Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

IOT-Based Malware Detection Framework Using Polymorphic AES and Blockchain with Proof of Work Mechanism

Sanjay Kumar[1*], Dr. C.S. pillai[2]
[1]Assistant professor, Department of CSE(AI&ML), Don Bosco Institute of Technology, Kumbalgodu, Mysore Road, Bengaluru-560074*
[2]professor, Department of CSE (Data Science), ACS College of Engineering, Kambipura, Mysore Road, Bengaluru-560074
[1]Corresponding Author Email: sanjaykumar@dbit.co.in*

ARTICLE INFO

Received: 30 Dec 2024

Revised: 05 Feb 2025

Accepted: 25 Feb 2025

ABSTRACT

In recent years, the attack detection framework used by IoT systems for monitoring has been used to collect and analyze data related to detecting user behavior, predicting potential attacks, and responding in a predetermined manner. This manuscript introduces the innovative multi-agent system and blockchain (BC) technology to enhance data security and detection capabilities in an attack. The primary data sources are initially collected from the freely accessible dataset obtained from the Kaggle platform. The Multiple Imputation-Chained Equations preprocessing handles missing values so that the data's integrity is not compromised. After preprocessing, the data is encrypted using Polymorphic Advanced Encryption Standard (AES), safeguarding private information. Then, the encrypted data is safely stored in a BC environment using a Proof of Work (PoW) mechanism that guarantees validity and immutability in recorded data and resistance to unauthorized modification. Then, the proposed framework deploys the Multi-Scale Channel Attention Residual Network (MSC-Att-ResNet), which analyzes the encrypted data for malicious patterns. To detect intrusions, the Clouded Leopard Optimizer (CdLO) algorithm continually monitors the network activity with fixed predefined threshold values to identify potential attacks. The proposed method is simulated via the Python environment. The evaluation metrics accuracy, false negative rate (FNR), encryption and decryption time, and Matthew's correlation rate (MCC) are evaluated through a comparative analysis with existing approaches. The overall accuracy of 99.01%, MCC of 97.16%, FNR of 2.60, ET, and DT of 174.79ms are obtained by the proposed framework.

Keywords: Internet of Things, Secure Data Transmission, Malware Detection, Blockchain Technology, Deep Learning, Polymorphic Advanced Encryption Standard, Consensus Mechanism.

INTRODUCTION

Internet of Things (IoT) devices are rapidly growing in all sectors- health, manufacturing, smart cities, and homes [1]. Devices connected are very convenient and functional, allowing uninterrupted communication and automation in networks; however, the more IoT grows, the more vulnerabilities [2]. In many aspects, IoT devices lack strong security mechanisms. These put them highly at risk from cyberattacks [3]. Because of this, the task of securing those devices and networks has become very paramount [4]. Safety communication and protection of sensitive information from malicious actors are among the key requirements if the IoT ecosystems remain intact [5]. A comprehensive view of IoT security is considered through proactive and reactive elements for detection and prevention [6]. Toward this end, it is developing attack detection frameworks that continually monitor an IoT network for suspicious activities in real-time [7]. It is the particular answer to stopping malicious attacks such as malware infiltration, data breaches, and denial-of-service (DoS) attacks that compromise the functionality of entire IoT networks [8]. Such systems can also be reviewed, analyzed, and implemented to continue monitoring them [9]. It would ensure quick anomaly detection so that suitable action can be taken to minimize security risks before they escalate further. One of the biggest challenges with securing IoT networks is the heterogeneity of the devices and data associated with them. IoT networks generate multitudes of data from multiple sensors, devices, and endpoints, and the efficient processing and security of these large datasets become a challenge [10]. Not all threats will be state or advanced persistent; cyber threats do

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

evolve. So, it is challenging for traditional, rigid security solutions that are acquired and then continuously updated. With such attacks, there is an urgent need for advanced data protection techniques to be applied in the form of encryption, which would ensure that all sensitive information is kept confidential, even in the event of interference [11]. Encryption, therefore, provides some measure of safety of data from unauthorized access and is, therefore, a part of any such IoT-based security framework [12].

The incorporation of machine learning and deep learning models into attack detection frameworks has become a very strong instrument in the security enhancement process [13]. Due to capabilities to learn from historical data, learn patterns, and predict new ones, machine, and deep learning models are increasingly enhancing how cyber threats can be detected more accurately and within timelines [14]. The deep learning models can, therefore distinguish between normal and malicious activities by analyzing large volumes of network traffic and device behavior to improve, as a whole, efficiency in the detection process of an attack [15]. The intelligent approach not only makes the defense mechanism stronger but, on the other hand, reduces the possibility of false positives ensuring that genuine threats are addressed well within the shortest possible time [16]. Finally, blockchain technology in IoT-based security frameworks integrates into decentralized and tamper-resistant data storage and verification [17]. The feature an immutable ledger presents in blockchain enables the safe recording of all transactions and network activities without unauthorized changes or modifications [18]. With its decentralized nature, the resilience of IoT networks to cyberattacks can be heightened, ensuring the integrity and confidentiality of the data handled intact [19]. In summary, the integration of encryption, deep learning, and blockchain provides holistic security support against the emerging security threats facing IoT networks so they can be robust and secure [20].

Motivation:

Despite advancements in IoT technologies and DL methodologies in the malware detection arena, existing solutions still face several challenges toward robust security and privacy assurance. Current solutions are missing effective encryption mechanisms to protect sensitive data at the time of transmission with IoT networks from unauthorized access and cyberattacks. Further, BC technology brings in stronger integrity and transparency in data; however, most of the existing malware detection frameworks fail to exploit the decentralized nature and consensus mechanisms of BC fully, hence causing bottlenecks and possible inefficiencies in handling data. On the other hand, attackers are evolving malware techniques very fast; thus, deep learning models which can adapt themselves to new threats in real-time are required. Unfortunately, most of the frameworks fail to integrate self-aware dynamic learning functionality and thus leave old systems detecting outdated notions behind. Therefore, there is a need to combine holistic approaches of IoT-based malware detection frameworks with advanced DL algorithms, strong encryption approaches, and BC technology into a comprehensive solution that is efficient, adaptive, and safe in the adaptation of prevention of emerging cyber threats within IoT environments.

The main contributions of the proposed framework are encompassed as follows:

- ❖ To leverage a multi-agent system with blockchain (BC) technology to improve data security and strengthen Internet of Things (IoT) attack detection capabilities.
- ❖ To address the missing values in the preprocessing stage using the Multiple Imputation-Chained Equations (MICE) technique, thereby preserving data integrity.
- ❖ Implement polymorphic AES (P-AES) encryption to secure the conversion of plaintext into ciphertext and safeguard private information.
- ❖ To ensure secure storage in the BC environment using a Proof of Work (PoW) mechanism, promoting data immutability and resistance to unauthorized modification.
- ❖ To introduce the Multi-Scale Channel Attention Residual Network (MSCAtt-ResNet) for effectively analyzing encrypted data to detect malicious patterns.
- ❖ To employ the Clouded Leopard Optimizer (CdLO) algorithm for continuous network activity monitoring, utilizing threshold values to enhance intrusion detection accuracy.

The upcoming sections are prearranged as follows: Section 2 outlays the related work, Section 3 deliberates over the suggested approaches, Section 4 presents the results and discussion, and the conclusion of the suggested framework is deliberated in Section 5.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

RELATED WORKS: A BRIEF REVIEW

Among the numerous research works on IoT-based malware detection frameworks using deep learning with encryption approaches. Some of the recent research works are discussed in this section,

In 2022, Ali, *et.al.,* [21] have presented a neural network-based Industrial IoT Blockchain-based secure searchable encryption method for healthcare systems. Here a group theory-based BSS algorithm that integrates hybrid DNN for efficient intruder detection inside IoT networks. A BC-based approach was first designed for privacy preservation specifically in the context of patient health records within the IoMT. BC was used here as a distributed database through homomorphic encryption (HE) for safe keyword access along with key revocation. The suggested approach provided secure sharing, efficient processing, and transparency in the healthcare data. However, it had the disadvantage of higher computational complexity as computed from encryption processes.

In 2023, Kumar, *et.al.,* [22] have developed a deep learning method guided by blockchain for safe data transfer in an IoT-enabled HC system. Here designed the BC-orchestrated DL approach for Protected Data Transmission in IoT-enabled HC systems that would be referred to as "BDSDT." Scalable BC architecture was developed to ensure data integrity and secure transmission through the mechanism of ZKP mechanism. Data storage costs were lowered through application by using the IPFS for off-chain storage. To enhance the security of data, Ethereum smart contracts were utilized. The validated data was then fed into a deep learning model that combines Deep Sparse Autoencoder (DSAE) and Bidirectional LSTM (BiLSTM), on ID for the HC network. However, there were huge computational overheads due to DL and BC integration in the considered approach.

In 2024, Saravanan, *et.al.,* [23] have developed RNN optimization for BC-IDS in IoT applications. Here the concept of BC-based African Buffalo (BC-AB) with the RNN model was suggested to improve security and detect intrusion. Normal user datasets along with malware were collected, encrypted with Identity-Based Encryption, and stored securely in the blockchain. The model used the application of RNN to identify intrusion within the cloud environment. AB Optimization, in the prediction phase of RNN, was deployed to ensure that intrusion monitoring was always done. However, with this approach comes the disadvantage that it delays real-time detection because encryption and BC storage require much computing.

In 2023, Al Hwaitat, *et.al.,* [24] have established BC-based authentication for safe IoT networks. A suggested model used data from IoT sensors, authenticated and encrypted it using homomorphic encryption, which appears for the first time using this approach, allowing for the execution of operations on encrypted data, users' data encrypted at the user layer, outsourced to the cloud, with possible application of statistical and ML operations on the encrypted data. IoT-based networks involve several thousands of tiny sensors attached to the human body including heart rate, blood pressure, temperature, and sugar levels. The high volume of data generated during the application process needed training, testing, validation, and an efficient authentication system, which was taken care of by the model itself by using a hybrid deep learning approach. Another negative aspect of the model was increased computational overhead in the process of encrypting data.

In 2022, Ali, *et.al.,* [25] have developed a BC-HCS using homomorphic safe search-able encryption based on the DL scheme. A distributed database for BC with DL-based secure searchable capability has been developed using HE that would allow the user to access the data securely via search. Secure key revocation and updates on policies have also been incorporated within the system. To test suggested access control strategies, an IoT dataset was used to compare with benchmark models. Algorithms were deployed on Hyperledger through smart contracts, and the suggested approach was tested against existing approaches. The results manifest a salient enhancement towards security, anonymity, and monitoring of the user's behavior but it introduces key management complexity at a higher level.

In 2023, Chidambaranathan, *et.al.,* [26] have established DL to enable BC-based electronic health data attack detection. The EHW, a mobile PHR application, was developed using the BC and FHIR standards to achieve the needed interoperability in data exchange with multiple patient data sources. The EHW app allowed patients to receive their most recently collected health information from multiple platforms. During its development, APIs were co-developed across all tiers ensuring interoperability. The PHR had an IoT-based architecture that considered the non-functional aspects of data privacy, security, and performance. The deep learning model processes the data it has

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

collected by using a GAN to detect attacks and authenticate PHRs. Regarding the GAN model, challenges were observed concerning the stability of training.

In 2023, Navaneethan, *et.al.,* [27] have improved a DL model to guarantee data security and integrity in an IoT-based BC application for e-commerce. To solve cyberattack-related issues in the IoT-based e-commerce BC networks, the Hybrid Interactive Autodidactic School-Based TL Optimization (HIASTLO) algorithm was suggested. Within the network, the approach extracted and rejected several cyberattacks while DL techniques were used to optimize the weight and bias of the neural networks. Various performance metrics, such as accuracy, precision, and recall, were used to check the detection of cyberattacks. In addition, MudraChain and NormaChain were adopted to validate the transaction time, but the model cannot manage complex patterns of attacks.

PROPOSED METHODOLOGY

This manuscript introduces the innovative multi-agent system and blockchain (BC) technology to enhance data security and detection capabilities in an attack. Figure 1 indicates the workflow of the suggested method.

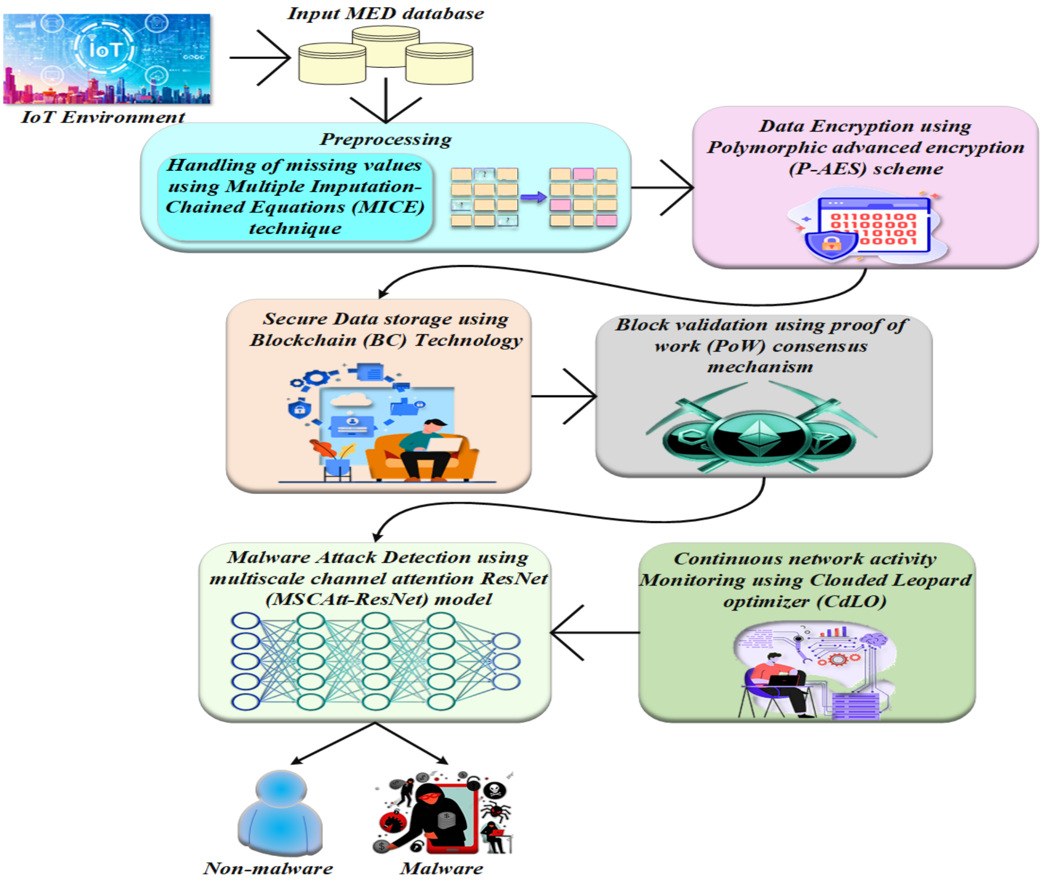
IoT
IoT Environment
Input MED database
Preprocessing
Handling of missing values using Multiple Imputation-Chained Equations (MICE) technique
Data Encryption using Polymorphic advanced encryption (P-AES) scheme
Secure Data storage using Blockchain (BC) Technology
Block validation using proof of work (PoW) consensus mechanism
Malware Attack Detection using multiscale channel attention ResNet (MSCAtt-ResNet) model
Continuous network activity Monitoring using Clouded Leopard optimizer (CdLO)
Non-malware
Malware

Figure 1: Workflow of the Suggested Method

Initially, the primary information sources are collected from the Malware Executable Detection (MED) dataset obtained from the Kaggle platform. The Multiple Imputation-Chained Equations preprocessing handles missing values for the collected data so that the data's integrity is not compromised. After preprocessing, the data is encrypted using Polymorphic Advanced Encryption Standard (AES) which encrypts plaintext to a ciphertext, safeguarding private information. Then, the encrypted data is safely stored in a BC environment using a Proof of Work (PoW) mechanism that guarantees validity and immutability in recorded data and resistance to unauthorized modification. Then, the proposed framework deploys the Multi-Scale Channel Attention Residual Network (MSCAtt-ResNet), which analyzes the encrypted data for malicious patterns. To detect intrusions, the Clouded Leopard Optimization

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

(CdLO) algorithm continually monitors the network activity with fixed predefined threshold values to identify potential attacks. The proposed method is simulated via the Python environment.

Data Acquisition

The "Malware Executable Detection" dataset [28] from Kaggle provides a collection of features gathered from executables to help users classify files as malware or benign. This database consists of 373 instances, of which 72 are non-malicious and 301 are malicious. The dataset entails attributes that are reflections of the behavior and structural characteristics of executable files, which include byte sequences and other operational data. It is designed to facilitate the pursuit of cybersecurity research, especially in malware detection, and may be applied to train ML models to identify potential threats. This resource is valuable for anyone studying classification tasks and anomaly detection in cybersecurity.

Preprocessing Stage

After data acquisition, preprocessing is performed to handle the missing values present in the raw database. Traditional missing value imputation [29] schemes maximize the computational efficacy, especially for larger databases. The proposed framework introduces a Multiple Imputation-Chained Equation (MICE) strategy to enhance the superiority of the data. For each of n imputed dataset points evaluate $\tilde{P}_x, x = 1, 2, 3, \ldots n$, are calculated for every attribute P of interest along with the evaluation of the variance of $\tilde{P}_x$ represented by Z_x. Then, the pooled point evaluates of P, the nearby imputation variance $\widehat{Z}$ between imputation variance Q are deliberated as,

$$\widehat{P} = \frac{1}{n}\sum_{x=1}^{n}\tilde{P}_x, \widehat{Z} = \frac{1}{n}\sum_{x=1}^{n} Z_x \quad and \quad Q = \frac{1}{n-1}\sum_{x=1}^{n}\left(\widehat{P}_x - \widehat{P}\right)\left(\widehat{P}_x - \widehat{P}\right)' \tag{1}$$

The evaluated variance of $\widehat{Z}$ can be formulated as,

$$X = \widehat{Z} + \left(1+\frac{1}{n}\right)Q \tag{2}$$

Here, the parameter $\left(1+n^{-1}\right)$ is multiplied by Q that maintains fine-tuning for additional variance due to the presence of finite imputations n to evaluate $\widehat{Z}$. This fine-tuning is required to determine the accurate references with minimum n. In other words, the scrutiny would be minimized in minute y values or minimal confidence intervals. The steps involved in pooling and continuous imputation outcomes are represented as Rubin's rules. Information about P and proposition are then dependent on the student's t approximation which can be formulated as,

$$\sqrt{K}\left(\widehat{P}-P\right) \sim t_l, v = (n-1)\left[1+\frac{n\widehat{P}}{(n+1)Q}\right] \tag{3}$$

Here, v deliberates the degrees of freedom. The parameter $r = \frac{n\widehat{P}}{(n+1)Q}$ in v is the ratio of Q to $\widehat{Z}$ and determines the relative enhancement in variance because of the missing data. In addition to this, $\beta = \frac{1}{r+1}$ is the information

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

missing rate for Z, and $e = \frac{100n}{n+\beta}\%$ indicates the efficacy of $\hat{Z}$ using n imputed datasets relative $\hat{Z}$ to the infinite number of imputed datasets.

Secure Data Encryption using P-AES Technique

The preprocessed data are then secured using an efficient encryption scheme to safeguard from unwanted malicious attacks. Nowadays, AES [30] techniques are highly effective in data security but rely on secure key distribution and management. In large-scale systems or environments where multiple users or devices need access, securely generating, storing, distributing, and renewing keys can be complex and vulnerable to mismanagement. Hence, the proposed scheme proposes an innovative polymorphic advanced encryption scheme (P-AES) is introduced that involves a dynamic, evolving key structure, allowing it to adapt its encryption method based on the data or environment, making it harder for attackers to exploit a fixed pattern.

Initialization Phase

One block of size 16 bytes is processed at a time by the suggested cipher. The following is how this input block is replicated into the state matrix:

$$\begin{bmatrix} M_{0,0} & M_{0,1} & M_{0,2} & M_{0,3} \\ M_{1,0} & M_{1,1} & M_{1,2} & M_{1,3} \\ M_{2,0} & M_{2,1} & M_{2,2} & M_{2,3} \\ M_{3,0} & M_{3,1} & M_{3,2} & M_{3,3} \end{bmatrix} \tag{4}$$

In simple words, the state content $M_{0,0}$ is indicated as hexadecimal. The block cipher mode of maneuver stipulates how all x blocks are managed by the cipher. AS recommended by the NIST, five modes: Electronic Codebook Mode (ECB), Cipher Block Chaining Mode (CBC), Cipher Feedback Mode (CFB), Output Feedback Mode (OFB), and Counter Mode (CTR). The ECB mode is highly apprehensive hence it indicates the patterns of plaintext. However, there is no vulnerability present in any other modes other than insecurity. Here, CBC mode is introduced, and the proposed P-AES can sustain a key of 16, 24, or 32 bytes in length. For better consistency, the length of the key is considered 32 bytes in the remaining process.

$$k = \left[B_0 \left| B_1 \right| \left| B_2 \right| .....B_{28} \left| B_{29} \right| \left| B_{30} \right| \left| B_{31} \right| \right] \tag{5}$$

Here, B indicates the bytes, and k indicates the keys. After key generation, the below values are evaluated for both sender and receiver which can be deliberated as,

$$B\_substitution\_i = (<\text{int}> B_{31}) \bmod 8 \tag{6}$$

$$row\_shifting\_i = (<\text{int}> B_{30}) \bmod 4 \tag{7}$$

$$column\_mixing\_i = (<\text{int}> B_{29}) \bmod 4 \tag{8}$$

Clearly,

$$\begin{aligned} &B\_substitution\_i \in \{0,1,2,3,4,5,6,7\}, \\ &row\_shifting\_i \in \{0,1,2,3\}, \quad and \\ &column\_mixing\_i \in \{0,1,2,3\} \end{aligned} \tag{9}$$

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Here, i represents the indices. The P-AES process determines the number of rounds and the scheduling process of the key are same as the conventional AES.

Altered Sub-byte Phase

Assume that the bytes in the array state have the binary value $(10111001)_2$. The hexadecimal byte representation is indicated as $(B9)_{16}$. This value is then substituted with various values present in the S-box. The substitution process is performed by taking the left-most 4-bits $(B)_{16}$ in row-index, and 4-bit right-most $(9)_{16}$ in the column index. Hence, $(B9)_{16}$ is substituted within the value positioned in the row $(B)_{16}$ column $(9)_{16}$ in the S-box which is indicated as $(56)_{16}$. For the decryption process, similar steps are performed. For a better understanding of the P-AES technique in the altered sub-byte stage, assume the value of $B\_substitution\_i$ which has been excerpted from the key using equation (6) is 2. During the altered sub-byte phase, the byes having each bit in the state arrays are modified by shifting circularly to the left by $7-B\_substitution\_i$. After shifting the bits of the bytes $(10111001)_2$, it is be represented as, $(00110111)_2$ and in the hexadecimal, it is indicated as, $(37)_{16}$. Finally, in the S-box, it is indicated as, $(9A)_{16}$.

The state arrays are looked up in the inverse S-box manner for the decryption process. In the next stage, bits present in the state array are shifted circularly to the right by the $7-B\_substitution\_i$. For better clarification, applying altered sub-bytes to the byte $(9A)_{16}$ and $B\_substitution\_i$ is 2. Initially, the lookup $(9A)_{16}$ performed in the inverse S-form. The outcome is $(37)_{16}$ or $(00110111)_2$. Then, the bits of the bytes are shifted circularly to the right using $7-B\_substitution\_i$ and the outcome is $(10111001)_2$ or $(B9)_{16}$.

Altered Shift Row Phase

To determine the P-AES altered shifts rows, assume the value of $row\_shifting\_i$, which has been excerpted using the key by equation (7) is 3. The steps involved in the altered shift row process are blemished below:

- No modification occurs in the third row of the state matrix.
- The zeroth row is shifted circularly by one byte on the left end.
- The first row is shifted circularly by two bytes in the left end.
- The second row is shifted circularly by three bytes in the left end.

The value of $row\_shifting\_i$ determines the initial row that is not shifted. Upcoming rows are shifted circularly by the offsets 1, 2, and 3 on the left end. In the same way, the value of $row\_shifting\_i$ is recovered in the decryption phase. This value indicates the row state has not shifted and the upcoming circular rows are shifted annually by 1, 2, and 3 bytes to the right end respectively.

Altered Mix Column Phase

Similar to AES, the state matrix is multiplied in the mix column matrix. In the decryption process, the multiplication process is performed using an inverse matrix and Galois field (2^8). This process contemplates a durable

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

dissemination effect for every column, in which all the byte subsidizes dissimilar to define the byte's new values of that column.

In the proposed altered mix columns, the order of the rows is obtained during the simulation process based on the value of $column\_mixing\_i$, which is deliberated in equation (8) is 3. For this case, the third row in the evasion mix column matrix is in the zeroth row in the altered mix column matrix. In the same way, rows 1, 2, and 3 are considered in the developed P-AES altered shift row matrix. The altered shift row matrix is deliberated as given below:

$$\begin{bmatrix} 03 & 01 & 01 & 02 \\ 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \end{bmatrix} \tag{10}$$

In the decryption process, the inverse altered mix column matrix is rearranged similarly. If $column\_mixing\_i$ is equal to 3, the reverse altered mix column matrix can be formulated as,

$$\begin{bmatrix} 0B & 0D & 09 & 0E \\ 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \end{bmatrix} \tag{11}$$

Finally, the data is secured efficiently with minimal computation and morphs dynamically based on the type, priority level, and amount of data present in the database. Figure 2 indicates the Flowchart of the Proposed P-AES Mechanism.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/
Research Article

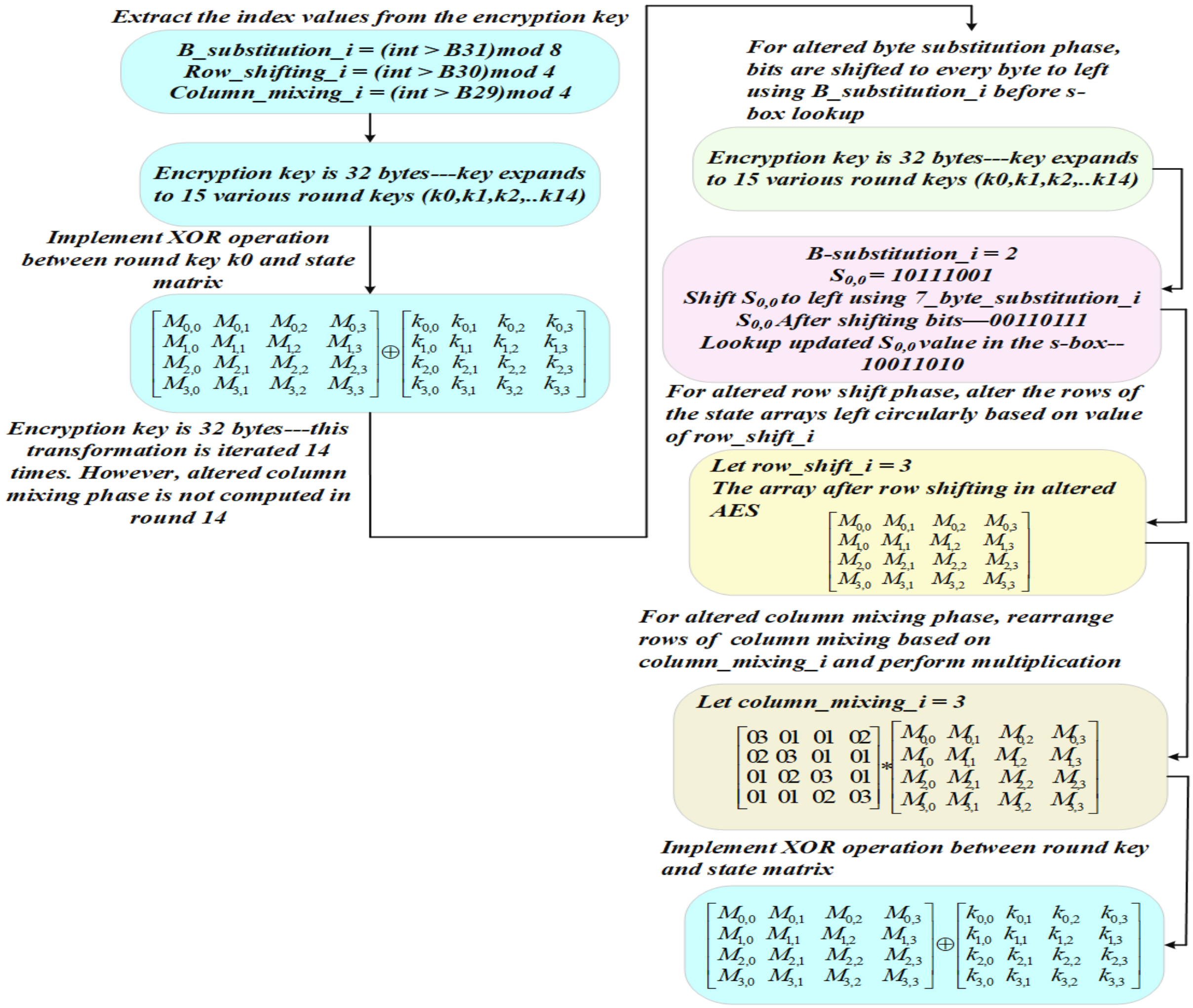
Extract the index values from the encryption key
B_substitution_i = (int > B31)mod 8
Row_shifting_i = (int > B30)mod 4
Column_mixing_i = (int > B29)mod 4
Encryption key is 32 bytes---key expands to 15 various round keys (k0,k1,k2,..k14)
Implement XOR operation between round key k0 and state matrix
Encryption key is 32 bytes---this transformation is iterated 14 times. However, altered column mixing phase is not computed in round 14
For altered byte substitution phase, bits are shifted to every byte to left using B_substitution_i before s-box lookup
Encryption key is 32 bytes---key expands to 15 various round keys (k0,k1,k2,..k14)
B-substitution_i = 2
S0,0 = 10111001
Shift S0,0 to left using 7_byte_substitution_i
S0,0 After shifting bits—00110111
Lookup updated S0,0 value in the s-box--10011010
For altered row shift phase, alter the rows of the state arrays left circularly based on value of row_shift_i
Let row_shift_i = 3
The array after row shifting in altered AES
For altered column mixing phase, rearrange rows of column mixing based on column_mixing_i and perform multiplication
Let column_mixing_i = 3
Implement XOR operation between round key and state matrix

Figure 2: Flowchart of Proposed P-AES Mechanism

Secure Data Storage using BC Technology

Generally, the BC is considered the set of blocks, and these blocks contain four phases such as data related to transactions (Ethereum, bitcoin), hash value generation for present, and existing blocks, and timestamp. In addition, the BS is defined as the disseminated, general digital ledger utilized for storing transaction information based on assorted points. Figure 3 depicts the Structure of BC-based Secure Data Transmission

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

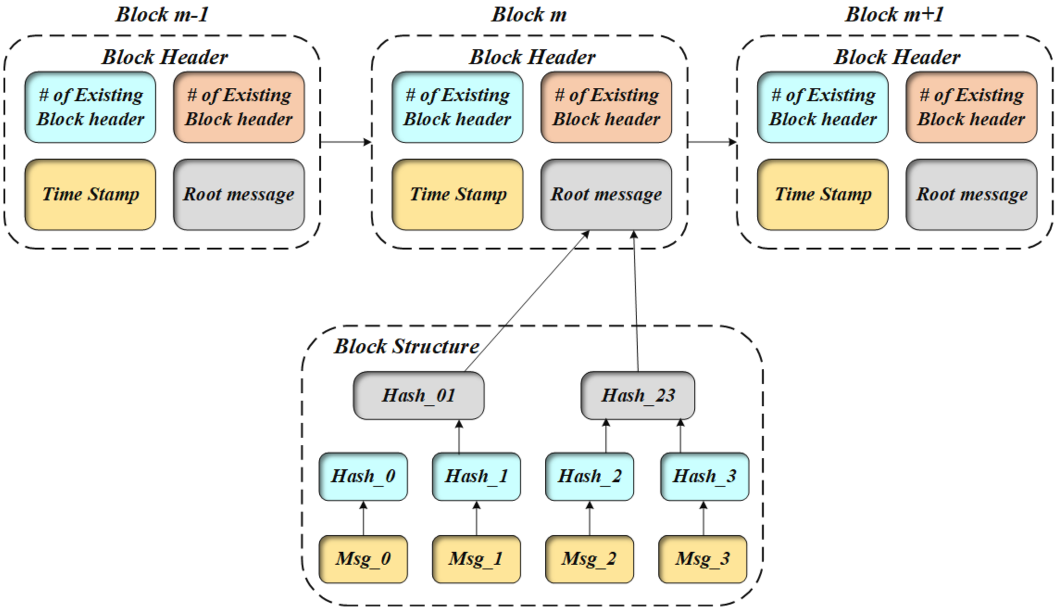

Figure 3: Structure of BC-based Secure Data Transmission

Therefore, when an attacker tries to descend data, every block lacks the cryptographic value of an existing block. All transactions are generated using the application of the cryptographic hash values that every miner verifies. It is encapsulated with a similar value to the total ledger and contains blocks of all transactions. The BC can stake the ledger of shared details, confidential, and security deployment. Distributed storage is another source in BC and a high number of data can be stored and joined from the present block to the existing block using a smart contract mechanism. Lite-Coin, Monero-DB, swarm, Sia coin-DB, interplanetary file system (IPFS), and several other aspects have been implemented for the present distributed database.

Block Validation using the PoW Consensus Mechanism

The proof of work (PoW) was initially described by Dwork and Naor in the early 1990s, and Nakamoto employed it in a 2008 "Bitcoin paper." PoW was the first widely used consensus technique. PoW has been employed by numerous prominent financial institutions. To generate a legitimate block of transactions in PoW, each node must contend with the others using their computer capacity. The nodes that engage in this competition must solve a cryptographic challenge. Every block contains a value known as a nonce. Since the entire block's cryptographic value should drop below a predetermined level (referred to as weight), the miner must receive a nonce value to safeguard the block. As a result, mining would become more statistically complex. A miner node that starts working on a puzzle may be given the ability to create a new block. A PoW puzzle is difficult to solve. Although there is a transaction fee, the service provider determines how much it is cost effective. Additionally, the entire BC network pays the miner the "mining fee." The impartiality of the protocol is the main way in which this method has advantages. A miner has a comparatively high chance of producing blocks and receiving payment if their computational capacities account for $x\%$ of the system's total resources. The intruder's computational power needs to vie with other "legitimate nodes" of the entire system to construct blocks that are "useful" to them. The difficulty of resolving the computational conundrum is another benefit of PoW. PoW ensures that the blockchain is not only computationally secure (through PoW) but also cryptographically resilient (through polymorphic encryption).

Malware Detection using MSCAtt-ResNet Model

The BC-secured data is then fed into the DL model to identify the existence and non-existence of malware attacks in the IoT network. At present, the Residual network (ResNet) [31] plays an essential role in learning the hierarchical features, which can help in identifying subtle patterns in malware behavior that might be missed by simpler models. However, ResNet can overfit the training data, leading to poor generalization on unseen malware. Hence, the

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

suggested framework proposes a multiscale channel attention ResNet (MSCAtt-ResNet) model to determine the malware attacks with minimal complexity.

The proposed MSCAtt-ResNet comprises dual parallel branches and the entire block is separated into three stages: the initial phase, multiscale feature extraction (FE) phase, and channel attention (CAtt) mechanism.

Initial Phase:

This phase allows to extract features randomly using a single convolution (Conv) layer. It can be formulated as,

$$X_1 = w^0_{7\times 7} \times N_{m-1} + B^0 \tag{12}$$

Here, w and B indicates the weights and bias respectively. The kernel size is indicated as, 7×7, N_{m-1} represents the input, and X_1 indicates the outcome of the initial phase.

FE Phase:

Here, a dual pass branch of various Conv kernels $(5\times 5, 7\times 7, \textit{ and } 9\times 9)$ to determine the FE process. Moreover, batch normalization (BN) is included after each conv layer except in 5×5 Conv layer. After the first layer of each MS block, a rectified linear unit (ReLU) is provided. For generating the supplementary context, identity-based skip connections are included. Based on phase 1, complex implementation is undergone and it can be formulated as,

$$\begin{aligned} Z_{11} &= \left(w^{11}_{5\times 5} * X_1 + B^{11}_{5\times 5} \right) \sigma \\ Z_{12} &= \left(w^{12}_{5\times 5} * Z_{11} + B^{12}_{5\times 5} \right) \sigma \\ Z_1 &= X_1 + Z_{12} \end{aligned} \tag{13}$$

$$\begin{aligned} Y_{11} &= \left(w^{11}_{7\times 7} * X_1 + B^{11}_{7\times 7} \right) \sigma \\ Y_{12} &= \left(w^{12}_{7\times 7} * Z_{11} + B^{12}_{7\times 7} \right) \sigma \\ Y_1 &= X_1 + Y_{12} \end{aligned} \tag{14}$$

$$\begin{aligned} K_{11} &= \left(w^{11}_{9\times 9} * X_1 + B^{11}_{9\times 9} \right) \sigma \\ K_{12} &= \left(w^{12}_{9\times 9} * Z_{11} + B^{12}_{9\times 9} \right) \sigma \\ K_1 &= X_1 + K_{12} \end{aligned} \tag{15}$$

$$V_1 = \left[Z_1, Y_1, K_1 \right] \tag{16}$$

Here, w and B indicates the weights and bias respectively. The intermediate outcomes of $5\times 5, 7\times 7, \textit{ and } 9\times 9$ are indicated as Z_1, Y_1, and K_1 respectively. V indicates the concatenation, and the parameters Z_1, Y_1, and K_1 are determined by identity-based skip connections. For phase 2, the same outcomes are obtained and it is formulated below:

$$\begin{aligned} Z_{21} &= \left(w^{21}_{5\times 5} * X_1 + B^{21}_{5\times 5} \right) \sigma \\ Z_{22} &= \left(w^{22}_{5\times 5} * Z_{11} + B^{22}_{5\times 5} \right) \sigma \\ Z_2 &= X_1 + Z_{22} \end{aligned} \tag{17}$$

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

$$\begin{aligned} Y_{21} &= \left(w_{7\times7}^{21} * X_1 + B_{7\times7}^{21} \right)\sigma \\ Y_{22} &= \left(w_{7\times7}^{22} * Z_{11} + B_{7\times7}^{22} \right)\sigma \\ Y_2 &= X_1 + Y_{22} \end{aligned} \tag{18}$$

$$\begin{aligned} K_{21} &= \left(w_{9\times9}^{21} * X_1 + B_{9\times9}^{21} \right)\sigma \\ K_{22} &= \left(w_{9\times9}^{22} * Z_{11} + B_{9\times9}^{22} \right)\sigma \\ K_2 &= X_1 + K_{22} \end{aligned} \tag{19}$$

$$V_2 = \left[Z_2, Y_2, K_2 \right] \tag{20}$$

The parameter X_2 indicates the outcome of 1×1 Conv, while other parameters are the same as phase 1. Several residual connections are included in the entire network making the training process simpler. The skip connection used in the developed framework prevents distortion of useful features.

CAtt Module:

To prevent the feature independencies between the channels, the CAtt module is introduced. During, the squeeze phase, the global average pooling (GAP) is emphasized in the aggregation process. All feature channels are changed to arithmetic, which has a global receptive field at a particular extent. The outcome dimension matches the input feature channels and it can be formulated as,

$$L_c = F_{sq}\left(\vartheta_c\right) = \frac{1}{h\times w}\sum_{x=1}^{h}\sum_{y=1}^{w}\vartheta_c\left(x, y\right) \tag{21}$$

Here, L_c indicates the GAP operation, and $\vartheta_c\left(x, y\right)$ deliberates the value of c^{th} layer feature ϑ_c at $\left(x, y\right)$. Figure 4 deliberates the Architecture of Proposed MSCAtt-ResNet Technique

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

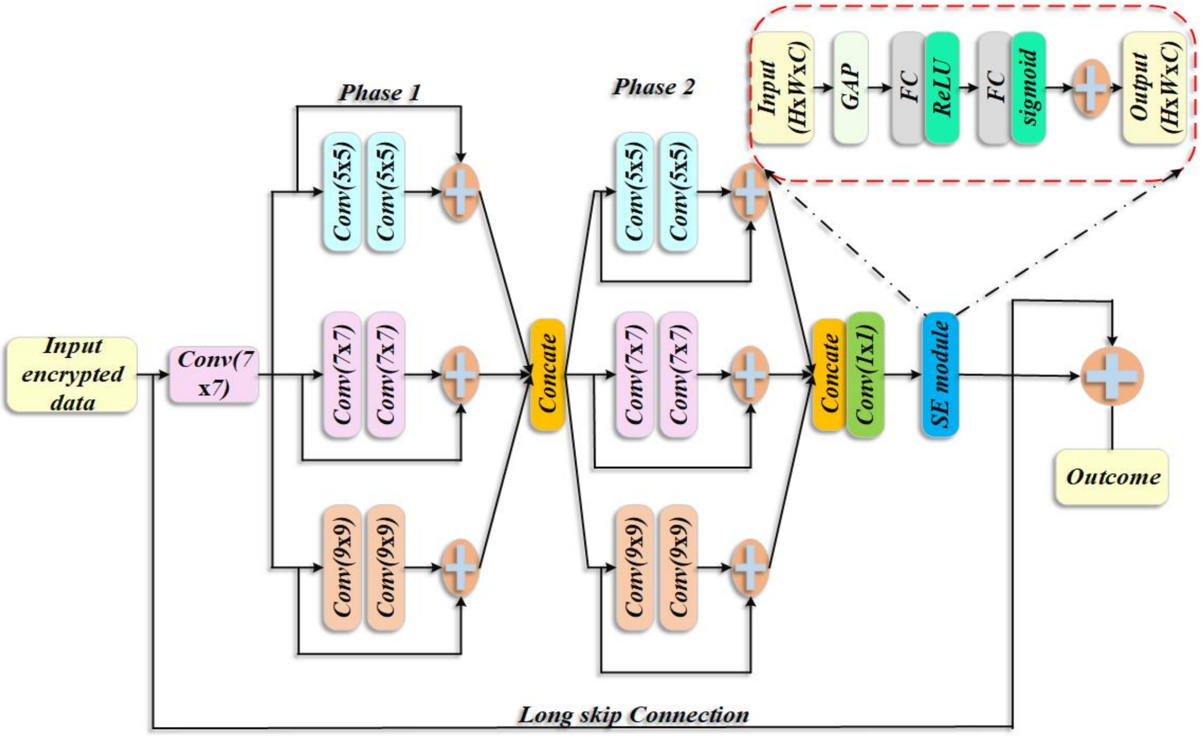

Figure 4: Architecture of Proposed MSCAtt-ResNet Technique

The gate operation is indicated as LSTM, which introduces weights for every feature mapping. The sigmoid function is selected and the simulation process is indicated as,

$$u = F_{ex}\left(L, w\right) = f\left(w_2\left(w_1 L\right)\sigma\right) \tag{22}$$

Here, F_{ex} indicates the excitation process, f represents the sigmoid function, and σ signifies the ReLU function, u represents the outcome statistics. For every component, $\tilde{\vartheta}_c = u_c . \vartheta_c$, whereas $\tilde{\vartheta}_c$ indicates the outcome. The CAtt module is formulated as, $CAtt\left(.\right)$, and the outcome obtained from this phase is emphasized below:

$$N_m = CAtt\left(.\right) \tag{23}$$

Here, N_m represents the outcome feature maps based on the input N_{m-1}.

Parameter Tuning using CLO Technique

The proposed MSCAtt-ResNet technique causes high complexity while training with larger data. This may lead to the loss of essential features and subject to increased error. To overcome this issue, parameters like batch size, learning rate, epochs, and dropout rates are tuned before providing the data into the proposed network model. Metaheuristic optimizers update the model parameters with a globally optimal solution to perform this. The proposed framework introduced a Clouded Leopard Optimizer (CLO) [32] to tune the weight parameters of the network model. Clouded leopards (CLs) are unsociable and shy cats that possess two behaviors. The CL normally climb upon the tree to digest their food and rest after attacking and nourishing their prey. Hence, they spend most days on trees resting and this behavior makes to modify their location adjacent to where they are positioned. The stepwise procedure for the proposed CLO technique is depicted as follows:

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Step 1: Initialization Phase

The CLO technique is one of the metaheuristic populations oriented in which the CL is encompassed as the candidate solution of this technique. The location of each CL within the search space defines the decision variables. In this stage, the CL's location is initialized and it can mathematically be formulated in equation (10),

$$Z_u : z_{u,v} = LB_v + rand\left(UB_v - LB_v\right), \quad u = 1,2,....,M, \quad v = 1,2,.....n \tag{24}$$

Here, Z_u indicates the location of u^{th} CL in the search space, $z_{u,v}$ represents the value of v^{th} decision variable (DV), M indicates the total CLs, n indicates the DVs, $rand$ signifies the random numbers range between 0 and 1, UB_v and LB_v symbolizes the upper and lower bounds of v^{th} DV.

Step 2: Random Generation

After the initialization, randomly choose the most appropriate solution from the set of input parameters.

Step 3: Fitness Function

The CL optimizer utilized fitness function (FF) for analyzing the optimality of the proposed classifier model and it is mathematically formulated in equation (25),

$$f = \min\left(error\ rate\right) \tag{25}$$

Step 4: Exploration Phase

The CLs come down from the tree during nighttime and hunt their prey. This behavior causes their position to be updated which allows other candidates to detect different locations of search space globally. Finally, the location of CL moving the tree can be mathematically formulated in equation (26),

$$Z_u^{P1} : z_{u,v}^{P1} = z_{u,v} + rand\left(L_v - z_{u,v}\right), \quad for\ u = 1,2,....,\frac{M}{2}, \ v = 1,2,...,n \tag{26}$$

Based on the target prey, the position gets updated and it can be mathematically formulated in equation (27),

$$Z_u^{L1} : z_{u,v}^{L1} = \begin{cases} z_{u,v} + rand_{u,v}\left(L_{u,v} - X \times z_{u,v}\right), & f_u^L < f_u \\ z_{u,v} + rand_{u,v}\left(z_{u,v} - X_{u,v} L_{u,v}\right), & otherwise \end{cases} \tag{27}$$

If the new location has a better objective function, it replaces the previous location based on CL and it can be formulated in equation (28),

$$Z_u = \begin{cases} Z_u^{L1}, & f_u^{L1} < f_u \\ Z_u, & otherwise \end{cases} \tag{28}$$

Here, Z_u^{L1} represents the updated location for u^{th} CL, $z_{u,v}^{L1}$ represents the v^{th} dimension, f_u^{L1} indicates the FF value, $rand$ signifies the random numbers range between 0 and 1, $Iguana$ indicates the location of the iguana (i.e., the location of the best candidate), L_v signifies the v^{th} dimension, X manipulates the integer ranges between 1 and 2. Moreover, L_u indicates the ground location of the CL, $L_{u,v}$ signifies the v^{th} dimension, f_u^L indicates the FF value,

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

and $\lfloor . \rfloor$ represents the floor function. However, the updated solution of the CLO is not more effective as it falls into earlier convergence problems and fails to achieve a globally optimal solution.

Step 5: Exploitation Phase

After hunting and devouring their prey, CLs go to the woods to relax and digest their meal. They consequently rest on trees for the majority of the day. The CL's behavior causes a shift in its orientation near its current location. This tactic is an example of neighborhood exploration and exploitation in meta-heuristic algorithms, where the algorithm searches for improved solutions around the ones it has already found. Using equation (29), a random place close to each CL's origin is created to replicate their behavior. Then, the following equation (30) replaces the prior position if the value of the goal function increases in the new location.

$$z^{L2}_{u,v} = z_{u,v} + \frac{LB_v + rand_{u,v} \times \left(UB_v - LB_v\right)}{k} \times \left(2rand_{u,v} - 1\right) \tag{29}$$

$$Z_u = \begin{cases} Z^{L2}_u, & f^{L2}_u < f_u \\ Z_u, & otherwise \end{cases} \tag{30}$$

Here, Z^{L2}_u deliberates the updated position introduced for u^{th} CL (i.e., updated candidate solution) based on the exploitation phase of CLO, $z^{L2}_{u,v}$ indicates u^{th} CL (i.e., decision attributes), Z^{L2}_u signifies the objective function value, $rand_{u,v}$ encompasses the random numbers ranging between 0 and 1.

Step 6: Return the Best Optimal Solution

Step 7: Termination

Finally, the parameters of the SAtt-AE technique are tuned using the CLO, repeating step 3 until the $k = k + 1$ stopping criteria are met. Figure 3 indicates the Flowchart of the Proposed CLO technique.

RESULTS AND DISCUSSION

The proposed framework is processed and simulated via the Python platform and a freely accessible MED database [28] is utilized for the training process. The proposed method is processed under Intel(R) Core (TM) i5-4300M CPU with 4GB installed RAM using a 64-bit operating system. For training, testing, and validation, 80%, 10%, and 10% of the data are considered respectively. A total of 100 epochs, with a population size of 100, and a maximum iteration of 100 are deliberated. Moreover, the learning rate of 0.005, and batch size of 16 are emphasized for the simulation process.

Assessment Measures

Performance indicators like accuracy, Matthew's correlation coefficient (MCC), false negative rate (FNR), encryption time (ET), decryption time (DT), reliability, security level, and throughput are scrutinized to better understand the proposed approach.

Accuracy

It determines the model's overall accuracy, accounting for both TP and TN. It is calculated using equation (31),

$$Accuracy = \frac{T_n + T_p}{T_p + F_n + F_p + T_n} \tag{31}$$

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

MCC

A metric used to assess the validity of multi-classifications, especially when there is an imbalance between the classes, and it is assessed using equation (32),

$$MCC = \left(\frac{T_p \times T_n - F_p \times F_n}{\sqrt{(T_p + F_p)(T_p + F_n)(T_n + F_p)(T_n + F_n)}} \right) \tag{32}$$

FNR Analysis

It is the measure used in statistics and diagnostic testing to quantify the part of definite optimistic cases that are incorrectly notorious as negative by a test and it is depicted in equation (33),

$$FNR = \frac{F_n}{F_n + T_p} \tag{33}$$

Encryption Time (ET)

Encryption time refers to the amount of time taken by an encryption algorithm to convert plaintext data into ciphertext. It is calculated using equation (34),

$$K_{encryption} = \frac{d_{data}}{R_{encryption}} + K_{overhead} \tag{34}$$

Here, $K_{encryption}$ indicates the ET, d_{data} deliberates the Size of the data to be encrypted in bits, $R_{encryption}$ signifies the rate of encryption (Bits per second), and $K_{overhead}$ denotes the overhead time.

Decryption Time (DT)

Decryption time refers to the amount of time required by a decryption algorithm to convert ciphertext back into its original plaintext form. It is calculated using equation (35),

$$K_{decryption} = \frac{d_{data}}{R_{decryption}} + K_{overhead} \tag{35}$$

Here, $K_{decryption}$ indicates the DT, d_{data} deliberates the Size of the data to be decrypted in bits, $R_{decryption}$ signifies the rate of decryption (Bits per second), and $K_{overhead}$ denotes the overhead time.

Throughput

Throughput refers to the number of packets or amount of data that can be transmitted securely through the IoT network per unit of time. It is calculated using equation (36),

$$Throughput = \frac{Number\ of\ \ Packets\ Transmitted}{Total\ time\ Taken} \tag{36}$$

4.2. Confusion Matrix Analysis

In this section, the Confusion matrix (CM) is analyzed for the developed framework under different classes. The confusion matrix is one of the most essential and effective analyses that assist in a better understanding of the proposed approach over misclassified outcomes. Figure 5 indicates the CM Analysis of the suggested Method

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

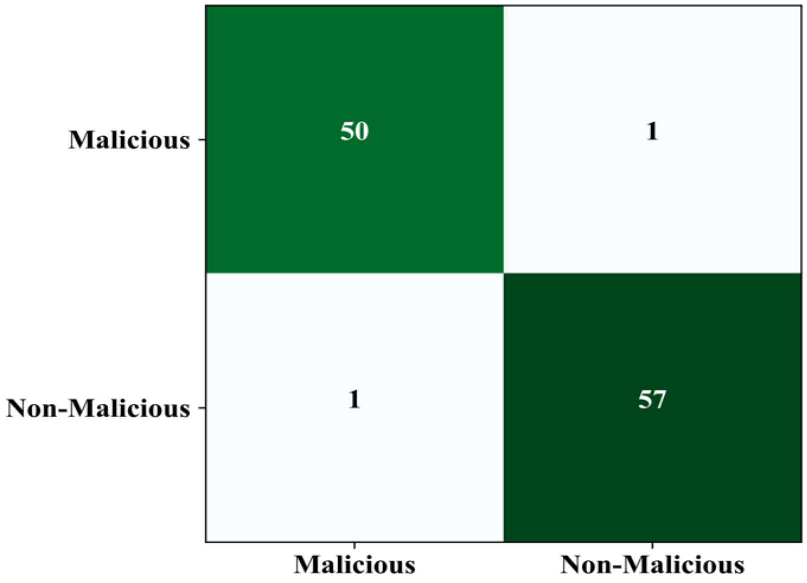

Figure 5: CM Analysis of the Suggested Scheme

The CM in Figure 5 represents the performance of a classification model in identifying malicious and non-malicious instances. The matrix consists of four quadrants, each indicating a different outcome for the model's predictions. The top-left quadrant represents TP, where the model correctly identifies malicious instances as malicious. In this case, the model correctly classified 50 instances as malicious. This value indicates that the model is generally accurate in detecting malicious cases. The top-right quadrant represents FP, where the model incorrectly identifies non-malicious instances as malicious. Here, only one is misclassified, suggesting the model has a low rate of mistakenly labeling non-malicious instances as malicious. The bottom-left quadrant shows FN, where the model incorrectly labels malicious instances as non-malicious. Similar to the FP, there is only one FP. This low count signifies that the model rarely misses malicious instances. Finally, the bottom-right quadrant represents TN, where the model correctly identifies non-malicious instances as non-malicious. The model correctly classified 57 instances as non-malicious, further demonstrating its accuracy in recognizing benign cases.

Simulation Analysis of Proposed Scheme over Traditional Methods

In this section, the performance achieved by the proposed method over the existing schemes is deliberated via graphical illustration. Several existing methods like GAtt-GAN, ResNet, AE-LSTM, CAtt-ResNet, and LSTM techniques are compared with the proposed BC-PoW-PAES-CdLO-MSCAtt-ResNet technique framework. The comprehensive scrutiny of the attained effectiveness is depicted below:

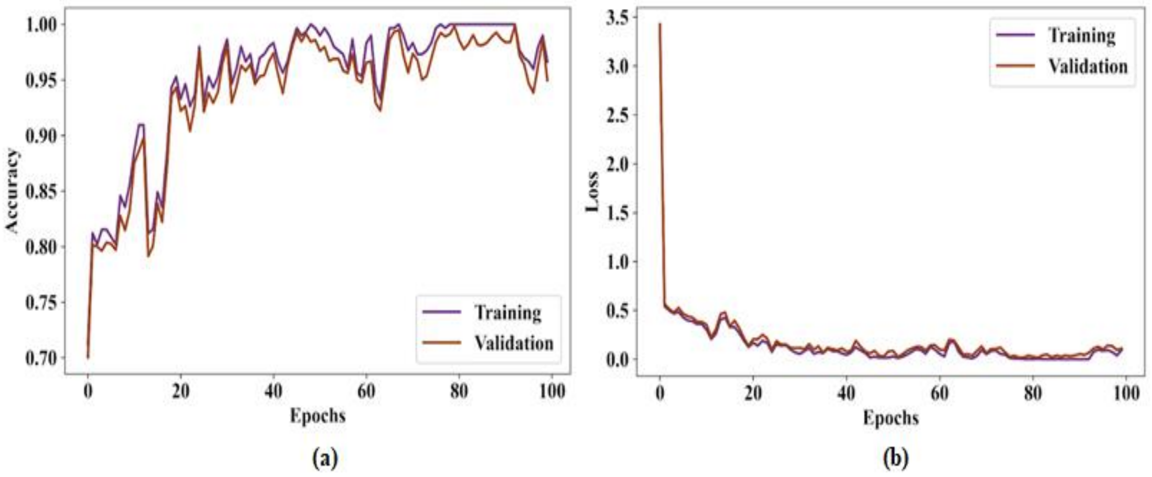

Figure 6: Training and Validation Analysis, (a) Accuracy, and (b) Loss

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Figures 6(a) and 6(b) indicate the training and validation analysis under accuracy and loss respectively. Here, both training and validation accuracy improved rapidly at the beginning, reaching above 95% by around 30 epochs. After this point, accuracy stabilizes, fluctuating between 95% and 100%, indicating strong performance with minimal overfitting. In plot (b), which displays loss, both training and validation loss start high but decrease sharply within the first 10 epochs from 3.5 to below 0.5. After this rapid decline, the loss continues to decrease gradually and stabilizes near zero, suggesting the model learns effectively and reaches convergence without major overfitting.

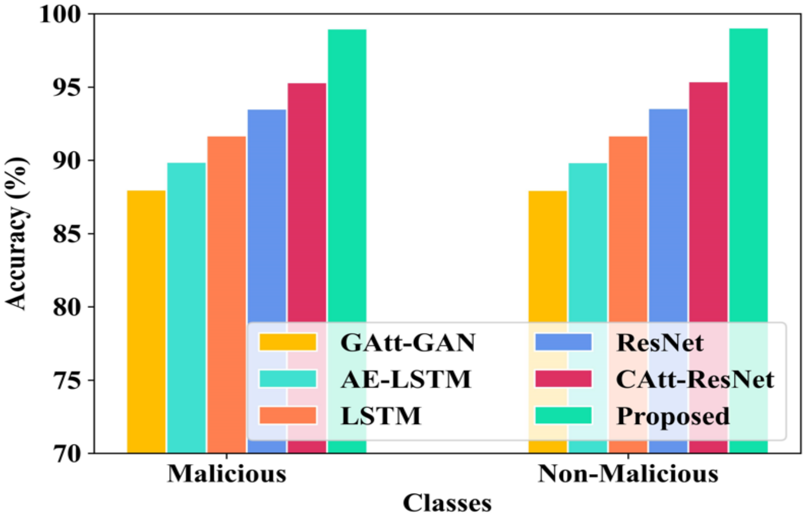

Figure 7: Accuracy Analysis by Varying Conventional Schemes

Figure 7 deliberates the Accuracy Analysis by Varying Conventional Schemes. The graphical representation shows that the proposed CdLO-MSCAtt-ResNet technique obtained better detection performance while being associated with conventional schemes. For detecting the malicious class, the existing GAtt-GAN, AE-LSTM, LSTM, ResNet, CAtt-ResNet, and the proposed CdLO-MSCAtt-ResNet technique obtained an accuracy of 87.98%,89.87%, 91.68%, 95.30%, and 98.98% respectively. For detecting the non-malicious class, the existing GAtt-GAN, AE-LSTM, LSTM, ResNet, CAtt-ResNet, and the proposed CdLO-MSCAtt-ResNet technique obtained an accuracy of 87.95%, 89.85%, 91.67%, 93.55%, 95.37%, and 99.04% respectively.

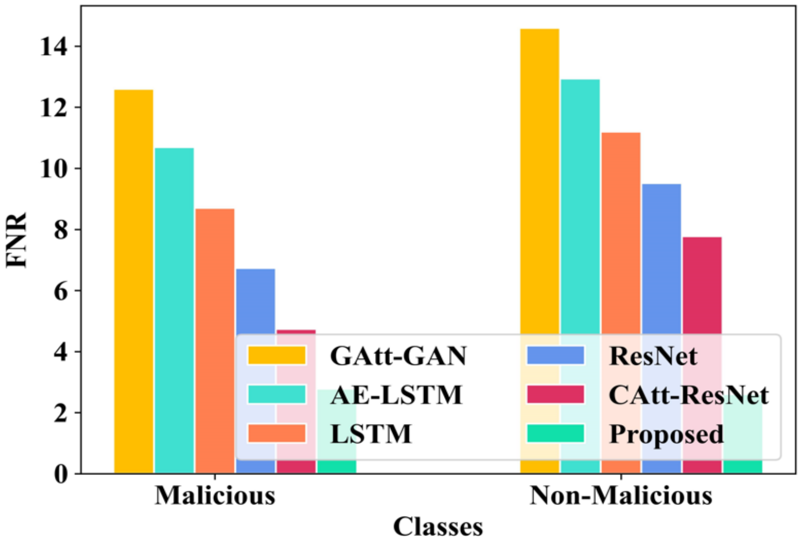

Figure 8: FNR Analysis by Varying Conventional Schemes

Figure 8 indicates the FNR Analysis by Varying Conventional Schemes. The graphical representation shows that the proposed CdLO-MSCAtt-ResNet technique obtained minimal error while being associated with conventional schemes. For detecting the malicious class, the existing GAtt-GAN, AE-LSTM, LSTM, ResNet, CAtt-ResNet, and the

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

proposed CdLO-MSCAtt-ResNet technique obtained an FNR of 12.59, 10.69, 8.69, 6.73, 4.73, and 2.78 respectively. For detecting the non-malicious class, the existing GAtt-GAN, AE-LSTM, LSTM, ResNet, CAtt-ResNet, and the proposed CdLO-MSCAtt-ResNet technique obtained an FNR of 14.59, 12.93, 11.19, 9.51, 7.77, and 2.60 respectively.

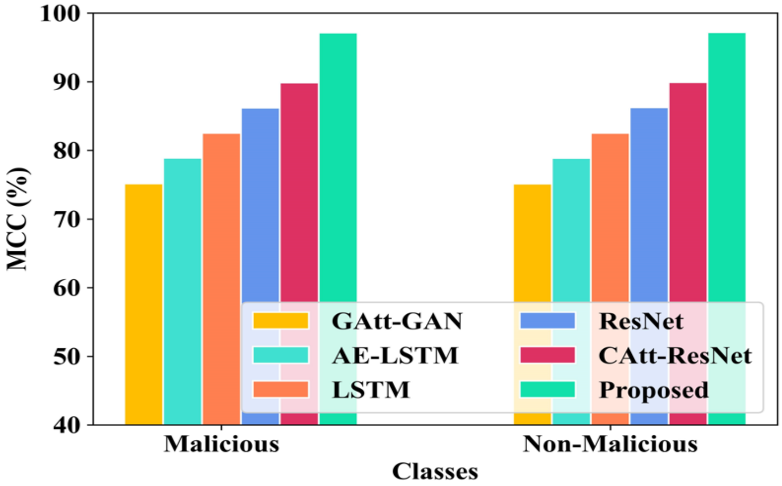

Figure 9: MCC Analysis by Varying Conventional Schemes

Figure 9 indicates the MCC Analysis by Varying Conventional Schemes. The graphical representation shows that the proposed CdLO-MSCAtt-ResNet technique obtained better detection performance while being associated with conventional schemes. For detecting the malicious class, the existing GAtt-GAN, AE-LSTM, LSTM, ResNet, CAtt-ResNet, and the proposed CdLO-MSCAtt-ResNet technique obtained an MCC of 75.14%, 78.88%, 82.52%, 86.20%, 89.84%, and 97.13% respectively. For detecting the non-malicious class, the existing GAtt-GAN, AE-LSTM, LSTM, ResNet, CAtt-ResNet, and the proposed CdLO-MSCAtt-ResNet technique obtained an MCC of 75.11%, 78.86%, 82.52%, 86.24%, 89.90%, and 97.19% respectively.

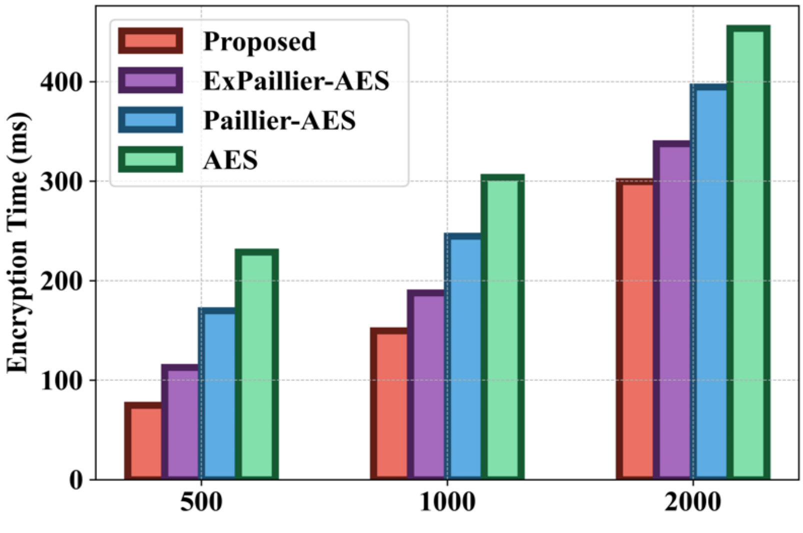

Figure 10: ET Analysis by Varying Key Size

Figure 10 signifies the ET Analysis by varying key sizes. As the data size increases, the encryption time for each scheme also rises, reflecting the increased computational effort required for larger datasets. Among all the existing schemes, the Proposed P-AES method consistently exhibits the shortest encryption time across all data sizes, suggesting a more efficient encryption process. For 500 key sizes, the existing ExPaillier-AES, Paillier-AES, AES, and proposed P-AES obtained the ET values of 112.91s, 169.91ms, 228.91ms, and 74.91ms respectively. For 1000 key sizes, the existing ExPaillier-AES, Paillier-AES, AES, and proposed P-AES obtained the ET values of 187.82ms, 244.82ms,

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

303.82ms, and 149.82ms respectively. For 2000 key sizes, the existing ExPaillier-AES, Paillier-AES, AES, and proposed P-AES obtained the ET values of 337.65ms, 394.65ms, 453.65ms, and 299.65ms respectively.

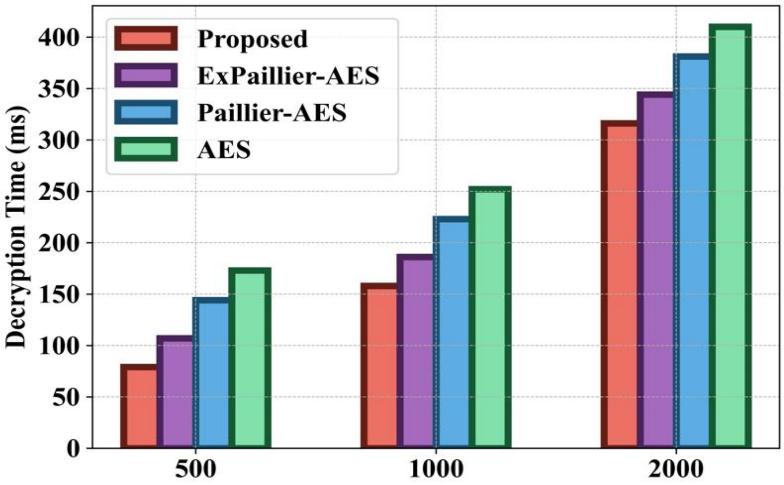

Figure 11: DT Analysis by Varying Key Size

Figure 11 emphasizes the DT Analysis by varying key sizes. As the data size increases, the encryption time for each scheme also rises, reflecting the increased computational effort required for larger datasets. Among all the existing schemes, the Proposed P-AES method consistently exhibits the shortest encryption time across all data sizes, suggesting a more efficient encryption process. For 500 key sizes, the existing ExPaillier-AES, Paillier-AES, AES, and proposed P-AES obtained the DT values of 112.91s, 169.91ms, 228.91ms, and 74.91ms respectively. For 1000 key sizes, the existing ExPaillier-AES, Paillier-AES, AES, and proposed P-AES obtained the DT values of 187.82ms, 244.82ms, 303.82ms, and 149.82ms respectively. For 2000 key sizes, the existing ExPaillier-AES, Paillier-AES, AES, and proposed P-AES obtained the ET values of 337.65ms, 394.65ms, 453.65ms, and 299.65ms respectively.

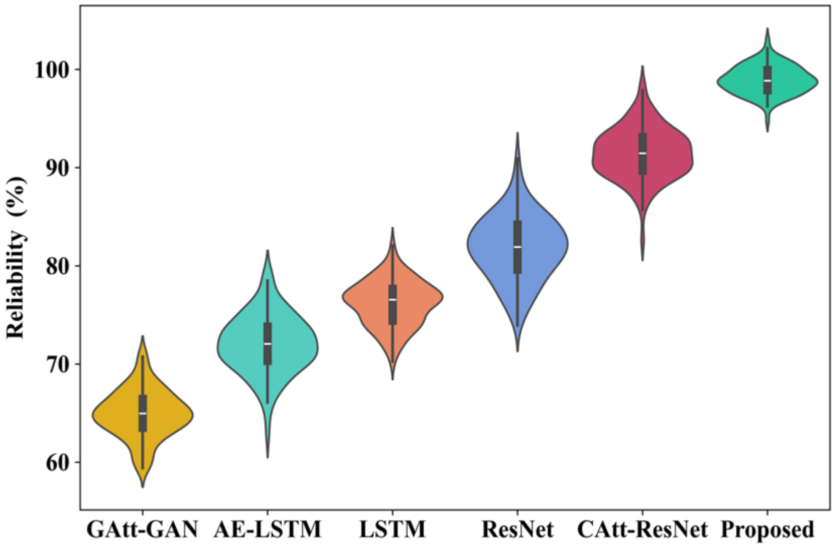

Figure 12: Reliability Analysis by Varying Conventional Schemes

Figure 12 indicates the Reliability Analysis by Varying Conventional Schemes. The graphical representation shows that the proposed CdLO-MSCAtt-ResNet technique obtained better detection performance while being associated with conventional schemes. By analyzing the reliability for the existing GAtt-GAN, AE-LSTM, LSTM, ResNet, CAtt-ResNet, and the proposed CdLO-MSCAtt-ResNet technique obtained the value of 64.74%, 71.8%, 76.25%, 81.54%, 91.6%, and 99.03% respectively.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

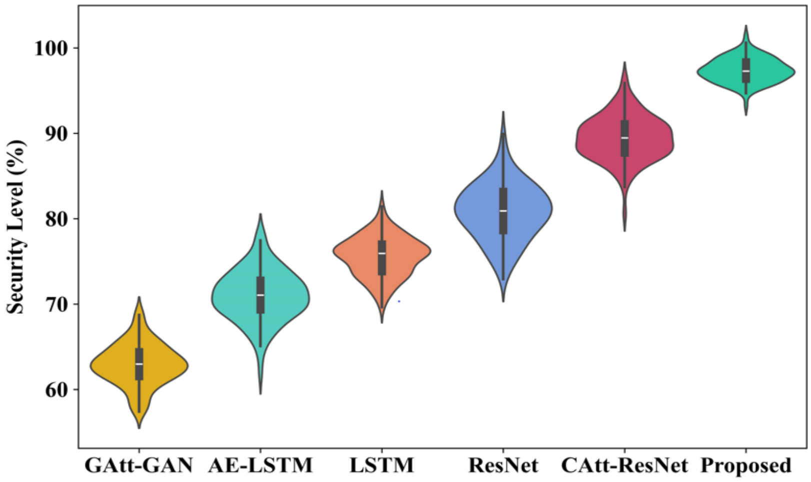

Figure 13: Security Level Analysis by Varying Conventional Schemes

Figure 13 determines the security Level analysis by varying conventional schemes. The graphical representation shows that the proposed CdLO-MSCAtt-ResNet technique obtained a better security level while being associated with conventional schemes. By analyzing the security level for the existing GAtt-GAN, AE-LSTM, LSTM, ResNet, CAtt-ResNet, and the proposed CdLO-MSCAtt-ResNet technique obtained the value of 62.74%, 70.8%, 75.64%, 80.54%, 89.6%, and 97.49% respectively.

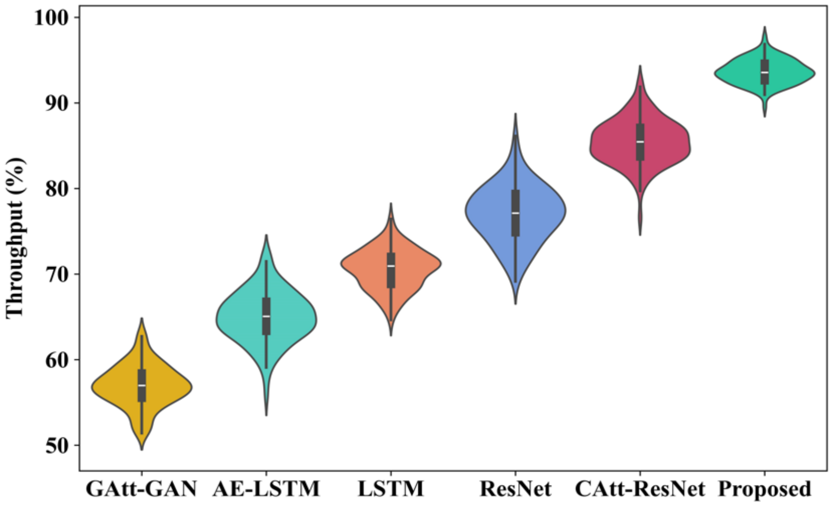

Figure 14: Throughput Analysis by Varying Conventional Schemes

Figure 14 emphasizes the throughput analysis by varying conventional schemes. The graphical representation shows that the proposed CdLO-MSCAtt-ResNet technique obtained a better throughput while being associated with conventional schemes. By analyzing the throughput for the existing GAtt-GAN, AE-LSTM, LSTM, ResNet, CAtt-ResNet, and the proposed CdLO-MSCAtt-ResNet technique obtained the value of 56.74%, 64.8%, 70.64%, 76.75%, 85.6%, and 93.75% respectively.

CONCLUSION

The proposed framework introduced and investigated the multi-agent system integrated with BC technology presents a robust framework for enhancing data security and intrusion detection capabilities in the realm of cybersecurity. By leveraging the MED dataset, the approach effectively addresses data integrity through Multiple Imputation-Chained Equations for handling missing values. The use of Polymorphic AES for data encryption ensures that sensitive information remains protected while being stored in a blockchain environment that employs a Proof of Work mechanism, thereby ensuring data validity and resistance to unauthorized alterations. The deployment of the

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

MSCAtt-ResNet allows for comprehensive analysis of encrypted data, effectively identifying malicious patterns. Additionally, the Clouded Leopard Optimization algorithm provides a proactive monitoring system for network activities, enhancing the framework's ability to detect intrusions in real-time. The impressive performance metrics, including an accuracy of 99.01%, an MCC of 97.16%, and a low false negative rate of 2.60, underscore the efficacy of the proposed system. These results not only highlight the potential of integrating advanced technologies in cybersecurity but also pave the way for more resilient systems capable of adapting to evolving threats. However, the PoW mechanism enhances data immutability, it may also lead to scalability issues as the size of the blockchain grows, potentially hindering system efficiency. In the future, the suggested framework will be extended by enhancing the framework to accommodate a wider variety of datasets will strengthen its applicability across different scenarios in cybersecurity.

REFERENCE

[1] Ranjan, A.K. and Kumar, P., 2024. Ensuring the privacy and security of IoT-medical data: a hybrid deep learning-based encryption and blockchain-enabled transmission. Multimedia Tools and Applications, pp.1-26.

[2] Kumar, R., Kumar, P., Tripathi, R., Gupta, G.P., Garg, S. and Hassan, M.M., 2022. A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network. Journal of Parallel and Distributed Computing, 164, pp.55-68.

[3] Kumar, R., Kumar, P., Aloqaily, M. and Aljuhani, A., 2022. Deep-learning-based blockchain for secure zero touch networks. IEEE Communications Magazine, 61(2), pp.96-102.

[4] Sathiya, R.R., Rajakumar, S. and Sathiamoorthy, J., 2023. Secure blockchain based deep learning approach for data transmission in IOT-enabled healthcare system. International Journal of Computer and Engineering Optimization, 1(01), pp.15-23.

[5] Kumar, P., Kumar, R., Gupta, G.P., Tripathi, R. and Srivastava, G., 2022. P2tif: A blockchain and deep learning framework for privacy-preserved threat intelligence in industrial iot. IEEE transactions on industrial informatics, 18(9), pp.6358-6367.

[6] Ahamad, D. and Hameed, S.A., 2023. Two level blockchain-based privacy preservation framework in IoT with heuristic fusion mechanism-aided deep learning architecture. Internet of Things, 24, p.100917.

[7] Karthik, G.M., Kalyana Kumar, A.S., Karri, A.B. and Jagini, N.P., 2023. Deep intelligent blockchain technology for securing IoT-based healthcare multimedia data. Wireless Networks, 29(6), pp.2481-2493.

[8] Kumar, P., Kumar, R., Kumar, A., Franklin, A.A., Garg, S. and Singh, S., 2022. Blockchain and deep learning for secure communication in digital twin empowered industrial IoT network. IEEE Transactions on Network Science and Engineering, 10(5), pp.2802-2813.

[9] Mrabet, H., Alhomoud, A., Jemai, A. and Trentesaux, D., 2022. A secured industrial Internet-of-things architecture based on blockchain technology and machine learning for sensor access control systems in smart manufacturing. Applied sciences, 12(9), p.4641.

[10] Dhifallah, W., Moulahi, T., Tarhouni, M. and Zidi, S., 2023. Intellig_block: Enhancing IoT security with blockchain-based adversarial machine learning protection. International Journal of Advanced Technology and Engineering Exploration, 10(106), p.1167.

[11] Sankaran, K.S. and Kim, B.H., 2023. Deep learning based energy efficient optimal RMC-CNN model for secured data transmission and anomaly detection in industrial IOT. Sustainable Energy Technologies and Assessments, 56, p.102983.

[12] Awotunde, J.B., Gaber, T., Prasad, L.N., Folorunso, S.O. and Lalitha, V.L., 2023. Privacy and security enhancement of smart cities using hybrid deep learning-enabled blockchain. Scalable Computing: Practice and Experience, 24(3), pp.561-584.

[13] Gebremariam, G.G., Panda, J. and Indu, S., 2023. Blockchain-Based Secure Localization against Malicious Nodes in IoT-Based Wireless Sensor Networks Using Federated Learning. Wireless communications and mobile computing, 2023(1), p.8068038.

[14] dos Santos, F.C., Duarte-Figueiredo, F., Robson, E. and dos Santos, A.L., 2024. Enhancing a fog-oriented IoT authentication and encryption platform through deep learning-based attack detection. Internet of Things, 27, p.101310.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

[15] Gaur, R., Prakash, S., Kumar, S., Abhishek, K., Msahli, M. and Wahid, A., 2022. A machine-learning–blockchain-based authentication using smart contracts for an ioht system. Sensors, 22(23), p.9074.

[16] Rajasekaran, P. and Duraipandian, M., 2024. Secure cloud storage for IoT based distributed healthcare environment using blockchain orchestrated and deep learning model. Journal of Intelligent & Fuzzy Systems, (Preprint), pp.1-16.

[17] Sharma, B., Sharma, L., Lal, C. and Roy, S., 2023. Anomaly based network intrusion detection for IoT attacks using deep learning technique. Computers and Electrical Engineering, 107, p.108626.

[18] Alserhani, F.M., 2024. Integrating deep learning and metaheuristics algorithms for blockchain-based reassurance data management in the detection of malicious IoT nodes. Peer-to-Peer Networking and Applications, pp.1-27.

[19] Sharma, P., Moparthi, N.R., Namasudra, S., Shanmuganathan, V. and Hsu, C.H., 2022. Blockchain-based IoT architecture to secure healthcare system using identity-based encryption. Expert Systems, 39(10), p.e12915.

[20] Mishra, S. and Chaurasiya, V.K., 2024. Hybrid deep learning algorithm for smart cities security enhancement through blockchain and internet of things. Multimedia Tools and Applications, 83(8), pp.22609-22637.

[21] Ali, A., Almaiah, M.A., Hajjej, F., Pasha, M.F., Fang, O.H., Khan, R., Teo, J. and Zakarya, M., 2022. An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. Sensors, 22(2), p.572.

[22] Kumar, P., Kumar, R., Gupta, G.P., Tripathi, R., Jolfaei, A. and Islam, A.N., 2023. A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system. Journal of Parallel and Distributed Computing, 172, pp.69-83.

[23] Saravanan, V., Madiajagan, M., Rafee, S.M., Sanju, P., Rehman, T.B. and Pattanaik, B., 2024. IoT-based blockchain intrusion detection using optimized recurrent neural network. Multimedia Tools and Applications, 83(11), pp.31505-31526.

[24] Al Hwaitat, A.K., Almaiah, M.A., Ali, A., Al-Otaibi, S., Shishakly, R., Lutfi, A. and Alrawad, M., 2023. A new blockchain-based authentication framework for secure IoT networks. Electronics, 12(17), p.3618.

[25] Ali, A., Pasha, M.F., Ali, J., Fang, O.H., Masud, M., Jurcut, A.D. and Alzain, M.A., 2022. Deep learning based homomorphic secure search-able encryption for keyword search in blockchain healthcare system: A novel approach to cryptography. Sensors, 22(2), p.528.

[26] Chidambaranathan, S. and Geetha, R., 2023. Deep learning enabled blockchain based electronic heathcare data attack detection for smart health systems. Measurement: Sensors, p.100959.

[27] Navaneethan, M. and Janakiraman, S., 2023. An optimized deep learning model to ensure data integrity and security in IoT based e-commerce block chain application. Journal of Intelligent & Fuzzy Systems, 44(5), pp.8697-8709.

[28] https://www.kaggle.com/datasets/piyushrumao/malware-executable-detection

[29] Mbona, S.V., Mwambi, H. and Ramroop, S., 2023. Multiple imputation using chained equations for missing data in survival models: applied to multidrug-resistant tuberculosis and HIV data. Journal of Public Health in Africa, 14(8).

[30] Altigani, A., Hasan, S., Barry, B., Naserelden, S., Elsadig, M.A. and Elshoush, H.T., 2021. A polymorphic advanced encryption standard–a novel approach. IEEE Access, 9, pp.20191-20207.

[31] Li, X., Xu, F., Lyu, X., Tong, Y., Chen, Z., Li, S. and Liu, D., 2020. A remote-sensing image pan-sharpening method based on a multi-scale channel attention residual network. IEEE Access, 8, pp.27163-27177.

[32] Trojovská, E. and Dehghani, M., 2022. Clouded leopard optimization: a new nature-inspired optimization algorithm. IEEE Access, 10, pp.102876-102906.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.