Trust Management in Edge Computing

The main objective of the report is to analyze the different implementation techniques of trust management in the field of edge computing. In order to save time, memory and other computing resources the demand of edge computing is now increased due to which many security risks have been raised. One of the risks is trust management. Trust management basically establishes a trust mechanism between different edge devices in order to check the nature of data. The report consists of some approaches towards implementation of trust mechanisms like multi-layered fusion mechanism, block chain and trust management for IoT devices. These approaches have done the same work in different scenarios using different algorithms. In addition every method has different accuracy percentages in different factors like some are better in only reducing security risks but some also provide increment in speed with low memory usage along with high security protection. But comparative analysis of these proposed solutions show that the method of block chain is better because it reduces bad nodes more accurately, makes the system more secure, reliable and fast at low cost.

I. INTRODUCTION

A. Edge Computing

Edge Computing is the branch of distributed computing that brings data storage and computation closer to the location where it is needed to improve response times and save the major part of bandwidth.[1] It follows the topology structure instead of technology. The major goal of edge computing is to reduce the cost of delivery and have low latency nearer to the requests. The need and increase of Iot devices also affect the increase of edge computing devices. Because the massive amount of data to be computed at the data centers. This edge computing is now one of the most emerging fields in distributed computing because of transfer data with minimum latency.

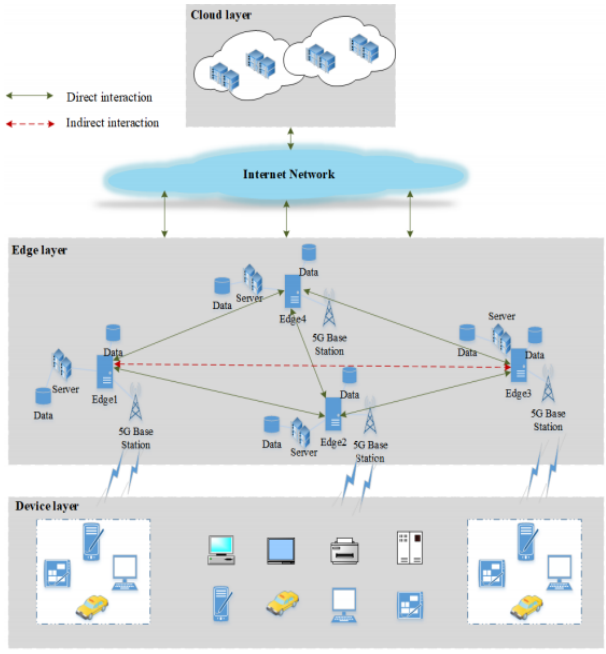


Figure 2. Edge computing architecture

B. Security Issues in Edge Computing

The field of edge computing is now the need of the hour due to which many security and privacy issues have been raised. Many organizations are trying to overcome these security risks in order to make their system more secure and private. One of the most important factors in the security section of edge computing is Trust Management. Trust Management basically removes and corrects the nodes with malicious behavior and errors.

C. Trust Management in Edge Computing

Moreover, Trust management increases the efficiency of the edge system by adding a bridge type connection between input nodes and cloud. Trust mechanism uses different algorithms based on the architecture of the edge system.[2] Every algorithm has its own trust formula which gives us the cost of the algorithm as well as number of malicious nodes in the system so that we can improve our algorithm to remove more and more such malicious nodes.

D. Project Scope

The scope of our project mostly covers the issues which have been created as a result of absence trust management and how trust management solves these issues.
Architecture of Edge Computing Systems
Working of trust Mechanism Algorithms
Different applications of Trust mechanism

E. Project Objectives(s)

The main objective of this research based project is to analyze the effect of trust mechanisms in edge based computing systems.

- How Trust Management plays its role of in edge computing
- How Trust management reduce errors in edge devices
- How trust management system choose algorithm based on edge system
- How trust management reduce latency of system
- How multi layer trust management mechanisms work
- How trust management increases the system efficiency

F. Overview of project

Chapter 2: In this chapter we discuss the already mentioned solutions of this problem as Literature review.
Chapter 3: This chapter contains results and analysis based on the literature review.
Chapter 4: This chapter shows the comparative analysis of different solutions used in literature review. In the end we will discuss the best one.
Chapter 5: This chapter tells the improvements proposed in the literature review results. We will use basic knowledge of distributed systems in order to improve these algorithms.
Chapter 6: conclusions and recommendations
Chapter 7: This chapter have references

II. LITERATURE REVIEW

A. An Efficient and Credible Multi-Source Trust Fusion Mechanism Based on Time Decay for Edge Computing

In edge computing the main problem is malicious nodes which produce an error due to which the error information regarding feedback provided by the node will affect the result of local perception. In order to solve this problem a node trust evaluation mechanism system has been introduced. The system establishes a trust management relationship mechanism between the nodes of edge devices in an open edge computing environment.[2] At the end we use a multi-source trust fusion algorithm. Which basically increases the efficiency of the system and interaction success rate over other existing models in the system.

Kantert et al.[3] a computer engineer proposed a new self-maintenance trust system in order to decrease the number of malicious nodes in the edge system. This system has functionality of enabling the autonomous based servers from different administrative domains to share their resources in grid-like situations. This grid-like system is different from others because this system supposes that there are some selfish individuals or malicious type service providers. Therefore, Kantert et al. designed a system which evaluates and manages trust in edge data centers.

In this proposed trust mechanism method for edge computing, the edge layer is responsible for the completion of trust computing. Which reduces the overall load on the cloud devices and makes the whole algorithm more efficient in terms of performance. The second way is all feedback of the nodes must be sent to the cloud center for more processing. In the model,the important factors that affect trust can be abstracted, and the degree of trust is usually normalized. [4]

In order to verify the effectiveness of the proposed trust computing scheme, Java implementation based software DRM is used on operating systems like Mac, Windows, Linux etc. Moreover, for the comparison of correct nodes and malicious nodes we use DRM (Distributed Reputation Management) software. In addition some softwares is used for security checking like VEC (Vehicular Edge Computing). This experiment shows that the accuracy of nodes increases, which reduces the situation of malicious node deception. Experiment got accuracy upto 80%. [2]

B. Trust Management in Edge Computing by means of Blockchain Technologies

The Internet of Things (IOT) has become an trending technology that comprises a network of sensors which has to connect with edge nodes to communicate with cloud services.This kind of communication is flexible but is vulnerable to various security issues.

- Sensors can interact with malicious nodes intended to steal data
- An edge node accepting data from malicious sensor intended to corrupt the preprocessing data
- A malicious adversary to attack interchange of messages between sensors and edge nodes.

To provide secure communication deployment of trust management based architecture are of immense preference.Trust Management process works with a Trusting node (TN) which tries to establish trust on an To-be Trusted Node (TBTN) by assigning a trust degree.TN nodes have to look into the reputation and trust degrees of the TBTN nodes.The Communication between Trust providers can be corrupted by malicious messages.

1. BlockChain

Blockchains are tamper evident and tamper resistant digital ledgers implemented in a distributed fashion without a central authority.

Permissionless Blockchain

- Anyone can join the network
- read the ledger data validate transactions
- ledgers can replicate the transactions.

Permissioned Blockchain

- Formed by a set of transacting parties
- validation is controlled by a set of selected nodes.

The technology of Block chain is proposed to provide a secured and reliable fetch of trust degrees from the nodes.

2. Proposed blockchain based trust management

Block chain based trust management provides tamper proof data and ensures the integrity and trustworthiness of the trust information verification.This mechanism strengthens privacy in data sharing. BlockChain trust management systems are designed to receive trust estimation to perceive the reputation of a device in a network .Hence, these estimations are shared between other devices in the network without any corruption.Block chain provide a distributed system which ensures network security ,integrity of data and guarantee trust information

confidentiality, integrity and privacy during sharing. [5]

Key features of BlockChain trust management:

- Tamper-proof network: A reliable sharing of trust information on the network
- Information validation: trust reputation is validated by members
- Authentication and verification: Edge nodes are added using authentication
- Real time Assessment: trust estimates are retrieved in real time

A permissioned Block chain is used in which blocks are created by edge nodesEdge nodes are responsible for the validation of the blocks .IOT devices send requests to the edge nodes for the trust degrees of the TBTN .The edge nodes then provides the trust degrees to IOT devices.
In this case, BlockChain is used to store wallets of the trust evaluation of the nodes in the network.The communication between TN and TBTN is represented as a transaction.The blocks are validated using the comparisons of trust estimates of past interaction and latest ones. [6]

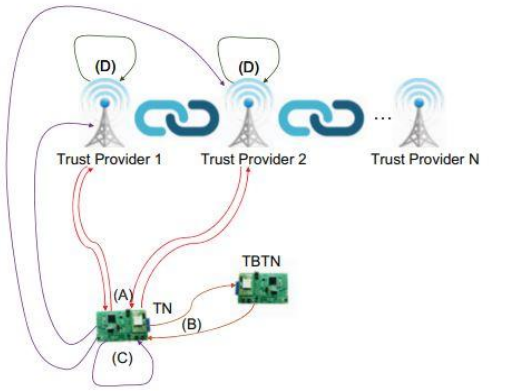


Fig. 4. The proposed blockchain-based trust management solution.

C. IoT Edge Computing Trust Management Mechanism

As Internet of Things (IoT) technology is evolving, more users are participating in smart cities via smart mobile devices (smart phones, smart watches, wearables etc.) or variable sensors. The main challenge in smart city IoT edge computing systems is finding trustworthy participants. Every IoT device is not reliable. Some smart IoT devices can harm your network as well as service, lowering the quality of service in your platform. Accordingly, we propose a dynamic black-and-white list-based smart device selection recommendation mechanism and solve how trusted participants are selected. This will improve the service quality of IoT in smart cities. We will check the stability and validity of trust mechanisms by introducing evolutionary game theory. The Lyapunov theory is being utilized to show how trust management methods work and how stable they are. The effectiveness is confirmed by doing analysis on smart cities air quality monitoring systems and health monitoring systems. Experiments show that interconnection of end devices is facilitated by trust management mechanisms and malicious attacks are also resisted.

As IoT is developing, Mobile Edge computing (MEC) has become a hotspot for industry research. Cloud computing is used in developing Mobile Edge computing, this helps in

- reducing network bandwidth
- response time of service requests is reduced
- power consumption is reduced
- improved data security

Smart cities operations are managed by using cloud computing, IoT, big data analytics etc. This helps in improving the quality of life for city dwellers. These include intelligent homes, smart health care, smart transportation, and intelligent weather predictions. There are multiple smart devices which play an important role in the sensor layer. These smart devices (personal laptop, smart phone, sensor etc.) communicate with each other and help in computing accurate data for smart city management. Edge service providers receive this data via intelligent terminals and then process it. When users simultaneously send large amounts of data to the edge service provider, this reduces the latency of the service due to the large amount of data transmitted. In smart cities, The main challenge here is to select trusted participants because some smart IoT devices can maliciously damage networks and services. This affects the quality of the system. However, in truly smart cities, IoT edge computing systems are subject

to many malicious attacks and security risks. Thus service providers need trust management mechanisms to secure their systems and improve quality of smart device support behaviour and improve user satisfaction.[8] Recommended mechanism for smart device selection is based on dynamic black and white lists, this helps in solving problems of selecting trusted participants. It was confirmed whether the performance of the proposed regulatory mechanism is exceptional. [9]

1. Key features in this study

- apply a reliability calculation method based on multi-intelligent devices and multi-edge centres.
- trust relationship between smart devices and edge service providers
- personalized device selection recommendation mechanism based on dynamic blacklist and whitelist
- Introduction to evolutionary game theory and theoretical research on the validity and stability of trust management mechanisms.
- Lyapunov's theory is used to demonstrate the effectiveness and stability of the trust management mechanism.
- Effectiveness verified through smart city personal health monitoring and management systems and the air quality monitoring and analysis system.

III. RESULTS AND ANALYSIS

This section includes the individual analysis and comparative analysis based on the Literature Review.

A. Individual Results

In this part we will discuss and report the results of different experiments mentioned in literature review.

1. Multi-Source Trust Fusion Mechanism In Edge Computing

Definition
A distributed system proposed that implements the multi source trust management system for edge computing devices, that assures secure data access through trustworthy cloud service providers.

Effect on Edge Computing
Multi Source trust management system reduces the malicious nodes in the edge computing. The malicious nodes basically produce errors in the feedback of nodes given by the system which affects the local perception. [2]

Results
According to the experiments done in section 2.1 the accuracy of normal nodes have been achieved upto 80% and the nodes with malicious data have reduced to 20%

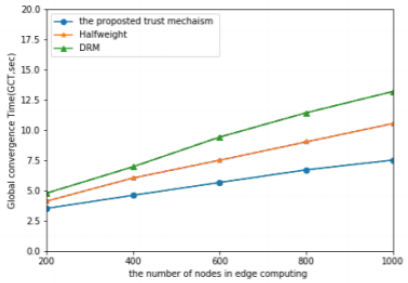


Figure 4. The proportion of MNs is 20% and that of PCN is 20%.

Table 1. Parameters and their possible value.

Parameters	Possible Values	Description
m	200	the total number of devices
n	1000	the number of edge nodes
t	1000	time-steps of simulation running
Δt	20	time-window for trust computing
PCN	20%, 40%	the percentage of collaborative nodes
MN	20%, 40%	the percentage of malicious nodes

2. Trust Management using BlockChain

Definition:
BlockChain Trust Management in edge computing for secured retrieval of trust estimates.

Effect on Edge Computing:

The Blockchain Systems has shown resilience towards malicious nodes.

Results:
The system is proven to be resilient to malicious attacks for a percentage of bad nodes, about 40% of the total number of network nodes. [5]

Simulation parameter	Value
Simulation tool	Ns3-3.13
Simulation run time	2 hours
Simulation coverage area	50m x 50m
Nodes distribution	Random
Total number of nodes	50..100
Number of malicious nodes	20%, 40%
trust update period	300s
Initial trust value	0.5
trust interval	0..1
Multichain mining diversity	0.3
Multichain Block size	8Mb
Multichain Transaction size	4Mb

TABLE I
NETWORK RELATED PARAMETERS USED IN SIMULATION ANALYSIS

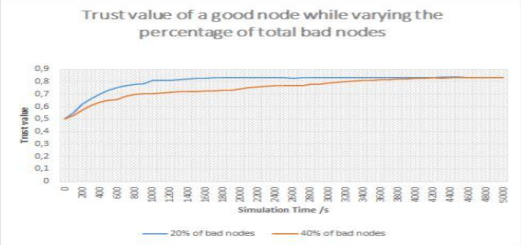


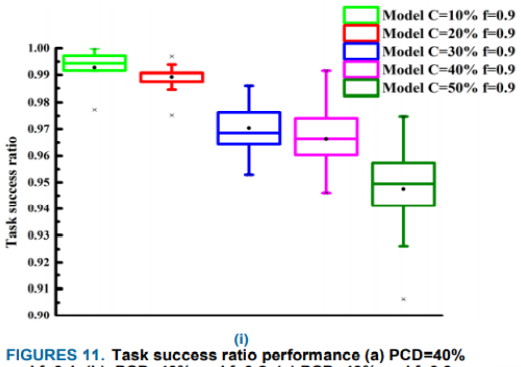
Fig. 4. Well behaved node trust evolution

3. IoT Edge Computing Trust Management Mechanism For Smart Cities

Definition:
A Reliable IoT Edge Computing Trust Management Mechanism

Effect on Edge Computing:
By Filtering smart IoT devices in our network chances of malicious nodes is reduced in edge computing.

Results:
According to the experiments done in section 2.3 Task success ratio varies on percentage of malicious users. As the malicious users ratio increases, task success ratio decreases, But the decrease is very slow which indicates that the model used in this study has robust performance. The accuracy of task success ratio reaches 80%.



FIGURES 11. Task success ratio performance (a) PCD=40% and f=0.1. (b) PCD=40% and f=0.2. (c) PCD=40% and f=0.3. (d) PCD=40% and f=0.4. (e) PCD=40% and f=0.5. (f) PCD=40% and f=0.6. (g) PCD=40% and f=0.7. (h) PCD=40% and f=0.8. (i) PCD=40% and f=0.9.

B. Comparative Analysis

1. Multi Source Trust Fusion Mechanism

Trust fusion Mechanism provides a way of trust management using Grid like structures.

Pros

Security

- Secure algorithm for trust update
- Reward and punishment mechanism for nodes
- Multi source trust mechanism : Direct trust and recommendation trust

Cons

Efficiency

- High processing power required for Algorithms
- Low speed

2. IoT Edge Computing Trust Management Mechanism

Pros

Personalization

- Personalized content perception
- Personalized device recommendation system

Cons

Efficiency

- Personalization causes security threats

3. Trust Management in Edge Computing using Block Chains

Block Chains in Trust Management are built up to induce trust on the basis of system security ,reliability,data sharing and transparency.

Pros

Enhanced Security

- Tamper-proof decentralized architecture
- Architecture for collaborative processing activities in edge computing
- End to end encryption is provided to prevent unauthorized access
- A higher level of privacy of nodes is ensured through the architecture.

Efficient Data sharing

- Smart contracts and consensus
- Optimized sharing and exchange of data

Efficiency

- Processing speed is high
- Less processing powers needed

Cons

Data Modification is Difficult

- Modification of data is not easy
- codes are to be be rephrased
- Hectic mechanism

According to the Analysis ,multi source fusion mechanism, Iot trust management and trust management using BlockChains in edge computing are very useful techniques for maintaining a reliable interaction of nodes in edge computing.

4. Quantitative Analysis

Percentages Amount of Reduced Malicious Nodes

Multi Source Trust Management	20% and 40%
Iot Trust Management	10% to 50%
BlockChain based Trust Management	20% and 40%

Accuracy of Blockchain is similar to multi fusion technique but higher than IOT trust management technique

5. Qualitative Analysis

Multi Source fusion mechanisms based on grid like structures provide security through reward and punishment mechanisms of nodes.High processing algorithms are used which require high processing powers whereas in IoT trust management technique, provides a personalized behaviour of requests but is less efficient in terms of security.However,trust Management using BlockChain relatively higher security using decentralization and distributed systems, processing powers are comparatively low.Moreover, data access is difficult but data sharing is efficient due to smart contracts.Therefore,BlockChain proves to be more reliable in trust management in edge computing.

IV. PROPOSED IMPROVEMENTS

In this section we proposed some improvements in the solutions we extract from analysis of literature review by using basic knowledge of trust management mechanisms.

A. Improvements Proposed in Solution 2.1

In section 2.1 we use a multi layer fusion trust management system in order to remove malicious nodes. This is another trust management known as Agent-based Trust Model (ATSN). In this system we use promiscuous mode to monitor the behavior of

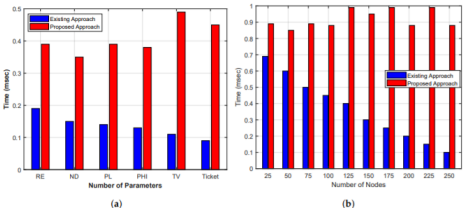
malicious nodes and normal nodes and then classify them as good or bad ones. [9]

We use this trust space equation

$$RS = \{\langle p, n\rangle | \, p, n \in R;\ p, n \geqslant 0;\ t = p + n\}$$

This model make major improvements like,

- Decrease computation cost
- Minimize memory usage
- This solution removes malicious nodes as well as **decreases the negative effect** of malicious nodes which are undetected by the system.
- Calculate the trust values of nodes more accurately.



B. Improvements proposed in Solutions 2.2

Use of Proof of Stake for Improving working of BlockChain technology.Techniques are to be tested results are not shared yet.

C. Improvements proposed in Solutions 2.3

We are unable to find any mechanism which can improve the performance of these solutions. But we hope we can find some solutions in future in order to increase the accuracy of these solutions.

V. CONCLUSION AND RECOMMENDATIONS

A. Conclusion

This paper presents a reliable Trust Management mechanism for edge computing. Trust Management mechanism is introduced to cater the security needs of edge computing because edge computing is not limited to certain companies, It will become an infrastructure like 5G. In this paper we have compared three major algorithms of Trust Management Multi-Source Trust Fusion Mechanism, Block Chain Mechanism and IoT Edge Computing Trust Management Mechanism. Experiments show what issues were created as a result of absence of trust management and how trust management solves these issues. Architecture and Working of trust Mechanism Algorithms were discussed. In Conclusion Trust management increases the efficiency of the edge system by adding a bridge type connection between input nodes and cloud. It uses different algorithms based on the architecture of the edge system. Every algorithm has its own trust formula which gives us the cost of the algorithm as well as number of malicious nodes in the system so that we can improve our algorithm to remove more and more such malicious nodes. So, by observing critical analysis we can say that blockchain is better then all in terms of accuracy, speed and cost.

B. Recommendations

In this paper we have seen three types of trust management mechanisms in edge computing, but in reality there are many other trust management techniques.

- As Edge computing is becoming more and more popular, security risks are increasing day by day.
- Trust management still needs much research as it is an emerging technology. Companies should start working on improving trust management mechanisms so that security is not compromised.

- There are many different methods and means to build the trust model, therefore it is also necessary to standardize it to improve the universality of the model.

REFERENCES

[1] H. Hamilton. "What is Edge Computing", *The Network Edge Explained*. *cloudwards.net*. Retrieved 2019-05-14.

[2] W Wenping, X .Li, L H. Liyang Hu, Y. Li "An Efficient and Credible Multi-Source Trust Fusion Mechanism Based on Time Decay for Edge Computing" *Trustworthy Distributed Computing and Service, Ministry of Education*, Vol 5, 19 March 2020

[3] JK. Kantert, S. Edenhofer, Sven Tomforde, Christian Müller-Schloer,"Representation of Trust and Reputation in Self-Managed Computing Systems",Vol 2, 26-28 Oct. 2015

[4] X. Liu "Initial Study on the Architecture of Field Observation in the 5G Era" , *2018 IEEE 5G World Forum (5GWF),*15-18 April 2019.

[5] A. Lahbib, K. Toumi, A. Laouiti, A. Laube, S. Martin, "Blockchain based trust management mechanism for IoT", *2019 IEEE Wireless Communications and Networking Conference (WCNC),* 15-18 April 2019.

[6] Marcello Cinque, Christian Esposito, Stefano Russo, "Trust Management in Fog/Edge Computing by Means of Blockchain Technologies", *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. 30 July-3 Aug. 2018

[7] B. Wang, M. Li, X. Jin, C. Guo, "A Reliable IoT Edge Computing Trust Management Mechanism for Smart Cities", *Technology: Electrical engineering. Electronics. Nuclear engineering,* Vol 6, 15 July,2017.

[8] B. Wang, M. Li, X. Jin, C. Guo, "A Reliable IoT Edge Computing Trust Management Mechanism for Smart Cities", *IEEE Access,* Vol 5, 06 March 2020

[9] G. Han, J. Jiang, L. Shu, J. Niu, H, Chao, "Management and applications of trust in Wireless Sensor Networks: A survey", *Journal of Computer and System Sciences* Volume 80, Issue 3, May 2014, Pages 602-617