Received: June 26, 2023. Revised: August 24, 2023.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

DLBIoT: Deep Learning and Blockchain for IoT Secure Architecture

Mayar M. Moawad[1]* **Magda M. Madbouly[1]** **Shawkat K. Guirguis[1]**

[1]*Department of Information Technology, Institute of Graduate Studies & Research, Alexandria University, 163 Horreya Avenue, El-Shatby 21526, P.O. Box 832, Alexandria, Egypt*
* Corresponding author's Email: igsr.mayar.mostafa@alexu.edu.eg

Abstract: The internet of things (IoT) has been industrializing in a variety of real-world implementations to improve human life. As IoT becomes more industrialized, a huge portion of data is being generated by various devices. Edge, Fog, and Cloud security is a topical issue associated with data storage, managing, or processing systems. Once an attack occurs, it has irreversible and disastrous effects on the development of IoT. Therefore, many security systems have been proposed and implemented for the sake of system security. So, this study consists of three steps based on deep learning, and blockchain for IoT (DLBIoT) architecture security. BoT-IoT and TON-IoT datasets are utilized to demonstrate the DLBIoT, also, the performance was measured using a variety of metrics. Results indicate that the proposed architecture is more efficient than other systems. DLBIoT architecture reaches an approximately 5 % increase for F1-Score compared to DT, NB, RF, and TP2SF. Also, the proposed architecture has simultaneously displayed an accuracy of 98.9% that increases steadily as the Learning Rate increases. Additionally, DLBIoT architecture may be utilized for real-time IoT applications.

Keywords: Blockchain, Cyberattacks, DL, Internet of things security, Intrusion detection.

1. Introduction

As technology advances in the community, novel opportunities have arisen that can facilitate our everyday lives and afford more proficient services or production approaches [1]. The internet of things (IoT) is reshaping human technological adaptation in everyday life. IoT applications are extremely diverse, ranging from critical applications such as smart cities, and health-related industries to industrial IoT [2]. The primary objective of IoT technologies is to ease processes in various fields and enhance one's life satisfaction [1].

IoT security has become a critical concern. The threat posed by infected Internet-connected things not only endangers IoT security but also endangers the entire internet ecosystem, which may exploit vulnerable things such as smart devices [3]. During the previous few years, the IoT system has been subjected to various attacks, making manufacturers and users more cautious about developing and deploying IoT devices. IoT attacks are classified into two types: physical attacks and cyber-attacks. Physical attacks physically destroy IoT devices. In this instance, attackers did not require the network to be able to attack the system. Thus, this form of threat is utilized on tangible IoT devices such as mobile phones, cameras, sensors, routers, and so much more, causing the service disrupted by the attackers. Second, cyber-attacks are a kind of threat in a wireless network that spots various IoT devices by attacking the system to be enabled to control (i.e., alter, destroy, delete, or steal) the user's data.

Consequently, IoT attacks cause a threat to the network's ability to protect user privacy, authentication, integrity, identification, and authorization. These characteristics should be considered when developing any security protocol to combat IoT system attacks [4].

Artificial intelligence (AI) has grown in popularity in the last years due to advances in machine learning (ML), particularly deep learning (DL) and reinforcement learning, demonstrating its utility in a huge range of applications where classification or regression problems play a crucial role [2]. IoT application generates a big portion of data. Before any data is computed, it must first go through the verification process to eliminate any malicious or spare data. A lot of security issues are addressed by ML as Distributed denial-of-service (DDoS), jamming, eavesdropping, authentication, Injection of false data, etc. [5].

For a secure, scalable IoT network, in contrast, a blockchain promoting a robust network over untrusted parties has lately grown in popularity [6]. It provides privacy in an IoT network by delivering the features of decentralization and an immutable distributed ledger. Blockchain decentralization enables the safe exchange of information and resources between each node in an IoT network, eliminating centralized control dependence and many-to-one traffic flows while providing ample data for big data analysis. As a result, it resolves the issue of a single-point failure, inadequate training data, and shorter communication delay. Additionally, the unchanging distributed ledger securely holds data in the form of blocks that are cryptographically controlled by each member node about all the nodes that make up an IoT network. This feature stops malicious tampering with training data, which in turn makes an IoT network very responsive to data poisoning threats [6]. Despite that, blockchain technology addresses security issues such as Identification verification, managing trust, privacy, data integrity, secure communication, authorization, Information sharing, and access control [5].

1.1 Problem definition

The continuous development and implementation of smart and IoT-based technologies have opened up new avenues for technological advancements in various life's aspects. Therefore, it comes as no surprise that applying security solutions in this environment is a challenging problem. Therefore, cyber security is now an international concern. Many techniques were introduced in cyber security as discussed in the literature review. So, this paper proffers an improved Intrusion Detection architecture to aid in the solution of cyber security issues by combining Blockchain and DL in IoT. They can work together to solve IoT challenges. DL is being integrated into IoT to make the network more efficient and self-sufficient. One of the challenges is combining DL methods with IoT to ameliorate the efficiency of IoT applications. Combining these techniques, focusing on balancing computational cost and efficiency, is critical for next-generation IoT networks. Considering the requirements of DL, and IoT requires a complete overhaul of the communication stack from the physical layer to the application layer. Therefore, applications built on top of the modified stack will benefit significantly, also, it will be easier to deploy the network.

1.2 Motivation and key challenges

Unsurprisingly, there has been extensive research on a variety of topics, including data security, privacy, and trust, as well as the detection and prevention of cyberattacks. For the creation of smart cities, several issues must be resolved. The following are the main issues list:

1. It is difficult to create a security mechanism for dynamic, large-scale smart city networks of IoT, edge, fog, and cloud that can accurately and efficiently distinguish between normal behaviors and irregular observations.
2. Creating a confidentiality and integrity technique for converting the original data is difficult.
3. Creating a reliable sensing system to distinguish between unreliable and trustworthy IoT nodes at the device layer of the IoT architecture.
4. Providing highly scalable distributed off-chain and on-chain storage for IoT infrastructure in a smart city with a platform for real-time sharing data. In smart cities, decentralized architecture enhances fault tolerance and expands as a whole scalability. Even so, it can be difficult to guarantee verifiable, traceable, and reliable services while using the cloud, fog, and edge architecture that is presently available.

1.3 Key contributions

1. The DLBIoT architecture is presented in this paper. An identifier blockchain reputation system is created to uphold trust among IoT nodes at the Device layer of the IoT architecture. Additionally, DLBIoT uses enhanced proof of work (ePoW) based on blockchain technology and principal component analysis (PCA) to prevent inference and poisoning threats to achieve confidentiality and integrity. Lastly, a DL-based intrusion detection module is implemented to identify suspicious activity within the smart city network.
2. An interplanetary file systems (IPFS)-enabled off-chain and a blockchain-enabled on-chain mechanism called CloudBlock, FogBlock, and EdgeBlock to resolve the issues with the current Cloud-Fog-edge architecture and redundancy in IoT data. The DLBIoT is deployed using the Cloud-Fog-Edge Block architecture because it supports data integrity, traceability, and validity facilities within and between IoT nodes.

3. Accuracy, detection rate, precision score, and F1 score are used to gauge how efficient the proposed DLBIoT is.

1.4 Strength points of DLBIoT

There are many advantages of the proposed DLBIoT architecture.

1. It is easy to implement, deploy and can efficiently detect 98.9% of the attacks found in highly dynamic and heterogeneous networks of IoT smart cities.
2. The address-based blockchain reputation system can proficiently calculate the reputation score of the participating IoT nodes and therefore builds trustworthiness in the network.
3. The confidentiality and integrity module integrates blockchain technology with PCA-based dimensionality reduction techniques to prevent inference and poisoning attacks. The aforementioned approach has considerably improved the overall performance of the proposed architecture.
4. Integration of blockchain technology in edge, fog, and cloud infrastructures enables verifiability, traceability, and reliability.

Finally, the paper is organized as follows: in Section 2 literature survey on security and privacy issues of IoT. The proposed methodology is described in section 3. The results & discussion explain the DLBIoT architecture in section 4. The conclusion of the study is summarized in section 5.

2. Literature survey

The latest study on trust management, blockchain technology, privacy protection, and peculiarity detection systems, as ML algorithms, is utilized in IoT-powered smart cities and their networks. Numerous investigations have been performed in optimizing trustworthiness among IoT nodes in the literature. In [7] presented a Trust Chain. This model uses a three-layered trust management framework using a consortium blockchain for assigning trust and reputation scores among supply chain participants. Hence, authors [8] present PrivySharing, a blockchain-based innovative framework for privacy-preserving and secure IoT data sharing in a smart city environment. The proposed scheme is distinct from existing strategies in many aspects. By segmenting the blockchain network into different channels, each of which consists of a limited number of authorized organizations and handles a particular type of data such as health, smart car, or smart energy data privacy is maintained. However, it can’t incorporate the concept of the fog nodes based on existing mobile BTS stations and also devise a mechanism for secure integration of IoT devices with the blockchain network.

The blockchain network is classified into various channels for processing a specific type of data from the smart car, smart energy, etc. However, data collection is done by utilizing an encryption technique. Where [9] presented a framework for reversible privacy-preserving k-means clustering. To remove the correlation between original and protected data, this approach employs swap, modification, and deletion techniques. A deep blockchain IoT framework is designed by [10]. For a privacy-preserving blockchain with smart contracts and anomaly detection, Bidirectional long short-term memory is used [11]. Another work in [11], presented a trustworthy privacy-preserving secured framework (TP2SF) for developing a sustainable smart city, by integrating blockchain and ML techniques. This framework comprises three modules; First an address-based blockchain reputation system. Second a two-level privacy-preserving mechanism. Third, a security model using the XGBoost technique is presented. The performance of the proposed TP2SF framework was evaluated with the original and transform datasets of ToN-IoT and BoT-IoT. The experimental results demonstrated that the proposed TP2SF framework outperforms some of the existing state-of-the-art techniques in terms of accuracy, detection rate, precision, and F1 score. However, a few challenges have been identified such as with the increase in participating IoT nodes, time taken in file uploading and block mining gradually increases.

To enhance the privacy and security of IoT data authors in [12] presented a privacy-preserving and secure framework (PPSF) and an intelligent blockchain framework that integrates blockchain and PCA-based transformation and ML approach for IoT-driven smart cities. Gradient boosting anomaly detector (GBAD) is used in the intrusion detection scheme for training and assessing the suggested scheme based on two IoT network datasets. The findings revealed that the proposed PPSF framework achieves better performance compared with peer privacy-preserving intrusion detection techniques. Also, the framework can be used to provide security and privacy in IoT and its application networks, organizational, and social areas where security and privacy are of prime importance. However, the security system can degrade due to massive data processing and analysis.

In [13] introduced a new approach to cyberattack prediction that showed the clustering of the attack data using an unsupervised learning approach before the classification and prediction of attacks. The approach achieves a greedy layer-by-layer learning process that best represents the features useful for predicting cyberattacks in a dataset of benign and malignant traffic. However, this approach is applied to only three attack types in one dataset, which is not substantial for measuring performance on most evolving attack types due to the complexity of analyzing and predicting them. In [14] introduced an extensive investigation of the security threats to blockchain and discussed similar real attacks by expanding popular Blockchain systems. They reviewed the security augmentation outcomes for blockchain technology.

To this end, [6] presents BlockDeepNet, which is a Blockchain-based secure DL that combines DL and blockchain to support secure collaborative DL in IoT. In BlockDeepNet, collaborative DL is performed at the device level to overcome privacy leaks and obtain enough data for DL, whereas blockchain is employed to ensure the confidentiality and integrity of collaborative DL in IoT. The system infrastructure proposed describes a novel decentralized big data analysis approach wherein the learning task is performed at the device level and distributed by employing blockchain technology. The proposed BlockDeepNet system remarkably lowers the possibility of data being manipulated adversely by facilitating a secure and collaborative DL paradigm. Also, the experimental evaluation shows that BlockDeepNet can achieve higher accuracy for DL with acceptable latency and computational overhead of blockchain operation. Consequently, some components of the IoT network must be reconfigured to support the working procedure of BlockDeepNet. Our emphasis in this paper is on designing an authentication confidential and integrity-secured framework, that can protect original data in smart cities and has the potential to process various IoT data sources and their network traffic.

3. Proposed methodology

3.1 Dataset information

Two datasets are utilized:

(a)BoT-IoT dataset [15] contains various attacks such as DDoS, DoS, and Theft. The source files for the dataset are offered in a variety of formats, such as the original pcap files, the produced argus files, and CSV files. More than 72.000.000 records can be found in the 69.3 GB-sized files.

(b)TON-IoT dataset [15] has numerous recent smart city-based attacks, such as DoS, ransomware, and DDoS. A new testbed has been constructed at the IoT lab to connect multiple kinds of virtual computers, physical tools, hacking systems, cloud, fog, edge systems, and IoT sensors to simulate the functionality and scalability of automotive IoT.

3.2 Software and hardware

The DLBIoT architecture is implemented in a software development environment, which is Python programming language, and Blockchain Technology. The model hardware development environment was implemented using a laptop computer with the following specifications: Processor: Intel (R), Core (TM) i7-7500U CPU@ 2.70GHz, RAM: 8 GB, system type: the 64-bit operating system, and Microsoft Windows 10 Pro Enterprise 64-bit is the running operating system.

3.3 Proposed DLBIoT architecture

The DLBIoT architecture contains two main steps, the first step is Pre-processing, and the second step is intrusion detection system. DLBIoT architecture is applied in each block (edge, fog, cloud) as explained in section 3.4 to ensure data authentication, confidentiality, integrity, and identification. Table 1 shows a list of notations.

3.3.1. Pre-processing module

In this part, the data passes through two stages, the first stage is the Authentication module, and the second stage is the confidentiality and integrity module. The following subsections provide an in-depth explanation of each stage.

3.3.1.1. Authentication module

The first module constitutes the pre-processing of the database, which includes the steps shown in Fig. 1. First, compute the *CTh* value for each IoT node [11], using Eq. (1).

$$CTh = \text{range}(\min(\text{di}), \max(\text{di})) \tag{1}$$

Second, the Rps is calculated for identifying trustworthiness among IoT nodes, so compute Rps for each IoT node based on $Txscore$ and *CTh* values, using Eq. (2), based on the results, Rps is classified into three categories to honest (trust), general, and dishonest [11].

$$Rps = \frac{\text{Txscore}/_{10}}{\text{No\_of\_Tx}} \tag{2}$$

A higher Rps of a node contributes to higher trust in the true observation of the node. The trusted value

Table 1. Notation list

Symbol	Definition
CTh	Confidence Threshold
D_i	Database
Rps	Reputation Score
$Txscore$	Transaction Score
No_of_Tx	Number of Transaction
m	Size of the input vector
P	Size of the output vector
hi	Hidden Layer
Nf	Non-Linear Activation Function
x	Input for Sigmoid Function

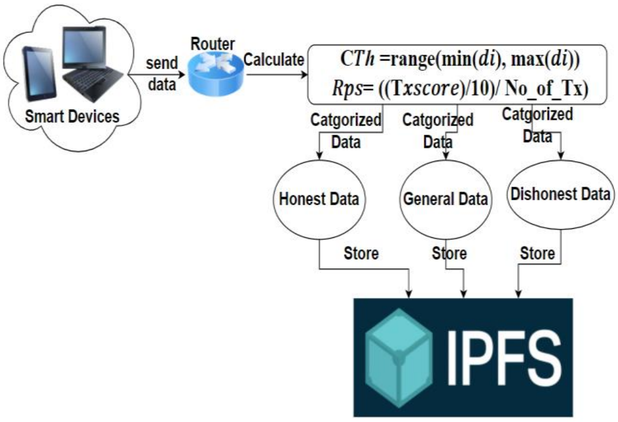

Figure. 1 Overview of authentication module

is saved in the IPFS distributed system, where IPFS stores this information in the distributed hash table. Also, IPFS assigns the unique addressable hash of the sensor information, and for long-term storage, data is sent to the cloud, while in the blockchain network, the message digest containing Rps and $Txscore$ of honest, general and dishonest nodes are stored. Blockchain technology helps in data authentication and is used for maintaining privacy [11, 15].

3.3.1.2. Confidentiality and integrity module

The trust information along with the raw data is sent to the Confidentiality and Integrity module. In this module, blockchain is used. Then, second-level privacy is introduced. The following subsections explain each stage. Also, Fig. 2 explains the flow of work in the Confidentiality and Integrity Module.

3.3.1.2.1. Blockchain-based confidentiality and integrity

Blockchain-based privacy extends the concept of a blockchain protocol that works on a peer-to-peer basis to provide encrypted data transfers or network nodes securely. Such authenticated messages form a chain of records or blocks stored on each participating edge or fog or cloud node that ensures the validity of the transaction, ensuring that no data can be removed or falsified from the ledger i.e., supports immutability and decentralization [17]. To describe the proposed technique, let us assume that a dataset includes a list of records. Each record, of the corresponding message digest, includes a secure hash function that preserves raw data integrity. This secure hash function generates a unique fingerprint of fixed-length output known as a one-way cryptographic hash with different structures and fixed bitlengths as output. The reason for constructing blocks using message digest is that the one-way cryptographic hash prevents poisoning attacks owing to the avalanche effect [11] (modifying one bit of data can change the message digest completely). Thus, this process maintains the integrity of IoT data. The generated blocks in the network include various information such as Block_Index, Previous_Hash, timestamp, Data ($Txvalue$), $Txscore$, Rps, proof, Current_Block_Hash. The chain of blocks in the blockchain ledger is maintained using the hash of the previous block. This technique considerably improves verifiability, as any modification in the data block generates an avalanche effect and it can be easily verified in real-time smart city networks [11]. In the context of blockchain technology, the integrity of the hash chain is verified during the creation of new blocks, using a distributed set of rules named the consensus mechanism [18]. However, the traditional consensus approach i.e., proof-of-work (PoW) is computationally intensive due to finding high proof and different difficulty levels for the hash integrity in the network [19]. Therefore, in this paper, an ePoW technique is presented. This method is less computationally intensive in terms of proof generation and maintaining hash chain integrity. Once the ePoW is executed successfully, the message digest is disseminated to a blockchain network, then the second level of privacy is applied to the raw data generated by IoT-driven smart city. The ePoW is utilized to provide the first level of privacy to the dataset of BoT-IoT and ToN-IoT, for verifying raw data records and preventing poisoning attacks, and inference that could learn from system-based ML [15, 16].

3.3.1.2.2. PCA-based confidentiality and integrity

Once the ePoW is executed successfully, the message digest is disseminated to the blockchain network, and then the second level of privacy is applied to the raw data generated by the IoT-driven smart city. The second level includes feature mapping, feature selection, feature normalization, and feature transformation. The above-aforementioned steps are discussed below.

Received: June 26, 2023. Revised: August 24, 2023.

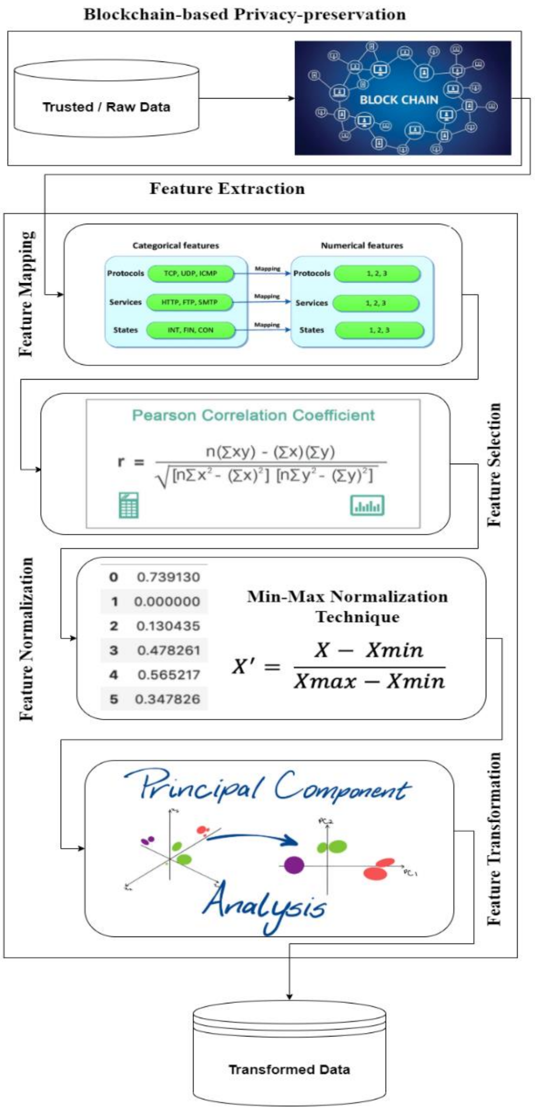

Figure. 2 Overview of confidentiality and integrity module

✓ Feature Mapping: The network traffic of IoT comprises both numeric and categorical features. A mapping function is used to transform categorical variables into numeric ones. For example, protocol features of the ToN-IoT dataset are converted into ordered numbers such as 1, 2, etc [20]. The reason for this is that the proposed second-level privacy-preserving mechanism can deal efficiently with numeric features.

✓ Feature selection: Feature selection is a process of identifying the appropriate features and then discarding the irrelevant ones, intending to obtain a subset of features that best represent the problem with minimum performance degradation in a smart city environment. The proposed DLBIoT architecture uses pearson correlation coefficient (PCC) based simplest statistical approach. This technique is used to measure the similarity between the given two variables [21]. The lowest-ranked attributes are chosen, as being the most significant ones, and are used by DLBIoT for transformation.

✓ Feature Normalization: The data generated by IoT sensors are of different magnitudes. In DLBIoT architecture, the min-max normalization technique is used, as it removes bias from the IoT network traffic without changing its statistical properties. In this method, for every particular feature, the minimum value gets converted into 0, the maximum value gets converted into 1 and other values get transformed into decimal points between 0 and 1 [12].

✓ Feature Transformation: PCA [11] is used for transforming the original raw data into a new shape such that the private knowledge and private data remain undisclosed. PCA is a powerful transformation technique that increases the utility system of intrusion detection. This is a statistical technique that transforms a set of features using orthogonal transformations into a collection of values of linearly uncorrelated variables without losing much information. The output is a new form of transformation called principal components. These components are sorted from the largest possible variance to the lowest.

3.3.2. Intrusion detection module

The transformed data obtained from the confidentiality and integrity module is further used by the DL algorithm especially a multilayer perceptron (MLP) model [22], having three or more layers with one input layer, one or more hidden layers, and an output layer in which each layer has many neurons or units in mathematical notation as shown in Fig. 3. We select the number of hidden layers by following a hyper-parameter selection method. The information is transformed from one layer to another layer in a forward direction with neurons in each layer fully connected. MLP is defined mathematically as $O : R^m * R^p$.The computation of each hi is mathematically defined as:

$$hi(x) = \mathrm{N}f\left(w_i^T x + b_i\right) \tag{3}$$

where $h_i : R^{d_i-1} \rightarrow R^{d_i}, \mathrm{N}f : R \rightarrow R, w_i \in R^{d*d_i-1}, b \in R^{d_i}$, d_i denotes the size of the input, Nf is either a sigmoid (values in the range [0, 1]) or a tangent function (values in the range [1, -1]). For the classification problem of multi-class, the proposed model uses the SoftMax function as the non-linear activation function. SoftMax function outputs the probabilities of each class and selects the largest value among probability values to give a more

Received: June 26, 2023. Revised: August 24, 2023.

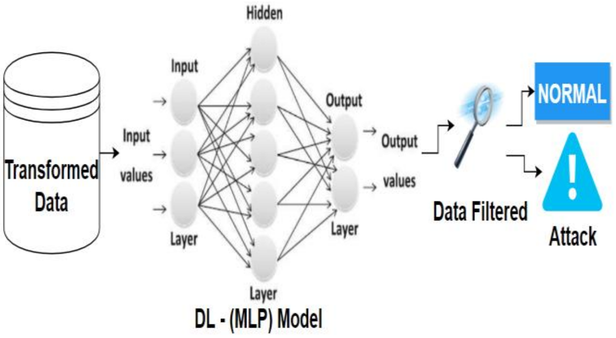

Figure. 3 Intrusion detection module using DL

accurate value. The mathematical formulae *sigmoid*, and *SoftMax* activation and classification function are given below.

$$sigmoid = \frac{1}{1+e^{-x}} \tag{4}$$

$$SoftMax(x_i) = \frac{e^{x_i}}{\sum_{j=1}^{n} e^{x_j}} \tag{5}$$

DL algorithm [23] is used to assort data into normal and different attack types, based on which abnormal class administrator is notified.

3.4 Proposed architecture in smart city

A deployment of DLBIoT architecture for intrusion detection systems in the smart city is deployed on the edge side, fog side, and cloud side respectively to remedy the restrictions of self-contained architectures and to benefit from collaborative networks (as discussed in Section 3). More, to take the privilege of blockchain technology completely, we have integrated blockchain and IPFS at the edge, fog, and cloud sides.

3.4.1. Edge block

Once there is a request for the data for a service, it is generated from IoT devices at the device layer of the smart city. The network traffic is forwarded to Edge Block using the nearest gateway. At Edge Block, the former consists of sensors (packet sniffing devices) that intercept incoming packets and derivatives of the aspects associated with them. To verify the trust for IoT sensor nodes' data, the Authentication module is designed to compute the reputation score for each registered IoT node, based on transaction and *CTh* value. A higher *Rps* of a node contributes to higher trust in the true observation of the node. Depending on the outcome, the transaction is categorized into three types: honest, general, and dishonest. The transaction or raw data is saved in IPFS, while in the blockchain network, the message digest containing *Rps* and *Txscore* of three types for nodes are stored.

The raw data is sent to the confidentiality and integrity module along with the trust data. In this module, a message digest with proof of hash is generated using blockchain-based ePoW. The message digest is then distributed throughout the blockchain network. This method verifies chains of data records and prevents inference attacks that could be learned from system-based ML. Finally, the DL algorithm [23] is utilized to categorize data into normal and different attack types, depending on which anomalous class administrator is alerted. For a normal transaction the required information (*info*), if available at the edge side is provided and in case the *info* is not available, the security *info* along with the request is sent to fog block [15].

3.4.2. Fog block

At the Fog Block, the group of fog nodes, *Fg* = {*fg*1, *fg*2, *fg*3...*fgk*} maintains a blockchain ledger for on-chain storage and IPFS for off-chain storage [10]. Once the fog block receives a request for the *info*, the aforementioned procedure is followed and service is given to the requester, for attack instances, the administrator is alerted and in case the *info* is not available, the security *info* with the request is sent to cloud block [15].

3.4.3. Cloud Block

Cloud Block consists of various types of datacentric provided by various vendors. For the intended system, we have utilized four datacentrics A, B, C, and D. These are the entities that make up the Cloud-Block network; the intended DLBIoT architecture is deployed at each datacentric to make a blockchain network. This approach builds user trust by making the network immutable, auditable, and verifiable [24]. When the cloud block receives an *info* request, the aforementioned procedure is followed, and the service is given to the requester, while the administrator is notified of all attack instances. The intended system takes the benefit of collaborative cooperation between edge-fog-cloud architecture and integrates Blockchain, and DL to design a secure sustainable smart city [15].

4. Results and discussion

In the following subsections, the configuration section, parameter settings for the proposed approach over BoT-IoT and TON-IoT training data sets are discussed. The model evaluation section analyses the

Table 2. Dl parameters setting

Parameter	Value
Learning Rate	0.01-0.9
Number of Epoch	100
Hidden Nodes	10-100
Batch Size	10000
Classification function	SoftMax
Activation function	Sigmoid

Table 3. Confusion matrix for proposed DLBIoT architecture (Average)

		Predicted Class	
		Condition Positive (P)	**Condition Negative (N)**
Actual Class	**Condition Positive (P)**	98.9%	1.1%
	Condition Negative (N)	1.1%	98.9%

Table 4. Confusion matrix for TP2SF (Average)

		Predicted Class	
		Condition Positive (P)	**Condition Negative (N)**
Actual Class	**Condition Positive (P)**	95.7%	4.3%
	Condition Negative (N)	4.3%	95.7%

performance of the model to test its capability to detect attacks.

4.1 Configuration

4.1.1. Parameter settings

Parameter values for the intrusion detection model are selected. These parameters are chosen to rely on various experiments on training data sets. Experiments are done in different settings utilizing multiple parameter combinations. DL parameters are selected and presented in Table 2.

4.1.2. Evaluation metrics

The effectiveness of the DLBIoT architecture most commonly depends on the metrics for evaluation. A confusion matrix of binary classification is a 2*2 table formed by counting the number of the four outcomes of a binary classifier [25].

4.2 Model evaluation

In this section, the performance of Blockchain and DL for optimal detection is evaluated to test their capability in detecting attacks. To further verify the proposed model for detecting attacks, a comparison with some existing methods is conducted.

Experiment 1: DL validation to show its role in attack detection for enhancing accuracy

Aim: This experiment is conducted to investigate the role of Blockchain and DL to validate their role in the intrusion detection module for enhancing accuracy. The DL algorithm is provided in this study to detect the attacks and improve the proposed DLBIoT architecture. It compares the TP2SF and the proposed DLBIoT architecture for different datasets with a confusion matrix.

Observations: Tables 3, and 4, reveal that DL for attack detection achieves better results with the confusion matrix correlated to the TP2SF procedure. For both TON-IoT and BoT-IoT datasets, DLBIoT architecture produces an approximate increase in detecting attacks compared to TP2SF.

Discussions: The way DLBIoT architecture works is that facilitates capturing the attacks efficiently. Moreover, DL decreases comparison numbers in attack detection. In general, the feature selection problem has a multi-modal character because of multiple optimum solutions in the search space. Consequently; the way works facilitates capturing the attacks efficiently. As a result, a conventional evolutionary process can lead to convergence while leaving the rest of the search space unexplored.

Experiment 2: Assessment with different values of learning rate & hidden nodes

Aim: The objective of the second set of experiments is to test the accuracy of the training sample of the DLBIoT architecture with different learning rates and hidden nodes. If the model has more enrolled samples, the chance of a correct hit increases.

Observations: The accuracy of the proposed DLBIoT architecture achieves better results with the increasing number of training documents. For all values of documents, accuracy has been increased by approximately 5 % on average. This means that training the model will increase the accuracy of detecting attacks.

Discussions: As shown in Fig. 4, presents the training time of the DLBIoT architecture with different learning rates and hidden nodes. The X-axis represents learning rates as 0.01, 0.1, 0.3, 0.5, 0.7, and 0.9. The Y -axis represents the time taken in seconds for different No. of hidden nodes of 10, 20, 40, 60, 80, and 100 which had been increased statically to study the time impact when the hidden nodes expand. Also as in Fig. 5, as expected, the accuracy of the DL model with different learning rates and hidden nodes. We studied the accuracy concerning differing No. of hidden nodes in the

Received: June 26, 2023. Revised: August 24, 2023.

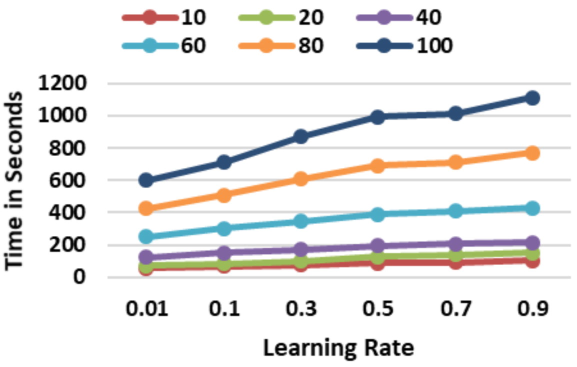

Figure. 4 Learning rate vs time

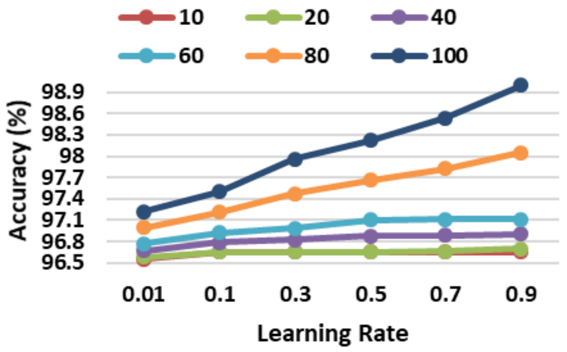

Figure. 5 Learning rate vs accuracy

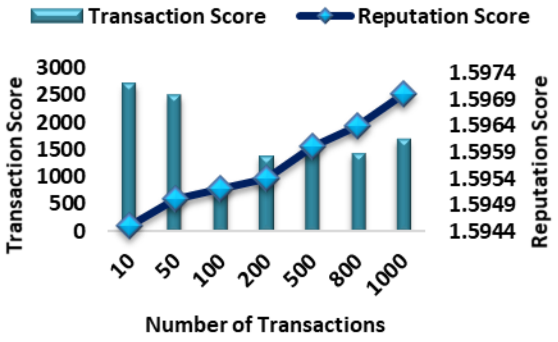

Figure. 6 Transaction score vs reputation score

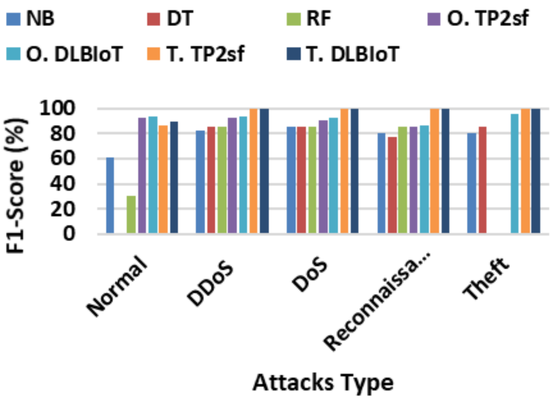

Figure. 7 Comparison in terms of F1-score using BoT-IoT dataset

system. It can be seen that the accuracy increases steadily as the learning rate increases. This increase has been done at the expense of the time taken to train the model, but this time is negligible compared to the time spent in the testing phase.

Experiment 3: Performance of system with different training samples

Aim: The third set of experiments aims to check the performance of the suggested DLBIoT architecture in terms of Transaction score, and Reputation score for ToN-IoT and BoT-IoT datasets.

Observations: The execution concerning these computations with differing No. of transactions in the system. It can be seen that the T$xscore$ increases steadily as the No. of transactions is increased.

Discussions: As per the intended system, we have computed the Rps of IoT nodes by deploying 100 IoT nodes in the Ethereum network. Each IoT node present in the framework is assigned a specific address in the blockchain network. The transactions performed by these nodes are utilized to determine T$xscore$ against CTh. The generated score is utilized for trust evaluation by calculating $\mathcal{Rps}$ for generated transactions. Fig. 6 shows the T$xscore$ and $\mathcal{Rps}$ for 1000 transactions. These scores are calculated for ToN-IoT and BoT-IoT datasets, which contain valid transaction values ''Honest'' for available features.

Experiment 4: Comparative study to show that implementing PCA prevents attacks effectively

Aim: To validate the benefits of implementing PCA for preventing attacks; this experiment compares the DLBIoT architecture with related detecting attack models that utilize algorithms decision tree (DT), Naive Bayes (NB), random forest (RF), and TP2SF [11, 26, 27]. The experiment reported for datasets TON-IoT and BoT-IoT by original data and transformed data by applying PCA measured in terms of F1-Score for all the used datasets.

Observations: It is observable that the results of the PCA-based preventing attack model are better than those depending on DT, NB, RF, and TP2SF. The results of BoT-IoT datasets are shown in Fig. 7. A great observation is that DLBIoT architecture detects Normal attacks where DT can't detect them. Also, in Theft attacks where RF, and in the original data TP2SF can't detect them while DLBIoT detects them. Fig. 8 for the TON-IoT dataset reveals the superiority of the suggested model for attack detection in terms of F1-Score. An important observation is that DLBIoT architecture detects Injection and MITM attacks where DT and RF can't detect them. The recommended DLBIoT architecture achieves an approximately 5 % increase for F1-Score compared to DT, NB, RF, and TP2SF. Moreover, it can be

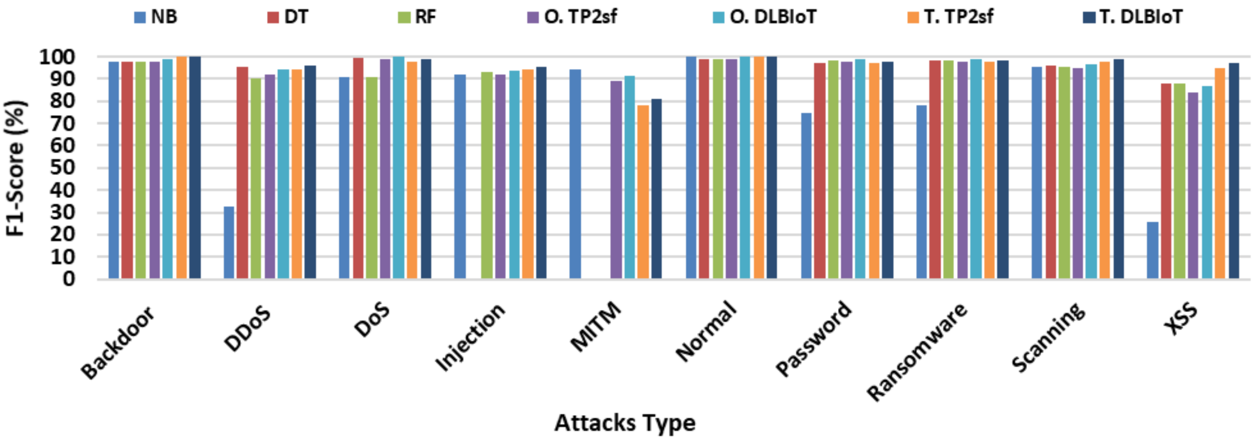

Figure. 8 Comparison in terms of F1-Score using the TON-IoT dataset.

seen that; the proposed system outperforms in most of the cases for detecting different attack vectors present in both datasets. These results confirm the superiority of the suggested architecture for detecting attacks regarding different datasets. In general, for all datasets, the proposed model yields an increase in F1-score.

Discussions: One possible explanation of these results is that the suggested architecture relies on PCA to capture attacks. Furthermore, implementing DLBIoT architecture is done which facilitates cutting out the attacks effectively. Furthermore, incorporating PCA into infrastructure improves security and privacy.

5. Conclusion

A DLBIoT architecture for developing a sustainable smart city adapts blockchain and DL techniques. This DLBIoT architecture consists of three modules: (a) an authentication module that depends on the reputation system; (b) a confidentiality and integrity module; and (c) a DL intrusion detection model. Finally, a deployment system known as DLBIoT was proposed to address the shortcomings of the current Cloud-Fog-Edge architecture. The system's performance is assessed using the BoT-IoT and TON-IoT datasets. In terms of AC, DR, PR, and F1-Score, the results show that the suggested DLBIoT architecture outperforms some of the present state-of-the-art techniques. Hereafter, the suggested DLBIoT architecture will be extended by implementing a prototype that verifies the overall architecture security parameters. This could help to enhance the overall privacy and security requirements of emerging smart cities. Finally, we will expand on this work by employing different load balancing criteria, which can improve network performance overall.

Conflict of interest

The authors declare that they have no conflict of interest to report regarding the present study.

Author contributions

Conceptualization, MMM, SKG, and MMM*; methodology, SKG, and MMM*; software, MMM*; validation, MMM, and SKG; formal analysis, MMM, SKG, and MMM*; investigation, MMM, and SKG; resources, MMM*; data curation, MMM*; writing-original draft preparation, MMM*; writing-review and editing, MMM, and SKG; visualization, MMM*; supervision, MMM, and SKG; project administration, MMM, SKG, and MMM*; funding acquisition, MMM*

References

[1] S. Nizetic, P. Solic, D. L. G. D. Artaza, and L. Patrono, “Internet of Things (IoT): Opportunities, Issues and Challenges Towards a Smart and Sustainable Future”, *Journal of Cleaner Production*, Vol. 274, 2020, doi: 10.1016/j.jclepro.2020.122877.

[2] Y. B. Zikria, M. K. Afzal, S. W. Kim, A. Marin, and M. Guizani, “Deep Learning for Intelligent IoT: Opportunities, Challenges and Solutions”, *Computer Communications*, Vol. 164, pp. 50-53, 2020, doi: 10.1016/j.comcom.2020.08.017.

[3] A. R. Javed, F. Shahzad, S. Rehman, Y. B. Zikria, I. Razzak, Z. Jalil, and G. Xu, “Future Smart Cities: Requirements, Emerging Technologies, Applications, Challenges, and Future Aspects”,

Cities, Vol. 129, p. 103794, 2022, Doi: 10.1016/j.cities.2022.103794.

[4] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine Learning Based Solutions for Security of Internet of Things (IoT): A Survey", *Journal of Network and Computer Applications,* Vol. 161, 2020, doi: 10.1016/j.jnca.2020.102630.

[5] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: Challenges and Solution using Machine Learning, Artificial Intelligence and Blockchain Technology", *Internet of Things,* Vol. 11, 2020, doi: 10.1016/j.iot.2020.100227.

[6] S. Rathore, Y. Pan, and J. Park, "BlockDeepNet: A Blockchain-Based Secure Deep Learning for IoT Network", *Sustainability*, Vol. 11, pp. 1-15, 2019, doi: 10.3390/su11143974.

[7] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "Trustchain: Trust Management in Blockchain and IoT Supported Supply Chains", In: *Proc. of IEEE International Conference on Blockchain*, Atlanta, USA, pp. 184–193, 2019, doi: 10.1109/Blockchain.2019.00032.

[8] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, "PrivySharing: A Blockchain-Based Framework for Privacy-Preserving and Secure Data Sharing in Smart Cities", *Computers and Security,* Vol. 88, 2020, doi: 10.1016/j.cose.2019.101653.

[9] C. Y. Lin, "A Reversible Privacy-Preserving Clustering Technique Based on K-Means Algorithm", *Applied Soft Computing,* Vol. 87, 2020, doi: https:10.1016/j.asoc.2019.105995.

[10] O. Alkadi, N. Moustafa, B. Turnbull, and K. R. Choo, "A Deep Blockchain Framework Enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks", *IEEE Internet Things Journal*, Vol. 8, Issue 12, pp. 9463-9472, 2020, doi: 10.1109/JIOT.2020.2996590.

[11] P. Kumar, G. P. Gupta, and R. Tripathi, "TP2SF: A Trustworthy Privacy-Preserving Secured Framework for Sustainable Smart Cities by Leveraging Blockchain and Machine Learning", *Journal of Systems Architecture,* Vol. 115, 2021, doi: 10.1016/j.sysarc.2020.101954.

[12] P. Kumar, R. Kumar, G. Srivastava, G. P. Gupta, R. Tripathi, T. R. Gadekallu, and N. N. Xiong, "PPSF: A Privacy-Preserving and Secure Framework using Blockchain-based Machine-Learning for IoT-driven Smart Cities", *IEEE Transactions on Network Science and Engineering*, Vol. 8, pp. 2326-2341, 2021, doi: 10.1109/tnse.2021.3089435.

[13] A. E. Ibor, F. A. Oladeji, O. B. Okunoye, and O. O. Ekabua, "Conceptualisation of Cyberattack Prediction with Deep Learning", *Cybersecurity,* Vol. 3, pp. 1-14, 2020, doi: 10.1186/s42400-020-00053-7.

[14] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A Survey on the Security of Blockchain Systems", *Future Generation Computer Systems,* Vol. 107, pp. 841-853, 2020, doi: 10.1016/j.future.2017.08.020.

[15] M. M. Moawad, M. M. Madbouly, and S. K. Guirguis, "Leveraging Blockchain and Machine Learning to Improve IoT Security for Smart Cities", In: *Proc. of the 3rd International Conference on Artificial Intelligence and Computer Vision,* Springer, 2023, doi: 10.1007/978-3-031-27762-7_21

[16] R. Kumar and R. Tripathi, "Blockchain-based Framework for Data Storage in peer-to-peer Scheme using Interplanetary File System", *Handbook of Research on Blockchain Technology,* pp. 35–59, 2020, doi: 10.1016/B978-0-12-819816-2.00002-2.

[17] U. Bodkhe, S. Tanwar, K. Parekh, P. Khanpara, S. Tyagi, N. Kumar, and M. Alazab, "Blockchain for Industry 4.0: A Comprehensive Review", *IEEE Access,* 2020, doi: 10.1109/ACCESS.2020.2988579.

[18] A. A. Alli and M. M. Alam, "The Fog Cloud of Things: A Survey on Concepts, Architecture, Standards, Tools, and Applications", *Internet Things,* Vol. 9, p. 100177, 2020, doi: 10.1016/j.iot.2020.100177.

[19] A. Kaur, A. Nayyar, and P. Singh, "Blockchain: A path to the Future", *Cryptocurrencies and Blockchain Technology Applications,* Wiley, pp. 25–42, 2020, doi: 10.1002/9781119621201.

[20] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Towards a Lightweight Detection System for Cyber-attacks in The IoT Environment using Corresponding Features", *Electronics,* Vol. 9, 2020, doi: 10.3390/electronics9010144.

[21] M. Nssibi, G. Manita, and O. Korbaa, "Advances in Nature-inspired Metaheuristic Optimization for Feature Selection Problem: A Comprehensive Survey", *Computer Science Review,* Vol. 49, 2023, doi: 10.1016/j.cosrev.2023.100559.

[22] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, "Anomaly-based Intrusion Detection System for IoT Networks Through Deep Learning model", *Computers and Electrical Engineering*, Vol. 99, 2022, doi: 10.1016/j.compeleceng.2022.107810.

[23] S. Bhattacharya, P. K. R. Maddikunta, R. Kaluri, S. Singh, T. R. Gadekallu, M. Alazab, and U.

Tariq, "A Novel PCA-Firefly based XGBoost Classification Model for Intrusion Detection in Networks using GPU", *Electronics*, Vol. 9, 2020, doi: 10.3390/electronics9020219

[24] K. Gai, J. Guo, L. Zhu, and S. Yu, "Blockchain Meets Cloud Computing: A Survey", *IEEE Communications Surveys & Tutorials*, Vol. 22, pp. 2009-2030, 2020, doi: 10.1109/COMST.2020.2989392

[25] J. Xu, Y. Zhang, and D. Miao, "Three-Way Confusion Matrix for Classification: A Measure Driven View", *Information Sciences*, Vol. 507, pp. 772-794, 2020, doi: 10.1016/j.ins.2019.06.064

[26] A. Sharma, E. S. Pilli, A. P. Mazumdar, and P. Gera, "Towards Trustworthy Internet of Things: A Survey on Trust Management Applications and Schemes", *Computer Communications*, Vol. 160, pp. 475-493, 2020, doi: 10.1016/j.comcom.2020.06.030.

[27] W. Haider, N. Moustafa, M. Keshk, A. Fernandez, K. K. R. Choo, and A. Wahab, "FGMCHADS: Fuzzy Gaussian Mixture-based Correntropy Models for Detecting Zero-Day Attacks from Linux Systems", *Computers and Security*, Vol. 96, 2020, doi: 10.1016/j.cose.2020.101906.