

# Blockchain-enabled collaborative anomaly detection for IoT security

Ananda Ravuri<sup>1\*</sup>, Dr.M. Sadish Sendil<sup>2</sup>, Moshe Rani<sup>3</sup>, A. Srikanth<sup>4</sup>, Dr.M.N. Sharath<sup>5</sup>, Dorababu Sudarsa<sup>6</sup>, and Koppuravuri Gurnadha Gupta<sup>7</sup>

<sup>1</sup>Intel Corporation, Hillsboro, Oregon 97124, USA

<sup>2</sup>Department of Emerging Technologies, Guru Nanak Institute of Technology, Ibrahimpatnam, Telangana, India, 501506

<sup>3</sup>Department of ECE, Hyderabad Institute of Technology and Management, India

<sup>4</sup>Department of EEE, Institute of Aeronautical Engineering, Hyderabad, India

<sup>5</sup>Rajeev Institute of Technology, Hassan, India

<sup>6</sup>Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, Andhra Pradesh, India, 522302

<sup>7</sup>Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur District, Andhra Pradesh, India, 522302

**Abstract.** Protection of the Internet of Things (IoT) has become a significant concern due to the widespread use of IoT technologies. Conventional Intrusion Detection Systems (IDS) have challenges when used in IoT networks because of resource restrictions and complexities. Blockchain Technology (BCT) has significantly altered organizations' financial behavior and effectiveness in recent years. Data security and system stability are crucial concerns that must be tackled in blockchain systems. The study suggests a mechanism called Deep Blockchain-Enabled Collaborative Anomaly Detection (DBC-CAD) for security-focused distributed Anomaly Detection (AD) and privacy-focused BC with smart contracts in IoT networks. A Modified - Long Short-Term Memory (M-LSTM) based Deep Learning (DL) algorithm with a multi-variable optimization approach has been used for the AD approach. The multi-variable optimization technique has been used to set the hyperparameters. The Ethereum framework creates privacy-focused BC and smart contract techniques that safeguard decentralized AD engines. The proposed M-LSTM model has the highest detection rate of 99.1%. The findings show the effectiveness of the proposed systems in identifying assaults on IoT networks.

## 1 Introduction to IDS and CAD

An IDS is created to identify hostile activities to safeguard the system or network being attacked. An independent IDS can protect a single target organization. Still, it cannot create links for interaction and exchange of notifications and incident data to safeguard large networks or IoT systems from highly dispersed attacks or attacks propagating across several

---

\* Corresponding author: Ananda.ravuri@intel.com, ananda.ravuri@gmail.com

domains. This work may be made easier with CAD [1]. A CAD offers a comprehensive perspective of massive networks, unlike solitary IDS, which monitors intrusion incidents at a specific location. The CAD's effectiveness lies in providing shared data of intrusion activities across various domains by exchanging attack details across dispersed IDS.

IoT is a composite of multiple levels, including the network layer [2]. The network layer architecture is rooted in the conventional tiers of web communication and primarily handles the flow of information packets between clients. The network layer in IoT design is intricate and susceptible, which results in several security concerns. Multiple security structures are implemented to tackle the security concerns [3]. Such frameworks and gadgets must be installed in the IoT architecture to address security concerns properly. Regrettably, most security procedures need significant processing power and storage [4]. Nevertheless, inexpensive authentication and encryption procedures may address the limitations.

The high quantity of nodes in the IoT, such as servers or components, is a primary factor contributing to security vulnerabilities [5]. An attack on one node might fail the entire network. Typical security concerns IoT systems encounter include botnets, Distributed Denial of Service (DDoS) attacks, ransomware, distant capturing, routing assaults, and data leaking. Using a firewall as the primary protection against attacks on IoT devices is unsuccessful because of the diversity and complexity of IoT designs.

Recently, IDS have become popular because of their strength. James [6] first presented the idea of an Anomaly Detection System (ADS) in 1980 and put out a specification. ADSs aim to identify intruders inside a certain region. Within an IoT setting, an intrusion refers to a host attempting to enter nodes without authorization. An ADS comprises three major characteristics: an agent, an evaluation engine, and an action component. The agent is only accountable for gathering details from the data channel by recording activities. The analytical engine detects evidence of infiltration and creates notifications. The reaction module operates based on the results it gets from the evaluation engine. Over time, ADS have improved in reliability and efficiency, although attackers have also created a wider range of attack methods to bypass these detection mechanisms.

Conventional ADS are not equipped to handle the many network levels of the IoT [7]. Recent advancements in automated systems have prompted investigators to use CAD together with a variety of Machine Learning (ML) techniques such as Artificial Neural Networks (ANN), DL, and Reinforcement Learning (RL). Conventional ANN have constraints when it comes to handling the intricacies of CAD. Addressing these deficiencies is essential for fulfilling the potential of CADs in practical applications.

## **2 Interrelated works of IDS, IoT, BCT**

CAD through BCT has become a promising strategy in the ever-changing field of IoT security. This literature review examines the latest progress and approaches suggested in this field, emphasizing the creative solutions shown in different research studies. Alharbi et al. (2023) introduced a framework for CAD systems in IoT networks based on BCT. The architecture enhanced malware detection precision and dependability by enabling collaborative threat information sharing using BCT [8].

Ali et al. (2024) reviewed Blockchain and federated learning-based intrusion detection methods for industrial IoT networks. The assessed methods probably improved intrusion detection accuracy, data privacy, and model security. Benefits include improved cooperation and confidentiality protection, while obstacles may involve the intricacy of deploying and overseeing blockchain-driven solutions in industrial environments [9].

Cui et al. (2021) suggested a federated learning method that enhances security and privacy for detecting anomalies in IoT networks. The strategy improved AD accuracy and privacy protection compared to centralized solutions [10]. Wei et al. (2021) presented an

altered blockchain DPoS consensus method incorporating anomaly detection and reward-punishment mechanisms. Benefits include enhanced resistance against assaults. However, drawbacks may include computational burden and implementation intricacy [11].

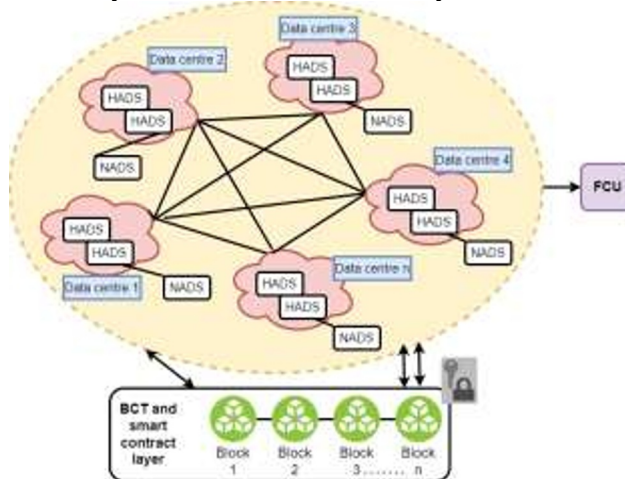
Li et al. (2023) introduced a security management system for CAD in smart cities that utilizes blockchain technology. The framework probably improved smart city contexts' danger detection and response capabilities [12]. Varela-Vaca et al. (2024) introduced a model for automated, reliable, collaborative procedures leveraging blockchain & IoT connectivity, specifically targeting fraud identification. The system most likely accomplished dependable cooperation and fraud detection capabilities across the collaborating organizations [13].

Abou El Houda and colleagues (2024) suggested using Blockchain-Enabled Federated Learning to improve CAD in Vehicular Edge Computing. The suggested technique is expected to improve intrusion detection accuracy and privacy preservation in-vehicle edge computing contexts [14]. Alkadi et al. (2020) developed a sophisticated blockchain-based collaborative intrusion detection solution to safeguard IoT and cloud networks. The system probably showed strong intrusion detection abilities and enhanced resistance against cyber-attacks [15]. Benefits include improved intrusion detection and teamwork, while obstacles may include computational burden and scalability issues.

The literature review has highlighted the increasing importance of using BCT for CAD to enhance the security of IoT systems. This study highlights several techniques and frameworks created to tackle the complex difficulties in IoT security, drawing on current research findings.

### 3 Proposed method

Building and deploying the suggested CAD on any computer architecture is possible because of its virtualization technology and diversified approach. Many cloud service providers can share warning information and log files about hazardous software activity. The usefulness of shared data is severely restricted if such intrusion detection solutions are unreliable and properly integrated. When developing a CAD for the cloud, several obstacles are brought about by the peculiarities of cloud computing. Effective detection of internal and external assaults with minimal False Positives (FP) and False Negatives (FN) is one of the desirable attributes. The capacity to fluctuate over the whole cloud's network of data centers. The framework would guarantee data privacy, reliability, and consistency across all CAD nodes, offering maximum security resistance to combat zero-day attacks.



**Fig. 1.** The framework of a cloud-based CAD network

To illustrate how Host-based ADS (HADS) and Network-based ADS (NADS) operate together to apply AD analysis at the virtual machine and network levels, Fig. 1 depicts a cloud-based CAD network framework. Through implicit trust, several ADS inside the same cloud domain work together to exchange information or notify intrusion occurrences. On the other hand, in instances of collaboration or treachery attacks, malevolent nodes might skew the results and make alert aggregation less effective. The privacy of information during live transfer across multiple cloud providers is an increasing problem in CAD. Attacks attempting to change data, logs, or transmissions are also a concern.

A BCT transaction is shared across participant network nodes to hold the unprocessed alarm data provided by the ADS. As a result, they may be safely archived in the Fundamental Controller Unit's (FCU) directory structure for future use for regulation and forensic inquiry. Before adding transactions to the ledger blocks indefinitely, each player (cloud data center) executes a consensus process to ensure they are legitimate. This approach verifies that the FCU database contains only legitimate alerts, making it resistant to tampering and transparent so that cloud suppliers can see where their information is on the BCT.

To better monitor identity, especially in a blockchain that is accessible to everyone, each CAD member data center node must first build a smart contract that is linked to other nodes via a registry-based category. The smart contracts are organized on each ADS within the cloud-based BCT network. Based on regulations set in the smart contract, each participant ADS node may pick which partner node to trade data with, considering factors like country code, location, zone, and kind of company. A data center or cloud provider can't join the CAD system unless it registers with the FCU and gets an identification number consisting of private and public keys.

With DBC-CAD, data interchange is quick, alarms are correlated, and recorded security incidents are fully understood. Forecasting capabilities are also provided. Also, by integrating smart contracts into the BCT, a data security framework may be established to control recognized alarms according to predetermined criteria.

In addition, the decentralized FCU may process a tiny piece of the ledger off-chain, which means that resource-constrained device nodes only need to retain a limited portion. This is made possible by the intrinsic capabilities of the BCT and smart contract-based systems. In this way, IoT devices may validate and distribute the validity of notification events throughout a BCT by acting as lightweight clients. On the other hand, the decentralized FCU processes all incoming transactions and keeps the whole blockchain ledger as a miner node; therefore, it requires a high hash rate. Lastly, the DBC-CAD results are received and placed on it sequentially to guarantee the Blockchain's inviolability and durability.

### **3.1 DL-based CAD using M-LSTM**

M-LSTM networks have become an effective tool for CAD facilitated by BCT in IoT security. Using M-LSTMs' capacity to recognize temporal relationships and the sequential structure of IoT data streams, this method makes it easier to spot unusual patterns that might be signs of security breaches in IoT networks. AD becomes more of a collaborative process with BCT's help, allowing dispersed IoT devices to share data and reach a consensus safely. Anomaly detection can be done more accurately and faster using M-LSTM-based models since they can capture long-range relationships in IoT data.

LSTM and M-LSTM are functionally and architecturally identical; the main difference is that M-LSTM uses many variables. The multi-variable optimization technique was used to set the hyperparameters. An LSTM model is an RNN version. Several industries have used this well-known predictive time series architecture, which successfully combines data with future predictions. The LSTM's internal architecture is similar to the RNN's as it is a variant of the RNN. A substitute for time series prediction, the inner layer connection enables the

information to be transported back and forth. Separating rules and making predictions about future data points is the job of the RNN-based prediction model. Given its use in backpropagation, it is also likely to impact weight updates significantly. The existing RNNs are limited by the gradient vanishing limitation, whereas LSTM gets around that. LSTM has three gates: the input gate, the output gate, and the forgotten gate. The addition of the forgetting gateway is what makes LSTM effective in reducing the impact of gradients. The LSTM also benefits greatly from the memory cell. The following equations are used as activation functions in all three gates of LSTM:

$$Fg_u = \beta[X_{fg} \times (H_{u-1} + y_u) + v_{fg}] \quad (1)$$

$$It_u = \beta[X_{it} \times (H_{u-1} + y_u) + v_{it}] \quad (2)$$

$$Ot_u = \beta[X_{ot} \times (H_{u-1} + y_u) + v_{ot}] \quad (3)$$

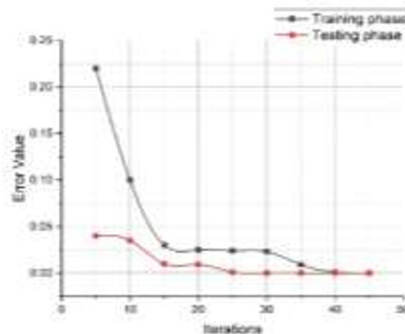
Equations denote the forgetting, input, and output gate functions (1)-(3). The elements in this equation are the sigmoid function ( $\beta$ ), the weight function ( $X$ ), the input value ( $y$ ), the secret state ( $H$ ), and the partial vector ( $v$ ). When training RNNs, batch size is crucial. It reveals how many samples were used for the system's loading update.

The hyperparameters of prediction algorithms are a good way to ensure their accuracy. This means that the parameters of the model need to be custom-made. This page offers optimum values for the duration, batch size, and window size parameters. Because of their great efficiency, algorithms inspired by nature are preferred by researchers. However, these methods are inherently unpredictable and need careful selection of the input factors, such as population density, productivity, and elevation. The various variables will either enter a local optimum or need more processing time without precise calibration. Given these challenges, this work has used the multi-variable optimization method for LSTM optimization. This method is easy to implement and does not need any tuning variables.

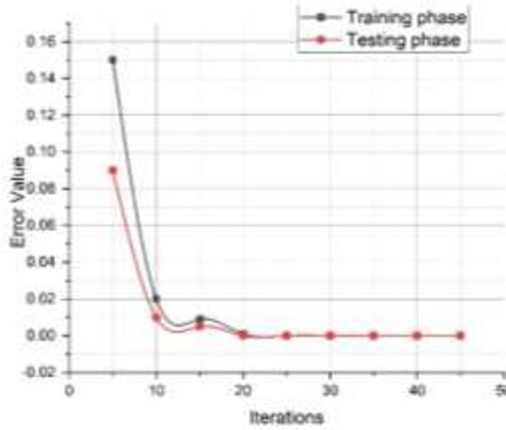
Finally, the M-LSTM model has been constructed, trained, and validated to categorize attack events efficiently. The Python software Keras DL was used to construct the M-LSTM model. The dataset has been split into two: 1) training, which accounts for 80% of the total, and 2) testing, which accounts for 20%. During the implementation, M-LSTM yields the most accurate model for detecting errors. It was trained to analyze each row of the testing data set to evaluate the model. After that, each row is labeled as an attack or regular record.

## 4 Results and discussion

The suggested DBC-CAD has been tested using the BoT-IoT network database [16]. Parameters like accuracy, detection rate, and processing time have been analyzed to measure how well CAD works. Several ML techniques, including Support Vector Machine (SVM), Random Forest (RF), and Naive Bayes (NB), have been evaluated with the M-LSTM-based CAD model.



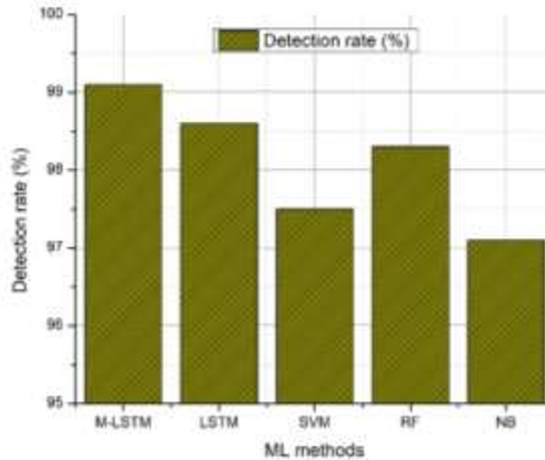
(a) LSTM



(b) M-LSTM

**Fig. 2.** Error value for (a) LSTM and (b) M-LSTM during the training and testing phase in the proposed DBC-CAD framework

Fig. 2 depicts the error value for LSTM and M-LSTM during the training and testing phase in the proposed DBC-CAD framework. The number of iterations in which the error value has been evaluated has increased. The accuracy of the model is assessed using RMSE. Furthermore, the test and train's accuracy decreases with large error values during the first iteration. However, the accuracy greatly improves, and the error value drops as the number of repetitions rises. When the number of iterations approaches 25 or 20, respectively, the test errors in the LSTM and M-LSTM reach zero. Consequently, it has been determined that the suggested M-LSTM algorithm has been appropriately trained to identify AD.



**Fig. 3.** Detection rate (%) of the proposed M-LSTM against other ML methods in the DBC-CAD framework

Within the DBC-CAD framework, the detection rates (%) attained by several machine learning (ML) techniques, such as M-LSTM, LSTM, SVM, RF, and NB, are shown in Fig. 3. The proposed M-LSTM model has the highest detection rate, which is 99.1%. This indicates that it performs better than other approaches like LSTM (98.6%), SVM (97.5%), RF (98.3%), and NB (97.1%). This demonstrates the M-LSTM approach's efficacy in precisely detecting anomalies and highlights its potential as a reliable AD solution inside the DBC-CAD framework.

## 5 Conclusion

The article proposes a Deep Blockchain-Enabled Collaborative Anomaly Detection (DBC-CAD) method for security-oriented distributed AD and privacy-oriented Blockchain with smart contracts in IoT networks. An M-LSTM-based DL algorithm using multi-variable optimization for the AD method has been employed. The hyperparameters were established using a multi-variable optimization approach. The Ethereum framework is used to develop privacy-centric Blockchain and smart contract methods that protect decentralized AD engines. The proposed M-LSTM model achieves a detection rate of 99.1%, the highest among the ML models. The results demonstrate the efficacy of the suggested solutions in detecting attacks on IoT networks.

## References

1. K. Bai, A. Zhang, Z. Li, R. Heano, C. Wang, L. Carin. *Collaborative Anomaly Detection*. arXiv preprint arXiv:2209.09923, (2022)
2. H. Tahaei, F. Afifi, A. Asemi, F. Zaki, N.B. Anuar. *The rise of traffic classification in IoT networks: A survey*. J Netw Comput Appl., **154**, (2020)
3. S. Hajiheidari, K. Wakil, M. Badri, N.J. Navimipour. *Intrusion detection systems in the Internet of things: A comprehensive investigation*. Computer Networks, **160**, 165-191, (2019)
4. M.G. Samaila, M. Neto, D.A. Fernandes, M.M. Freire, P.R. Inácio. *Challenges of securing Internet of Things devices: A survey*. Security and Privacy, **1**, 2, (2018)
5. S. Bhattarai, Y. Wang. *End-to-end trust and security for Internet of Things applications*. Computer, **51**, 4, 20-27, (2018)
6. A.M. Chu, M.K. So. *Organizational information security management for sustainable information systems: An unethical employee information security behavior perspective*. Sustainability, **12**, 8, (2020)
7. V. Ponnusamy, M. Humayun, N.Z. Jhanjhi, A. Yichiet, M.F. Almufareh. *Intrusion Detection Systems in Internet of Things and Mobile Ad-Hoc Networks*. Comput Syst Sci Eng., **40**, 3, 1199-1215, (2022)
8. S. Alharbi, D. Alghazzawi, A. Hakeem, L. Mohaisen, L. Cheng, A. Attiah. *A Blockchain-Based Collaborative Intrusion Detection Systems Framework*. IEEE Internet Things J., (2023)
9. S. Ali, Q. Li, A. Yousafzai. *Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: A survey*. Ad Hoc Netw., **152**, (2024)
10. L. Cui, Y. Qu, G. Xie, D. Zeng, R. Li, S. Shen, S. Yu. *Security and privacy-enhanced federated learning for anomaly detection in IoT infrastructures*. IEEE Trans. Ind. Inform., **18**, 5, 3492-3500, (2021)
11. Y. Wei, L. Liang, B. Zhou, X. Feng. *A modified blockchain DPoS consensus algorithm based on anomaly detection and reward-punishment*. In 13<sup>th</sup> International Conference on Communication Software and Networks (ICCSN), 283-288, (2021)
12. W. Li, C. Stidsen, T. Adam. *A blockchain-assisted security management framework for collaborative intrusion detection in smart cities*. Comput. Electr. Eng., **111**, (2023)
13. Á.J. Varela-Vaca, R.M. Gasca, D. Iglesias, J.M. González-Gutiérrez. *Automated trusted collaborative processes through blockchain & IoT integration: The fraud detection case*. Internet of Things, (2024)

14. Z. Abou El Houda, H. Moudoud, B. Brik, L. Khoukhi. *Blockchain-Enabled Federated Learning for Enhanced Collaborative Intrusion Detection in Vehicular Edge Computing*. IEEE Trans. Intell. Transp. Syst., (2024)
15. O. Alkadi, N. Moustafa, B. Turnbull, K.K.R. Choo. *A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks*. IEEE Internet Things J., **8**, 12, 9463-9472, (2020)
16. N. Koroniotis, N. Moustafa, E. Sitnikova, B. Turnbull. *Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset*. Future Gener. Comput. Syst., **100**, 779-796, (2019)