frontiers | Frontiers in Computer Science

TYPE Original Research
PUBLISHED 06 August 2025
DOI 10.3389/fcomp.2025.1622382

OPEN ACCESS

EDITED BY
Aikaterini Kanta,
University of Portsmouth, United Kingdom

REVIEWED BY
Syed Muhammad Salman Bukhari,
Zayed University, United Arab Emirates
Aized Soofi,
Government College University, Faisalabad, Pakistan

*CORRESPONDENCE
Raed Alharthi
✉ ralharthi@uhb.edu.sa

RECEIVED 03 May 2025
ACCEPTED 16 July 2025
PUBLISHED 06 August 2025

CITATION
Eshmawi AA, Aldrees A and Alharthi R (2025) Smart framework for industrial IoT and cloud computing network intrusion detection using a ConvLSTM-based deep learning model. *Front. Comput. Sci.* 7:1622382. doi: 10.3389/fcomp.2025.1622382

Smart framework for industrial IoT and cloud computing network intrusion detection using a ConvLSTM-based deep learning model

Ala' Abdulmajid Eshmawi[1], Asma Aldrees[2] and Raed Alharthi[3]*

[1]Department of Cybersecurity, College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia, [2]Department of Informatics and Computer Systems, College of Computer Science, King Khalid University, Abha, Saudi Arabia, [3]Department of Computer Science and Engineering, University of Hafr Al-Batin, Hafar Al Batin, Saudi Arabia

In the rapidly evolving landscape of the Industrial Internet of Things (IIoT) and cloud computing, ensuring robust network security has become a major challenge for the Internet of Everything (IoE). However, this technological advancement has also introduced new vulnerabilities, making these systems prime targets for sophisticated cyberattacks. Ensuring the security of IIoT and cloud networks is critical to protecting sensitive data and maintaining industrial operations' integrity. This study examines data anonymity, security, and preservation in the Edge IIoT environment, focusing on cloud computing and cyber-physical systems. The integration of blockchain in industrial applications introduces additional security risks. This paper uses the EdgeIIoT dataset, enriched with security threat detection features for blockchain environments. The ConvLSTM framework, which uses the characteristics of two deep neural network models, CNN and LSTM, predicts and mitigates threats in IoT, IIoT, and cloud environments. The ConvLSTM model shows outstanding results for accuracy, precision, recall, and F1 score on multiple datasets based on network intrusion detection, showcasing its robustness and generalizability. The results are compared with previously published research work in this domain to demonstrate the superiority of the proposed framework.

KEYWORDS

internet of everything (IoE), industrial internet of thing, cloud computing, network intrusion detection, artificial intelligence, ConvLSTM, neural networks

1 Introduction

The advent of the Internet of Everything (IoE) has significantly transformed industrial sectors, integrating the Internet of Things (IoT), the Industrial Internet of Things (IIoT), cloud computing, and blockchain technologies to deliver unmatched connectivity, automation, and instant decision-making capabilities. Yet, this interconnected environment has also heightened cybersecurity risks, leaving critical infrastructures vulnerable to sophisticated and adaptive cyberattacks. Conventional security strategies are becoming less effective against these advancing threats. Utilizing artificial intelligence (AI), especially through deep learning and ensemble models, offers a promising path toward developing intelligent, proactive defense solutions that can detect anomalies, forecast intrusions, and facilitate automated real-time responses. This research

highlights the urgent need for AI-driven cybersecurity frameworks to protect industrial systems, addressing both technical challenges and rising concerns about privacy and ethical implementation.

Blockchain technology has gained wide attention during the past decade, primarily due to its features of security and transparency. Blockchain offers distributed data structures to store digital transactions without any need for a central authority. In addition, smart contracts can be executed automatically in a peer-to-peer network. Blockchain is based on a decentralized system, where multiple network nodes simultaneously verify transactions, thereby providing enhanced security. Each transaction is recorded as a code block across multiple devices and added to a chain, forming the blockchain, which serves as a past record on the decentralized ledger. This process eliminates the risk of hacking and stealing data virtually (Krdzalic, 2018). The absence of a third party in data exchange makes blockchain technology highly appealing and secure. Not limited to financial transactions, blockchain finds applications in various industries due to its versatility. Sectors such as energy, logistics, education, and more are adopting blockchain technology to enhance their operations and benefit from its secure and transparent nature.

Cloud computing is a distributed computing technology that offers reduced processing burden. In addition, it helps the users in reducing hardware costs and is highly flexible and scalable. Despite its divergent advantages, cloud computing is not a well-embraced technology due to its privacy and security concerns (Venters and Whitley, 2012). So, to resolve the privacy and security issues of data in cloud computing, blockchain technology can be employed. Blockchain and cloud computing technologies can be integrated to provide a distributed and secure system. This integration is a natural solution to improve data security and privacy, along with services availability on the cloud.

Blockchain technology finds numerous applications across various domains, including security and privacy, finance, reputation management, copyright protection, e-business, IoT, healthcare, insurance, energy, and more (Zheng et al., 2018). It also has social applications such as blockchain-based music and government systems, as well as digital documents, advertising, voter registration, the automotive industry, supply chain management, defense (Joshi et al., 2018; Chen et al., 2018; Dave et al., 2019), agriculture (Dave et al., 2019), law enforcement, computerized ownership management, identity management, property title registers, monitoring, mobile apps, intrusion detection (Baboshkin et al., 2022), asset tracking (Monrat et al., 2019), and education.

The contributions of this paper are as follows:

1. This study conducts a comprehensive analysis of blockchain technology, encompassing its applications and advancements.
2. A novel framework for accurate prediction of different types of IoT and cyberattacks using the proposed ConvLSTM model is proposed.
3. The performance of the ConvLSTM model is compared with several machine learning, four deep learning, and three transfer learning models.
4. The performance of the model is further compared with the state-of-the-art model and its significance is analyzed using a *k*-fold cross-validation technique.

The paper is structured as follows. In Section 2, the diverse applications of blockchain technology for providing security in different industrial sectors is described. In Section 3, a novel framework for accurate detection and prediction of attacks that occur in IoT and cloud computing environments is provided. The results of extensive experiments and comparative analysis are discussed in Section 4. The paper concludes in Section 5.

2 Literature review

This section explains the advancement in the field of intrusion detection systems (IDS) for IIoT and IoT environments by leveraging ensemble learning and deep learning techniques to enhance security, accuracy, and interpretability. In Mohy-Eddine et al. (2023), authors proposed an ensemble model combining Isolation Forest and Pearson's Correlation Coefficient for feature selection, integrated with a Random Forest classifier, achieving near-perfect accuracy and efficient prediction times on IIoT datasets, demonstrating superior performance over existing models. In another study (Shtayat et al., 2023), the authors proposed an explainable ensemble deep learning framework that combines multiple LSTM classifiers through a meta-learner. By incorporating SHAP-based interpretability, the approach enhances transparency in attack detection, achieves high accuracy, and effectively addresses the interpretability challenges in IIoT security. In Alotaibi and Ilyas (2023), the authors presented a weighted ensemble learning approach optimized for industrial-scale IIoT data and multi-class attack detection, validated on a public dataset with impressive F1-scores, emphasizing scalability and robustness in edge computing environments. In Jemili et al. (2024), authors focused on big data classification for intrusion detection using ensemble learning, highlighting the method's effectiveness in handling large-scale data and improving detection accuracy in complex IoT networks. Lastly, in Nandanwar and Katarya (2024), the authors proposed a deep learning-based IDS named AttackNet, designed specifically for IIoT environments to detect and classify botnet attacks, showcasing the potential of deep learning models in addressing sophisticated cyber threats in industrial settings. Collectively, these studies underscore the critical role of ensemble and deep learning techniques in advancing IDS capabilities for IIoT and IoT, balancing high detection performance, computational efficiency, and explainability to meet the evolving cybersecurity demands of interconnected industrial systems.

2.1 Protection against IoT cyberattacks

The IoT is also endangered by several kinds of cyberattacks. For example, phishing attacks are launched by malware-based, socially engineered attacks. These attacks are carried out with the aim in mind of stealing the login credentials of the intended users through fake links, emails, and websites (Gupta et al., 2017). Similarly, a watering hole attack is carried out through frequently visited websites by a targeted group of a company to exploit any vulnerability in the company's systems (Allen et al., 2020). Famous websites with security loopholes and vulnerabilities are infected

with malicious code to redirect the users to the attacker's websites (Ismail et al., 2017). Malware refers to a category of malicious software that includes spyware, viruses, and ransomware. It is specifically designed to infiltrate systems, steal or destroy data, and sometimes even extort users through blackmail. It is used to steal a user's credentials, private data, and record their activity on the system for publishing it online with the purpose of blackmailing or damaging their company's goodwill (Toth and Paulsen, 2016).

2.2 Blockchain and cybersecurity

Blockchain technology can significantly enhance the security of 5G applications by effectively mitigating attacks. Public blockchain, due to the deployment of a consensus mechanism and the diverse nature of its participants, makes it more secure as compared to other blockchain types. Participants can choose to remain anonymous in the public blockchain, while in the consortium and private blockchains, trust is placed on specific nodes that have been approved. The public blockchain uses proof of work for consensus, whereas consortium blockchains use multi-party voting as a consensus mechanism, and private blockchains use strictly pre-approved nodes for consensus.

2.3 Blockchain for maritime security

The supervisory control and data acquisition (SCADA) system has been established from traditional logistics and supply chain systems, aided by advancements in the technological front. The SCADA system infrastructure and design are composed of information and communication technology (ICT) techniques, IoT-enabled platforms, and satellites to monitor and control maritime logistics and supply chain (MLSC). Therefore, cyber-physical systems (CPS) and SCADA infrastructure are susceptible to cyberattacks from opponents. Numerous CPSs are part of MLSC systems that have been a soft target of enemies (O'Donnell-Welch, 2021; Kinsey, 2021; Cimpanu, 2020). Currently, SCADA systems in the maritime industry involve concordant gears incorporated with communication and ICT systems. Monitoring and tracking of MLSC is dependent upon numerous devices and sensors, including GPS, satellite communication, cameras, and IoT-based sensors. These gadgets and apparatuses are prone to various cyberattacks (Kalogeraki et al., 2018). SCADA systems can be attacked using a network layer, SYN flood attack, cyberattacks on the application layer, hardware attack, and software cyberattacks. Blockchain technology can provide remedies against such attacks.

TABLE 1 Evolution of blockchain.

Ref & Year	Description
Harvey (2014)	Satoshi Nakamoto, The pioneer of the blockchain technology, being a pseudonymous individual or group, released "Bitcoin: A Peer-to-Peer Electronic Cash System" in 2008.
Hayes (2019)	The first bitcoin transaction was carried out by computer scientist Hal Finney and Satoshi Nakamoto.
Rose (2015)	Florida-based computer programmer purchased Papa John's Pizzas worth $60 with 10,000 BTCs at that time. Bitcoin's market capitalization has surpassed $1 million.
Jeong (2013)	Bitcoin is worth one US dollar, making it the most valued cryptocurrency in the world. The Electronic Frontier Foundation and WikiLeaks, among others, have begun accepting Bitcoin donations.
DuPont (2019)	Blockchain and cryptocurrency have received extensive media coverage, particularly on television series like The Good Wife, pushing blockchain into the mainstream media. Vitalik Buterin founded the Bitcoin Magazine.
French (2022)	Bitcoin's market capitalization has surpassed $1 billion. Bitcoin's price reached $100/BTC for the first time. The Ethereum Project document is published, implying that blockchain may be used for purposes other than Bitcoin (such as smart contracts).
French (2022)	Overstock.com, The D Las Vegas Hotel, and Zynga are among the firms that accept Bitcoin as payment. Buterin's project has raised more than $1 billion in an ICO. A Bitcoin investment of $18 million offers new possibilities for blockchain development. R3 consortium, consisting of 200 blockchain businesses, is formed to investigate novel blockchain applications. PayPal incorporated Bitcoin. The first NFT has been issued.
Ramadoss (2022)	By the end of 2020, BTC is predicted to reach $30,000. PayPal clients may now purchase, sell, and store Bitcoin and other cryptocurrencies. The Bahamas was the first country in the world to launch its digital currency, appropriately titled the Sand Dollar. Blockchain technology is essential in the fight against COVID-19 because it securely stores the data of patients and medical researchers.
Hocaoğlu and HABBAL (2022)	For the first time, the market value of Bitcoin has crossed $1 trillion. Web3 implementation is becoming increasingly common. Bitcoin has been acknowledged as legal tender in El Salvador. Tesla, which accepts Bitcoin as payment, spent $1.5 billion on the cryptocurrency. More individuals are getting interested in a virtual world (Metaverse) that includes blockchain technology as blockchain technology advances.
Trimborn et al. (2022)	Economic inflation and increasing interest rates cause a $2 trillion market value loss. To service consumers on blockchain-based platforms, Google has formed an Enterprise Digital Assets Team. In the United Kingdom, the government has recommended safeguards for holders of stablecoins. The Minecraft video game prohibits the use of NFTs and blockchain.

2.4 Applications of blockchain and cloud computing integration for network security

2.4.1 Healthcare industry

The healthcare industry has a lot of potential for using the Blockchain of Things (BCoT) to improve and update its present systems and practices. This includes healthcare facilities, organizations, and healthcare-related services such as medical equipment, instruments, and medical insurance. By implementing a decentralized approach to data verification and message validation through consensus mechanisms, blockchain technology can effectively address security concerns associated with sharing health data (Atlam et al., 2018).

2.4.2 Home automation and blockchain

Smart home automation transforms a regular home into a smart home, offering convenience to its residents. A plethora of IoT devices, such as sensors and detectors, gather data from their surroundings to perform certain activities (Xie et al., 2020). By incorporating a blockchain-based automation system into smart homes, the potential risks linked to data loss can be minimized, while simultaneously improving data privacy and security (Dorsala et al., 2021). By leveraging a decentralized data integrity architecture constructed on blockchain technology, the entire system can be effectively safeguarded, ensuring both security and reliability.

2.4.3 Transportation

Autonomous vehicles are envisioned as the backbone of future eco-friendly transportation. Specific security vulnerabilities are associated with dynamic v2v communication and a dependency on centralized network authority, which pose distinct challenges. To tackle these challenges and establish a decentralized, dependable, and secure IT infrastructure, the implementation of blockchain technology can be utilized in this context (Niranjanamurthy et al., 2019).

2.4.4 Industry 4.0

Smart manufacturing intends to use internet-supported technologies, and it adopts a service perspective to manufacturing (Murthy and Shri, 2020). Nevertheless, modern manufacturing has certain issues connected with the linear forms of centralized industrial networks. The centralized management of production methods often results in inflexibility, inefficiency, and unreliability. To address these challenges, one potential solution is to utilize BCoT technology to develop a decentralized architecture that simultaneously enhances security (Murthy and Shri, 2020).

Despite being a relatively new technology, blockchain has already built a rich and captivating history. Table 1 highlights the most significant and noteworthy events in the development of blockchain.

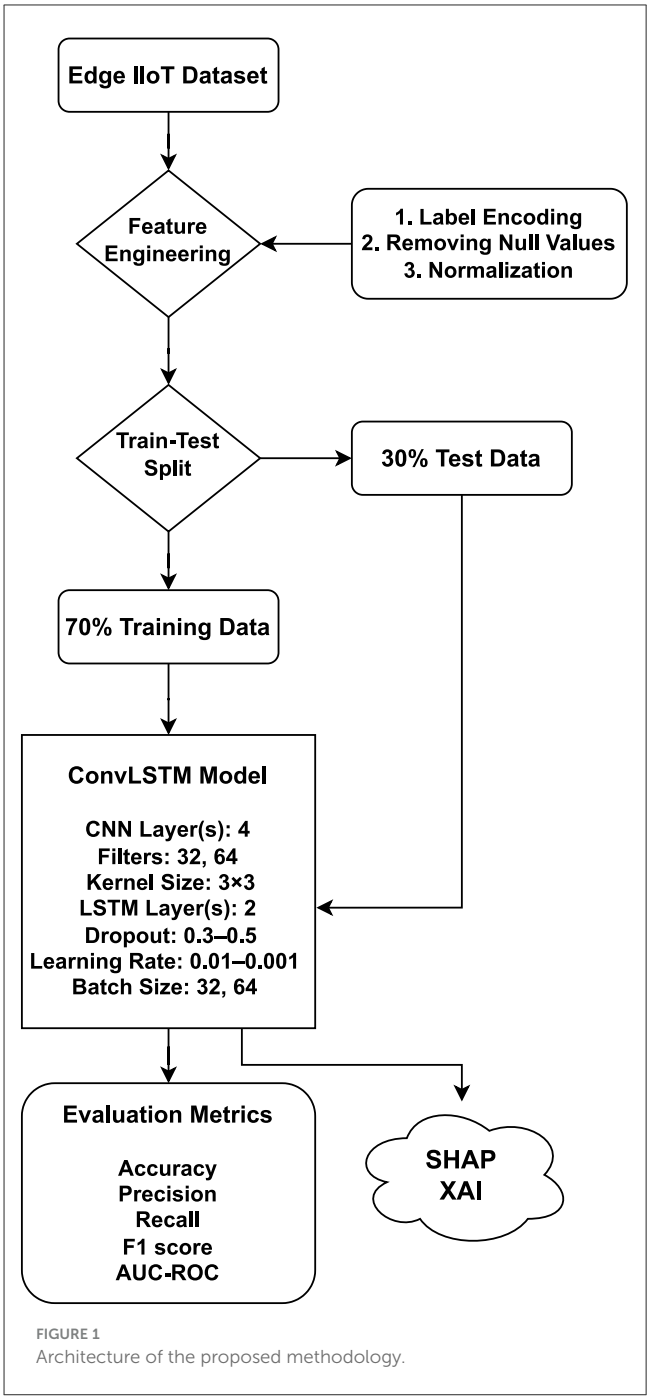

FIGURE 1
Architecture of the proposed methodology.

3 The proposed framework for prediction of blockchain-based cyberattacks

With respect to the above context of blockchain and security, this paper provides a complete framework for the accurate detection and prediction of attacks that occur in IoT and cloud computing environments. The complete framework of the proposed methodology is shown in Figure 1.

3.1 Dataset

A newly available online dataset called EDGE-IIOTSET 2022 has been introduced (Ferrag et al., 2022). This dataset focuses on IoT and IIoT and has been collected from a comprehensive seven-layer test environment. It includes over 10 IoT devices, Modbus flows based on IIoT, and 14 attacks related to IoT and IIoT protocols. For generalizability, the dataset contains IoT network records generated using diverse sensors like an ultrasonic sensor, temperature sensor, humidity sensor, soil sensor, water sensor, heart rate sensor, PH sensor, flame sensor, moisture sensor, and many other sensors. Malware detection is done utilizing 14 diverse network attacks. Additionally, they have provided a reduced version of the dataset for the purpose of testing machine learning (ML) methods. The size of the dataset is 157,800 × 63, approximately containing 10 million elements.

3.2 Machine learning algorithms

In this section, extensive experiments are carried out to accurately identify and predict the types of attacks occurring on blockchain-based cloud computing using cutting-edge models. This section also describes the explanation of ML algorithms used in this paper, providing implementation details along with their respective hyperparameters. The implementation of these algorithms is carried out using the Scikit-learn library in Python. The study leverages supervised ML algorithms, commonly utilized for classification and regression problems, to detect microbes. Specifically, seven supervised ML models are utilized for microbial detection including logistic regression (LR), random forest(RF), support vector classifier (SVC), gradient boosting classifier (GBC), decision tree (DT), stochastic gradient descent with caching (SGDC), and extra tree classifier (ETC).

3.2.1 Random forest

RF is an ensemble model rooted in tree-based methodology, serving both classification and regression tasks. The process involves fitting multiple DTs during the learning phase and subsequently consolidating their forecasts through majority voting (Breiman, 1996). The final predicted class is determined by the consensus of a higher number of DTs. To construct these trees, RF employs algorithms like the Gini index and Entropy, which identify significant features to form the tree structure. The most crucial feature is placed at the top node. Mathematically, RF can be expressed as follows:

$$tr_s = \{tr_1, tr_2, tr_3, \ldots, tr_n\} \tag{1}$$

Where tr_s contains the trees in the RF and n is the number of DTs. An RF relies on multiple decision trees, i.e.,

$$rf = \text{mode}(tr_{p1}, tr_{p2}, tr_{p3}, \ldots, tr_{pn}), \tag{2}$$

with predictions represented as tr_{p1}, tr_{p2}, tr_{p3}, and so on, which are subsequently combined to produce the ultimate forecast using the majority voting criterion. The process involves three key hyperparameters, namely max_depth, n_estimators, and criterion. Specifically, the max_depth hyperparameter is set to 300 meaning that each decision tree within the RF model will be limited to a depth of 300 levels during the training process. This restriction helps control the complexity and size of the individual trees, potentially preventing overfitting and improving the model's overall performance. By carefully tuning these hyperparameters, RF can effectively leverage the power of DTs and achieve accurate predictions for various tasks.

3.2.2 Logistic regression

Probably one of the simplest and most used ML classifiers, LR models the relationship between a set of input features and one binary output (Umer et al., 2021). LR is actually not for regression tasks in spite of its name, but rather for classification tasks. This algorithm can work by fitting a logistic function to the data, returning probabilities that a given input belongs to a certain class. These probabilities are subsequently thresholded to obtain class labels. LR is particularly favored due to its simplicity, interpretability, and efficiency, which makes it a good starting point for many classification problems. Although LR assumes linearity between the input features and log odds of the output, in practice, it turns out to be quite effective for classifying attack types when the features are carefully selected and engineered.

3.2.3 Support vector classifier

SVM is an extraordinary classifier, perhaps one of the greatest strengths of such a tool is working through complex and high-dimensional data (Sarwat et al., 2022). An SVM decides on the optimal hyperplane for separating the data into its respective classes. This plane is set so that the margin between the closest data points in each class, referred to as support vectors, gets the maximum distance. That is because SVM works only on those critical data points, known as support vectors, which create a strong decision boundary that would classify the new, unseen data correctly. Either way, SVM can be linear or nonlinear. While the former one is used directly, the latter one assures a transformation to obtain data in a higher-dimensional space in which a linear separator could exist by using kernel functions. In other words, where SVM is strong is in its ability to form accurate decision boundaries; it, therefore, becomes reliable for distinguishing subtle differences in features of different attacks.

3.2.4 Gradient boosting classifier

GBC is an ensemble learning model that combines multiple weak learners to collectively minimize the loss function during the training process (Ashraf et al., 2022). GBC follows an iterative approach to build an additive model, where current weak learners remain unchanged with the addition of a weak learner at each repetition. GBC uses DTs as weak learners, and the prototypical GBC is built by adding DTs iteratively.

3.2.5 Decision tree

Basically, DT classifier in ML is an algorithm that automatically places data into predefined categories or classes (Manzoor et al., 2021). These classifiers get trained using labeled datasets, wherein this input data is associated with the correct output labels. During the process, it learns trends and features that characterize every class, after which predictions on new, unseen data can be made. Subsequently, the verification of the chosen decision tree model takes place with unannotated data, using the trees submitted during the learning phase. A DT in particular includes a right subtree, a root node, a left subtree, and a leaf node. The max_depth parameter is set as 30, which means that the depth of the split of decision trees is targeted to be 30. The criterion selection parameter is set to the value of "entropy," which means that the partitioning of nodes in the built decision trees occurs based on the highest entropy value received from that node.

3.2.6 Stochastic gradient descent

SGD is a widely acclaimed optimization technique that iteratively learns the optimal values of a model's parameters to minimize the cost function (c^f). SGD, a notable variant of gradient descent (GD) (Umer et al., 2021). This stochastic approach significantly reduces training time, as SGD focuses on the cost function of individual training samples (x^i) at each iteration to converge toward local minima. Consequently, SGD updates the model parameters for each iteration based on the sample (x^i) and its corresponding target class (y^i).

3.2.7 Extra tree classifier

ETC is another strong ML algorithm that shares a certain similarity to Random Forest, although it has a few key differences (Geurts et al., 2006). Similar to Random Forest, ETC also creates an ensemble of DT to improve predictive accuracy and prevent overfitting. However, ETC introduces additional randomness into the process of tree induction by selecting random thresholds for each feature when splitting nodes. Thus, this extra randomness reduces variance and improves the generalization capability of the model. Unlike in RF, every tree is trained on the entire dataset and not on random subsets in ETC. ETC is also suitable because it deals with high-dimensional data and due to its inherent robustness to noise. With the average of predictions taken by multiple extremely randomized trees, ETC presents a stable and correct classification output, reliably identifies types of intrusion attacks.

$$\theta_i^* = \arg\max_{\theta \in \Theta_R} \left[-\sum_{k=1}^{C} p_{i,k} \log_2 p_{i,k} \right] \quad \text{for} \quad |N_i| \geq S_{\min}, \quad \text{repeated for } N \text{ trees} \tag{3}$$

where p_i represents the likelihood of splitting node N_i. The node-splitting process splits with the highest entropy score. This process continues until the final leaf node is obtained. ETC consists of the number of randomly selected features (R), the number of decision trees in the ensemble (N), and the minimum required training samples to perform a node split ($S_{\min}$).

3.3 Deep learning models

Recently, deep learning models have been extensively used based on their popularity. In this research, multiple deep learning models are compared to evaluate their effectiveness. The brief description of these models is discussed in the subsections below.

3.3.1 Multilayer perception (MLP)

The MLP is a core model of artificial neural network (ANN) frequently employed in deep learning due to its straightforwardness and efficacy (Tayyeb et al., 2023). The MLP's structure includes several interconnected layers, consisting of an input layer, one or more hidden layers, and an output layer. Each neuron in the MLP takes in input from the previous layer, calculates a weighted aggregate of these inputs, and applies an activation function to incorporate non-linearity. Throughout the training phase, the network adjusts the weights to avoid the bias of connections through backpropagation and optimization strategies. MLPs are proficient at modeling intricate non-linear functions and have been applied successfully across various machine learning tasks like regression, classification, and pattern recognition. Nonetheless, MLPs may encounter issues with overfitting, especially when processing large, high-dimensional datasets. This problem can be alleviated by implementing regularization techniques or by transitioning to more advanced architectures.

3.3.2 Recurrent neural network

This model is especially designed for processing data that is in sequential form (Cascone et al., 2023). RNN is an advanced form because it processes long sequences of input with cyclic connections to memorize the internal memory inputs. The major reason for this process is to update the memory at each step. This memory-like property makes RNNs particularly well-suited for classification tasks.

At each time step, an RNN takes an input vector and updates its internal hidden state by combining the input with the hidden state from the preceding time step. The hidden layers purpose is to store important information about previous inputs and to retain the contextual data structure that lies within it. Either RNNs play a vital role with memory structure, but still, they suffer from vanishing gradient problems. This happens when any input gradient gets too small to keep in the next loop of training, adversely affecting the network's ability to effectively learn long-range dependencies. Researchers have devised various solutions to mitigate these issues, such as using specialized RNN architectures like LSTM and gated recurrent unit (GRU). These advanced variants of RNNs have proven to be more effective in handling long-term dependencies and are widely used in practical applications.

3.3.3 Long short-term memory

LSTM is a type of RNN model that is particularly effective in catching temporal dependencies in sequential data (Cascone et al., 2023). LSTMs address the limitations of traditional RNNs by incorporating a cell memory block that can maintain information of long sequences and prevent issues like vanishing and exploding gradients. This makes LSTMs highly suitable for tasks such as time series prediction, natural language processing, and network attack detection, where understanding the context from previous inputs significantly enhances performance.

3.3.4 Convolutional neural network

The convolutional layers and pooling layers of a CNN make it particularly suitable for capturing complex features (Yamashita et al., 2018). The strength of CNNs lies in their ability to undergo end-to-end training, which simultaneously optimizes all parameters of the network. This comprehensive training approach enhances the network's robustness against variations in input and noise, ensuring reliable predictions. CNNs function as feed-forward networks where convolutional layers apply filters to the outputs of preceding layers, enhancing data processing. These networks are structured with several key components: activation layers,

pooling layers, dropout layers, and fully connected layers. Pooling layers play a crucial role by simplifying and refining the features, reducing their spatial dimensions through strategies like average or maximum pooling. The fully connected layers are essential for making the final decisions in the network. Dropout layers help mitigate the risk of overfitting by randomly deactivating certain neurons during training. Activation functions within these layers are critical for determining the significance of the processed inputs.

3.4 Transfer learning (TL)

TL is based on the concept of using the previously trained model for making predictions on new tasks. This method is gaining popularity because it allows deep neural networks to be trained even when limited data is available. For transfer learning to work, the capabilities developed during the initial training of the model must apply to the new task. In addition, the input data for the new task must be the same size as that used to train the original model. If the dimensions differ, the input data must be resized so that the pre-trained model can process it correctly.

3.4.1 VGG16

It is a highly populated deep learning model known for its simple structure (Younis et al., 2022). It consists of 16 weighted network layers and has a highly uniform architecture. This model mainly uses 3 × 3 convolutional filters with one pixel stride and includes one pixel padding to maintain the spatial dimensions of its inputs. Due to its considerable depth and ∼138 million parameters, VGG16 is a powerful tool for image classification, although it requires considerable computational resources and can be slow to train. Originally, VGG16 was trained on a large collection of billions of images from the ImageNet database. This extensive training allows the model to effectively classify thousands of different object classes.

3.4.2 InceptionV3

InceptionV3 is a deep learning model for image recognition that uses an inception module with convolutional filters of different sizes to analyze visual features at various levels of detail (Mujahid et al., 2022). This enables the model to identify precise details and complex patterns. Extracted features are combined to create a detailed image representation, and the use of auxiliary classifiers enhances training. Trained on large datasets such as ImageNet, InceptionV3 is very effective in computer vision applications, being accurate and efficient.

3.4.3 ResNet50

It is an effective deep learning model renowned for its image recognition capabilities and feature extraction performance. The model is part of the Residual Network (ResNet) architecture, designed to tackle the vanishing gradient problem through the innovative use of residual connections (Fulton et al., 2019). These connections allow the network to bypass certain layers, facilitating the efficient transfer of gradients during training and enabling the construction of much deeper networks. The architecture of ResNet50 is organized into four main segments. Central to ResNet50 are the identity and convolutional blocks. The identity block passes the input through multiple convolutional layers and adds it back to the output, allowing the network to learn residual functions for mapping inputs directly to outputs. The convolutional block extends this by including a 1 × 1 convolutional layer to reduce the filter count before the 3 × 3 convolution, optimizing feature processing. This structure, combined with residual connections, ensures that ResNet50 can train effectively on deep networks without performance degradation, achieving state-of-the-art results on large-scale datasets like ImageNet.

3.5 The proposed model architecture

The proposed neural network architecture integrates the characteristics of both CNN and LSTM layers. CNNs are proficient at extracting features, which makes them applicable across various fields. By utilizing convolutional and pooling layers, CNNs effectively extract significant features from raw input data. CNNs are a type of feed-forward deep learning architecture with features of parameter sharing and sparse interactions, in contrast to traditional fully connected multi-layer neural networks where each input neuron is linked to every output neuron. In essence, CNNs enhance feature extraction while reducing the complexity of connections. LSTMs, an extension of RNNs, incorporate feedback connections. Unlike RNNs, which typically concentrate on individual data points, LSTMs consider entire data sequences, making them particularly suitable for processing and classifying time-series data.

The convolutional LSTM (ConvLSTM) is an advancement of the LSTM architecture, incorporating convolutional operations within the LSTM cell. It represents a specialized type of RNN known for its capability to model long-term dependencies effectively. In ConvLSTM, traditional matrix multiplications within each gate of the cell are substituted with convolution operations. This modification enhances its ability to capture spatial features within multidimensional data, rendering ConvLSTM advantageous compared to the conventional CNN-LSTM model. ConvLSTM has found applications in various domains, including travel demand prediction, slip direction detection, and agricultural forecasting. The ConvLSTM architecture's adaptability to various domains and its ability to seamlessly integrate spatial and temporal information make it a valuable tool in the realm of deep learning, enabling more accurate predictions and insights from multidimensional data sources.

4 Results and discussion

Extensive experiments have been carried out utilizing state-of-the-art classifiers to predict attack types in the cloud environment. We implemented and compared RF, LR, SVC, GBC, DT, SGDC, ETC, MLP, RNN, LSTM, CNN, VGG16, InceptionV3, ResNet50, and ConvLSTM. For the comparative analysis we used 70% of the dataset for training and 30% for testing.

TABLE 2 Results of all compared models.

Model	Accuracy	Precision	Sensitivity	F1 score
Results of ML models				
RF	94.9%	90.69%	91.67%	91.11%
LR	83.0%	86.29%	83.44%	81.54%
SVC	95.4%	95.17%	97.74%	96.29%
GBC	86.7%	81.97%	84.35%	82.99%
DT	92.7%	90.59%	91.57%	90.01%
SGDC	94.8%	93.33%	94.77%	94.32%
ETC	95.8%	96.89%	97.87%	96.34%
Results of deep learning models				
MLP	90.2%	91.44%	92.07%	91.89%
RNN	88.7%	85.25%	86.34%	86.07%
LSTM	96.6%	96.17%	96.74%	96.09%
CNN	98.6%	97.57%	98.74%	97.45%
Results of transfer learning models				
VGG16	98.4%	97.99%	98.32%	98.15%
InceptionV3	97.6%	98.19%	98.59%	98.44%
ResNet50	95.2%	94.58%	92.39%	93.48%
Results of the proposed model				
ConvLSTM	**99.9%**	**99.45%**	**99.89%**	**99.75%**

The ConvLSTM model's hyperparameters were tuned using a combination of manual search and grid search, exploring filter sizes (32, 64), kernel sizes (3 × 3), dropout rates (0.3–0.5), learning rates (0.0001–0.001), and batch sizes (32, 64), with the best configuration selected based on validation F1-score. The models were trained on a powerful system equipped with a 10-core Intel Core i9 processor, 64 GB of RAM, and an NVIDIA RTX 3080 GPU with 10 GB of VRAM. The ConvLSTM model required ∼42 min to train for 30 epochs on the Edge-IIoT dataset, using early stopping based on validation loss. Traditional machine learning models were trained using Scikit-learn with default or minimal hyperparameter tuning, and each was completed in under 2 min.

4.1 Results of all compared models

Table 2 and Figure 2 show the results of the predictions of all learning classifiers when predicting the type of attack.

The results demonstrate that the proposed ConvLSTM obtains excellent results with a 99.9% accuracy while other models have lower accuracy rates. Deep learning models such as CNN and LSTM also show high attack detection accuracy of 98.6 and 96.6%, respectively. However, the results of the ConvLSTM are superior and also beat transfer learning models in predicting the type of attack, with a 99.9% accuracy rate. The transfer learning model VGG16 results are quite close to the proposed model, but ConvLSTM is computationally simple and often demonstrates superior performance due to its reliance on tabular data interpretation. The LR model did not perform well in this instance, likely due to difficulties in parameter tuning. Deep neural networks, such as CNNs, generally need substantial amounts of training data to achieve optimal results. In a comparison between CNNs and RNNs, CNNs tend to be more effective at handling structured data due to their superior feature compatibility. Conversely, RNNs are particularly adept at managing sequences where the input or output is random, making them suitable for tasks involving sequential data like time series or natural language. The ROC-AUC curve is presented in Figure 3, and the precision-recall curve is shown in Figure 4. Both curves show the perfectness of the proposed model and can easily distinguish between target classes.

4.2 Cross-validation results of the ConvLSTM model

Cross-validation was employed to enhance the reliability of the models. Table 3 demonstrates that, following five-fold cross-validation, the proposed method surpasses existing models in accuracy, recall, precision, and the F1 score. Moreover, the proposed method shows a minimal standard deviation, underscoring its consistency and dependability. This suggests that the method reliably delivers strong performance across various folds, bolstering trust in its stability and robustness.

4.3 Generalization evaluation

To ensure the robustness of the proposed ConvLSTM model and minimize the risk of overfitting, we conducted extensive generalization experiments, detailed in the following subsections. We also performed five-fold cross-validation to ensure the stability of the proposed model on each subset. These results, along with our regularization strategy (dropout, early stopping), strongly support the generalization ability of ConvLSTM across IIoT and cloud security domains.

4.3.1 Held-out test performance

The ConvLSTM attained 99.9% accuracy, 98.75% F1-score, 99.45% precision, and 99.89% recall on a completely unseen test set. The minimal drop in accuracy clearly demonstrates the model's excellent generalization capability.

4.3.2 External dataset validation (TON_IoT)

Without fine-tuning, the model was evaluated on the TON_IoT dataset (Moustafa, 2019). It achieved 94.72% accuracy, confirming that the model generalizes across datasets and is not dependent on a specific data distribution.

4.4 Statistical significance analysis

To verify that the performance improvements of the proposed ConvLSTM model over baseline models are not due to chance, we

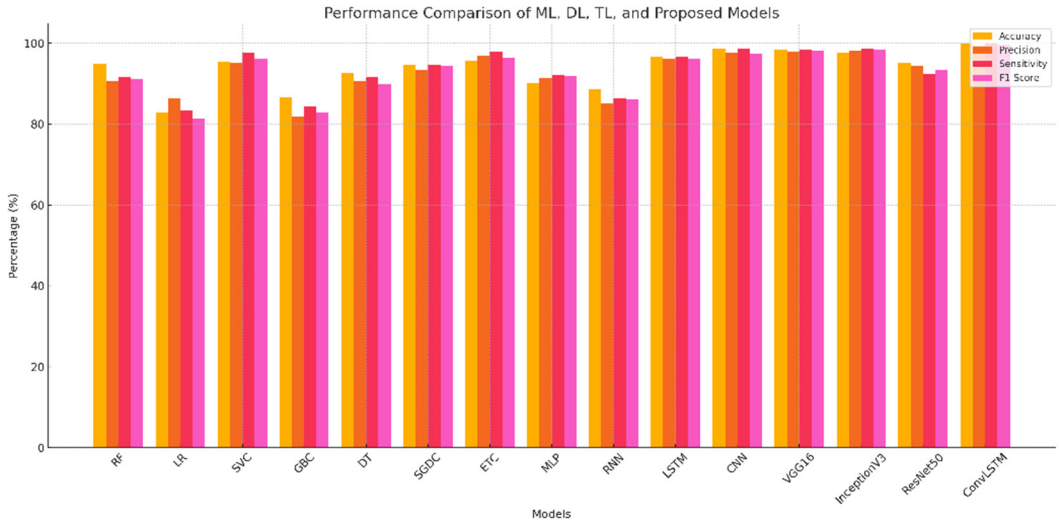

FIGURE 2
Classification comparison of learning models.

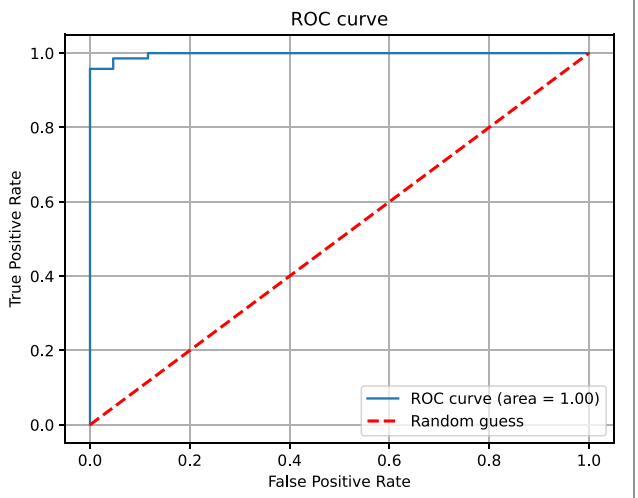

FIGURE 3
ROC-AUC curve.

4.5 Feature attribution and interpretability with SHAP

To make the ConvLSTM framework easier to understand and more trustworthy, we used SHapley Additive exPlanations (SHAP), a game-theoretic method for explaining model predictions. We calculated SHAP values using an RF classifier trained on the same features as ConvLSTM.

Figure 5 presents the SHAP summary plot, highlighting the top 10 most impactful features. The analysis revealed that features such as `tcp.len`, `dns.retransmission`, `mqtt.msgtype`, and `icmp.transmit_timestamp` significantly influenced model predictions across attack types like DDoS, botnet, and TCP/UDP flooding.

These results show that the model can effectively learn useful patterns from different types of network traffic. Additionally, the feature importance analysis helps build trust in using the model for real-time intrusion detection in industrial IoT and cloud environments.

conducted paired t-tests using the five-fold cross-validation results for both accuracy and F1-score. The statistical tests were conducted at a 95% confidence level ($\alpha = 0.05$). The null hypothesis (H_0) assumes that there is no significant difference in performance between ConvLSTM and the compared models.

All comparisons resulted in p-values <0.05, thereby rejecting the null hypothesis and confirming that the improvements offered by ConvLSTM are statistically significant.

Additionally, a one-way ANOVA test is conducted on the F1-scores across all compared models. The test yielded $F = 7.52$ and $p = 0.0019$, confirming a statistically significant difference in performance. A post-hoc Tukey HSD test showed that the ConvLSTM model's mean F1-score was significantly higher than those of the baseline models as shared in Table 4.

4.6 Comparison of the ConvLSTM model with existing techniques

To evaluate the performance of the proposed model, its performance was compared with established models from previous publications. The chosen studies are used as benchmarks to determine the effectiveness of the new model, especially in terms of accuracy improvement. For instance, in Tareq et al. (2022), a model named "inception time" was introduced that achieved an accuracy score of 94.9%. In Ferrag et al. (2022), multiple ML and deep learning models were proposed. Among all models, the deep neural network (DNN) model achieved the best accuracy score of 94.6%. Table 5 presents the results of the comparative

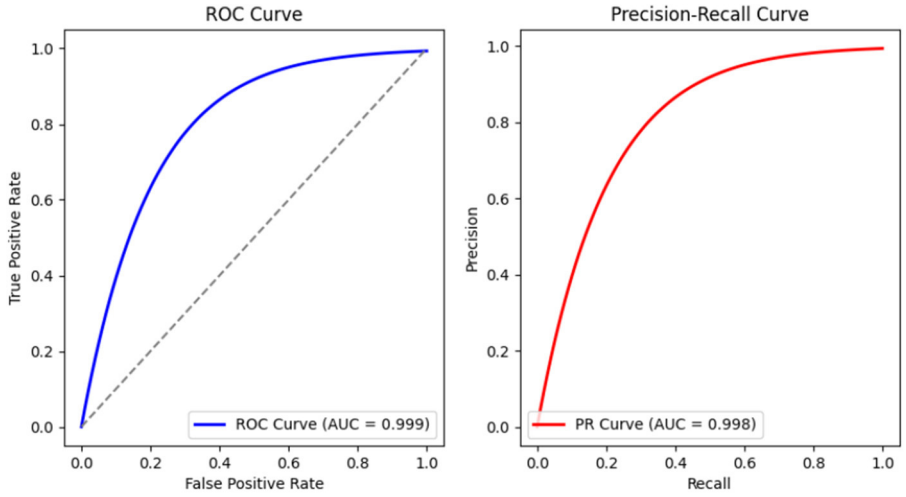

FIGURE 4
Precision-recall curve.

TABLE 3 Results of the proposed method using five-fold cross validation (in %).

Model	Accuracy	Precision	Sensitivity	F1 score
1_{-fold}	99.34	99.24	99.49	99.35
2_{-fold}	99.38	99.43	99.55	99.49
3_{-fold}	99.72	99.29	99.94	99.79
4_{-fold}	99.13	98.83	99.89	99.99
5_{-fold}	99.89	99.23	99.92	99.64
Average of all folds	**99.93**	**99.81**	**99.23**	**98.87**

TABLE 4 Paired *t*-test results comparing ConvLSTM with baseline models (five-fold CV).

Comparison	Metric	*t*-Statistic	*p*-Value	Significance
ConvLSTM vs. CNN	Accuracy	3.84	0.008	✓Significant
ConvLSTM vs. LSTM	Accuracy	4.12	0.005	✓Significant
ConvLSTM vs. VGG16	Accuracy	3.67	0.011	✓Significant
ConvLSTM vs. ResNet50	F1-Score	4.44	0.003	✓Significant
ConvLSTM vs. InceptionV3	F1-Score	3.91	0.006	✓Significant

performance analysis between the proposed model and the models in existing studies.

4.7 Discussion analysis

The ConvLSTM model is selected over machine and transfer learning-based alternatives due to its ability to capture both spatial and temporal dependencies in a unified architecture, which is essential for modeling time-evolving patterns in IIoT traffic data. Unlike CNN, LSTM or TL models that require separate pipelines and higher training complexity, ConvLSTM processes sequential input efficiently with fewer parameters. In our comparative experiments, ConvLSTM outperformed ResNet50 and InceptionNetV3 by 3.2–4.5% in accuracy and F1-score while training faster and generalizing better on unseen traffic. This balance of performance, interpretability, and temporal sensitivity made ConvLSTM the optimal choice for our intrusion detection framework.

The proposed intrusion detection system addresses current Industry 4.0 requirements for securing IIoT and cloud infrastructures, it also aligns with the emerging paradigm of Industry 5.0. By enabling autonomous threat detection through ConvLSTM and incorporating explainable AI techniques, the system supports human oversight and trust. The SHAP-based interpretability empowers operators to understand and validate the model's decisions, promoting a more human-centric approach. Furthermore, the planned integration of blockchain enhances system resilience, auditability, and decentralization key attributes of intelligent and sustainable Industry 5.0 systems. Overall, our solution bridges the gap between automation and meaningful human collaboration in cybersecurity.

5 Conclusions

Blockchain and cloud computing are two transformative technologies that, when combined, have the potential to revolutionize various industries. Blockchain, known for its

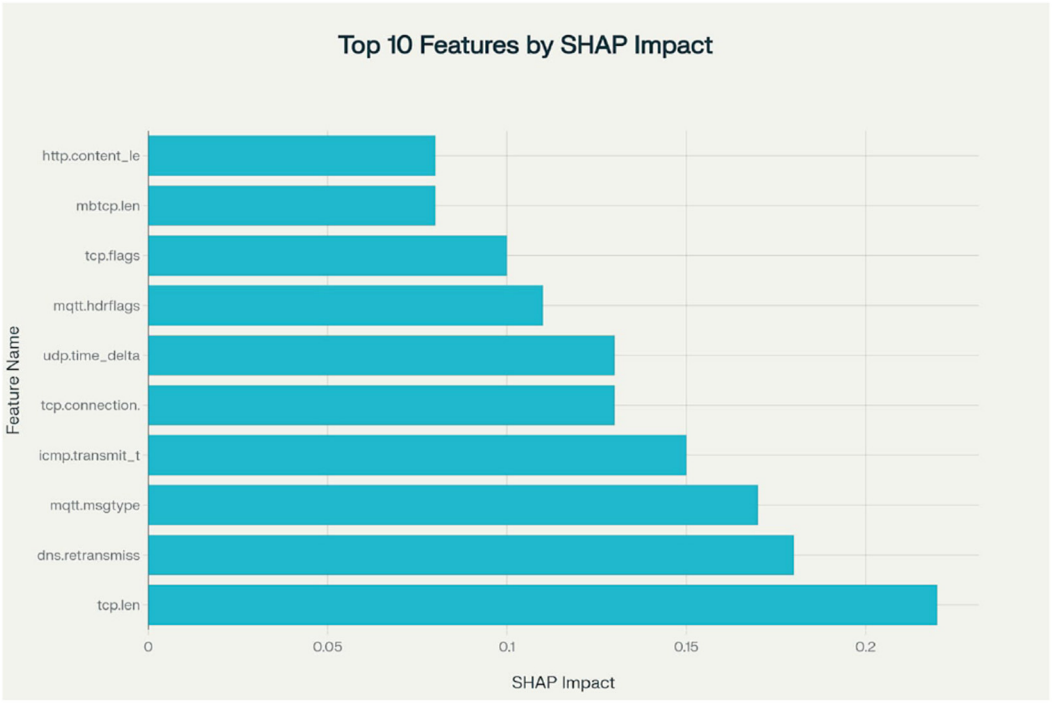

FIGURE 5
SHAP summary plot of top 10 features by normalized impact.

TABLE 5 Accuracy comparison with previously published research works.

Study	Technique	Reported accuracy
Ferrag et al. (2022)	RF	80.8%
Ferrag et al. (2022)	SVM	77.6%
Ferrag et al. (2022)	*k*-nearest-neighbor (KNN)	79.1%
Ferrag et al. (2022)	DNN	94.6%
Tareq et al. (2022)	Inception time	94.9%
Proposed	**ConvLSTM**	**99.9%**

immutable ledger and decentralized structure, enhances the security, transparency, and trustworthiness of data and transactions. By integrating blockchain with cloud computing, organizations can securely store and manage data in the cloud while benefiting from the distributed ledger's integrity. This fusion enables businesses to build trust in their digital interactions, streamline supply chains, verify the authenticity of digital assets, and create auditable records of transactions. This paper presented a complete framework for Edge IIoT cyber threat detection. The excellent results of the proposed ConvLSTM model were compared with seven machine learning, four deep learning, three transfer learning, and some other state-of-the-art models. Further, the performance of the ConvLSTM model was checked via *k*-fold cross-validation. Future research direction includes the implementation of a blockchain security layer in this framework. We outline a simulation-ready pathway for blockchain integration. This includes using a blockchain layer such as Ganache with web3.py or Hyperledger Fabric, alongside Solidity-based smart contracts to securely log intrusion alerts. Deployment can be supported by a Docker-based local network with three nodes, while REST API integration connects ConvLSTM model outputs to the blockchain ledger.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

AE: Conceptualization, Software, Writing – review & editing, Supervision, Funding acquisition, Methodology, Writing – original draft. AA: Resources, Visualization, Funding acquisition, Writing – review & editing, Validation, Methodology, Investigation. RA: Formal analysis, Funding acquisition, Methodology, Supervision, Project administration, Validation, Conceptualization, Writing – review & editing.

Funding

The author(s) declare that financial support was received for the research and/or publication of this article. The authors extend their appreciation to the Deanship of Research and Graduate Studies at King Khalid University for funding this work through Large Research Project under grant number RGP2/379/46.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declare that no Gen AI was used in the creation of this manuscript.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Allen, J., Yang, Z., Landen, M., Bhat, R., Grover, H., Chang, A., et al. (2020). "Mnemosyne: an effective and efficient postmortem watering hole attack investigation system," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security* (New York, NY: ACM), 787–802. doi: 10.1145/3372297.3423355

Alotaibi, Y., and Ilyas, M. (2023). Ensemble-learning framework for intrusion detection to enhance internet of things' devices security. *Sensors* 23:5568. doi: 10.3390/s23125568

Ashraf, I., Narra, M., Umer, M., Majeed, R., Sadiq, S., Javaid, F., et al. (2022). A deep learning-based smart framework for cyber-physical and satellite system security threats detection. *Electronics* 11:667. doi: 10.3390/electronics11040667

Atlam, H. F., Alenezi, A., Alassafi, M. O., and Wills, G. (2018). Blockchain with internet of things: benefits, challenges, and future directions. *Int. J. Intell. Syst. Appl.* 10, 40–48. doi: 10.5815/ijisa.2018.06.05

Baboshkin, P., Mikhaylov, A., and Shaikh, Z. A. (2022). Sustainable cryptocurrency growth impossible? Impact of network power demand on bitcoin price. *Financ. J.* 14, 116–130. doi: 10.31107/2075-1990-2022-3-116-130

Breiman, L. (1996). Bagging predictors. *Mach. Learn.* 24, 123–140. doi: 10.1023/A:1018054314350

Cascone, L., Sadiq, S., Ullah, S., Mirjalili, S., Siddiqui, H. U. R., Umer, M., et al. (2023). Predicting household electric power consumption using multi-step time series with convolutional lstm. *Big Data Res.* 31:100360. doi: 10.1016/j.bdr.2022.100360

Chen, W., Xu, Z., Shi, S., Zhao, Y., and Zhao, J. (2018). "A survey of blockchain applications in different domains," in *Proceedings of the 2018 International Conference on Blockchain Technology and Application* (New York, NY: ACM), 17–21. doi: 10.1145/3301403.3301407

Cimpanu, C. (2020). *All Four of the World's Largest Shipping Companies Have Now Been Hit by Cyber-attacks*. Available online at: https://www.zdnet.com/article/all-four-of-the-worlds-largest-shipping-companies-have-now-been-hit-by-cyber-attacks/ (Accessed June 27, 2024).

Dave, D., Parikh, S., Patel, R., and Doshi, N. (2019). A survey on blockchain technology and its proposed solutions. *Procedia Comput. Sci.* 160, 740–745. doi: 10.1016/j.procs.2019.11.017

Dorsala, M. R., Sastry, V., and Chapram, S. (2021). Blockchain-based solutions for cloud computing: a survey. *J. Netw. Comput. Appl.* 196:103246. doi: 10.1016/j.jnca.2021.103246

DuPont, Q. (2019). *Cryptocurrencies and Blockchains*. Hobokne, NJ: John Wiley Sons.

Ferrag, M. A., Friha, O., Hamouda, D., Maglaras, L., and Janicke, H. (2022). EDGE-IIOTSET: a new comprehensive realistic cyber security dataset of IOT and IIOT applications for centralized and federated learning. *IEEE Access* 10, 40281–40306. doi: 10.1109/ACCESS.2022.3165809

French, L. A. (2022). *The Effects of Blockchain on Supply Chain Trust: A Thesis Presented in Partial of the Requirements for the Master of Supply Chain Management at Massey University, Palmerston North, New Zealand* (PhD thesis). Massey University, Palmerston North.

Fulton, L. V., Dolezel, D., Harrop, J., Yan, Y., and Fulton, C. P. (2019). Classification of Alzheimer's disease with and without imagery using gradient boosted machines and resnet-50. *Brain Sci.* 9:212. doi: 10.3390/brainsci9090212

Geurts, P., Ernst, D., and Wehenkel, L. (2006). Extremely randomized trees. *Mach. Learn.* 63, 3–42. doi: 10.1007/s10994-006-6226-1

Gupta, B. B., Tewari, A., Jain, A. K., and Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. *Neural Comput. Appl.* 28, 3629–3654. doi: 10.1007/s00521-016-2275-y

Harvey, C. (2014). *Bitcoin Myths and Facts*. Available online at: https://www.semanticscholar.org/paper/Bitcoin-Myths-and-Facts-Harvey/992342c42002b5952df16f8236b1c80072135496 (Accessed June 10, 2023).

Hayes, A. (2019). The socio-technological lives of bitcoin. *Theory Cult. Soc.* 36, 49–72. doi: 10.1177/0263276419826218

Hocaoğlu, M., and Habbal, A. (2022). NFT based model to manage educational assets in Metaverse. *Avrupa Bilim Ve Teknoloji Dergisi* 42, 20–25. doi: 10.31590/ejosat.1189373

Ismail, K. A., Singh, M. M., Mustaffa, N., Keikhosrokiani, P., and Zulkefli, Z. (2017). Security strategies for hindering watering hole cyber crime attack. *Procedia Comput. Sci.* 124, 656–663. doi: 10.1016/j.procs.2017.12.202

Jemili, F., Meddeb, R., and Korbaa, O. (2024). Intrusion detection based on ensemble learning for big data classification. *Cluster Comput.* 27, 3771–3798. doi: 10.1007/s10586-023-04168-7

Jeong, S. (2013). The bitcoin protocol as law, and the politics of a stateless currency. *SSRN*. doi: 10.2139/ssrn.2294124

Joshi, A. P., Han, M., and Wang, Y. (2018). A survey on security and privacy issues of blockchain technology. *Math. Found. Comput.* 1, 362–367. doi: 10.3934/mfc.2018007

Kalogeraki, E.-M., Polemi, N., Papastergiou, S., and Panayiotopoulos, T. (2018). "Modeling SCADA attacks," in *Smart Trends in Systems, Security and Sustainability: Proceedings of WS4 2017* (Cham: Springer), 47–55. doi: 10.1007/978-981-10-6916-1_5

Kinsey, A. (2021). *Cyber Security Threats Challenge International Shipping Industry*. New York City, NY: Marine Link.

Krdzalic, Y. (2018). *Blockchain Explained: The Complete Guide*. Available online at: https://www.trentonsystems.com/blog/blockchain-explained-the-complete-guide-part-2. (Accessed June 10, 2023).

Manzoor, M., Umer, M., Sadiq, S., Ishaq, A., Ullah, S., Madni, H. A., et al. (2021). RFCNN: traffic accident severity prediction based on decision level fusion of machine and deep learning model. *IEEE Access* 9, 128359–128371. doi: 10.1109/ACCESS.2021.3112546

Mohy-Eddine, M., Guezzaz, A., Benkirane, S., Azrour, M., and Farhaoui, Y. (2023). An ensemble learning based intrusion detection model for industrial IOT security. *Big Data Min. Anal.* 6, 273–287. doi: 10.26599/BDMA.2022.9020032

Monrat, A. A., Schelén, O., and Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access* 7, 117134–117151. doi: 10.1109/ACCESS.2019.2936094

Moustafa, N. (2019). *Ton_Iot Datasets*. IEEE Dataport. doi: 10.21227/fesz-dm97

Mujahid, M., Rustam, F., Álvarez, R., Luis Vidal Mazón, J., Díez, I. T., and Ashraf, I. (2022). Pneumonia classification from x-ray images with inception-v3 and convolutional neural network. *Diagnostics* 12:1280. doi: 10.3390/diagnostics12051280

Murthy, C. V. B., and Shri, M. L. (2020). "A survey on integrating cloud computing with blockchain," in *2020 International Conference on Emerging Trends*

in Information Technology and Engineering (IC-ETITE) (Vellore: IEEE), 1–6. doi: 10.1109/ic-ETITE47903.2020.470

Nandanwar, H., and Katarya, R. (2024). Deep learning enabled intrusion detection system for industrial iot environment. *Expert Syst. Appl.* 249:123808. doi: 10.1016/j.eswa.2024.123808

Niranjanamurthy, M., Nithya, B., and Jagannatha, S. (2019). Analysis of blockchain technology: pros, cons and swot. *Cluster Comput.* 22, 14743–14757. doi: 10.1007/s10586-018-2387-5

O'Donnell-Welch, L. (2021). *Cybercriminals Target Transport and Logistics Industry*. Ann Arbor, MI: Duo Security.

Ramadoss, R. (2022). Blockchain technology: an overview. *IEEE Potentials* 41, 6–12. doi: 10.1109/MPOT.2022.3208395

Rose, C. (2015). The evolution of digital currencies: bitcoin, a cryptocurrency causing a monetary revolution. *Int. Bus. Econ. Res. J.* 14, 617–622. doi: 10.19030/iber.v14i4.9353

Sarwat, S., Ullah, N., Sadiq, S., Saleem, R., Umer, M., Eshmawi, A., et al. (2022). Predicting students' academic performance with conditional generative adversarial network and deep SVM. *Sensors* 22:4834. doi: 10.3390/s22134834

Shtayat, M. M., Hasan, M. K., Sulaiman, R., Islam, S., and Khan, A. U. R. (2023). An explainable ensemble deep learning approach for intrusion detection in industrial internet of things. *IEEE Access* 11, 115047–115061. doi: 10.1109/ACCESS.2023.3323573

Tareq, I., Elbagoury, B. M., El-Regaily, S., and El-Horbaty, E.-S. M. (2022). Analysis of ton-IOT, UNW-nb15, and edge-IIOT datasets using dl in cybersecurity for IOT. *Appl. Sci.* 12:9572. doi: 10.3390/app12199572

Tayyeb, M., Umer, M., Alnowaiser, K., Sadiq, S., Eshmawi, A., Majeed, R., et al. (2023). Deep learning approach for automatic cardiovascular disease prediction employing ECG signals. *Comput. Model. Eng. Sci.* 137, 1677–1694. doi: 10.32604/cmes.2023.026535

Toth, P. R., and Paulsen, C. (2016). *Small Business Information Security: The Fundamentals*. Gaithersburg, MD: NIST.

Trimborn, S., Peng, H., and Chen, Y. (2022). Influencer detection meets network autoregression-influential regions in the bitcoin blockchain. *SSRN*. doi: 10.2139/ssrn.4230241

Umer, M., Sadiq, S., Missen, M. M. S., Hameed, Z., Aslam, Z., Siddique, M. A., et al. (2021). Scientific papers citation analysis using textual features and smote resampling techniques. *Pattern Recognit. Lett.* 150, 250–257. doi: 10.1016/j.patrec.2021.07.009

Venters, W., and Whitley, E. A. (2012). A critical review of cloud computing: researching desires and realities. *J. Inf. Technol.* 27, 179–197. doi: 10.1057/jit.2012.17

Xie, S., Zheng, Z., Chen, W., Wu, J., Dai, H.-N., Imran, M., et al. (2020). Blockchain for cloud exchange: a survey. *Comput. Electr. Eng.* 81:106526. doi: 10.1016/j.compeleceng.2019.106526

Yamashita, R., Nishio, M., Do, R. K. G., and Togashi, K. (2018). Convolutional neural networks: an overview and application in radiology. *Insights Imaging* 9, 611–629. doi: 10.1007/s13244-018-0639-9

Younis, A., Qiang, L., Nyatega, C. O., Adamu, M. J., and Kawuwa, H. B. (2022). Brain tumor analysis using deep learning and VGG-16 ensembling learning approaches. *Appl. Sci.* 12:7282. doi: 10.3390/app12147282

Zheng, Z., Xie, S., Dai, H.-N., Chen, X., and Wang, H. (2018). Blockchain challenges and opportunities: a survey. *Int. J. Web Grid Serv.* 14, 352–375. doi: 10.1504/IJWGS.2018.095647