Int. J. Nonlinear Anal. Appl. 12 (2021) No. 2, 2189-2197
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2021.5368

Trust based blockchain security management in edge computing

D. Jayakumar[a,*], K. Santhosh Kumar[b], R. Sathya[c]

[a]Department of CSE, IFET College of Engineering, Villupuram, India
[b]Department of IT, Annamalai University, Chidambaram, India
[c]Department of CSE, Annamalai University, Chidambaram, India

(Communicated by Madjid Eshaghi Gordji)

Abstract

In this paper, an analysis is conducted on the data transmitted through the edge computing technique. The research creates a trust model that establishes direct, indirect, and mutual trust between the source and destination blocks when data is sent. That is, the study integrated blockchain as a model to transmit the data in a secured way through the blockchains, however, the intrusion in blockchains can be avoided based on trust based model. The simulation is conducted on various test beds and with existing blockchain mechanisms. The findings reveal that the suggested trust-based paradigm is successful at safeguarding data sent over the edge.

Keywords: MANET, Secured routing, Behavioural Trust Detection, Trust Degree.
2010 MSC: Please write mathematics subject classification of your paper here.

1. Introduction

Data from IoT devices is one of the assets of the data-driven economy since it leads to a variety of business models [5]. However, records contain sensitive data and the identity can be revealed if there has not been an adequate confidentiality mechanism [2]. In order to get financial advantage or other advantages on behalf of another party, for instance, a fraudulent agent with access to someone personal data may use his identity. The individual with an assumed identity could be adversely affected, particularly if he is responsible for the conduct of the perpetrator. Good confidentiality must also be enforced to preserve techniques and rules. From a legal point of view, in May 2018 the

*Corresponding author
Email addresses: jayakumarifetd@gmail.com (D. Jayakumar), santhosh09539@gmail.com (K. Santhosh Kumar), sathya_vai@yahoo.com (R. Sathya)

Received: February 2021 *Accepted:* April 2021

European Union (EU) a new data security statute, known as the General Data Protection Regulation (GDPR) in order to control excessive use of data and to improve the rights of consumers to their data [3]. It addresses the value of a philosophy of privacy that effectively requires the privacy of all engineering processes to be taken into consideration.
Worryingly, the IoT network characteristics, such as their distributed architecture, large size and a lack of resources, do not offer a protected platform for data-protection applications in terms of computing power, storage space, bandwidth, etc. Furthermore, typical IoT network implementations are structured in a clustered manner, which neglects the distributed character of IoT devices. This includes data gathering, data transmission, retrieval, sharing, and data destruction functions. This methodology has demonstrated the use of time-sensitive applications in delays and traffic jams and cannot therefore satisfy the criteria for IoT sensitive applications with ultra-low delays [10, 14, 15, 13, 7, 11].
The key idea behind blockchain is a solution to create good contact between untrustworthy and unknown individuals, while promoting IoT's distributed existence, removing the central authority with cloud computing [9, 4]. The key blockchain technology lies behind the use of all members of a collective shared archive of data known as the public chief. The related mechanism is called as "Proof of Work," and it is built up of data blocks linked by a cryptographic hash key (PoW).However, it is very difficult to implement the blockchain technology in the IoT context because of the complete calculation capacity necessary to resolve PoW puzzles for IoT devices with limited resources.
When data is transferred, this work develops a trust model that creates direct, indirect, and mutual trust between the source and destination blocks.That is, the study integrated blockchain as a model to transmit the data in secured way through the blockchains, however the intrusion in blockchains can be avoided based on trust based model.

2. Background

In this section we present briefly the principles and technologies behind conventional blockchains. In the sense of blockchain with trust, we use these principles to create a modern blockchain application to resolve privacy concerns and resource utilization in a decentralized context such as IoT.

2.1. Blockchain Overview

Due to its distributed and unchangeable data storage method, blockchain technology enables users to work in practically all fields like banks, supply chains and other transaction networks such as IoT, is a widely studied topics. Inherently, because of its public chief and the consensus mechanic known as PoW, blockchain technology is immune to data alteration. Once registered, information in a particular block can't be retroactively changed as it will invalidate all block hashes in a blockchain and violate the agreement reached amongst blockchain nodes.

2.2. Blockchain Architecture

For all practical purposes, a blockchain is a chain that points to the past of blocks that are connected by hashes. Both nodes have a copy of the blockchain, and each transaction decides the exact known 'position' to appear in the blockchain. Block has 6 parts; the pre-block hash, nonce, new block hash, root of Merkle.
Transactions usually include the address and address of the sender, the receiver and the value in the Bitcoin sense. However, these can differ according to the application. Each block header has a collection of metadata which helps validate any block in the public directory and connect to previous blocks. A public register allows anyone who is eligible to attend to the data and use the system.

The blockchain framework may, however, be built in a more centralized or decentralized way based on the application requirements. Because they are administered by a central authority who governs blockchain network access, private Blockchain systems are more centralised in this regard. Consortium blockchains, like private blockchains, are administered by a group of nodes rather than a single company.

2.3. Consensus and Mining

The process of verifying and linking the blocks created by the blockchain nodes to the blockchain genesis is known as mining. However, the approach is computationally demanding owing to the cryptographic challenge that must be solved in order to validate the cube. Miners are lauded for their ability to solve difficult mathematical challenges. There are two types of prizes available: fresh bitcoins and money.
According to the consensus, each blockchain node in the network will agree to add the new block to the chain.The contains mining and other laws, including limited period for mining, how to cope with blockchain separation, signing transactions in blockchain chains, award miners, and pick miners. Others methods in [1, 8, 12, 6] is programmed to reach any consensus between nodes, based on the usage environment, with specific features such as minimum resource requirements, protocol immunity, easy access control, and privacy.

2.4. Smart Contracts

One essential aspect of the blockchain is the intelligent contract agency because it fills the void in implementing the previously negotiated rules and requirements without a centralized body; in other words, it ties utility vendors to reputable customers, blockchain contracts or automated contracts in the directory. Smart contract features can be used for transactions. In addition to the same way as a standard contract does, they not only specify the rules and sanctions under a relationship but automatically implement the obligations.

3. Trust Detection Model

This section explains the network's node-to-node trust relationship. Direct and indirect trust are used to calculate the value of trust between the nodes.
Algorithm 1: Creation of Trust between the blockchains in Edge
Step 1: Create blocks
Step 2: Connect with the neighbor blocks
Step 3: Form direct trust between blocks
Step 4: Form indirect trust between blocks
Step 5: Form mutual trust between blocks
Step 6: Compute the entire trust between the blocks
Step 7: If the trust value is high, communication is established
Step 8: Else, the communication is discarded

3.1. Calculation of Trust

Direct trust

To some extent, the Direct Trust Model is assessed, which determines the level of trust in terms of node connectivity, constructive collaboration of nodes and network linkage. This direct trust establishes a relation between the nodes, and is a simple and evident indication of a direct trust level in

terms of their subjective actions. Here, a thorough study of the degree of direct trust with similarities and relations strength of the node is carried out. Analysis of the degree of indirect trust is often conducted using distance between nodes.
For the neighbouring node pair, the strength of the connection between the sensor nodes is used to determine a direct trust and its degree.

$d_r(u,v) = \frac{w(u,v)}{w(u)}$, where $d_r(u,v) \in (0,1]$

where
$w(u,v)$ – trust strength between nodes
$w(u)$ - total strength between neighboring nodes
The homogeneity of network nodes, or the overlap of comparable nodes, is common. The node's similarity is determined by comparing the mutual neighbours of any two surrounding sensor nodes. When the nodes are adjacent, the neighboring nodes appear to overlap more widely. The present node thus has a much lower seamlessness over a greater number of nearby nodes.
To find the direct trust of similarity, measured as, for an adjacent node pair. The similarity between sensor nodes is used

$d_s(u,v) = \sum_{t \in N(u) \in N(v)} (I(t))^{-1}$

where
$N(u)$ and $N(v)$ - neighboring node sets
$I(t)$ - penetration degree.
Finally, the direct trust is calculated as,
$d(u,v) = d_r(u,v) + d_s(u,v)$.

Indirect trust
The transit of information among the nodes is taken into consideration through indirect trust. Indirect linkages are established via intermediary nodes between non-adjacent nodes. As a result of applying a direct trust model between nearby nodes, it is possible to infer an indirect trust between non-adjacent nodes. In the transmission trust between the source and destination nodes, simple and multi-path approaches take different shapes. This measures the indirect trust of the single direction in the following:

$$i_s(u,v) = \begin{cases} mt\frac{d_{\max} - d_{u,v} + 1}{d_{\max}} & if\ d_{u,v} \le d_{\max} \\ 0 & if\ d_{u,v} > d_{\max} \end{cases}$$

$mt = min(d(u,u_1), d(u_1,u_2), ..., d(u_n,v))$
$d_{\max}$ - maximum trust transmission distance.
The theory indicates that the integrity and precision of information continues to diminish as the propagation distance increases.
Multi-path indirect trust gets maximum value after the estimation, as stated:
$i_m(u,v) = max_{paths(u,v)}\{i_s(u,v)\}$

where
$i_m(u,v)$ - indirect trust degree
Hence, the trust degree is given as,

Parameters	**Value**
Area	1500×1500m^2
Time	500 s
Protocol	AODV
Nodes	Normal: 50
Transmission range	250 m
Mobility	Random mobility
Maximum connections	50 nodes
Type of Traffic	CBR
Data size	512 bytes
Maximum packet speed	25 ms^{-1}

Table 1: Parameters for simulation

$$t(u,v) = \begin{cases} d(u,v) & if\ nodes\ are\ adjacent \\ i_m(u,v) & else \end{cases}$$

Mutual trust

The direct and indirect trust models are used to calculate the trust value between the nodes. The guiding node validates the trust that exists between node pairs, which isn't necessarily the same. Furthermore, a response to the node that received the message cannot be transmitted in the presence of malicious nodes.This produces unusual behaviour, which is given as an adjacent sensor nodes:

$$m(u,v) = \begin{cases} min\,(T(u,v)) & if min\,(T(u,v)) \geq x \\ 0 & else \end{cases}$$

where

x - trust tolerance degree

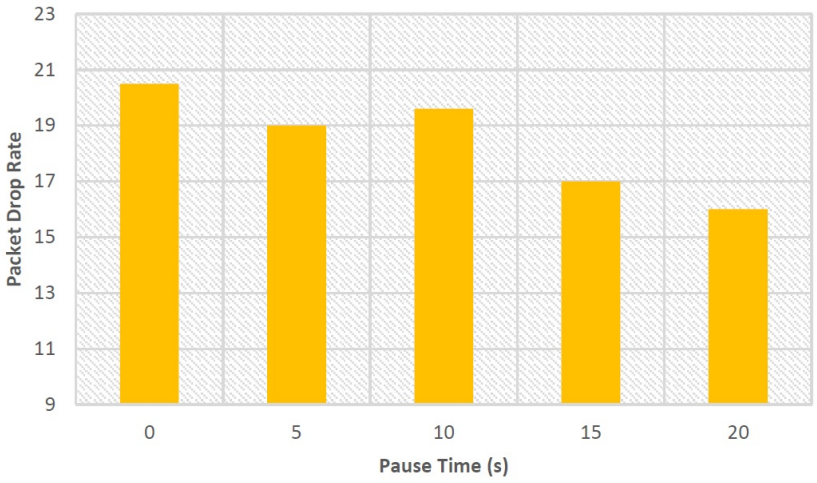
The translation of node trust into shared trust addresses nodes behaviour and eliminates the restrictions associated with the precision of detecting the trust levels.

4. Experiment Results and Analysis

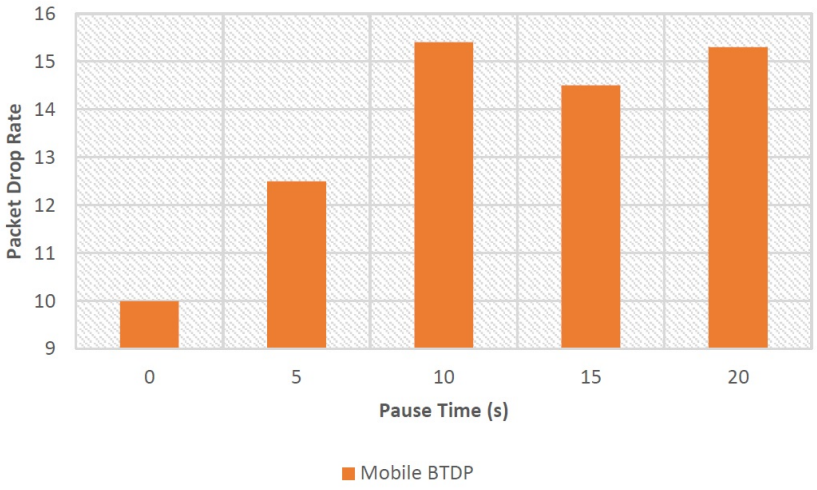
The findings of the detection rate, drop ratio, and false positive rate are presented in this section. The simulation parameters are shown in Table 1.

4.1. Packet Drop rate

The results of the suggested model's packet loss rate are shown in Figure 1. The simulation results demonstrate a lower packet loss rate and shorter pause periods.



(a) Attacks on reentrancy



(b) Access control vulnerabilities

Figure 1: Packet drop rate

4.2. False Positive Rate

Figure 2 shows the results of the recommended model's false positive rate. Simulated results show a decreased percentage of false positives and shorter wait durations.

4.3. Wormhole Detection Time

Figure 3 shows the results of the suggested model's detection time. The simulation findings reveal that when the pause times increase, the detection time decreases.

5. Conclusions

In this research, an edge computing trust model is used, which involves both direct and indirect trust, as well as reciprocal trust. between source and destination edge nodes through blocks. Data may be sent over blockchains thanks to the integration of blockchain with edge nodes. The trust paradigm, on the other hand, prevents blockchain incursion. Edge computing improves Rates of detection, false positives, and packet loss compared to other models, according to simulation data.

References

[1] M.N. Ahmed, A.H. Abdullah, H. Chizari, and O. Kaiwartya, *F3TM: Flooding Factor based Trust Management Framework for secure data transmission in MANETs*, J. King Saud Univ. Comput. Inf. Sci. 29(3) (2017) 269–280.

[2] A. Daniel, B.B. Kannan, and N.V. Kousik, *Predicting Energy Demands Constructed on Ensemble of Classifiers*, In: S.S. Dash, S. Das, B.K. Panigrahi (eds) Intelligent Computing and Applications, Advances in Intelligent Systems and Computing, Springer, Singapore, 2021.

[3] M. Gunasekaran, and K. Premalatha, *TEAP: trust-enhanced anonymous on-demand routing protocol for mobile ad hoc networks*, IET Inf. Sec. 7(3) (2013) 203–211.

[4] V. Laxmi, C. Lal, M.S. Gaur, and D. Mehta, *JellyFish attack: Analysis, detection and countermeasure in TCP-based MANET*, J. Inf. Sec. Appl. 22 (2015) 99–112.

[5] N. Marchang, and R. Datta, *Light-weight trust-based routing protocol for mobile ad hoc networks*, IET Inf. Sec. 6(2) (2012) 77–83.

[6] P.J. McNerney, and N. Zhang, *A study on reservation-based adaptation for QoS in adversarial MANET environments*, 8th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC), IEEE (2012) 677–682.

[7] Y. Natarajan, S. Kannan, and S.N. Mohanty, *Survey of Various Statistical Numerical and Machine Learning Ontological Models on Infectious Disease Ontology*, In: R. Satpathy, T. Choudhury, S. Satpathy, S.N. Mohanty, and X. Zhang (eds) Data Analytics in Bioinformatics, 2021.

[8] S. Qazi, R. Raad, Y. Mu, and W. Susilo, *Multirate DelPHI to secure multirate ad hoc networks against wormhole attacks*, J. Inf. Sec. Appl. 39 (2018) 31–40.

[9] R. Raja, V. Ganesan, and S.G. Dhas, *Analysis on improving the response time with PIDSARSA-RAL in Clowd-Flows mining platform*, EAI Endors. Trans. Energy Web 5(20) (2018) 1–4.

[10] S.B. Sangeetha, N.W. Blessing, and J.A. Sneha, *Improving the Training Pattern in Back-Propagation Neural Networks Using Holt-Winters' Seasonal Method and Gradient Boosting Model*, In: P. Johri, J. Verma, and S. Paul (eds) Applications of Machine Learning, Algorithms for Intelligent Systems, Springer, Singapore, (2020).

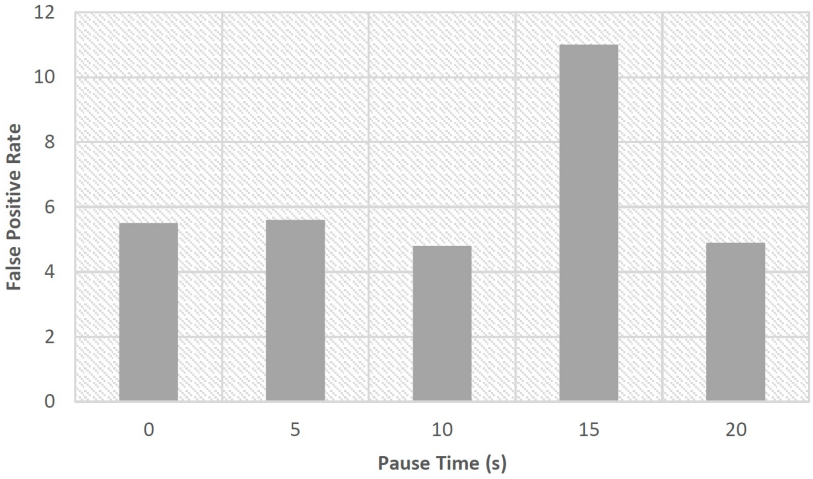
[11] S. Tan, X. Li, and Q. Dong, *Trust based routing mechanism for securing OSLR-based MANET*, Ad Hoc Networks 30(C) (2015) 84-98.

[12] D.S.K. Tiruvakadu, and V. Pallapa, *Confirmation of wormhole attack in MANETs using honeypot*, Comput. Secur. 76 (2018) 32–49.

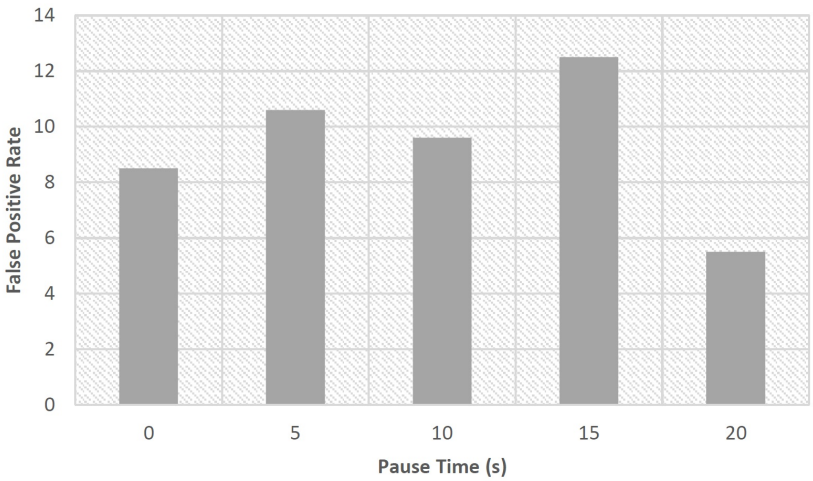
[13] B. Wang, X. Chen, and W. Chang, *A light-weight trust-based QoS routing algorithm for ad hoc networks*, Perv. Mobile Comput. 13(2014) (2014) 164–180.

[14] H. Xia, Z. Jia, X. Li, L. Ju, and E.H.M. Sha, *Trust prediction and trust-based source routing in mobile ad hoc networks*, Ad Hoc Networks 11(7) (2013) 2096–2114.

[15] N. Yuvaraj, K. Srihari, G. Dhiman, K. Somasundaram, A. Sharma, S. Rajeskannan, M. Soni, G.S. Gaba, M.A. AlZain, and M. Masud, *Nature-Inspired-Based approach for automated cyberbullying classification on multimedia social networking*, Math. Prob. Engin. 2021 (2021) 1–12.

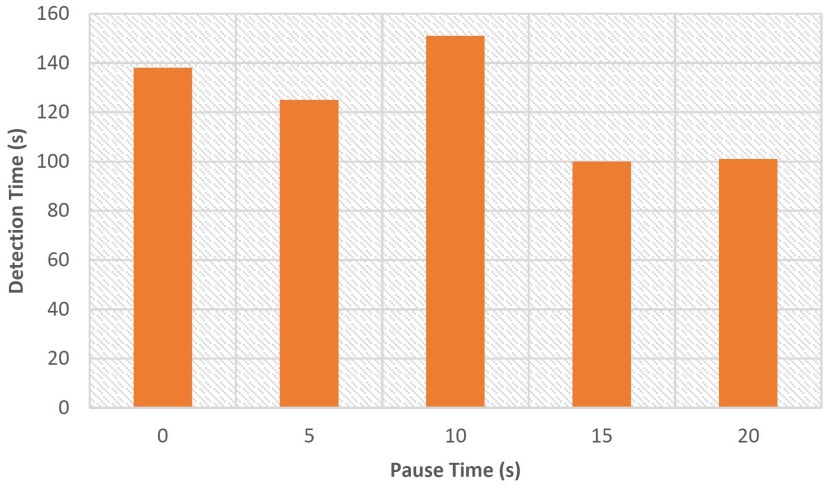


(a) Attacks on reentrancy

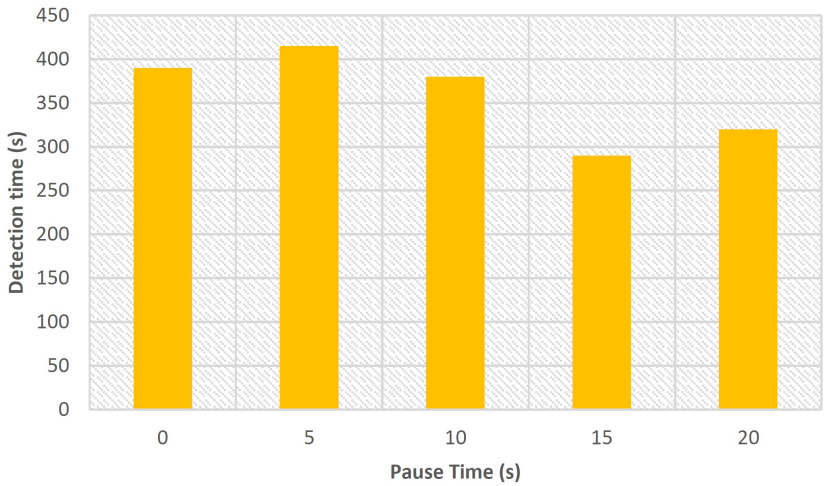


(b) Access control vulnerabilities

Figure 2: False Positive Rate



(a) Attacks on reentrancy



(b) Access control vulnerabilities

Figure 3: Detection time