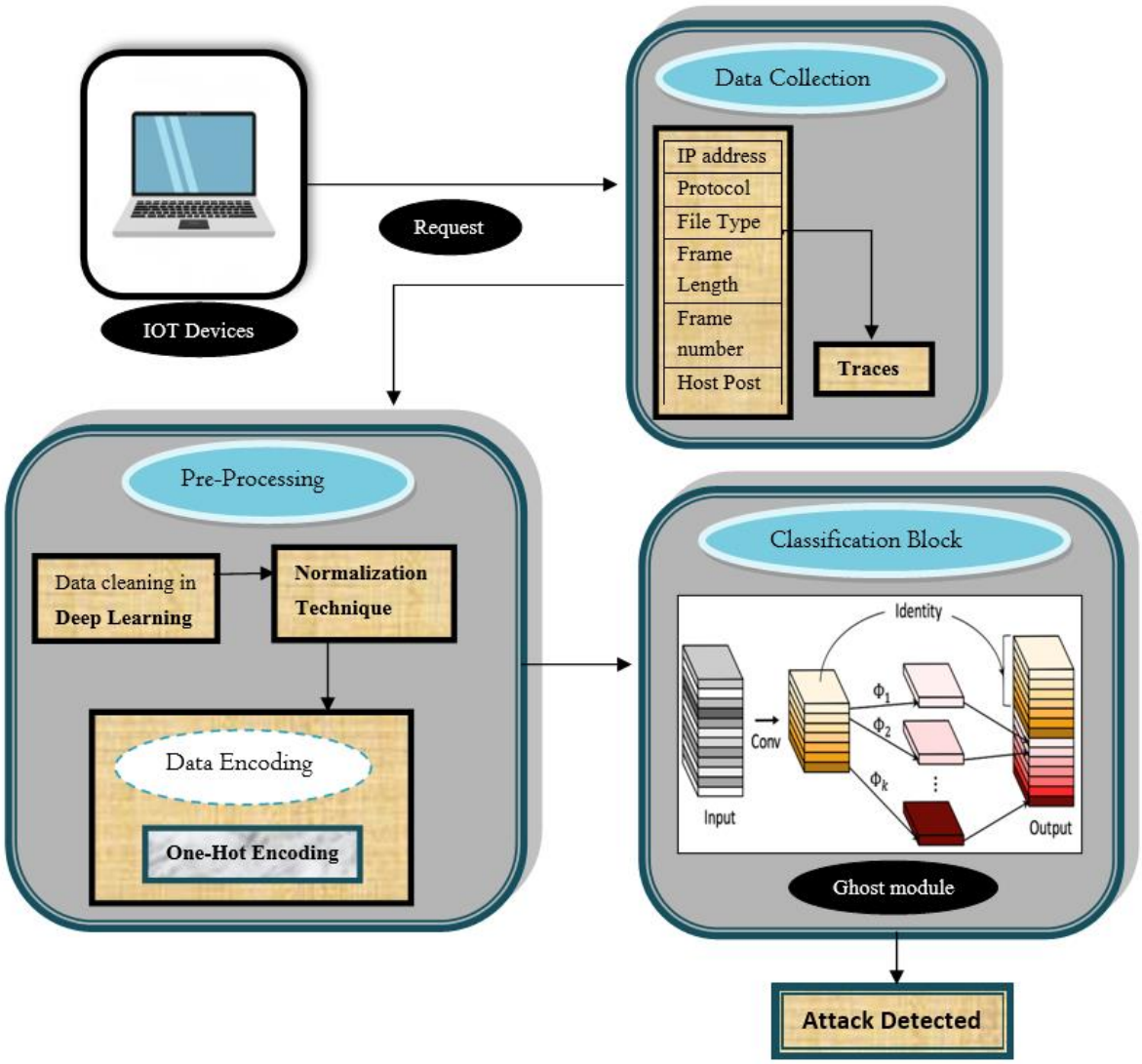


Figure 1. Proposed method

3.2 Pre-processing

The act of transforming unprocessed data into a format that a deep learning (DL) network can use is known as pre-processing. It is the most important and initial step in creating a deep learning model. Finding clean, prepared data is not always the case while working on a Deep Learning project. Before using data, users must also clean and prepare it. Therefore, to do this, we employ a data pre-processing method.

3.2.1 Data cleaning

Data cleaning is the process of fixing or deleting erroneous, corrupted, misleading, duplicate, or insufficient information from a dataset. The following Figure 2 shows the data cleaning steps

Steps involved in data cleaning

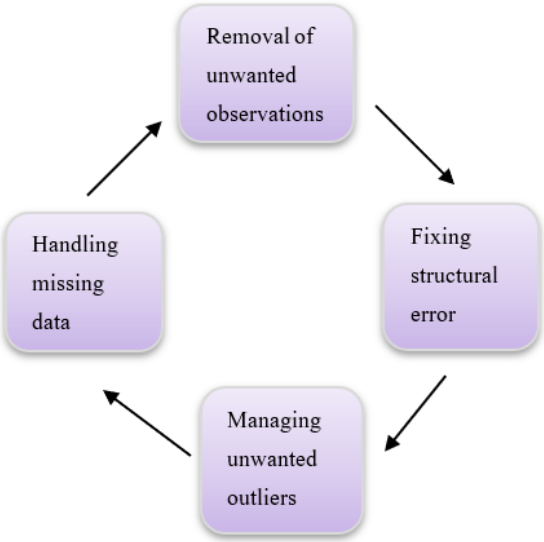


Figure 2. Data cleaning steps

3.2.2. Normalization

Data cleaning is the process of fixing or deleting erroneous, corrupted, misleading, duplicate, or insufficient information from a dataset for Deep Learning (DL). A set of data is transformed to be on a similar scale through normalization. Depending on the data itself, the purpose of machine learning models is typically to recenter and rescale our data so that it is between 0 and 1 or -1 and 1.

3.3 Data encoding

Data encoding is one of the tasks that is seen to be essential. In general, DL models carry out mathematical operations that can be carried out with a wide range of tools and methods. The process of encoding IOT data involves turning categorical data into integer format so that the models may use the converted data to produce and enhance predictions. In this proposed data cleaning technique method use one-hot encoding, it given brief as follows.

3.3.1 One-hot encoding

By one-hot encoding method the IOT data pre-processed, for textual data, the Deep Learning (DL) process is not suitable directly. Data has to be numeric. Hence, in this study for data pre-processing, One-hot vectors were used to encode the IOT text data. A basic way for representing strings with a finite set of values is one-hot encoding, which employs a sparse vector with one member set to 1 and all other elements set to 0. Neural networks frequently employ one-hot encoding because their activation functions call for input to fall within the discrete range of [0, 1] or [-1, 1].

A 1* N matrix (vector) that has 0s in every cell except for one that is used to uniquely identify a word is called a one-hot vector. Categorical data can be represented more expressively using one hot encoding. Three of these encodings [0, 0, 1] would each represent a word range of [good, good, bad]. For the experimental flow Figure 3 is shown as follows.

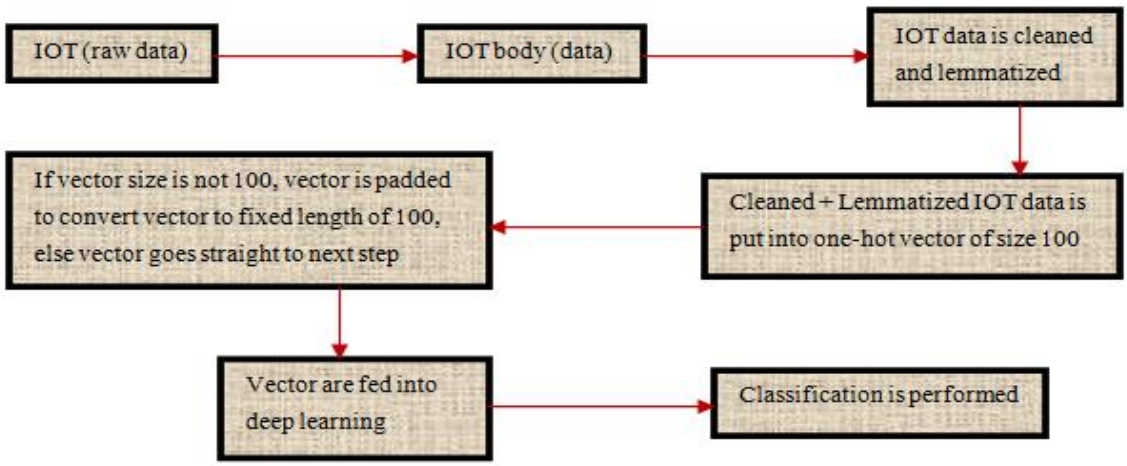


Figure 3. Experimental flow in IOT data

The IOT data utilized in this research was cleaned, lemmatized, and represented as one-hot encoded vectors Lemmatization combines a word's several spellings into one so they can be studied as a single entity. As a result, 100 was chosen as the study's arbitrary length, and padding was applied to all vectors to make them all the same length. These matrices were fed into a neural network or deep learner, and the vectors in these networks were then translated into a low dimensional space. This low dimensional space is represented in the neural network by a hidden layer, where the vocabulary size is smaller than the number of words.

3.4 Ghost Net

Ghost net is used for making decision to access or deny the user request based on the trust value and data owner attributes. The quantity of inference computation is minimized by the ghost net by using linear operations rather

than partial convolution. Convolutional Neural Networks (CNN) were created specifically for decision-making and identification in the ghost net. Rather of employing fully linked layers, which are excessively large to handle large amounts of data, CNNs create a local receptive field for every hidden layer neuron. In order to decrease the network's capacity, enhance the usefulness of its features, and extract multi-scale bottom-level features, a ghost module is induced in the CNN network, as shown in Figure. 4.

3.4.1. Ghost module Architecture

Within a convolutional layer's narrow local window, each neuron receives an input, as does the layer above it. The groups of weights connected to a particular receptive field define a filter. This network maintains the association between the pixels while identifying various characteristics of the inputs, including edges and embosses, using initialised random distributions.. By screening the resulting feature maps, the data is processed in this fashion. As a result, different filters produce different feature maps. The collection of kernels applied during the convolutional phases the same as the output depth in the convolutional layer.

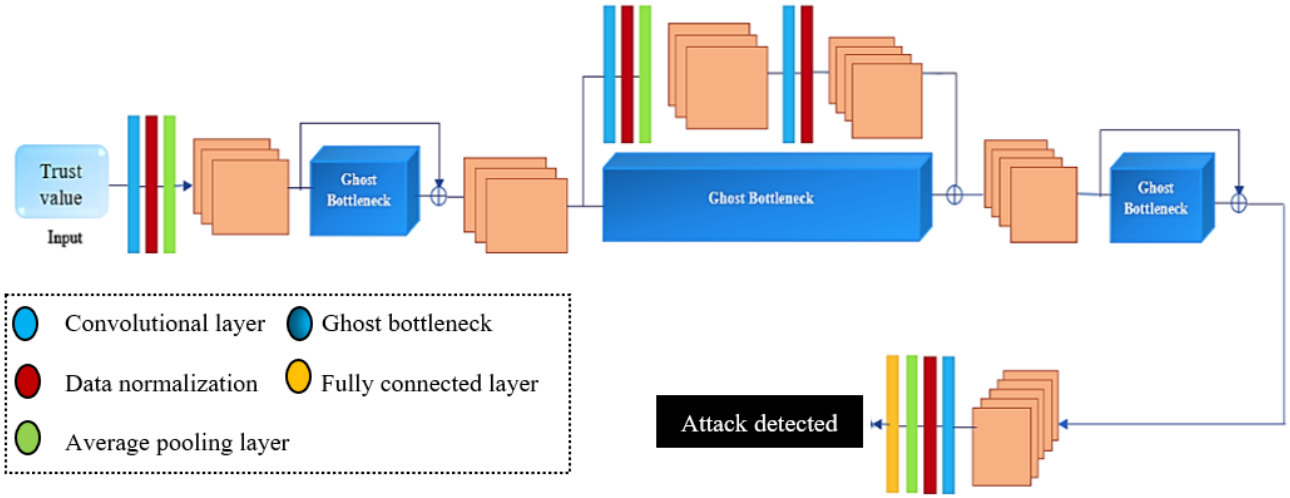


Figure 4. Architecture of Ghost module process

In particular, convolutional layer is considered$G_l \epsilon \mathbb{R}^{w_l * w_l * d_{l-1} * d_l}$, is the definition of the number of weights, where w_l stands for the spatial width and height of the filter, d_{l-1} for the data channels input, and d_l for the number of kernels. $S_{l-1} \epsilon \mathbb{R}^{N_{l-1} * N_{l-1} * K_{l-1}}$, which relates to the bias vector is included, is the representation of the l^{th}convolution process in this framework. It is the linear function obtained in equation (1) that multiplies the equivalent number of weights and the input volume of the layer. As a result, an arbitrary feature map $Z_l \epsilon \mathbb{R}^{N_l * N_l * K_l}$ is obtained, accurately locating identified features within the input data.

$$Z_l = G_l * S_{l-1} + bias_l \quad (1)$$

Equation (2) states that the local receptive field receives the element-wise product of each input element and filter weight when convolutional kernels are applied to the input data. Here, since $\hat{s_i}$and $s_i$are the spectral indices as well as $a, b, \hat{a}$ and $\hat{b}$ are the indexes across the spatial ratios for the input or output data and the weights, $a = \hat{a} - [N_{l-1}/2]$ and $b = \hat{b} - [N_{l-1}/2]$ are interpreted by the recentered spatial indexes.

$$Z_l^{a,b,s_i} = \sum_{\hat{a}\hat{b}\hat{s_i}} G_l^{\hat{a},\hat{b},\hat{s_i}} * S_{l-1}^{a+\hat{a},b+\hat{b},\hat{s_i}} + bias_l^{s_i} \quad (2)$$

As a result, the final output feature maps are obtained by learning the nonlinearities of the data using a non-linear activation function H( ). as $S_l \epsilon \mathbb{R}^{N_l * N_l * K_l}$,

$$S_l = \mathcal{H}(Z_l) \quad (3)$$

Where, $\mathcal{H}$ is applied as Fully Connected (FC) layer, It is typically employed in methods for back propagation. reducing the number of convolutional kernels developed and the number of superfluous feature maps in order to lower the amount of computing storage needed for CNN. Ghost Bottleneck is a reusable module that reduces model size and its structure is similar to the simple residual block in CNN, which is made up of two stacked Ghost modules as shown in Figure 5. A stride of 2 is a depth wise convolution that links two Ghost modules.

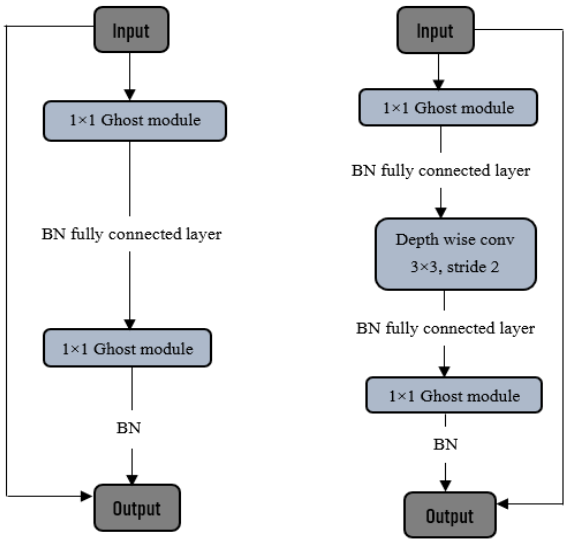


Figure 5. Ghost Bottleneck structure

From each input, a ghost component retrieves intrinsic feature maps, and every single channel of the intrinsic feature maps is given a linear kernel by the paired convolutional layer. The intrinsic feature maps $\tilde{S}_l$ may be easily updated in several simple ways, and the output feature maps S_l are generated as Ghosts. The group known as $S_l \epsilon\ \mathbb{R}^{N_l * N_l * \tilde{K}_l}$ for these intrinsic feature maps is generated by a main convolution from equation (1); the number of kernels is determined by $G_l \epsilon\ \mathbb{R}^{w_l * w_l * d_{l-1} * \tilde{D}_l}$ applied to the input layer data, where $\tilde{D}_l < d_l$

Consequently, a variety of discounted linear techniques are used to each intrinsic feature of $\tilde{S}_l$ in order to construct M ghost features, which are stated in equation (4), in order to obtain the genuine w_l feature maps.

$$S_l^{s_i,q} = \varphi_{s_i,q}\left(\tilde{S}_l^{s_i}\right),\ \forall t = 1, \ldots . \tilde{D}_l, \forall q = 1, \ldots . \tilde{w}_l \qquad (4)$$

The intended $d_l = w * \tilde{D}_l$ feature maps are therefore produced. The resultant volume of the paired layer is combined with the resultant volume of the point-wise layer and moved to the next block. Once the first bottleneck has been eliminated, the second bottleneck needs several convolutions in the shortcut relation to regulate the size of its input feature maps. Furthermore, each feature is combined and optimized by the pooling module, which then provides the outcomes to the two Fully Connected Layers (FC) for use as classifiers in deciding whether to approve or reject user requests.

4. RESULTS AND DISCUSSIONS

Simulations have been performing to evaluate the IDA scheme in IOT security system. Here, the Matlab is used to simulate the Intrusion Detection Architecture (IDA). The detection in IOT intrusion system is maintained by Attack Detection Set or Thread Detection Set with the Network Intrusion Detection System (NIDS) which perform as a detector in IOT system.

The UNSW-NB15 dataset is used to monitor the network problem or system activity problem for malicious or anomalous behavior in the IOT security system applications. The UNSW-NB15 dataset's NetFlow-based format, referred to as NF-UNSW-NB15, has been created and labelled with the appropriate attack categories. There are 1,623,118 data flows in total, of which 1,550,712 (95.54%) are benign and 72,406 (4.46%) are attack samples. So, that here for the IDA it dedicates NIDS to detect the IOT intrusion which detects easily when compared to other.

4.1 Performance metrics

This section presents the simulation results of proposed IDA performance metrics namely Communication overhead, Throughput, Attack graph index, Delay analysis, Signaling Overhead, Attack detection rate with malicious node, Communication cost and Energy consumption. The amount of time it takes a node to process a packet is referred to as computational overhead. The time between the packet being fully received and the node completing its processing should be considered.

After this period, the node might eventually have another packet prepared for transmission.

4.1.1 Communication overhead

Communication overhead factor for the authentication schemes (shown in Figure 6), neglecting protocol overhead. When compared to other methods, the IDA has a larger overhead. Proposed an Intrusion Detection Architecture (IDA) it is built on the device, internet, and semantic architectural views for understanding IoT systems.

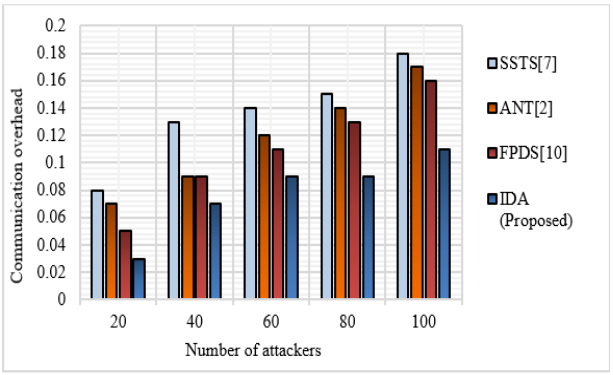


Figure 6. Communication overhead

In Figure 6 the communication overhead factors for authentication scheme compared with some existing techniques which are, Smart Security Transportation System (SSTS) [7], Activity Network Things (ANT) [2], Flexible Privacy-preserving Data Sharing (FPDS) [10] and proposed Intrusion Detection Architecture (IDA). The number of attackers takes within 100 of size, when compared to other three existing technique the IDA proposed is low, -75%, -50% and -38% of SSTS, ANT and FPDS is reduced in communication overhead when compared with proposed IDA as shown in graph Figure 6.

4.1.2 Throughput

The throughput in IOT security is refers to how much the IOT data is actually transfers during a particular period of time. The throughput figure is shown as follows Figure 7.

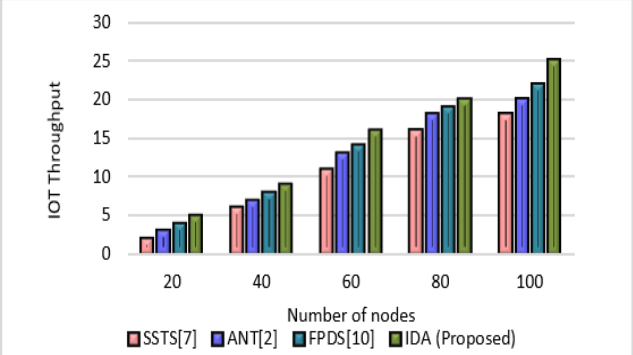


Figure 7. IOT throughput with number of nodes

The IOT throughput with average time is compared with existing three techniques which are, Smart Security Transportation System (SSTS) [7], Activity Network Things (ANT) [2], Flexible Privacy-preserving Data Sharing (FPDS) [10] and proposed Intrusion Detection Architecture (IDA). The number of nodes taken in n=10

<100. Compared with other three existing technique the proposed IDA is high in throughput, 33%, 20%, 13% of SSTS, ANT, FPDS is increased in throughput compared with proposed IDA is shown in Figure 7.

4.1.3 Attack graph

IOT's attack graph plays an important role in this process. IOT security graphs can be used to create multi-stage attack routes, each of which reflects a series of vulnerabilities that an attacker could use to break into a network. The attack graph index is shown below in Figure 8.

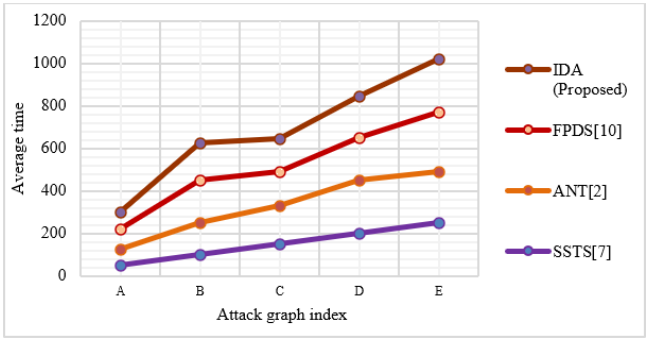


Figure 8. Attack graph index

The attack graph index with average time is compared with existing three techniques which are, Smart Security Transportation System (SSTS) [7], Activity Network Things (ANT) [2], Flexible Privacy-preserving Data Sharing (FPDS) [10] and proposed Intrusion Detection Architecture (IDA). Compared with other existing techniques the proposed IDA is high which shown in Figure 8.

4.1.4. Delay analysis

To determine the percentage of the IOT data delay is attributed to each party (contractor, owner, or neither), delay analysis includes estimating the delay and working backwards from it, delay analysis graph is shown in Figure 9.

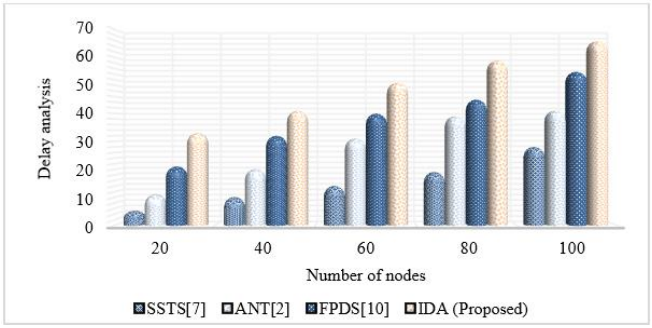


Figure 9. Resultant Graph of the Proposed System

The Delay analysis with number of nodes is compared with existing three techniques which are, Smart Security Transportation System (SSTS) [7], Activity Network Things (ANT) [2], Flexible Privacy-preserving Data Sharing (FPDS) [10] and proposed Intrusion Detection Architecture (IDA) in this graph Figure 9. Compared with other existing techniques the proposed IDA is high.

4.1.5. Signaling overhead

Signaling overhead which contains addition information to enhance performance of the wireless networks in IOT data. The signaling overhead figure in given below in Figure 10.

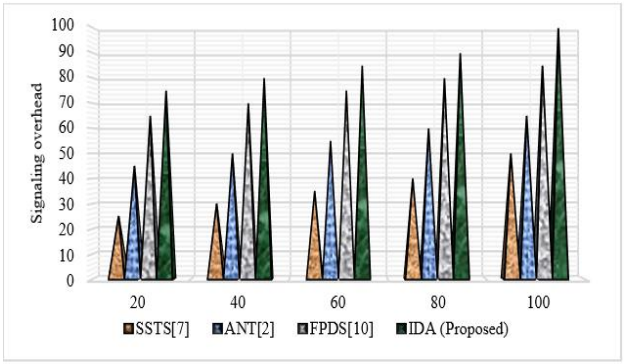


Figure 10. signaling overhead

The signaling overhead is compared with existing three techniques which are, Smart Security Transportation System (SSTS) [7], Activity Network Things (ANT) [2], Flexible Privacy-preserving Data Sharing (FPDS) [10] and proposed Intrusion Detection Architecture (IDA). In signaling overhead, compared with other existing techniques the proposed IDA is high which shown in Figure 10.

4.1.6. Attack detection

A technology called attack detection is used to track IOT data flow and identify any unauthorized entry or activity in the database environment. The attack detection graph is shown in Figure 11.

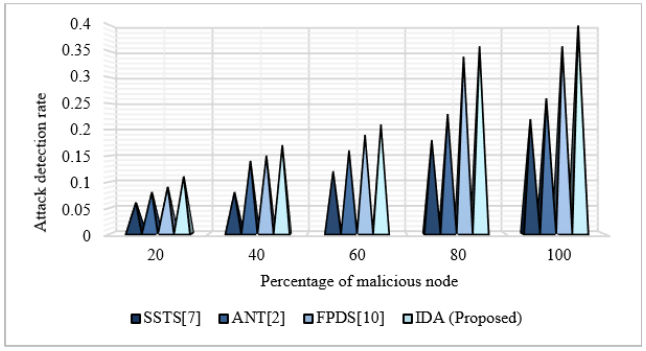


Figure 11. Attack detection rate vs malicious percentage node

The attack detection rate with malicious percentage node is compared with existing three techniques which are, Smart Security Transportation System (SSTS) [7], Activity Network Things (ANT) [2], Flexible Privacy-preserving Data Sharing (FPDS) [10] and proposed Intrusion Detection Architecture (IDA). The number of nodes is taken in between 10<100 of size. Compared with other existing techniques the proposed IDA is high which shown in Fig.11.

4.1.7. Communication cost

Communication cost of the IOT data is depends up on the size and complexity of undertaking data. Here, the communication cost is compared with others is shown in Figure.12

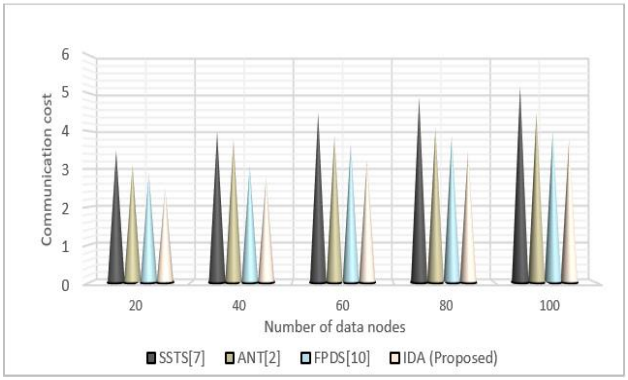


Figure 12. Communication cost with number of data nodes

The communication cost with number of nodes in data are compared with existing three techniques which are, Smart Security Transportation System (SSTS) [7], Activity Network Things (ANT) [2], Flexible Privacy-preserving Data Sharing (FPDS) [10] and proposed Intrusion Detection Architecture (IDA). Number of data nodes are taken in between 10<100 of size. Compared with other existing techniques the proposed IDA communication cost is low, -67%, -33%, -33% of SSTS, ANT, FPDS is reduced in communication cost when compared with proposed IDA. which is shown in Figure.12.

4.1.8. Energy consumption

IoT data enables a smart grid system to control power flow or substantially reduce energy consumption. The energy consumption is shown in graph Figure.13.

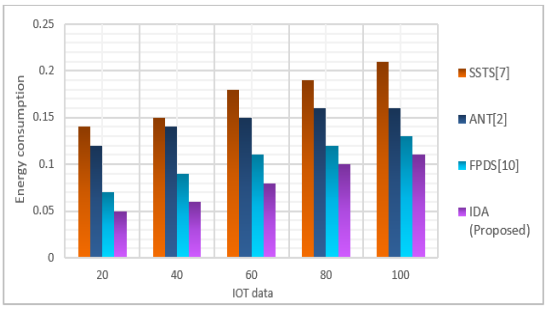


Figure.13. Energy consumption in IOT data

The energy consumption in IOT data is compared with other existing three techniques which are, Smart Security Transportation System (SSTS) [7], Activity Network Things (ANT) [2], Flexible Privacy-preserving Data Sharing (FPDS) [10] and proposed Intrusion Detection Architecture (IDA). Compared with other existing techniques the proposed IDA energy consumption is low which is shown in Figure 13.

5. CONCLUSION

Intrusion Detection Architecture (IDA) has been proposed in this paper, which helps to trace the Intrusion Data in IOT. The proposed Intrusion Detection Architecture (IDA) is performed in three stages namely, Data Collection, Pre-processing in Data encoding and Classification block. The efficiency of the proposed IDA approach has been determined using the evaluation metrics such as configuration latency, detection rate, accuracy, precision, recall rate, false detection rate. The Matlab is used to simulate the Intrusion Detection Architecture (IDA). The detection in IOT intrusion system is maintained by Attack Detection Set or Thread Detection Set with the Network Intrusion Detection System (NIDS) which perform as a detector in IOT system. The proposed method has been evaluated in terms of Communication overhead, Throughput, Attack graph index, Delay analysis, Signaling Overhead, Attack detection rate with malicious node, Communication cost and Energy consumption. The proposed method reduces the communication overhead of 75%, 50% and 38% than SSTS, ANT and FPDS existing techniques. In order to deliver dependable and secure IoT services that will be taken into consideration in the future, backup security solutions must be created and integrated with the DL-based security schemes.

CONFLICTS OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper**.**

FUNDING STATEMENT

No funding was received to assist with the preparation of this manuscript.

ACKNOWLEDGEMENTS

The authors would like to thank the reviewers for all of their careful, constructive and insightful comments in relation to this work**.**

REFERENCES

[1] R. Ding, H. Zhong, J. Ma, X. Liu, and J. Ning, "Lightweight privacy-preserving identity-based verifiable IoT-based health storage system", *IEEE Internet of Things Journal*, vol. 6, no. 5, pp.8393-8405, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[2] R. Sharma, and R. Arya, "Security threats and measures in the Internet of Things for smart city infrastructure: A state of art", *Transactions on Emerging Telecommunications Technologies*, pp.4571, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] L. Nemec Zlatolas, N. Feher, and M. Hölbl, "Security perception of IoT devices in smart homes", *Journal of Cybersecurity and Privacy*, vol. 2, no.1, pp.65-73, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] M.Y. ISMAIL, M.S. Beg, M.F. Jamlos, W.H. Azmi, N.H. Badrulhisam, and O.I. Awad, Potential and Limitation of Internet of Things (IOT) Application in the Automotive Industry: An Overview", *International Journal of Automotive and Mechanical Engineering*, vol. 19, no. 3, pp.9939-9949, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] S.S. Kute, A.K. Tyagi, and S.U. Aswathy, Security, "privacy and trust issues in internet of things and machine learning based e-healthcare", *Intelligent Interactive Multimedia Systems for e-Healthcare Applications*, pp.291-317, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Y. Wu, H.N. Dai, H. Wang, Z. Xiong, and S. Guo, "A survey of intelligent network slicing management for industrial IoT: integrated approaches for smart transportation, smart energy, and smart factory", *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp.1175-1211, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] H. Uddin, M. Gibson, G.A. Safdar, T. Kalsoom, N. Ramzan, M. Ur-Rehman, and M.A. Imran, "IoT for 5G/B5G applications in smart homes, smart cities, wearables and connected cars", In *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, pp. 1-5, 2019. IEEE. [CrossRef] [Google Scholar] [Publisher Link]

[8] K. Demestichas, N. Peppes, and T. Alexakis, "Survey on security threats in agricultural IoT and smart farming", *Sensors*, vol.20, no.22, pp.6458, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[9] P. Ratta, A. Kaur, S. Sharma, M. Shabaz, and G. Dhiman, "Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives", *Journal of Food Quality*, pp.1-20, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] E.S. Ali, M.K. Hasan, R. Hassan, R.A. Saeed, M.B. Hassan, S. Islam, N.S. Nafi, and S. Bevinakoppa, "Machine learning technologies for secure vehicular communication in internet of vehicles: recent advances and applications", *Security and Communication Networks*, 2021, pp.1-23, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] W.D. Lin, and M.Y. Low, "Concept design of a system architecture for a manufacturing cyber-physical digital twin system", In *2020 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, pp. 1320-1324, 2020. IEEE. [CrossRef] [Google Scholar] [Publisher Link]

[12] K.O.M. Salih, T.A. Rashid, D. Radovanovic, and N. Bacanin, "A comprehensive survey on the Internet of Things with the industrial marketplace", *Sensors*, vol. 22, no. 3, pp.730, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] A. Kumari, S. Tanwar, S. Tyagi, and N. Kumar, Verification and validation techniques for streaming big data analytics in internet of things environment. *IET Networks*, vol. 8, no. 3, pp.155-163, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[14] A. Attkan, and V. Ranga, "Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence-based key-security", *Complex & Intelligent Systems*, vol. 8, no. 4, pp.3559-3591, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[15] B. Alotaibi, "Utilizing blockchain to overcome cyber security concerns in the internet of things: A review", *IEEE Sensors Journal*, vol. 19, no. 23, pp.10953-10971, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[16] J. Franco, A. Aris, B. Canberk, and A.S. Uluagac, "A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems", *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp.2351-2383, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[17] I. Vaccari, E. Cambiaso, and M. Aiello, "Evaluating security of low-power internet of things networks", *International Journal of Computing and Digital Systems*, vol. 8, no. 02, pp.101-114, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[18] H.M. Akwetey, P. Danquah, and I. Asampana, "Critical infrastructure cybersecurity challenges: Iot in perspective", *arXiv preprint arXiv:2202.12970*. 2022. [CrossRef] [Google Scholar] [Publisher Link]

[19] Y. Zhang, B. Li, B. Liu, Y. Hu, and H. Zheng, "A privacy-aware PUFs-based multiserver authentication protocol in cloud-edge IoT systems using blockchain", IEEE Internet of Things Journal, vol. 8, no. 18, pp.13958-13974, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[20] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y.A. Bangash, "An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security", *IEEE Internet of Things Journal*, vol. 7, no. 10, pp.10250-10276, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[21] K.Y. Lam, S. Mitra, F. Gondesen, and X. Yi, "ANT-centric IoT security reference architecture—Security-by-design for satellite-enabled smart cities", *IEEE Internet of Things Journal*, vol. 9, no. 8, pp.5895-5908, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[22] S. Verma, Y. Kawamoto, and N. Kato, "A network-aware Internet-wide scan for security maximization of IPV6-enabled WLAN IoT devices", *IEEE Internet of Things Journal*, vol. 8, no. 10, pp.8411-8422, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[23] W. Zhou, C. Cao, D. Huo, K. Cheng, L. Zhang, L. Guan, T. Liu, Y. Jia, Y. Zheng, Y. Zhang, and L. Sun, "Reviewing IoT security via logic bugs in IoT platforms and systems", *IEEE Internet of Things Journal*, 8(14), pp.11621-11639, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[24] J. Zhang, Y. Wang, S. Li, and S. Shi, "An architecture for IoT-enabled smart transportation security system: a geospatial approach", *IEEE Internet of Things Journal*, vol. 8, no. 8, pp.6205-6213, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[25] J. Kim, P.V. Astillo, V. Sharma, N. Guizani, and I. You, "MoTH: Mobile Terminal Handover Security Protocol for HUB Switching based on 5G and Beyond (5GB) P2MP Backhaul Environment", *IEEE Internet of Things Journal*, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[26] F. Zhu, X. Yi, A. Abuadbba, I. Khalil, S. Nepal, and X. Huang, "Cost-Effective Authenticated Data Redaction with Privacy Protection in IoT", *IEEE Internet of Things Journal*, vol. 8, no. 14, pp.11678-11689, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[27] S. Hui, Z. Wang, X., Hou, X. Wang, H. Wang, Y. Li, and D. Jin, "Systematically quantifying IoT privacy leakage in mobile networks. *IEEE Internet of Things Journal*, vol. 8, no. 9, pp.7115-7125, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[28] H. Deng, Z. Qin, L. Sha, and H. Yin, "A flexible privacy-preserving data sharing scheme in cloud-assisted IoT", *IEEE Internet of Things Journal*, vol. 7, no. 12, pp.11601-11611, 2020. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

M. AmanullaKhan received M.E degree in applied electronics from Anna university in 2008, India working as an assistant professor in the department of Electronics and communication engineering at Mohammad Sathak Engineering college, India. His area of interest includes image processing, computer vision, Internet of things, pattern recognition bio metrics and gait recognition he presented various international conference events like IAEME, SCOPUS, and materials today, he has CSTA and ISTE membership. He has guided many computer vision projects and hands on programming MATLAB, PYTHON at various technical institutions around India**.**

M. Usha is currently working as an Associate Professor and HOD in MEASI Institute of Information Technology, Chennai. She has completed M.C.A. and M.Phil. in Computer Science from Bharathidasan University, Trichy. She has also done her M. Tech (CIT) and Ph.D. from Manonmaniam Sundaranar University, Tirunelveli. She has 20 years of teaching experience and she has published papers in Network Security in National and International journals and has presented in International Conferences and Seminars. Her area of interests includes Operating Systems, Artificial Intelligence, Machine Learning, Algorithms and ad-hoc networks especially FANET and Underwater Communication.

S. Ramesh received Ph.D. degree from Anna University, India. He received M.E degree from Anna University, India. He received B. Tech degree in Anna University, India. He is Working as an Associate Professor nearly 14 years still now in Department of Computer science Engineering, Krishnasamy college of Engineering & Technology, Anand Nagar, Kumarapuram, Cuddalore. He got Anna University Supervisor Recognition on 2021. His research interest includes Embedded system and Wireless sensor networks.

Arrived: 25.08.2023
Accepted: 25.10.2023