ISSN: 0067-2904

Developing Blockchain Algorithms in the IoT Network to Secure Data Integrity and System Scalability

Layla Safwat Jamil
College of Agricultural Engineering Sciences, University of Baghdad, Baghdad, Iraq

Received: 10/4/2022 Accepted: 23/5/2023 Published: 30/6/2024

Abstract

The Internet of Things and the blockchain are considered to be the major technologies that are linked together to support the flexibility, scalability, and integrity of the system. IoT devices have insufficient computing capacity in terms of processing data units and storage requirements. It requires efficient encryption algorithms. Nowadays, the IoT is facing several challenges, such as poor interoperability, security vulnerabilities, privacy, and a lack of industry standards. In this paper, a novel triple DES-based blockchain algorithm for the IoT network environment is designed to assure data integrity and system scalability. Initially, the IoT network modeling is framed with different network entities, smart devices, and communication devices. Based on the received requests, the required data are processed via the Triple DES technique. The IoT requests are processed and then authenticated using a blockchain interface. If it is verified, then the service is instantiated; otherwise, it is rejected. This blockchain interface performs similarly to the security gateway for web communication services. It prevents unauthorized third-party networks. The security layer is framed using Triple DES, which takes the least computational effort over the requested data. Here, the blockchain interface acts as an additional security layer that imbues all devices. It is clearly understood from the results that the proposed technique, blockchain-based Triple DES, outperforms the RSA algorithm in terms of computational time.

Keywords: Internet of Things; Blockchain technology; Encryption standards; Security; and Blockchain interfaces.

تطوير خوارزميات سلسلة الكتل في شبكة الإنترنت الأشياء لتأمين سلامة البيانات وتطوير قابلية النظام على التوسع

ليلى صفوت جميل
كلية علوم الهندسة الزراعية، جامعة بغداد، العراق

الخلاصة

يعتبر الدمج بين تقنيات إنترنت الأشياء وسلسلة الكتل دعم واضح لخصائص الأنظمة مثل المرونة والقابلية للتوسع وسلامة هذه الانظمة. ان اجهزة إنترنت الأشياء تعاني من قدرة حسابية غير كافية فيما يتعلق بمعالجة وحدات البيانات ومتطلبات التخزين. فهي تتطلب خوارزميات تشفير فعَّالة. في الوقت الحاضر تواجه تحديات عدة مثل التوافق الضعيف، وثغرات الأمان، والخصوصية، وعدم وجود معايير صناعية. في هذا

*Email: Layla.s@coagri.uobaghdad.edu.iq

البحث تم تصميم خوارزمية جديدة مستندة إلى Triple DES وسلسلة الكتل لبيئة شبكة إنترنت الأشياء بهدف ضمان سلامة البيانات وقابلية توسع النظام. في البداية، يتم تحديد نموذج شبكة إنترنت الأشياء بواسطة كيانات الشبكة المختلفة والأجهزة الذكية وأجهزة الاتصال. حيث يتم معالجة البيانات المطلوبة باستعمال تقنية Triple DES وثم التحقق منها باستعمال واجهة سلسلة الكتل. حيث يشترط هذا التحقق لتفعيل الخدمة، وإلا يتم رفضها. والتي تعمل بطريقة مشابهة لبوابة الأمان لخدمات الاتصال عبر الوب، حيث تمنع الشبكات غير المصرح بها. يتم إنشاء طبقة الأمان باستعمال تقنية Triple DES التي تستغرق وقتًا حسابيًا أقل على البيانات المطلوبة. وبدورها تعتبر كواجهة أمان إضافية تجمع بين جميع الأجهزة. يتضح بوضوح من النتائج أن التقنية المقترحة، التي تعتمد على سلسلة الكتل Triple DES تتفوق بشكل أفضل من خوارزمية RSA من حيث الوقت الحسابي.

1. Introduction

In the recent decade, an inclined growth has been observed in the Internet of Things (IoT) technologies that have impacted the lifestyles of humans [1]. The process of associating embedded wired and wireless technologies with the help of distributed and interlinked network structures is known as the "Internet of Things" (IoT). The arrival of smart objects has modernized the quality of life [2], [3]. Cyberattacks are recent attacks that slow down the growth of the Internet of Things (IoT). The IoT systems have to be supervised with preventive measures that diminish the security risks and enhance the security rate. IoT security is considered a significant area of research nowadays. As the modern era is technology-dominated, communication is achieved using modern technologies; for instance, IoT devices [4] are responsible for providing various services, including communication, and hence, they are required to undergo authentication procedures securely to ensure trustworthy and secure communication [5]. However, maintaining IoT connectivity with an efficient energy management system is challenging due to its diversified nature.

As we already know, the private key plays a significant role in the data security system. The computation of private keys is re-invented by the researchers. Following that, our proposed framework is designed with the same objective under blockchain technology [6]. The prior works made use of certificate-based public-key cryptography, which took more time to verify the users. The frequency of the certificate verification slows down when more users participate during the stipulated period. Therefore, the administration of the certificates becomes complex in terms of storage systems. To ease the data transactional process of cloud storage systems, a blockchain-based storage system with an optimization data solution is being focused on in this work [7].

The contributions to this paper are:

a) A decentralized storage mechanism using blockchain technology is introduced. The blockchain's storage preserves the IoT data. The proposed blockchain-based Triple DES method is decentralized, which ensures data integrity and the scalability of the systems.

b) Blockchain-based Triple DES models introduce well-encrypted IoT data that provides the efficiency of transaction verification in a consistent manner.

The research paper is arranged as follows:

Section 2 presents the “Literature Review” that portrays the reviews of existing privacy preservation-oriented techniques for IoT data in terms of merits and demerits. Section 3 presents the “Research Methodology,” which discusses the workings of the proposed techniques and the phases involved in the research methods. Section 4 presents the “Design of a Blockchain-Based Security Model” that presents the workings of blockchain technology in

IoT security. Section 5 presents the "Model Evaluation and Results" that portrays the simulation setup, performance metrics, and the achieved results. Section 6 presents the "Conclusion and Future Direction" that portrays the findings, suggestions, and recommendations of this research study.

2. Literature Review:

This section includes the study of various existing research methodologies on the security of data using blockchain technologies and provides a brief overview of significant research conducted in the realm of data security in IoT networks. Machine learning algorithms are prevailing in the long term to foster detection/prevention/classification that cover K-NN, K-means, SVM, decision trees, and I Bayes techniques. The author in [8] has presented an IDS model using a k-NN algorithm. Initially, the behaviors of the nodes were studied by differentiating normal and abnormal behaviors. Relying upon it, the abnormal features were extracted by following and broadcasting RREQ and RREP packets. It classified the normal and abnormal nodes based on the abnormal behaviors obtained. The frequent occurrence of RREQ messages was considered normal for nodes. Thus, the classified results have increased the classification accuracy. However, it reduces the efficacy of large-scale real-time applications. In [9], the scope of the K-Nearest Neighbor algorithm was studied to improve the lifetime of the wireless sensor nodes.

The aim of this study was to improve the efficiency of the active nodes. The transmission of data over a longer path has consumed more power and reduced battery life. The longer the distance, the more power is consumed. Thus, the communication risk of sensor nodes was increased due to poor connectivity. The authors have preserved 11% of energy consumption by optimizing active nodes. The deployment of k-NN in the IoT domain was designed to automatically recognize the malware. Thus, crypto-ransomware [10] with IoT applications was studied to locate the IoT malware. The connecting features of all IoT applications were studied to improve their utility functions. With the help of k-NN, the features related to storage and computing were done for normal and abnormal IoT devices. The system has yielded a detection rate of 95% and a precision rate of 89%. Object localization is another interesting problem that measures the effectiveness of the placed objects. With the help of the Global Positioning System (GPS) [11], the position of the objects was studied. This was further optimized by an improved k-NN that localizes the object position by estimating the Receiver Signal Strength Indicator (RSSI) and low energy. It has improved accuracy by 1.5% compared to conventional ML techniques.

Several techniques were published to monitor the IoT nodes using the Receiver Signal Strength Indicator (RSSI) [12] and Time Difference of Arrival (Toa) [13]. The evaluation of the accuracy is determined from the evaluation of the distance measurement and the noise prevailing in the deployed sensor nodes. A support vector machine (SVM) was developed to localize the objects [14]. The sensor nodes were revisited by the hyperplane of the SVM. The training set comprises geographical regions that define the domain of sensors and their classified regions. The nodes in the intersecting regions were localized using the SVM algorithm. It has given 98% accuracy, which is better than [12 and 13]. Furthermore, the design objectives of the training data have been organized using decision parameters like information and connectivity measures. However, the outliers in the training samples are discarded. In some cases, the limited computational capacity and processing power have identified nodes that are of low quality.

In order to ensure the quality of the data as well as expand the constraints of WSNs from the aspects of communication, computational complexity, and memory, a novel outlier detection method using ellipsoidal SVM was studied [15]. When the data arrives, it is projected into normals (or outliers), depending on the temporal information of the sensor nodes. The achieved results have given a higher classification rate with improved effectiveness. However, it is not suitable for real datasets or variable data distribution models. Numerous SVM techniques have been designed to support IoT applications. It intends to eliminate intruders in the network service and also improve data security. In alignment with that, signature-based SVM techniques were established, such as behavior-oriented techniques and dynamic analysis techniques.

To resolve this, a linear-based SVM technique [16] was introduced to detect IoT malware on smartphone devices. It helped to diversify the original and fake data. It has detected network bytes, inappropriate messages, and overflowing memory. High accuracy was achieved for all network attacks. It was evaluated for the detection of "epilepsy seizures" in the healthcare system. The data collected from the IoT sensors was explored by the electrical waves of the brain. The electrical features were identified using principal component analysis [17]. The features extracted from the PCM were fed into the input of the SVM classifier that detected epilepsy in normal people. It has improved the accuracy rate, and it is also effective for connected objects.

The performance of the conventional ML classifiers SVM and feed-forward neural networks was studied by [18]. The author designed an improved DBN that developed supervised and unsupervised training models. It is combined with the RBF to differentiate relevant and irrelevant features. By considering 122 input layers with 122 static features, five categories of IDS were detected. This was evaluated in the KDD Cup 99 datasets, which proved that the count of RBF layers under the DBN has outperformed the SVM and backpropagation algorithms. It achieved detection rates (DR), true positive rates (TPR), and false positive rates (FPR) equal to 93.49%, 92.33%, and 0.76%, respectively. A detailed architecture of DBN for IDS was still in the developmental stage because less analysis was conducted on dynamic features [19]. With the help of NSL-KDD datasets, the author described the role of static and dynamic features in designing the training classifiers. Due to the class imbalance issue, the results were not remarkable. The real-time applications of DBN with artificial neural networks (ANN) [20] were studied by tuning the hidden layers and the number of features. It was evaluated using 5-cross validation training models with 30 epochs. The designed model detected 3000 benign and 3000 malicious files. It achieved 96.1% accuracy with 400 features. From the above-conducted reviews, the security and privacy of the IoT data under blockchain technology are still in the under-development stage. The heterogeneous connections do not ensure the security and privacy of IoT communication. The scope of the data exchange system needs to be addressed in terms of quality of service.

The major key elements related to the IoT systems and their relationships were deployed to improve security in different scenarios. Since the devices were joined with different devices [21], the integrity of the data was not assured. The adoption of different vertical areas of the IoT was studied. In [22], the authors have explored the needs of IoT service providers. The adoption of Destiny Cellular Network with the 5G networks was explored to find out the second connected module. The scope of integrity in terms of service providers was discussed. 5G is managed by the characteristics of high visitor range density, high connection density, excessive mobility, and IoT ecology. Set the basic functions of the system [23]. In [24], the authors have presented a better scope of IoT threats in the case of maintaining data integrity.

Many IoT devices have combined with physical devices, allowing attackers to easily modify the integrity of the data. The information sensitivity of the wireless attackers scrutinized the complexity of the security algorithms. In [25], the combination and preservation of the IoT devices have faced weak login combinations. If it gains access, it deletes all network data on the smart device, which makes it unusable unless somebody physically gets access to the device to restart it to factory defaults. The malware has no other purpose but to be destructive, making the device unusable.

In blockchain networks, we like to combine symmetric and asymmetric encryption algorithms. AES is often used for data encryption and symmetric key sharing. RSA and ECC are used for secure key exchange, digital signatures, and public key infrastructure [26]. Triple DES, which is planned to be used in this research due to its performance and security compared to other algorithms, is summarized in the table below:

Table 1: Comparison of used Algorithm and other Algorithm

Algorithm	Key Type	Key Length	Speed	Security
Triple DES [22]	Symmetric	192-bit*	Moderate	Moderate
RSA [27]	Asymmetric	1024/2048/3072/4096-bit	Slow	High
ECC [28]	Asymmetric	224/256/384/521-bit	Moderate	High
Blowfish [28]	Symmetric	32-448-bit	Fast	Moderate
AES [22]	Symmetric	128/192/256-bit	Fast	High

However, from the comparison above, the use of Triple DES in an IoT blockchain network would involve a trade-off between security and performance. In the private network, it will be a better choice for more secure and efficient encryption algorithms like AES or ECC, especially if we consider that IoT devices can be updated or replaced to support these algorithms.

3. Research Methodology:

This section discusses the proposed methodology for developing an efficient blockchain-based security system for ensuring data integrity in IoT networks. The proposed detection model incorporates blockchain models. The subsection of the proposed workflow includes:

3.1 System model:

The conventional industrial architectures do not assure the traceability of locations, item delivery, or the product documents of workers. These are managed independently. The mishandling of the data, as well as the security policies of an organization, are not known, apparently. Though several phenomenal approaches for intercommunication and cross-management activities are available, the disjointed organization system looks for third-party authority to preserve environmental security. Security and privacy solutions are provided by the advent of blockchain technology. The system entities are:

a) Custom Device Server: It acts as a hub for all associated smart devices.
b) Adding layers of security to the home server by proposing data encryption techniques.
c) Exploiting the programming language could enable the server to execute on any device.
d) Eliminating smart devices from directly communicating with the IoT via smart devices.
e) The communication between the devices is done through the home servers.
f) The IoT network is decentralized using blockchain technology.
g) After adding the new distributed ledger that assesses the received requests based on the queries, the additional security layers are then inserted by means of encryption techniques.

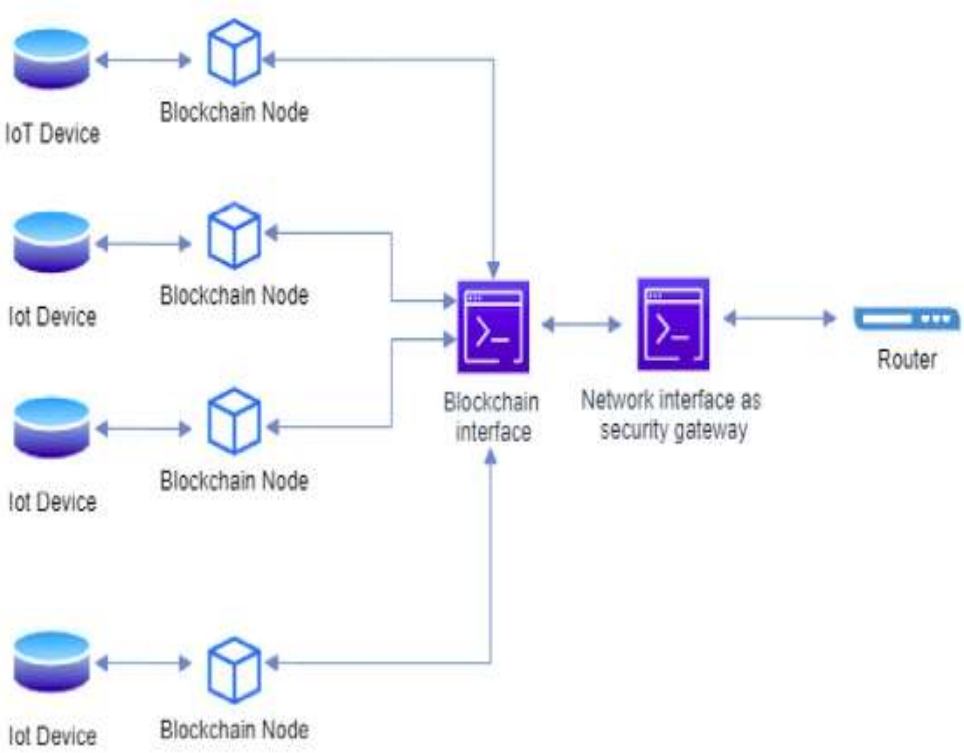

Figure 1: System Model

3.2 Preprocessing:

Here, blockchain logic is included in the home server. The incoming data is parsed and then validated by the blockchain. It creates new blocks and adds them to the distributed ledger. The mishandling of the hub device is done by the connected devices. It combines the smart devices with the IP network, which could ensure a trusting relationship. In order to enhance the security of the devices, hub-based solutions are dominated by blockchain technology. The leaked information was removed from the device in the correct format. The IoT data management node shares and encrypts the data using the Triple DES algorithm. In order to ensure the privacy of the user data, the blockchain interface merges with the blockchain nodes in case the leaked data does not allow a third party to be aware of the data content. The data management node receives the data segments, like copies and encoded data, and these are also preserved at the distributed storage nodes. This can eliminate the single point of failure issue in the case of data loss. However, the integrity of the data is not affected. Since the data management node generates the hash value of the encrypted file and forwards it to the IoT server systems, the blockchain interface preserves the hash data, the address of the hash data, and the identity. Once the transaction is confirmed, it is processed and shared with the other miners. Each data segment after verification is preserved by the set of blockchain nodes. The audit actions take place at each block to eliminate dishonesty.

6. 4. Design of blockchain-based security model:

This section will provide a brief explanation of the proposed blockchain algorithm model for data security. It has four suggestions for engaging blockchain technology. They are:

a) Filtering allows IoT services to access the blockchain network from approved IP addresses.

b) An additional security layer is added by implementing the interface that has been used to encrypt/decrypt the data leaving the blockchain network.

c) Adding a response module that could prevent the IoT services from leaving the

blockchain networks.
d) The repeated requests forwarded to the IoT layers are maintained in the distributed ledger to provide a smart device with a previous response.

Initially, the smart devices were focused on collecting data. Generally, smart devices make use of sensors to gather and assess the required data. It is processed and sent to the remote server. The limitation in processing power has lowered the quality of the data obtained from external sources, and it is poorly encrypted (or not encrypted properly). In order to ensure the data's security from external sources, the proposed security solution must intercept it. Blockchain will act as an interface so as to secure the information. It looks for new connection requests for every new transaction. The dataset is a collection of various transactions between ten nodes in the network, sorted into tables. These datasets include transactions along with data about the transaction hash, block number, timestamp, date and time, data value, and transaction fee. The total number of hashes for implementation is 30,703, compiled in ten groups [29].

The unique characteristic of blockchain technology is that it eliminates the need for third-party auditors. All interactions between honest users are administered by smart contracts (SCs). It is a small block of code that extracts information from the cloud nodes. It is used by the Ethereum address (EA) for the given transactional input. Ethereum functions permit the cloud users to read, write, or execute the code on the top layer of the Ethereum applications. The Ethereum Address (EA) is a unique address established by the Ethereum Network while performing inter-communication and intra-communication processes for each cloud user. Every piece of data has its own hash value, which is stored in the SCs. It is further used for data assessment. If any modification is made to the data, the hash value is also modified. Along with this responsibility, SCs have some more tasks like validating the registered users, verifying the authorized users, and administrating the outsourced data. The following are the properties of the smart contracts:
a) Methods: This function is similar to the task of a contractor. It defines the restricted access of all participants depending on their role in the cloud infrastructure. It is detailed in the role-based access control policies.
b) Modifiers: They alter the characteristics of the functions. It portrays the condition to be executed prior. Here, certain participants are allowed to execute the functions.
c) Variables: This is the value that changes based on the function calls and specified data type.
Smart contracts take control over the data and participants during the transactional process. It preserves the data before and after the modification is done. The distributed ledger holds the transaction details, which are then processed on the remote server. The local information on the remote server is held by the router. It has two components: the request header and the request body. The header contains details like the request URL, request method, status code, and version of the request. Most of the data in request headers is not used by remote servers, so it is eliminated. The request body has data used for parsing. To enhance the security of each request, a layer with encryption functionality is employed. Here, the triple DES encryption algorithm, which is a symmetric key block cipher, is used to enhance its security by applying the DES algorithm three times using three different keys (K1, K2, and K3), as explained in Figure 1 below:

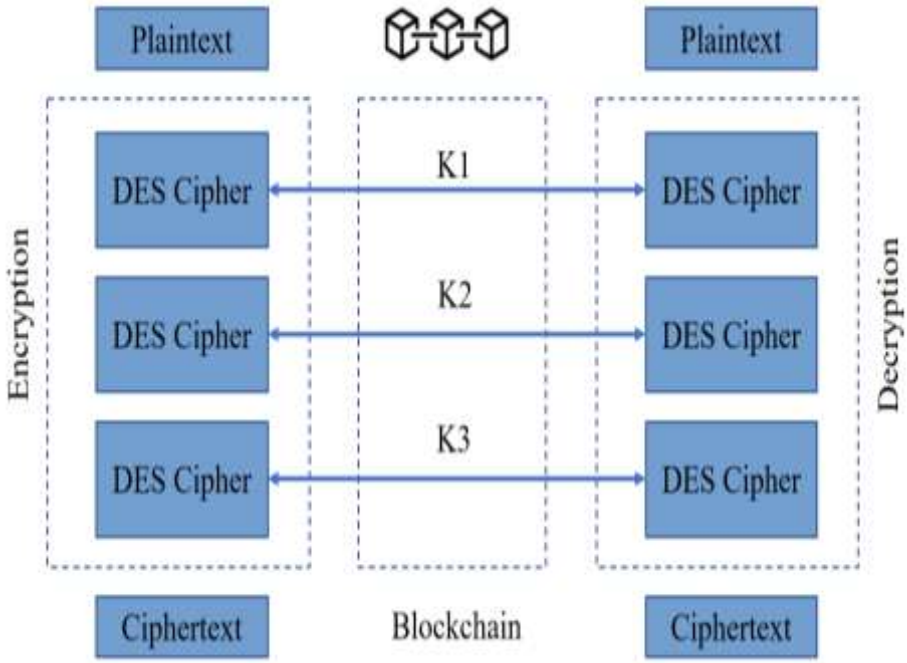

Figure 1: Triple DES Algorithm Structure in Blockchain Network

The description of the Triple DES algorithm structure:
For encryption: C3 = E (K3, D (K2, E (K1, P)))
For decryption: P = D (K1, E (K2, D (K3, C3)))
Where:
P represents the plaintext (input data),
C3 represents the ciphertext (encrypted data),
K1, K2, and K3 are the three 64-bit keys derived from the 192-bit key,
E represents the encryption operation using the DES algorithm,
D represents the decryption operation using the DES algorithm.
The request is sent from the server to the blockchain interface before processing in the web environment. Finally, the blockchain interface will be considered an interface for any IoT devices. The T-DES makes use of two permutations in the encryption process, which are used for the initial and final rounds. Along with that, 16 festal rounds are used. As per the defined security parameters, each round makes use of a 48-bit round key for each secret key generation. The permutation process holds 64-bit input that performs according to the network rules. However, fewer inputs and outputs are used for the inversion process. Each round has a left round and a right round, wherein each round is interlinked with the previous rounds to make cipher data. This process continues until the stopping criteria are met.

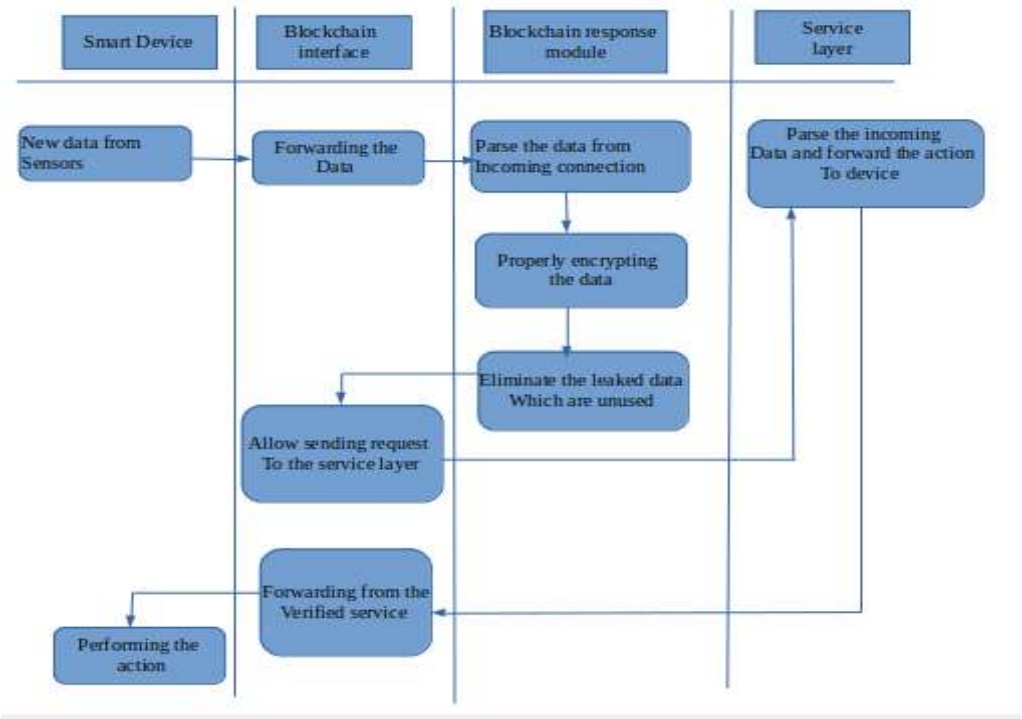

Figure 2: Activity diagram of the proposed technique**.**

5. Results and Discussions:

This section will provide an analysis of the simulation results and a performance evaluation of the proposed methodology.

5.1 Performance Evaluation:

In this section, the performance of the proposed technique is evaluated with respect to different performance metrics, and the respective results are discussed. Computational time is the most important metric that defines the efforts managed by the proposed mechanisms within the stipulated time. It helps to achieve the success rate of the designed applications.

a) Encryption time: It is the time taken to verify the private keys and then convert plaintext into ciphertext.

b) Decryption time: It is the time taken to verify the private keys based on the generated keys and then the conversion of ciphertext into plaintext.

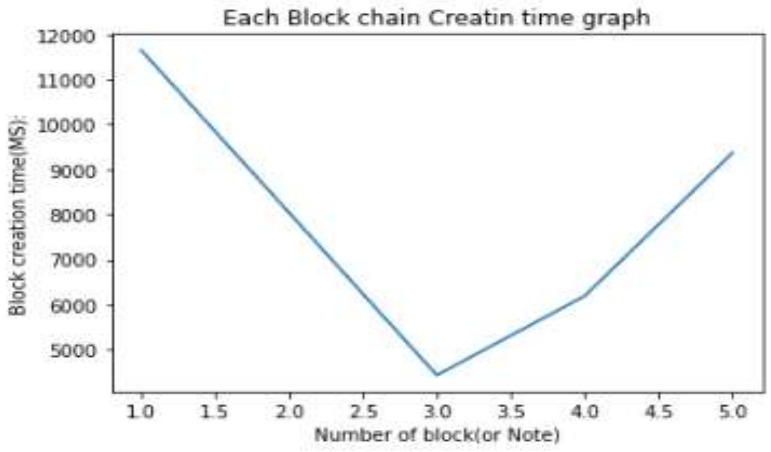

Figure 3: Creation of blockchain

Figure 1 presents the creation of a blockchain interface to the remote service. In order to assess the environment, blocks are created.

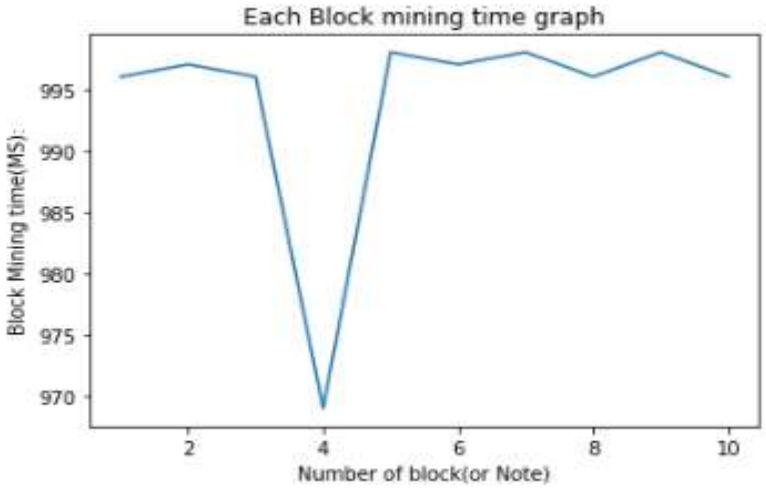

Figure 4: Block mining time

Figure 2 presents the block mining time analysis. During the communication between the layers, the data is splattered into different blocks, which are unaware of the IoT users. Based on the request made, the blocks are analyzed with their unique ids.

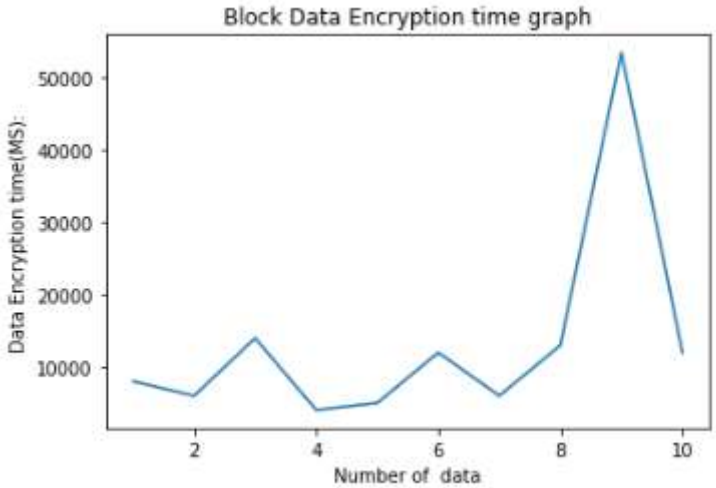

Figure 5: Encryption time analysis

Figure 3 presents the encryption time analysis of the proposed triple DES on the blockchain interface. It is explored on blocks of data with respect to time. It is observed from the graph that a significant amount of time is taken to compute the data blocks.

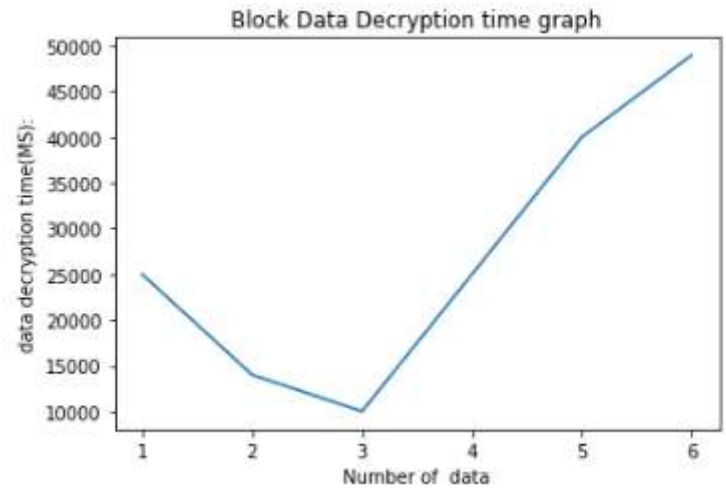

Figure 6: Decryption time analysis

Figure 4 presents the encryption time analysis of the proposed triple DES on the blockchain interface. It is explored on blocks of data with respect to time. It is observed from the graph that a significant and similar range of time is taken to compute the cipher data blocks.

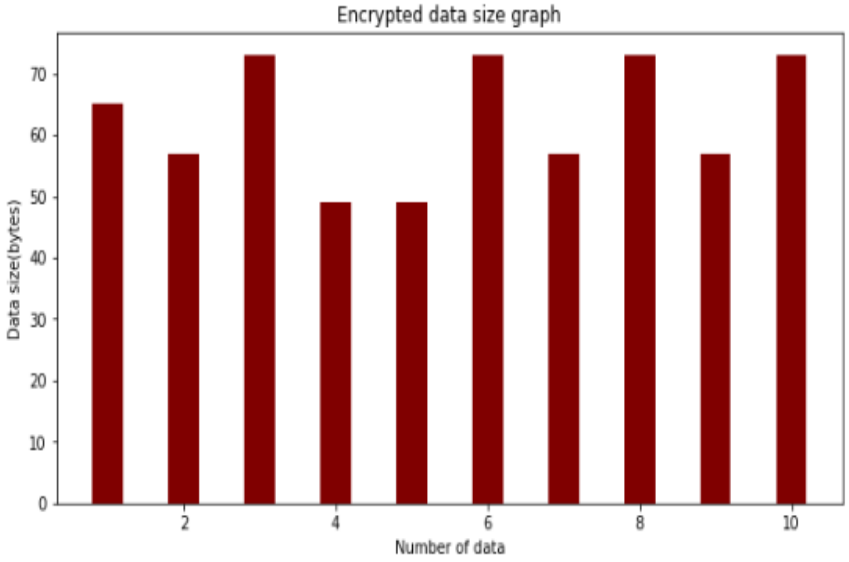

Figure 7: Data size consumed during encryption process

It is observed from the above figure that the proposed technique has taken fewer bytes to develop a blockchain interface.

5.2 Performance Comparison:

This section will provide a comparative analysis by comparing the performance of the proposed approach against the existing techniques with respect to accuracy and training time. The existing technique (Triple DES) is a symmetric key, 192-bit block cipher that outperforms and is faster than RSA, which is an asymmetric key pair and can be used in both public and private blockchain networks. It's slower than Triple DES, but it's more secure because of the complexity of the algorithm, and it comes after Triple DES in terms of computational time.

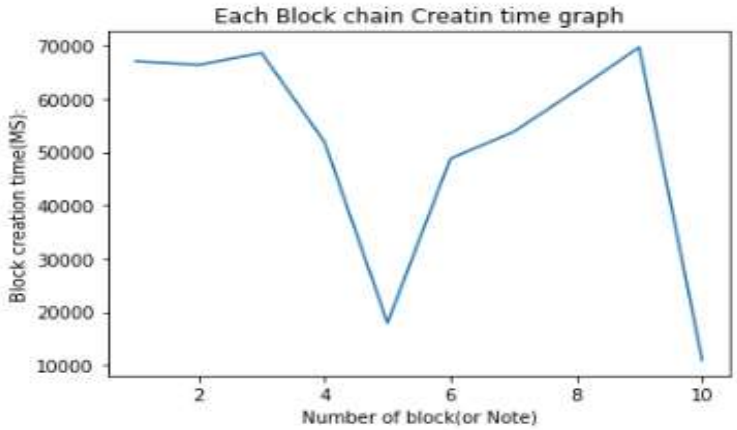

Figure 8: Creation time of blockchain module

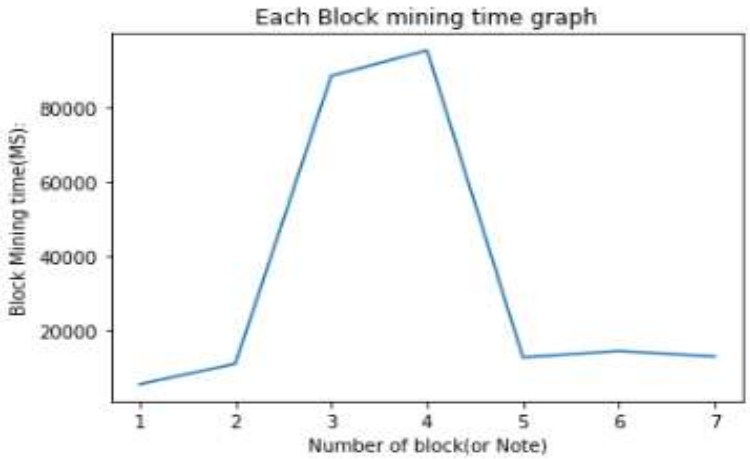

Figure 9: Block mining time

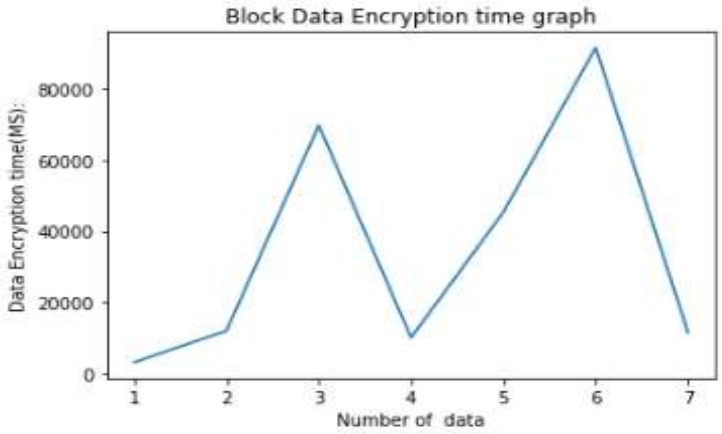

Figure 10: Encryption time analysis

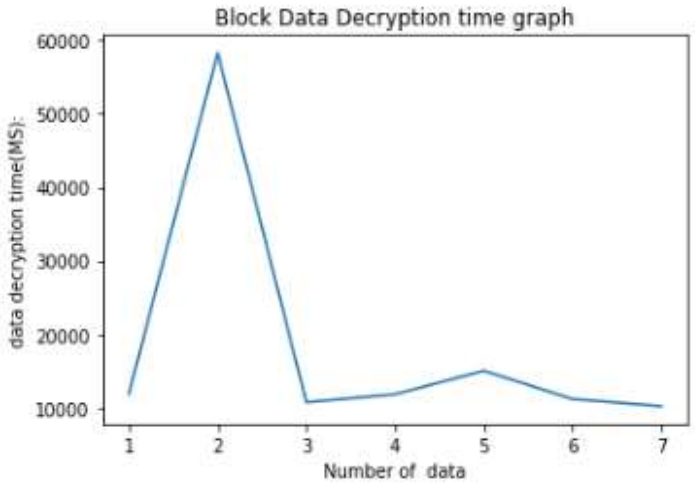

Figure 11: Decryption time analysis

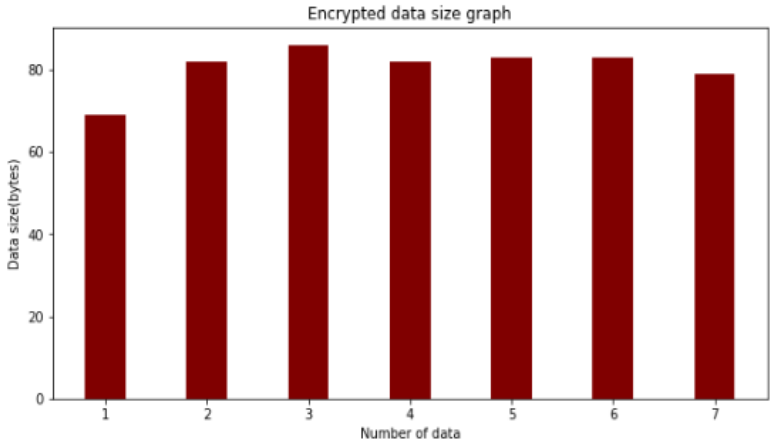

Figure 12: Data size consumed during encryption process

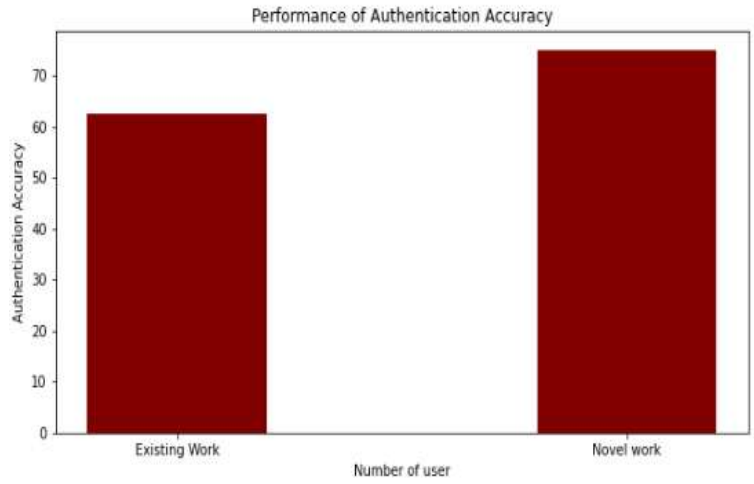

Figure 13: Accuracy of the authentication metric in blockchain interfaces

It is clearly understood from the above figure that the proposed technique works better than the existing technique. Irrespective of the number of users, the proposed techniques yield the best authentication service within the stipulated time.

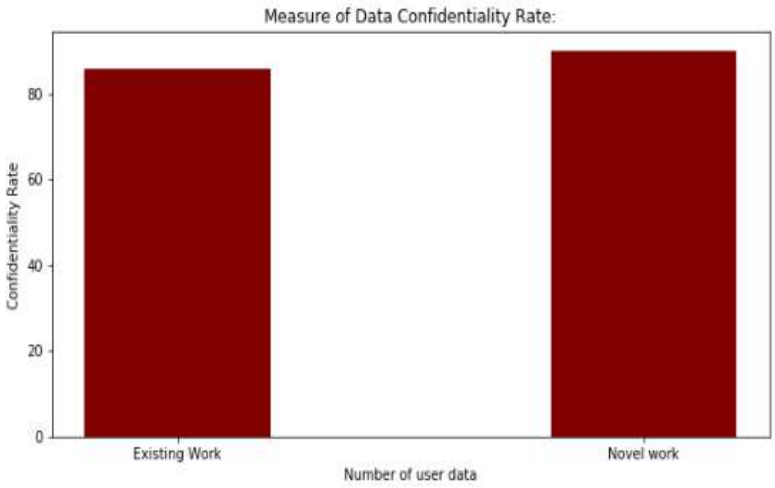

Figure 14: Confidentiality rate analysis

Figure 12 presents the analysis of the confidentiality rate. It measures how far the information is preserved during the assessment of the blockchain interface.

6. Conclusion:

In this research study, to ensure data integrity and system scalability in an IoT network context, a unique triple DES-based blockchain method is developed. Different network entities, smart devices, and communication devices are initially framed in IoT network modeling. The necessary information is compiled in response to requests. The blockchain interface is used to process and verify IoT queries. If it is confirmed, the service is created; otherwise, it is not. The blockchain interface acts as a web communication service's security gateway would. It blocks access to any networks that aren't approved. It is expected that the security requirements will be met after blockchain technology is included in the IoT storage system. The participants' honesty is taken as a given. The blockchain interface provides safety for the information being sent. Here, the data cubes are assembled using information provided by trustworthy people and obtained through data mining. Here, Miner is a node that functions in a way that is analogous to a neutral auditor. The issuers of cloud-based transactions compensate miners for their efforts in collecting data on those consumers. The distributed file system makes it possible for files stored on several sites to be accessed over a P2P network. Triple DES, which requires minimal computing effort to encrypt the desired data, forms the basis of the security layer. In this case, the blockchain interface provides an extra layer of protection that is embedded in every gadget. The rate of secrecy, the accuracy of authentication, and the number of blocks sent in a data transaction are all experimentally examined. When it comes to storing data from the Internet of Things, problems with data dependability, security, and privacy are efficiently resolved by this approach. The outcomes make it evident that the suggested method, blockchain-based Triple DES, is more efficient than the RSA algorithm.

References

[1] C. K. Metallidou, K. E. Psannis, and E. A. Egyptiadou, "Energy Efficiency in Smart Buildings: IoT Approaches," *IEEE Access*, vol. 8, pp. 63679–63699, 2020, doi: 10.1109/ACCESS.2020.2984461.

[2] X. Su, Z. Wang, X. Liu, C. Choi, and D. Choi, "Study to Improve Security for IoT Smart Device Controller: Drawbacks and Countermeasures," *Secur. Commun. Networks*, vol. 2018, p. 4296934, 2018, doi: 10.1155/2018/4296934.

[3] Z. A. Alizai, N. F. Tareen, and I. Jadoon, "Improved IoT Device Authentication Scheme Using Device Capability and Digital Signatures," in *2018 International Conference on Applied and Engineering Mathematics (ICAEM)*, 2018, pp. 1–5, doi: 10.1109/ICAEM.2018.8536261.

[4] J. Li, J. Wu, and L. Chen, "Block-secure: Blockchain based scheme for secure P2P cloud storage," *Inf. Sci. (Ny).*, vol. 465, pp. 219–231, 2018, doi: https://doi.org/10.1016/j.ins.2018.06.071.

[5] A. Totonchi, "(PDF) Smart Buildings Based On Internet Of Things: A Systematic Review," *Dep. Inf. Commun. Technol.*, no. November, 2018, doi: 10.6084/m9.figshare.19335590.v1.

[6] A. Verma, S. Prakash, V. Srivastava, A. Kumar, and S. C. Mukhopadhyay, "Sensing, Controlling, and IoT Infrastructure in Smart Building: A Review," *IEEE Sens. J.*, vol. 19, no. 20, pp. 9036–9046, 2019, doi: 10.1109/JSEN.2019.2922409.

[7] H. N. Rafsanjani, C. R. Ahn, and J. Chen, "Linking building energy consumption with occupants' energy-consuming behaviors in commercial buildings: Non-intrusive occupant load monitoring (NIOLM)," *Energy Build.*, vol. 172, pp. 317–327, 2018, doi: https://doi.org/10.1016/j.enbuild.2018.05.007.

[8] W. Li, P. Yi, Y. Wu, L. Pan, and J. Li, "A New Intrusion Detection System Based on KNN Classification Algorithm in Wireless Sensor Network," *J. Electr. Comput. Eng.*, vol. 2014, p. 240217, 2014, doi: 10.1155/2014/240217.

[9] M. M. Ahmed, A. Taha, A. E. Hassanien, and E. Hassanien, "An Optimized K-Nearest Neighbor Algorithm for Extending Wireless Sensor Network Lifetime BT," in *The International Conference on Advanced Machine Learning Technologies and Applications (AMLTA2018)*, 2018, pp. 506–515.

[10] A. Azmoodeh, A. Dehghantanha, M. Conti, and K.-K. R. Choo, "Detecting crypto-ransomware in IoT networks based on energy consumption footprint," *J. Ambient Intell. Humaniz. Comput.*, vol. 9, no. 4, pp. 1141–1152, 2018, doi: 10.1007/s12652-017-0558-5.

[11] Y. Peng, W. Fan, X. Dong, and X. Zhang, "An Iterative Weighted KNN (IW-KNN) Based Indoor Localization Method in Bluetooth Low Energy (BLE) Environment," *in 2016 Intl IEEE Conferences on Ubiquitous Intelligence Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, 2016, pp. 794–800, doi: 10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.0127.

[12] C. Sha and R. C. Wang, "A type of localization method using mobile beacons based on spiral-like moving path for wireless sensor networks," *Int. J. Distrib. Sens. Networks*, vol. 2013, 2013, doi: 10.1155/2013/404568.

[13] Y. Kwon, K. Mechitov, S. Sundresh, W. Kim, and G. Agha, "Resilient Localization for Sensor Networks in Outdoor Environments," in *25th IEEE International Conference on Distributed Computing Systems (ICDCS'05)*, 2005, pp. 643–652, doi: 10.1109/ICDCS.2005.68.

[14] D. A. Tran and T. Nguyen, "Localization In Wireless Sensor Networks Based on Support Vector Machines," *IEEE Trans. Parallel Distrib. Syst.*, vol. 19, no. 7, pp. 981–994, 2008, doi: 10.1109/TPDS.2007.70800.

[15] Y. Zhang, N. Meratnia, and P. J. M. Havinga, "Distributed online outlier detection in wireless sensor networks using ellipsoidal support vector machine," *Ad Hoc Networks*, vol. 11, no. 3, pp. 1062–1074, 2013, doi: https://doi.org/10.1016/j.adhoc.2012.11.001.

[16] M. Masum and H. Shahriar, "Droid-NNet: Deep Learning Neural Network for Android Malware Detection," in *2019 IEEE International Conference on Big Data (Big Data)*, 2019, pp. 5789–5793, doi: 10.1109/BigData47090.2019.9006053.

[17] J. A. de la O Serna, M. R. A. Paternina, A. Zamora-Méndez, R. K. Tripathy, and R. B. Pachori, "EEG-Rhythm Specific Taylor–Fourier Filter Bank Implemented With O-Splines for the Detection of Epilepsy Using EEG Signals," *IEEE Sens. J.*, vol. 20, no. 12, pp. 6542–6551, 2020, doi: 10.1109/JSEN.2020.2976519.

[18] H. Zhang, C. Q. Wu, S. Gao, Z. Wang, Y. Xu, and Y. Liu, "An Effective Deep Learning Based Scheme for Network Intrusion Detection," in *2018 24th International Conference on Pattern Recognition (ICPR)*, 2018, pp. 682–687, doi: 10.1109/ICPR.2018.8546162.

[19] M. Z. Alom et al., "A State-of-the-Art Survey on Deep Learning Theory and Architectures," *Electronics*, vol. 8, no. 3, 2019, doi: 10.3390/electronics8030292.

[20] S. Mahdavifar and A. A. Ghorbani, "Application of deep learning to cybersecurity: A survey," *Neurocomputing*, vol. 347, pp. 149–176, 2019, doi: https://doi.org/10.1016 /j.neucom.2019. 02.056.

[21] A. R. Kairaldeen, N. F. Abdullah, and A. Abu-samah, "Data Integrity Time Optimization of a Blockchain IoT Smart Home Network Using Different Consensus and Hash Algorithms," *Wireless Communications and Mobile Computing*, vol. 2021, no. Ml, Article ID 4401809, 2021.

[22] B. Bhat, A. W. Ali, and A. Gupta, "DES and AES performance evaluation," in *International Conference on Computing, Communication Automation*, 2015, pp. 887–890, doi: 10.1109/CCAA.2015.7148500.

[23] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, "Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios," *IEEE Access*, vol. 8, pp. 23022–23040, 2020, doi: 10.1109/ACCESS.2020.2970118.

[24] D. Kaliaperumal Rukmani et al., "A New Approach to Optimal Location and Sizing of DSTATCOM in Radial Distribution Networks Using Bio-Inspired Cuckoo Search Algorithm," *Energies*, vol. 13, no. 18, 2020, doi: 10.3390/en13184615.

[25] G. Kambourakis, C. Kolias, and A. Stavrou, "The Mirai botnet and the IoT Zombie Armies," in *IEEE Military Communications Conference (MILCOM)*, 2017, pp. 267–272, doi: 10.1109/MILCOM.2017.8170867.

[26] A. R. Kairaldeen, N. F. Abdullah, A. Abu-Samah, and R. Nordin, "Peer-to-Peer User Identity Verification Time Optimization in IoT Blockchain Network," *Sensors*, vol. 23, no. 4, 2023, doi: 10.3390/s23042106.

[27] Ç. K. Koç, F. Özdemir, and Z. Ödemiş Özger, " Partially Homomorphic Encryption," *Eds. Cham: Springer International Publishing*, 2021, pp. 37–41.

[28] D. Abbasinezhad-Mood and M. Nikooghadam, "Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications," *Futur. Gener. Comput. Syst.*, vol. 84, pp. 47–57, 2018, doi: https://doi.org/10.1016/j.future.2018.02.034.

[29] Blaž Podgorelec, "Dataset of transactions of 10 Ethereum addresses controlled by a private key, each has at least 2000 output transactions, which include a transfer of cryptocurrency, and all transactions are performed within no longer than three months period," *Zenodo*, Nov. 29, 2019. doi: 10.5281/zenodo.3557461.