A Novel Behavioral Monitoring based Trust Model for enhancing Edge Security using Adaptive Neuro-fuzzy Inference System

D. Jayakumar[1,*], K. Santhosh Kumar[2]

[1]Research Scholar, Department of Computer Science and Engineering, Annamalai University, Chidambaram, Tamilnadu, India

[2]Assistant Professor, Department of Information Technology, Annamalai University, Chidambaram, Tamilnadu, India

Email: jayakumarifetd@gmail.com; santhosh09539@gmail.com

Abstract

The Internet of Things (IoT) is in a recent state of instability due to the flooding of virtual data. It is believed that IoT and cloud computing have met their maximum thresholds and loading them with data after this point will only deteriorate their performance. Hence, edge computing has been introduced to mitigate the processing burden of IoT. To meet the security demands of edge computing, we intend to combine the method of blockchain along with edge computing for a better solution. Accordingly, this paper proposes the introduction of a novel blockchain model that is based on artificial neural networks and trust estimation called the behavioral monitoring trust estimation model. Performance metrics such as accuracy, precision, recall, and F-measure are calculated under normal conditions and under the injection of attacks like false data injection, booting attack, and node capturing. The proposed behavioral monitoring trust classification model is compared with existing classifiers like Naive Bayes, K-nearest neighbor, Auto Encoder, Random Forest, and Support Vector Machine, and is found to have improved performance. Additional evaluation parameters like execution time, encryption time, storage cost, computational overhead, energy efficiency, and packet drop possibility are also calculated for the proposed model and compared with existing blockchain techniques of Bitcoin, Ethereum, Hyperledger, Direct and indirect trust model, and mutual trust chain based blockchain model. The proposed model achieved an accuracy of 95%, a precision score of 90%, a recall score of 94%, and an F-measure of 94% indicating superior performance.

Keywords: Behavioral Monitoring; Trust; ANFIS; Edge Computing; Blockchain; Naive Bayes; K-nearest neighbor; Auto Encoder; Random Forest; Support Vector Machine

1. Introduction

A recent survey that has been conducted by the research firm Gartner says that 10 percent of cloud processing requests are being handled by anonymous entities outside the cloud [1]. It is predicted that this percentage of outsourcing of data storage and processing will reach a maximum of 75% in 2025. This is a clear indication of the degradation in performance of both cloud computing and IoT. But, both technologies are not to be blamed explicitly for this degradation. The only reason that could be accomplished for this performance degradation is the magnanimous upsurge of data that has been entering the network. Despite many recent improvements cloud centers are not able to achieve their guaranteed response time. This is because of the underlying traffic and processing overhead involved [2]. The characteristics of IoT that make it vulnerable to attacks are device heterogeneity, constrained resources, incessant reactions, dynamic infrastructure, no context awareness, diverse applications, and an attack-prone surface.

DOI: https://doi.org/10.54216/FPA.170204
Received: January 18, 2024 Revised: April 11, 2024 Accepted: September 15, 2024

Edge computing will remove this processing overhead from IoT and take it to the edge of the network as much as possible [3]. Experts opine that edge computing should be seen as an architectural improvement and a new kind of topology of data distribution and processing rather than seeing it as a new technology. Edge computing involves content caching and virtualization sometimes. Moving the processing overhead to the edge of the network means the required data should travel in the network to the particular node where processing is being done which requires special security mechanisms which unfortunately edge computing fails to provide. Likewise, measures like efficiency, scalability, speed, and reliability need to be addressed while implementing an edge computing framework [4]. The major risks involved in edge computing are data overflow, cost and complexity, reduced security, enhanced risk of privacy, interoperability constraints etcetera. This is where the blockchain comes into the scenario.

Blockchain which is believed to be the state-of-the-art data storage technology, transforms the traditional process of centralized data storage into a decentralized one which has way beyond advantages. Data giants like Singapore Exchange Limited, Sony Music of Japan, and Amazon retail services have shifted to blockchain technology in recent days [5]. Blockchain is capable of storing transactions and data in a chronological manner that cannot be tampered with and hence can achieve considerable security levels. It is usually used in types of business that involve transactions, payments, orders, and accounts that claim data as its lifeline. The immutable and tamper-proof nature of blockchain has made it such a prevalent security approach.

The main aspects of blockchain technology are easy auditability, decentralized storage, data anonymity, and network transparency. There are many types of blockchain networks available based on the area of application such as public blockchains, private blockchains, hybrid blockchains, permissioned blockchains, and consortium blockchains each having a bit of variation amongst themselves [6]. Blockchain is sometimes referred to as distributed ledger technology.

The architecture of a blockchain consists of multiple chains and each chain is composed of several blocks of transactions that have been recorded in the network on a time-stamped basis. The basic elements of each block comprise a header, number used only once (Nonce), transaction data, hash value, and address of the previous block [7]. It is to be noted that no particular person in the network can claim to be the owner of any block or any chain. Everything is publicly available but still immutable as making any simple change to any block will modify its hash value and this transformation will be reflected in the other blocks too. Hence, it is very easy to identify any such malpractices by attackers. There are many layers in a blockchain architecture such as the infrastructure layer, data layer, consensus layer, network layer, and application layer. There are many types of consensus available like proof of work, proof of stake, proof of capacity, and proof of elapsed time.

2. Literature Survey

Bocek, et al. [8] explain the various key areas in which blockchain can be successfully used such as the pharma supply chain and much more. This study provides a brief review of how blockchain should be used, where to use and where not to use etc. The study elaborates on the use of various blockchain management techniques such as fraud detection, identity management, document verification, and many others. The authors suggest the use of modum.io AG which is a blockchain architecture that consists of Ethereum blockchain network servers and mobile devices connected to the network. Smart contracts and sensors are attached to them and it is used for analyzing transactions that happen in medicinal products logistics.

Dorri, et al. [9] explain the need for an optimized blockchain technology for IoT framework. The authors have introduced a novel type of blockchain that has been specially designed for the usage of IoT devices, especially on a smart home architectural basis. The components of a blockchain-based smart home will include a smartphone, cloud network, and cloud storage. Various operations like storing data, accessing devices remotely, and monitoring them offline can be performed in this network. The underlying network is susceptible to attacks like modification, dropping a message, appending, denial of service, anonymity threats, etc.

Cao, et al. [10] presented a survey on the prevailing edge computing technologies and described the similarities and differences that exist between the two technologies of cloud computing and edge computing. Cloud computing is more global in the application domain, edge computing is considered to be a local one and the network bandwidth of cloud computing is more compared to that of edge computing. Cloud computing is more real-time in nature whereas edge computing is very low in real-time applications. The calculation mode seems to be large and centralized for cloud computing and small and disintegrated for edge computing The vital technologies that support the implementation of edge computing are mobility management, traffic offloading decision support, network control, key resource

DOI: https://doi.org/10.54216/FPA.170204
Received: January 18, 2024 Revised: April 11, 2024 Accepted: September 15, 2024

allocation, searchable encryption, caching possibilities, authentication switch, cross-domain platform, access control based on attributes and roles, etc.

Shala, et al. [11] explain the relationship that exists between blockchain technologies and trust management services. For making the IoT a decentralized service provider, the authors proposed robust trust metrics such as service rating and testing, response time for a request, rate of acceptance of service, uptime and downtime, the satisfaction of the requestor, maximum number of participation in the network and functional analysis of individual nodes. They proposed a new trust model based on these trust metrics that is well-suited for blockchain and IoT systems. The proposed model is compared with the existing trust models under the scenarios of bad-mouthing attacks, malicious attacks, ballot stuffing attacks, etc and the proposed trust model seems to produce more promising results than the existing ones.

Christidis & Devetsikiotis [12] introduced the concept of smart contracts that enable the integration of blockchains and the Internet of Things together. They define smart contracts as self-enforcing rules that do not depend on any background network conditions to be fulfilled. It can analyze itself and know when to apply and when not to apply. The paper also explains the basic structure of a blockchain, models of consensus that are used in a blockchain, and also deals with working modes of smart contracts. It describes the taxonomy of blockchain and several deployment scenarios where blockchain and IoT could be successfully integrated. The authors strongly believe that the integration of blockchain and IoT will be very powerful and bring about many notable revolutions in the technology domain.

Idrees, et al. [13] put forward the security concerns that blockchain technology could possibly face. The fields of blockchain include supply chain, logistics management, medical management, healthcare cargo, sporting, law enforcement, banking and finance, traffic management, manufacturing industries, and business authentication. The authors also elaborated on the methods that are used by blockchain systems for overcoming security threats such as homomorphic encryption and decryption, digital signature anonymity, multi-party security, zero-knowledge proof systems, etc. The paper clearly explains the opportunities that are available for blockchain in the above-mentioned industries along with the shortfalls that will be faced. The authors have also provided all possible solutions for overcoming the proposed challenges so that blockchain could emerge as a massive and powerful technology in the future.

Bhushan, et al. [14] have presented a study that portrays the architecture of BIoT that is nothing but the combination of blockchain and the Internet of Things. The basic requirements for such an integration, applications, advantages, and future modifications needed are explained by the authors. The IoT protocols stack consists of the application layer, session layer, transport layer, network layer, communication layer, and physical layer. The possible attacks that could enter the combined network could be device compromise, cloning of nodes, cyber-attacks, injection attacks, private data exposure, black hole attacks, brute force attacks, wormhole attacks, collision attacks, and much more. The authors firmly believe that the success of BIoT lies in its novel properties such as transparent audit, sequential data updates, no third-party involvement, peer-to-peer communication, and distributed and decentralized nature of services.

Al-Rakhami & Al-Mashari [15] have proposed a new blockchain trust system for use in the supply chain management. This paper concerns how blockchain and IoT can be merged and proposes a new trust model for the integration. The proposed work is simulated showcasing edge performance and security. The proposed trust model is based on three behaviors such as node authentication, message authentication, and node supervision. The IoT network is connected to supplier management, transporters, retailers, and other entities that belong to the supply chain. A node is considered to be authentic, suspicious, or malicious based on its behavior. The blockchain network uses a proof of work consensus model and takes up to 4.2 seconds to add 10 blocks to the created chain.

Ali, et al. [16] proposed a new trust-based blockchain model functioning on behavioral monitoring. It also measures trust zone levels. The role of the behavior monitor is to monitor the activity of every device connected to the network and analyze them with the help of autoencoders. The proposed model also uses trusted execution technology Intel SGX for achieving a secure environment. To evaluate the performance of the proposed system the authors induce Mirai attack and analyze the behavior of devices before and after the attack. Performance metrics such as accuracy and detection time are measured for the proposed model and the existing model.

Kolokotronis, et al. [17] proposed a new idea of trust-based blockchain and intrusion detection. Since blockchain architectures are prone to many types of attacks, the authors have proposed a new intrusion detection system that can identify attacks and prevent the network from further damage. For consensus protocol, proof of stake and proof of work models are utilized. The proposed system consists of blacklisted IPs, a lookup table, and an intrusion monitoring

DOI: https://doi.org/10.54216/FPA.170204
Received: January 18, 2024 Revised: April 11, 2024 Accepted: September 15, 2024

system. The intrusion detection system identifies the type of attack, the nature of the attacker, and the history of the attack to help us stop the intrusion further.

3. Proposed System

The proposed system aims to develop a behavior-monitoring device that is based on the Adaptive Neuro-Fuzzy Inference System (ANFIS). The device is called the behavior monitor whose role is to observe the behavior of every device participating in the blockchain network and analyze all of their characteristics deeply and finally arrive at a confidence level for each device individually and a zone as a whole.

The classifier finally classifies the device behavior as malicious or normal based on the input data collected and analyzed. It is also used to estimate trust where trust is defined as the analysis of device behavior that belongs to the same network. Figure 1 shows the framework of the proposed trust model.

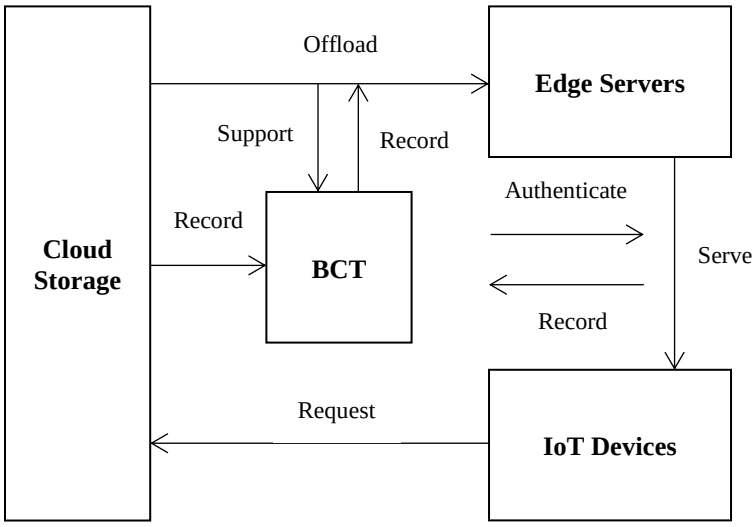

Figure 1. Proposed Behavioral Trust Model in Edge Computing Paradigm

In order to support this idea, a blockchain model based on artificial neural networks is implemented to overcome all the projection of risks in a critical decision-making scenario. To achieve this, the behavioral monitor needs to keep track of every transaction that has been recorded by each device using a sequence ID and hash ID value.

The main task of the monitor is to detect any abnormal behavior of the underlying devices and report to the master device immediately so that necessary preventive action can be taken. The proposed ANFIS-based trust model has three stages such as data collection, feature extraction, and classification training.

3.1. Data Acquisition

The input needed for the behavior monitor is collected from a variety of devices and sensors that have been connected to the IoT network chosen for the implementation of the proposed system. All transactions and data traffic in and out of the devices are collected immediately for analysis purposes. For training the classifier, two datasets are utilized both of which are benign in nature.

3.2. Feature Extraction

To train the Artificial Neural Network (ANN) classifier features such as protocols used by the devices, the hosts that are involved in the transaction, source and destination IP address, port number which was used for the transaction, MAC address of the device, etc. are extracted for each device and each transaction and stored in the blockchain storage.

3.3. Classification

DOI: https://doi.org/10.54216/FPA.170204
Received: January 18, 2024 Revised: April 11, 2024 Accepted: September 15, 2024

For the classification of a device in the network as anomalous or normal based on the extracted features, the Adaptive Neuro Fuzzy Inference System (ANFIS) model is used. It is a combination of artificial neural networks and a fuzzy inference system that is built based on the Takagi Sugeno fuzzy inference system. It contains simple if-then rules for estimating nonlinear functions and hence is believed to be a universal classifier that performs in a very intelligent manner. Both technologies are decent individually but combining both of them will result in excellent performance hence we have chosen to combine both of them and use them as a classifier.

3.3.1. Architecture of ANFIS

Adaptive Neuro Fuzzy Inference System (ANFIS) is based on an adaptive hybrid learning algorithm and contains five major layers. Layer 1 contains the input and layer 2 contains the fuzzification layer comprising the membership functions. The third layer contains normalization functions. The fourth layer consists of the defuzzification part and the fifth layer is the output layer [18]. Figure 2 shows the architectural diagram of ANFIS.

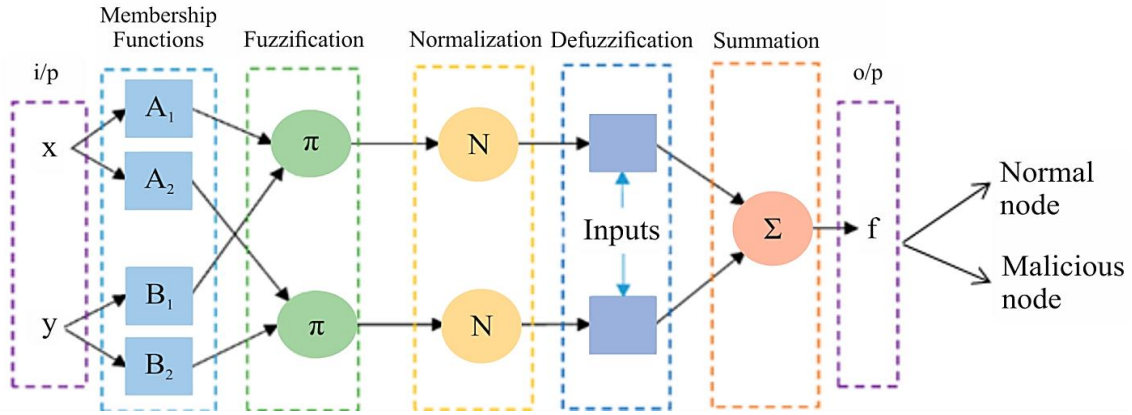

Figure 2. ANFIS Architecture

The advantage of this model is that it can self-learn and organize itself. It has also got the capability of self-tuning and it is good at decision making as well. It can deal with imperfect and partial values of input and produce efficient outputs and it can process any kind of information. The only disadvantage of considering the ANFIS model is the membership function identification and definition are based on the input. The major applications can be found in areas like data mining, control systems, decision support systems, pattern recognition, etc. Equations for all the five layers are represented in equations (1) to (5).

$$O_i^1 = \mu A_i(x),\ i = 1,2\ or\ O_i^1 = \mu B_{i-2}(y),\ i = 3,4 \quad (1)$$

$$O_i^2 = w_i = \mu A_i(x) \times \mu B_i(y),\ i = 1,2 \quad (2)$$

$$O_i^3 = \bar{w}_i = \frac{w_i}{w_1 + w_2},\ i = 1,2 \quad (3)$$

$$O_i^4 = \bar{w}_i f_i = \bar{w}_i(p_1 x + q_1 y + r_1),\ i = 1,2 \quad (4)$$

$$O_i^5 = \sum_i \bar{w}_i f_i = \frac{\sum_i w_i f_i}{\sum_i w_i} \quad (5)$$

where, x and y are the input values of node *I*; A_i and B_{i-2} are the linguistic values of a node *I*; w_i represents the firing strength of a rule *I*; (p_1, q_1, r_1) represents the parameter set, and $\bar{w}_i f_i$ is the consequent rule.

The objective of ANFIS is to find the best parameters based on which the network can adapt to attacks and unexpected conditions. The ANFIS algorithm is presented below. The first step is to load the input data of experimentation collected from the IoT devices and set initial values for default parameters. Run the model using inbuilt ANN min, diff fit Keras functions. Figure 3 shows the training and testing model workflow of ANFIS architecture.

ANFIS Algorithm

Step 1: Start

DOI: https://doi.org/10.54216/FPA.170204
Received: January 18, 2024 Revised: April 11, 2024 Accepted: September 15, 2024

Step 2: Load input data

Step 3: Initialize parameters

Step 4: For $c = 0.01$

Step 5: do

Step 6: Model = ANN (y, x, c, $step$)

Step 7: Fit = min(diff(Model.fit(ANN))

Step 8: End

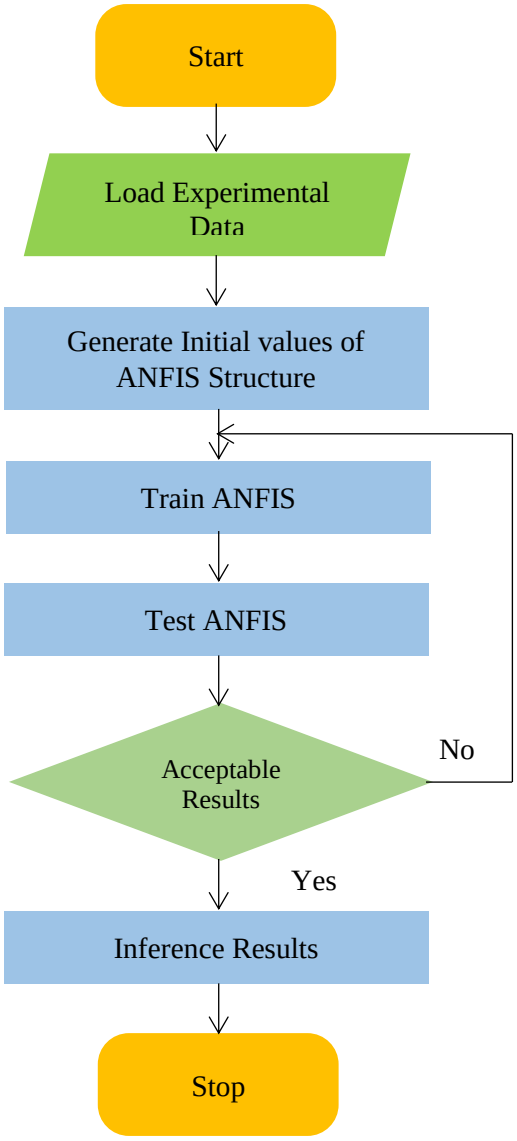

Figure 3. Workflow of ANFIS

3.4. Transaction Model

DOI: https://doi.org/10.54216/FPA.170204
Received: January 18, 2024 Revised: April 11, 2024 Accepted: September 15, 2024

In order to manage the transactions, three actions such as identity register, identity update, and identity withdrawal are used by this model. The identity register stores all the details about the individuals and devices involved in the network. It serves as a ledger and contains details like who has participated in the transaction, what has happened in the transaction, when the transaction has happened, etc. Identity update is a process of appending any updates that come into the network like public key upgradation, protocol change, etc. Identity withdrawal happens when any device wants to detach itself from the network. It stores all the transactions of the withdrawn node even after withdrawal including the details of when and why the node was removed. Two types of transaction models are used namely data access control and data offloading [19]. Two IoT devices namely IoT-A and IoT-B are considered. Figure 4 shows the sample of the transaction model happening between two IoT devices.

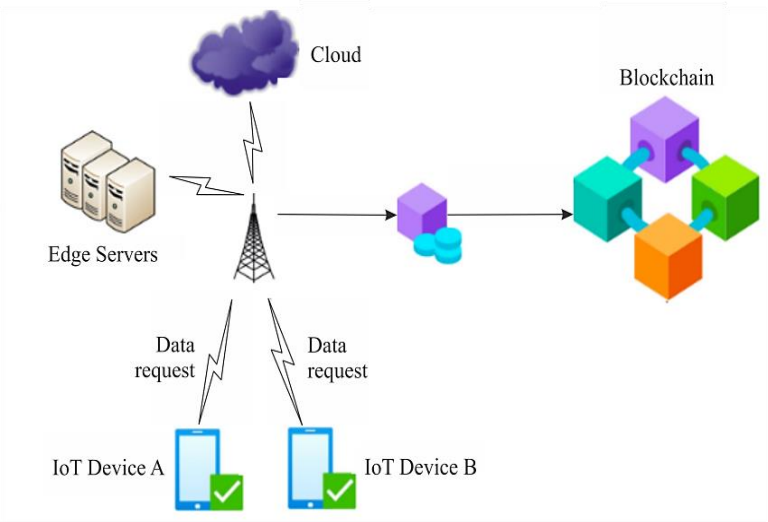

Figure 4. Transaction model between IoT devices

3.4.1. Data access control

In data access control, it is assumed that IoT-A has the capability of collecting data and IoT-B does not have the same capacity. A three-phase transaction is required now for device B to make use of device A's functioning. IoT-A and B have a smart contract between them that contains a critical message. IoT-B submits a request for data access to IoT-A. If IoT-B can read the data, a transaction will be generated and both devices will be able to achieve the desired result.

3.4.2. Data Offloading

In the case of Data Offloading, data is transferred from one location to another. In this scenario, it is assumed that IoT-B has storage resources and IoT-A does not have the same. This transaction also needs three steps where IoT-B has the authority to access the cache of information. Smart contracts are utilized by IoT-A for renting the resource. As a result of the contract, IoT-A would be charged, resulting in a transaction. IoT-B gets the data and gives it to device A.

4. Results and Discussions

The proposed system was executed with an experimental real-time dataset from Mabodi, et al. [20]. It contains data about malignant and benign tumors. Data was obtained by the authors from a webcam, a thermostat, and a security camera. Python is used for optimization and training purposes. The effectiveness of the proposed method is examined using performance metrics such as accuracy, precision, recall, and f-measure. The results are simulated and its performance is compared with existing classifiers such as Naive Bayes, K-Nearest Neighbor, Auto Encoders, Random Forest, and Support Vector Machine. Table 1 below shows the simulation parameters that are used to execute the proposed system.

Table 1. Simulation parameters

DOI: https://doi.org/10.54216/FPA.170204
Received: January 18, 2024 Revised: April 11, 2024 Accepted: September 15, 2024

Parameters	**Value**
Area	2500×2500 m^2
Time	400 s
Nodes	Normal: 50
Transmission range	200 m
Mobility	Random mobility
Maximum connections	100 nodes
Data size	1024 bytes
Maximum packet speed	20 ms^{-1}

Figure 5 below shows an accuracy comparison of the proposed model with Naive Bayes, K-Nearest Neighbor, Auto Encoders, Random Forest, and Support Vector Machine classifiers.

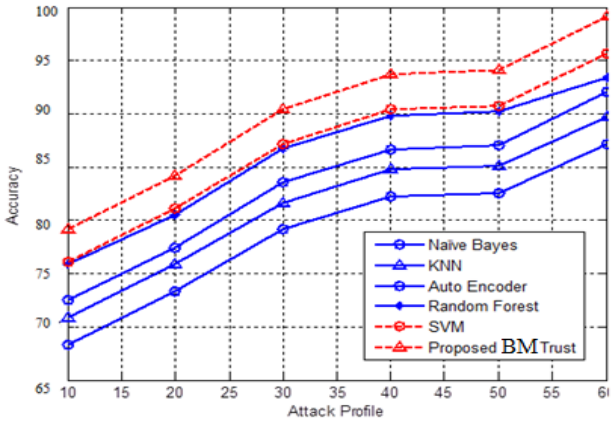

Figure 5. Accuracy comparison

Figure 6 below displays the precision comparison.

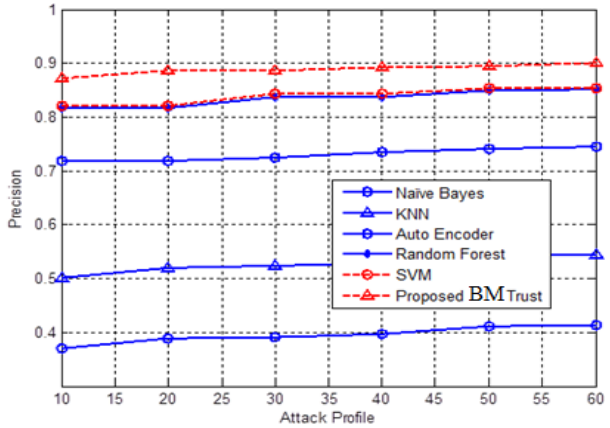

Figure 6. Precision comparison

Figure 7 illustrates the comparison of recall values of the proposed system and existing classifiers.

DOI: https://doi.org/10.54216/FPA.170204
Received: January 18, 2024 Revised: April 11, 2024 Accepted: September 15, 2024

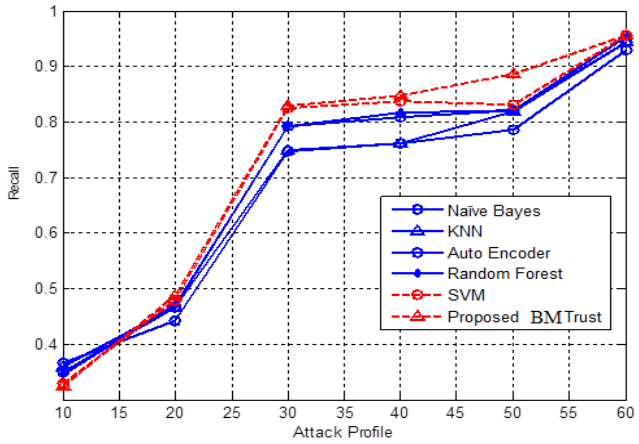

Figure 7. Comparison of Recall

Figure 8 shows the F-measure comparison of the proposed model with other classifiers.

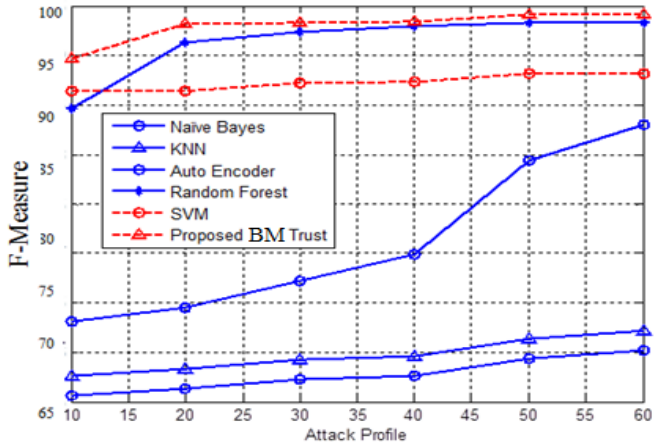

Figure 8. Comparison of F-measure

Figure 9 below shows the comparison of the detection time of the attack for the proposed model with Naive Bayes, K-Nearest Neighbor, Auto Encoders, Random Forest, and Support Vector Machine classifiers.

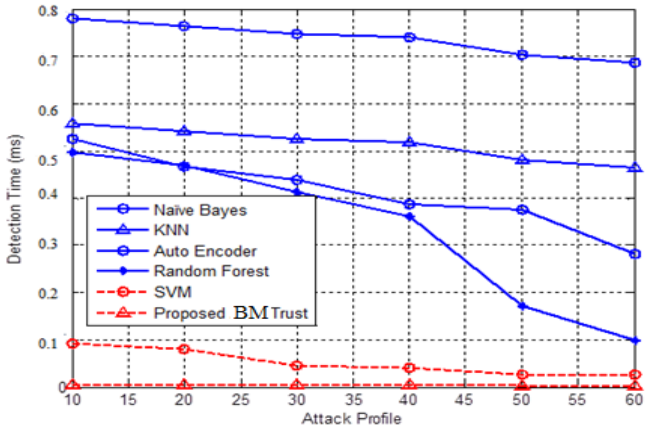

Figure 9. Detection time

DOI: https://doi.org/10.54216/FPA.170204
Received: January 18, 2024 Revised: April 11, 2024 Accepted: September 15, 2024

The proposed technique achieves a 99.80% true positive rate and a 0.5% false positive rate. The accuracy obtained is 95.00%, the precision score is 90.00%, the recall score is 94.00% and the F-measure is 94.00% which is all greater than the existing classifiers. Table 2 below shows the performance of the proposed model.

Table 2. Classification Performance

S. No.	Metrics	Values
1.	Accuracy	95.00%
2.	Precision	90.00%
3.	Recall	94.00%
4.	F1-Score	94.00%

Figure 10 shows the performance of the proposed Behavioral Monitoring trust model in terms of accuracy, precision, recall, and F-measure.

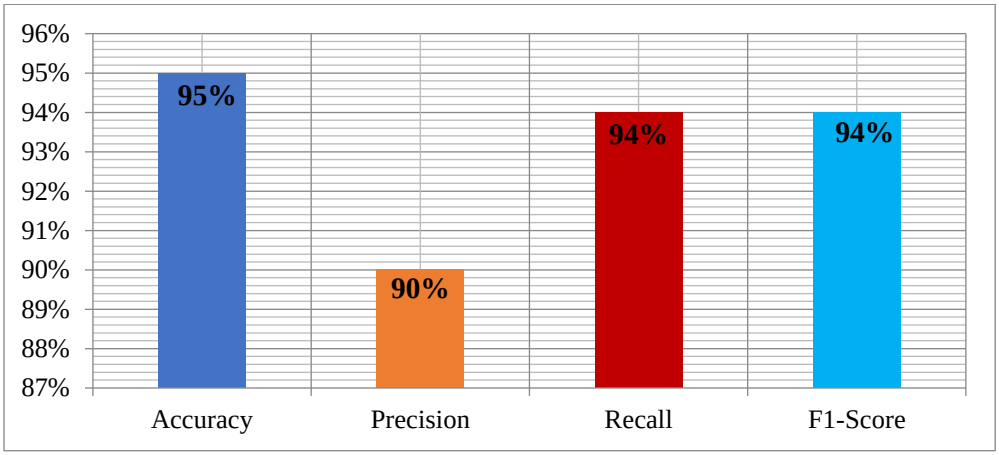

Figure 10. Performance of the proposed Behavioral Monitoring Trust model

Additional evaluation parameters like execution time, encryption time, storage cost, computational overhead, energy efficiency, and packet drop possibility are calculated for the proposed model and compared with existing algorithms like Bitcoin, Ethereum, Hyperledger, Direct and indirect trust-based blockchain model, and mutual trust chain model. These parameters are evaluated under normal network conditions and when three types of attacks are induced such as false data injection, booting attack, and node capturing. Execution time, Encryption time, Storage cost, and computational overhead are shown in Table 3 when the node-capturing attack is executed.

Table 3: Performance of algorithms under node capturing

Blockchain models	Execution Time	Encryption Time	Storage cost	Computational Overhead	Possibility of packet drops	Energy efficiency
Bitcoin	0.947	0.884	0.305409	0.825409	0.939309	0.995763
Ethereum	0.958	0.884	0.275947	0.825947	0.97438	0.995765
Hyperledger	0.960	0.9052	0.261991	0.872619	0.975342	0.995183

DOI: https://doi.org/10.54216/FPA.170204
Received: January 18, 2024 Revised: April 11, 2024 Accepted: September 15, 2024

Direct/indirect trust model	0.965	0.9054	0.236189	0.882361	0.977148	0.996007
Mutual trust model	0.978	0.9155	0.230365	0.902303	0.983761	0.996145
Proposed model	0.986	0.913	0.183394	0.911833	0.984215	0.996228

Table 4 shows the behavior of the algorithms during a false data injection attack.

Table 4: Performance of algorithms under false data injection

Blockchain models	**Execution Time**	**Encryption Time**	**Storage cost**	**Computational Overhead**	**Possibility of packet drops**	**Energy efficiency**
Bitcoin	0.980824	0.795615	0.333566	0.972014	0.666434	0.99887
Ethereum	0.981016	0.796866	0.330007	0.986401	0.669993	0.999434
Hyperledger	0.981094	0.802064	0.324798	0.986919	0.675202	0.999476
Direct/ indirect trust model	0.981992	0.812901	0.308694	0.996198	0.691306	0.999834
Mutual trust model	0.982174	0.819711	0.303654	0.998376	0.696346	0.999931
Proposed model	0.982747	0.822648	0.300478	0.998985	0.699522	0.999959

Table 5 tabulates the resulting performance of the algorithms when the booting attack is performed.

Table 5: Performance under booting attack

Blockchain models	**Execution Time**	**Encryption Time**	**Storage cost**	**Computational Overhead**	**Possibility of packet drops**	**Energy efficiency**
Bitcoin	0.96138	0.604428	0.32115	0.544712	0.67885	0.974218
Ethereum	0.96293	0.622364	0.313834	0.568991	0.686166	0.975825
Hyperledger	0.963646	0.625737	0.304943	0.569417	0.695057	0.975927
Direct/ indirect trust model	0.964219	0.630347	0.301431	0.574265	0.698569	0.97635
Mutual trust model	0.965951	0.645609	0.283194	0.58184	0.716806	0.976826
Proposed model	0.966107	0.647051	0.274924	0.589668	0.725076	0.977293

Figure 11 shows the performance of the proposed behavioral monitoring trust estimation method under various attacks.

DOI: https://doi.org/10.54216/FPA.170204
Received: January 18, 2024 Revised: April 11, 2024 Accepted: September 15, 2024

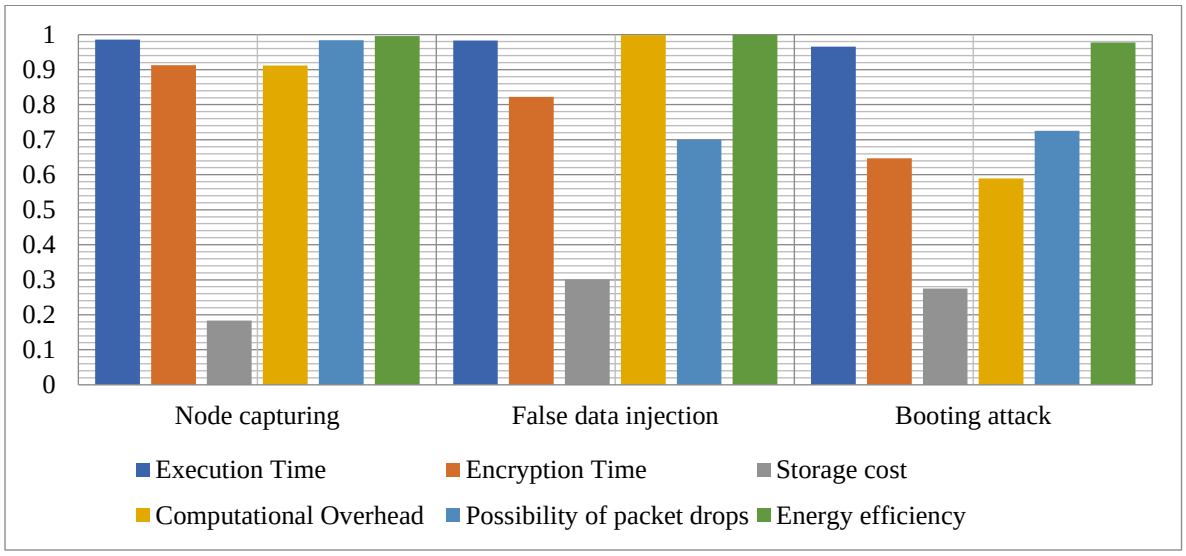

Figure 11. Performance of the proposed model under various attacks

5. Conclusion

There are many security issues concerned with IoT, some of which are flaws related to design, and protocol-level implementation. Edge computing is selected in this study to work hand in hand with IoT systems. However, there are several attacks that are very easy to apply in edge computing scenarios. Hence, this study proposes the integration of edge computing and blockchain along with a trust estimation model based on behavioral monitoring using the ANFIS model. The evaluation of the proposed model is estimated in terms of accuracy, sensitivity, specificity, f-measure, execution time, encryption time, storage cost, computational overhead, energy efficiency, packet drop possibility, and the final results are compared with Naive Bayes, K-nearest neighbor, Auto Encoder, Random Forest and Support Vector Machine, Bitcoin, Ethereum, Hyperledger, Direct and indirect trust model and mutual trust chain based blockchain model. From the results, it can be seen evidently that the proposed behavioral monitoring trust estimation method achieves higher performance than all other methods and it is quite competent in improving the edge security.

Funding: This study received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

[1] Wang, L., Zhu, H., Sun, J., Dai, R., Ma, Q., & Wei, X. (2020). Trust Assessment in Internet of Things Using Blockchain and Machine Learning. Research Square Platform LLC. https://doi.org/10.21203/rs.3.rs-110210/v1.

[2] Mohammadi, V., Rahmani, A. M., Darwesh, A. M., & Sahafi, A. (2019). Trust-based recommendation systems in Internet of Things: a systematic literature review. In Human-centric Computing and Information Sciences (Vol. 9, Issue 1). Springer Science and Business Media LLC. https://doi.org/10.1186/s13673-019-0183-8.

[3] Mishra, K. N., Bhattacharjee, V., Saket, S., & Mishra, S. P. (2022). Security provisions in smart edge computing devices using blockchain and machine learning algorithms: a novel approach. In Cluster Computing (Vol. 27, Issue 1, pp. 27–52). Springer Science and Business Media LLC. https://doi.org/10.1007/s10586-022-03813-x.

[4] Huh, S., Cho, S., & Kim, S. (2017, February). Managing IoT devices using blockchain platform. In 2017 19th International Conference on Advanced Communication Technology (ICACT) (pp. 464-467). IEEE.

DOI: https://doi.org/10.54216/FPA.170204
Received: January 18, 2024 Revised: April 11, 2024 Accepted: September 15, 2024

[5] Johnson, S., Scarlata, V., Rozas, C., Brickell, E., & Mckeen, F. (2016). Intel software guard extensions: EPID provisioning and attestation services. White Paper, 1(1-10), 119.

[6] A.S.M. Kayes, W. Rahayu, P. Watters, M. Alazab, T. Dillon and E. Chang, Achieving Security Scalability and Flexibility using Fog-Based Context-Aware Access Control, Future Generation Computer Systems, 107(1) (2020), 307-323.

[7] Al-Hasnawi, S. M. Carr, and A. Gupta, Fog-based local and Remote Policy Enforcement for Preserving Data Privacy in the Internet of Things, Internet of Things, 7(1) (2019), 1-15.

[8] Bocek, T., Rodrigues, B. B., Strasser, T., & Stiller, B. (2017, May). Blockchains everywhere-a use-case of blockchains in the pharma supply-chain. In 2017 IFIP/IEEE symposium on integrated network and service management (IM) (pp. 772-777). IEEE.

[9] Dorri, A., Kanhere, S. S., & Jurdak, R. (2017, April). Towards an optimized blockchain for IoT. In 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI) (pp. 173-178). IEEE.

[10] Cao, K., Liu, Y., Meng, G., & Sun, Q. (2020). An overview on edge computing research. IEEE Access, 8, 85714-85728.

[11] Shala, B., Trick, U., Lehmann, A., Ghita, B., & Shiaeles, S. (2020). Blockchain and trust for secure, end-user-based and decentralized IoT service provision. IEEE Access, 8, 119961-119979.Guo, S., Hu, X., Guo, S., Qiu, X., & Qi, F. (2019). Blockchain Meets Edge Computing: A Distributed and Trusted Authentication System. IEEE Transactions on Industrial Informatics, 1–1.

[12] Christidis, K., & DevetsikIoTis, M. (2016). Blockchains and smart contracts for the internet of things. Ieee Access, 4, 2292-2303.

[13] Idrees, S. M., Nowostawski, M., Jameel, R., & Mourya, A. K. (2021). Security aspects of blockchain technology intended for industrial applications. Electronics, 10(8), 951.

[14] Bhushan, B., Sahoo, C., Sinha, P., & Khamparia, A. (2021). Unification of Blockchain and Internet of Things (BIoT): requirements, working model, challenges and future directions. Wireless Networks, 27, 55-90.

[15] Al-Rakhami, M. S., & Al-Mashari, M. (2021). A blockchain-based trust model for the internet of things supply chain management. Sensors, 21(5), 1759.

[16] Ali, J., Ali, T., Alsaawy, Y., Khalid, A. S., & Musa, S. (2019, May). Blockchain-based smart-IoT trust zone measurement architecture. In Proceedings of the International Conference on Omni-Layer Intelligent Systems (pp. 152-157).

[17] Kolokotronis, N., Brotsis, S., Germanos, G., Vassilakis, C., & Shiaeles, S. (2019, July). On blockchain architectures for trust-based collaborative intrusion detection. In 2019 IEEE World Congress on Services (SERVICES) (Vol. 2642, pp. 21-28). IEEE.

[18] Bamakan, S. M. H., Faregh, N., & ZareRavasan, A. (2021). Di-ANFIS: an integrated blockchain–IoT–big data-enabled framework for evaluating service supply chain performance. Journal of Computational Design and Engineering, 8(2), 676-690.

[19] Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2021, May). A cooperative architecture of data offloading and sharing for smart healthcare with blockchain. In 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 1-8). IEEE.

[20] Mabodi, K., Yusefi, M., Zandiyan, S., Irankhah, L., & Fotohi, R. (2020). Multi-level trust-based intelligence schema for securing of Internet of Things (IoT) against security threats using cryptographic authentication. The journal of supercomputing, 76, 7081-7106.

DOI: https://doi.org/10.54216/FPA.170204
Received: January 18, 2024 Revised: April 11, 2024 Accepted: September 15, 2024