Secure Access Control Model for Cloud Computing Environment with Fuzzy Max Interval Trust Values

Aakib Jawed Khan[1]
Research scholar
Department of Electrical Engineering
JamiaMilliaIslamia
New Delhi, India

Shabana Mehfuz[2]
Professor
Department of Electrical Engineering
JamiaMilliaIslamia
New Delhi

***Abstract*—Cloud computing needs service provider with reliable communication for increasing the user trust. As existence of cloud depends on quality of services, evaluation of this trust value needs to be carried out by the cloud. Many of the web services provided by E-commerce, social sites, digital platform maintain this for the faith of user by estimating the reliability of service provider. This paper focuses on a model that can identify real nodes by its behavior in cloud. Here fuzzy max interval values have been evaluated from the transactional behavior of the node in fixed interval. By increase in transaction count, trust value of real node trust increases and trust value of malicious nodes decreases. The work is based on Role based Access Control (RBAC), which has three type of roles (Admin, Data owner, Node). Data owner content security was achieved by AES algorithm and only trusted node can access those resources. Experiment was performed by carrying out simulations on ideal and environment under attack. Analysis of evaluation parameters values shows that proposed model of fuzzy max interval trust is better as compared to other existing Domain Partition Trust Model (DPTM), for identification of malicious nodes.**

Keywords—Cloud computing; encryption; fuzzy logic; trust computing; role based access control; resource management

I. Introduction

Cloud computing offers web supported services on an efficacy source to the trade development. Shared resources are allotted to the service provider on rent where working and management of allotted resource is done independently. Therefore safety is a primary importance in the cloud atmosphere. The client loses the control of information in the cloud environment and therefore an appropriate faith system is necessary to guarantee safety and security of records [1]. As the cloud computing is collection of diverse narrow systems and embraces the associates from various surroundings, the safety in cloud is obscure. On one side, the safety machinery should offer warranty protection adequate to the client, on the further side, the safety machinery should not be too compound to put the clients into an inopportune circumstances. The flexibility of the client nodes and commercial operating systems has significant features for sustaining their wide acceptance. Conversely, that extremely similar directness and suppleness have been confirmed to be a dual edged weapon, since it brings difficulty, diminishes conviction degree and danger against safety. So there should be stability among the safety and the expediency [2]. While downloading records from the web, the clients mistakenly downloads damaging software such as key logger. The user-sensitive information such as login and password gets hacked by the software such as Spyware, Trojans etc. The service provider works with the client interface in order to access the cloud services. The information in the contaminated PC is no longer secure. Thus even after engaging every protection method such as installing antivirus software, there exist the threats of information getting hacked when we utilize the internet services of cloud computing [3].

A trust management system assists cloud service suppliers and clients to gather the advantage brought about by cloud computing equipment. Regardless of the advantages of trust management, more than a few problems connected to universal trust measurement mechanisms, doubted comments, poor verification of comments, solitude of applicants and the need of comments incorporation is still required to be tackled. Customary trust organization approaches such as the exercise of Service Level Agreement (SLA) are insufficient for compound cloud atmospheres. The unclear rules and uncertain scientific specifications of SLAs can guide cloud service clients to be incapable to recognize dependable cloud services [4, 5].

In this paper, a fuzzy max interval based trust model is given which uses centralized data updation. It identifies real node behavior by calculating the trust value and secures the data by using role based model and owner resource encryption.

Rest of the paper is organized as follows. Section II gives a brief literature survey of trust models in cloud computing. In Section III, proposed model has been presented. Section IV describes the results and implementation. Conclusion is given in Section V.

II. Literature Survey

In [6], authors has concentrated on investigation of secrecy and information sensitivity & safety issues in cloud structural design and atmosphere covering all the phases of existence cycle of statistics. In this paper, the authors detailed privacy protection, information protection, records separation, cloud safety and cloud computing. They have examined these subjects and as well given a key for determining these problems. These problems are chiefly at SPI (SaaS, PaaS, IaaS) level and the most important dispute is information distribution. Once work achieves security of data and privacy of data owner, paper has evaluated the trust on the basis of social relationship based on past transaction and energy availability of nodes.

In [7] authors have provided a platform to utilize an extensive variety of services that are based on the web to deal with our business events & a variety of services of data equipment. But in addition to all the benefits, it also boosts the risk for safety when a TTP (Trusted Third Party) is concerned. By connecting a TTP (Trusted Third Party) there still remains a possibility of heterogeneity of clients which affects safety on a cloud. In this investigation, the authors suggest a TTP (Trusted Third Party) autonomous approach for IDM (Identity Management) with the ability of utilizing unique information on unreliable information protection procedures for Building faith in Cloud Computing. By means of predicate information over the set information and utilizing multi association computation and computing and vigorous package method are the approaches utilized at this point. In this system the package has self-reliability checking procedure. It comprises of protection methods, privacy plans and virtual mechanism for strategy enforcement of these plans. The declaration lets the usage of IDM solicitation on untrustworthy clouds. Cloud computing is extremely effectual safety service that is based on conceptual knowledge. Information retrieval and safety of the data is the major area of work in cloud computing.

In [8] authors have suggested an innovative trust model with the help of an algorithm to reduce trust management load on system and increase malicious node detection accuracy. Detachment of nodes into domains is helpful for decreasing the overhead of trust management in terms of trust storage and computation. Domain and cross-domain sliding-windows are planned and operated to accumulate the nearly all fresh conviction values. Then, an algorithm is intended to calculate domain and cross-domain trust values for nodes, and a filter process is implemented to eliminate hateful trust assessments and hateful nodes from a domain.

Azad et al. [9] have proposed a node to node trust evaluation algorithm in IOT. Only standing social belief metric is measured in this learning. The applicants allocate a trust rate to the machine based on their knowledge and communications with the machine. Then, they drive faith values' cryptograms to the bulletin board. Using safe multi-party calculation procedures, the reputation activist analyzes the universal status of machine by using the information cryptograms in the bulletin panel.

Rafey et al. [10] have improved collaboration among trusted nodes and regulated the faith scores dynamically based on the node performance. In this work, node operation characteristics (e.g., node calculation power, assurance, perspective importance, and response), and node community characteristics (e.g., friendship, centrality, and connection) are measured. In the trust calculation stage, each node calculates in general faith values of further nodes supports on its own straight communications and proposals from further nodes. In addition, their representation incorporates the community relationships and background of contacts in the faith calculation. The trust correctness in this representation can be amplified by suggestions from false nodes that allocate superior trust values to their collection of associates.

In [11] author has developed a health environment for an effective network services with resistance against malicious node trust attacks. To calculate the trust paper has utilized node energy as well as social performance of node in the network based on social similarities. This paper has not considered the dynamic nature of nodes in the network.

So a model was required to overcome the problem of increase in the decision time for interdomain communication in de-centralized systems, as untrustworthy values are stored in the domain or cross-domain Algorithm [8]. Malicious nodes can increase the trust of other malicious node, hence detection of these kind of nodes is essential. An algorithm to monitor the behavior should be developed for the classification of nodes, as malicious nodes always produce some unfair pattern which can be identified.

Proposed model presents a fuzzy max interval based trust model in unreliable cloud access environment. The main contributions of the present work are:

1) For dynamic service adoption in cloud environment, a trust evaluation model with fuzzy max interval is provided while using centralized data updation which enhances the efficiency of proposed model.

2) Proposed algorithm identifies the real nodes by node behavior in cloud environment and calculates trust value for each node to assert the authenticity of the node.

3) To secure the data, it used role based model and owner resource encryption. It evaluates the proposed fuzzy max interval trust model by calculating the malicious node convergence and trusted node convergence.

Access Control Systems: There are three type of access control systems present, discretionary access control (DAC), Role based Access control and mandatory access control (MAC). Proposed strategy is works on RBAC. It is a model used in secured network for defining role and privileges. As per role, access of resources is granted. This model can be further enhance by monitoring role to role sequence of actions for finding malicious activity by the user / employee / etc. in a organization or network. This paper has also improved this monitoring system by estimating the user's social trust as per the series of actions performed.

III. Proposed Model

This section gives a brief review of the proposed model with the help of a block diagram along with the explanation of different section of the blocks. The proposed algorithm provides a complete architecture of the work as well. This work assumes an area with N number of nodes where one node communicates with other. Communication approach between two nodes is termed as transaction T. Paper has three types of roles; first is Admin, second is Data Owner, third is Node. Information of each node and transaction count, with successful number of transaction was centralized. Hence trust evaluation of the nodes was also centralized. Table I shows various symbols used in the proposed algorithm.

TABLE I. SYMBOLIC TABLE

Symbol	Meaning
N	Node
D_{ij}	Direct Trust between i, j nodes
CB	Centralize Bridge
T_t	Trust of ith node
S_t	Successful Transaction
M	Malicious Node
R	Real Node
K	Total Number of transaction between i, j node
Iij	Fuzzy Interval value of Ith node w.r.t. jth node
T_k	Kth transaction between nodes
M	Number of Window frame

A. Roles Definition

1) Admin (CB): This is centralized body in the model which takes care of all data owners, Node, and maintains different other information which is required for working securely. So admin manage all set of password, number of transaction, and trust value. Here all set of password, number of transaction, trust are also stored and updated by admin.

2) Data Owner (DO): This role acts as service provider where data stored by the owner is accessed by other type of Node. To enhance the security of data owner CB provides security access to DO for creating initial access of data. To further enhance the security, data is encrypted by using AES algorithm. Hence each data owner has its own set of Keys shared by DO to its user (Node). AES algorithm first encrypts the data and stores on cloud while its user can access this by search query.

3) Node: This role is created by DO, so if DO creates a Node then it can access DO data by search option. As DO has created this Node so reverse keys of AES were applied for that data owner Node. Search query of the node is first encrypted, so security of user query maintained by this operation. Entire searching function does not de-crypt resource (DO data). Search query is also encrypted for increasing the communication security, as work is performed on unreliable cloud.

4) Hierarchal cluster: All set of nodes as per types of services were grouped into set of clusters. As cluster size increases to a certain threshold, further clustering of nodes takes place. This is shown in Fig. 1. This reduces communication cost [12]. Information of these nodes in form of number of total transactions, number of successful transactions and trust score was maintained by centralized bridge CB.

5) Window: In this work, m size window moves to monitor the transaction behavior of various nodes in different domain of the network. Here after each m number of time frames, trust value of the nodes were evaluated. This can be understood by diagram present in Fig. 2, where each block is m^{th} time frame where any number of transactions may occur between nodes. This transaction may be of same or different domain. Fig. 3 shows the flowchart of malicious node detection.

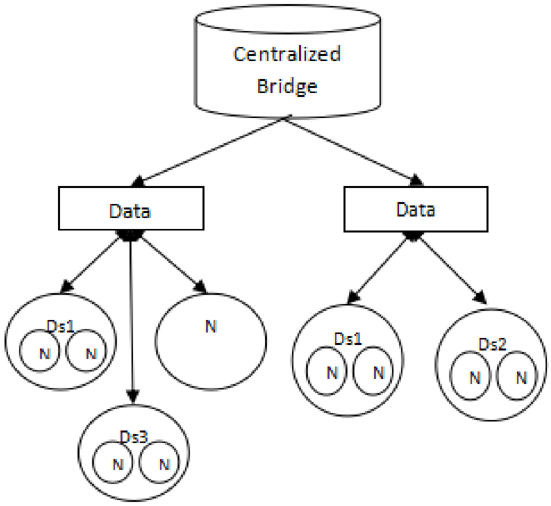

Fig. 1. Centralized Clustering of Nodes.

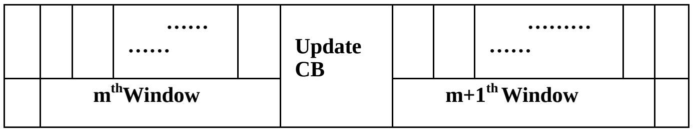

Fig. 2. Monitoring the Transaction behavior of Nodes.

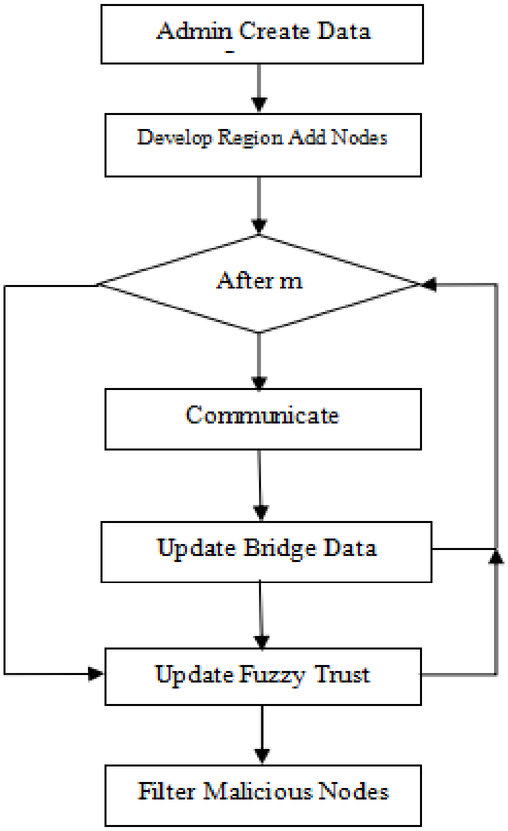

Fig. 3. Flowchart of Malicious Node Detection.

B. Direct Trust

A node can generate its trust on other node from its previous set of transactions. If Node *i* request a service of node *j* then transaction happen between *i*→*j*. Hence direct trust between them is evaluated by Eq. 1 and 2.

$$D_{ij} = \frac{S_t}{k} \quad (1)$$

$$S_t = \sum_i^k t_i \quad (2)$$

In equation 2 $t_i$is i_{th} transaction out of total k transaction happen between *i*→*j*. t_i is 1 when transaction is successful otherwise its value is 0. D_{ij} is direct transaction value for *i*→*j*. It means direct transaction value for j→I is different.

1) Centralized bridge: In this model all set of information related to node activities has been managed by this bridge [13]. Hence number of transactions between nodes and number of successful transactions S_t were managed by centralized bridge. This has trust value for the nodes as well. To evaluate trust of a node, proposed model uses Fuzzy Max Interval approach.

C. Fuzzy Max interval

Here a matrix of N x N was developed for the network. In this matrix each row is representing number of different combination of transactions occur between nodes of respected row, column [14]. Let that matrix is F whose dimension are NxN where each cell of M represents direct trust D_{ij}, value between nodes.

Eq. 3 generates max interval value.

$$I_{ik} = (Max(F_i) - F_{ik})k = \{1,2, \dots \dots . N \quad (3)$$

In equation 4 I_{ik} is the interval value of i^{th} node for other set of k nodes. Max(F_i) is the maximum value of F matrix for i^{th} row.

D. Trust Score

In this step one single value calculated corresponds to all set of fuzzy max interval, so this term is called as Trust score [15]. This is very simple as the step given in Eq. 3 of interval values is sum of trust score.

$$T_i = \frac{1}{\sum_{j=1}^{k} I_{ij}} \quad (4)$$

Hence by Eq. 4 trust value of nodes were evaluated by the centralized bridge.

E. Proposed Algorithm

```
Input: CB, m // S: Services
Output: T // Trust
DO←Create_DataOwner(CB)
N←Create_DataUser(DO)
R←Resources(DO) // R : Resources
CB←Hierarchal_cluster(N, R, CB)
Loop 1:m
    i ←Random(N)
    j ←Random(N)
    if i and j belong to same Domain D_s
        CB←Increase_Total_Transaction(CB, i, j)
        If t_ij is successful
            CB←Increase_Successful_Transaction(CB, i, j)
        EndIf
    OtherwiseifTj>β
        CB←Increase_Total_Transaction(CB, i, j)
        If t_ij is successful
            CB←Increase_Successful_Transaction(CB, i, j)
        EndIf
EndLoop
Loop i=1:N
    Loop j=1:N
        Dij←CB
        Fi←Dij
    EndLoop
    $I_{ik} = (Max(F_i) - F_{ik})$
    Ti←Trust_Score(Iik)
    CB[i]←Ti
EndLoop
```

Attacks: Proposed algorithm was tested for two types of attacks. The first one is black hole attack. In this attack malicious node takes a service request and do not fulfill that request hence successful count of transaction get reduced. So detection of these kinds of malicious nodes was carried out by checking the trust value where trust values decrease with increase in number of unsuccessful transactions. Here direct trust value of nodes reduces to zero. Malicious node detection by only using direct trust value is not sufficient.

The second type of attack for which algorithm was tested was, Group Attack. In this attack if more than one malicious node mutually increases successful transaction than direct trust of this node is higher, but it's relation with other set of nodes will help to identify this malicious action. Let us consider six nodes, one to four out of six are real nodes and last two are malicious in nature. After *m* frame centralized bridge have direct trust values as shown in Table II.

TABLE II. NODE DIRECT TRUST VALUE MATRIX AT CENTRALIZED BRIDGE

Nodes	1	2	3	4	5	6
1	Null	2/2	2/3	¾	0/2	0/4
2	3/3	Null	2/2	2/3	0/4	0/1
3	2/2	¾	Null	2/3	0/3	0/4
4	¾	2/3	¾	Null	0/1	0/2
5	2/3	3/3	2/3	4/5	Null	5/5
6	2/3	1/1	2/3	Nil	4/4	Null

In Table II, each cell is direct trust value between existing nodes. So interval score of 1st node is Max (Column 1) is 1, hence.

	I_{11}	I_{12}	I_{14}	I_{15}	I_{16}
I =	0	0	0.25	0.33	0.33

In similar way Interval value of 5th malicious node where Max(Column 5) is 1.

	I_{51}	I_{52}	I_{53}	I_{54}	I_{56}
I =	1	1	1	1	0

Hence Trust score of 1st node is 1.098 while 5th node trust value is 0.25. Hence in this way proposed model detects malicious node.

IV. Experiment and Results

Implementation of service provider trust evaluation in unreliable cloud environment was done on MATLAB platform. Here different number of virtual nodes with transaction were perform on this platform under windows operating system having 4GB RAM with I3 processor.

A. *Evaluation Parameters*

As various techniques involve different steps of working for classifying user query into appropriate category, it is highly required that proposed techniques or existing work should be compared on same experimental environment. This paper has used following parameters:

Malicious Node Convergence (MNC): This term is the ratio of number of malicious nodes to number transaction required to detect. Hence higher value of MNC ratio is better as it take low number of transaction for detection of malicious nodes.

$$MNC = \frac{NumberofMaliciousNodeinNetwork}{NumberofTransactionNeedtoDetect}$$

Trusted Node Convergence: This term is the ratio of number of Trusted nodes to number of transaction required to detect. Hence higher ratio value is better as it take low number of transaction.

$$TNC = \frac{NumberofTrustedNodeinNetwork}{NumberofTransactionNeedtoDetect}$$

B. *Results*

Comparison was done on three environmental situations, first was Ideal (No attack), second was Black Hole Attack and third was Group Attack. Comparison was done with Domain Partition Trust Model (DPTM) method proposed in [8].

1) Ideal Condition: In this environment proposed model FMI-TM (Fuzzy Max Interval-Trust Model) performs better as shown in Fig. 4 that convergence of trusted node detection was done in less number of transaction as compared to previous approach DPTM in [8]. As proposed model takes approx. 950 transaction for trusted node detection and DPTM takes 6300 transaction for same situation.

Fig. 5 shows that proposed model has increased the trusted node trust value in less number of transactions and maintained the value for further transactions effectively. While previous approach DPTM has also increased the trusted node trust value but it take large number of transaction. This high increase in trust value was achieved by using the trust score obtained from the fuzzy max interval in FMI-TM.

Above Fig. 6 shows that proposed model FMI-TM has increase maintain the trust value of trusted score above 0.8 in all sets of transaction. This trust value was retaining by centralized storage as Fuzzy Max Interval value got updated regularly in each domain.

a) Black hole and group attack: In this environment, proposed model FMI-TM (Fuzzy Max Interval-Trust Model) performs better as Fig. 7 shows that convergence of malicious node detection was done in less number of transactions as compared to previous approach DPTM in [8]. As proposed model takes approx. 8260 transaction for trusted node detection and DPTM takes 11780 transaction for same. In case of group attack as malicious node increases the trust value of other malicious node, so DP-TM takes larger transaction, while proposed FMI-TM takes less number of transactions for detection. This reduction of transaction was achieved by fuzzy based trust score.

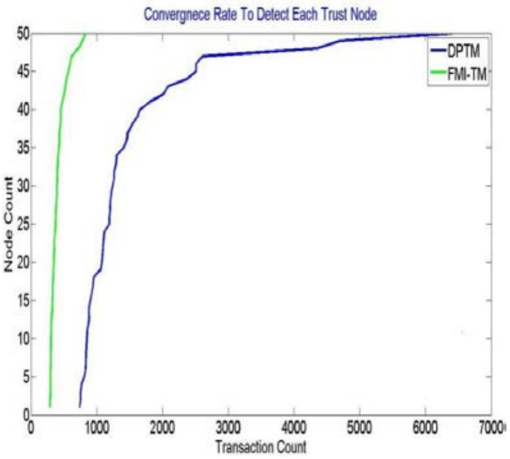

Fig. 4. Trusted Node Convergence based Comparison.

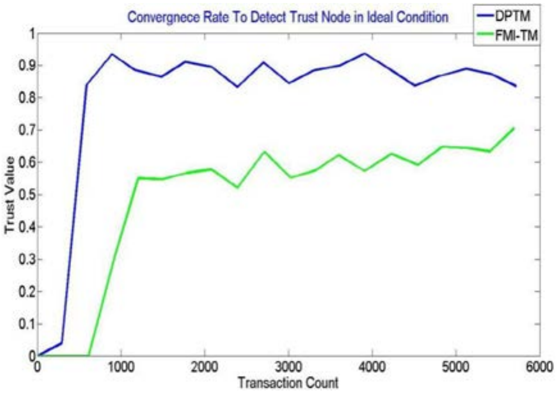

Fig. 5. Trusted Node Convergence based Comparison.

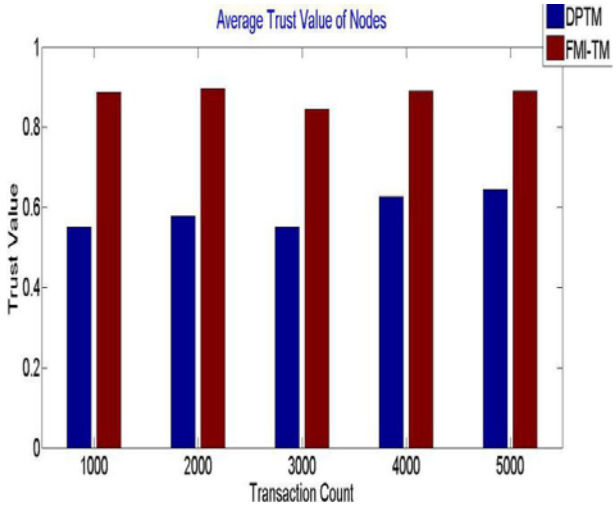

Fig. 6. Average Trusted node Trust value at different Number of Transactions.

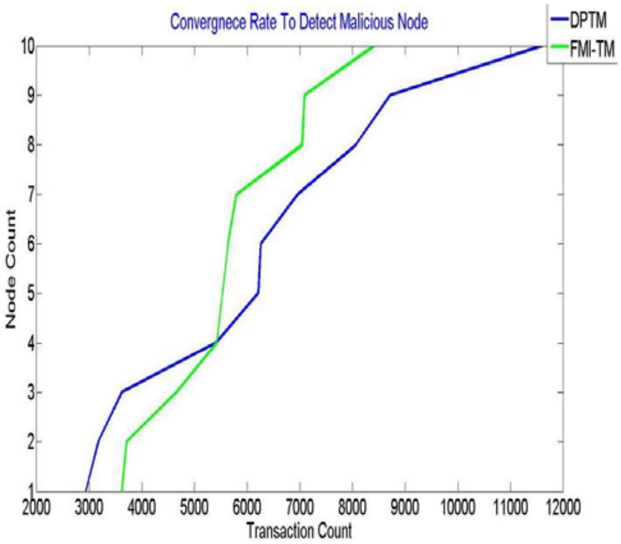

Fig. 7. Malicious node Convergence based Comparison for Black Hole Attack.

Fig. 8, 9 and 10 shows that proposed model has reduced the malicious node trust value in less number of transactions and maintained the value for further transactions effectively. While DPTM technique also decreases the trusted node's trust value but it involves large number of transactions. This high increase in trust value was achieved by using the trust score obtained from the fuzzy max interval in FMI-TM.

Fig. 11 and Fig. 12 shows that proposed model FMI-TM has reduced the average trust value of malicious score with increase in number of transactions. This pattern of decreasing trust value was obtained by the use of centralized storage and Fuzzy Max Interval value concept in proposed model.

Table III shows that proposed model has increased the convergence rate value of malicious and trusted nodes detection. It was obtained that under ideal condition convergence rate value was high while in attack environment this values decreases.

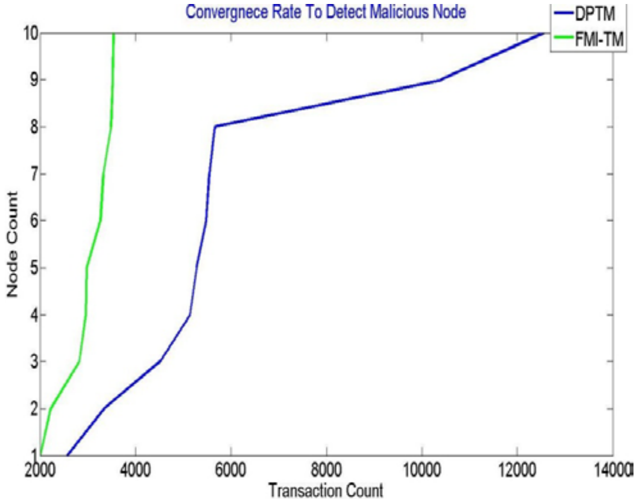

Fig. 8. Malicious node Convergence based Comparison for Group Attack.

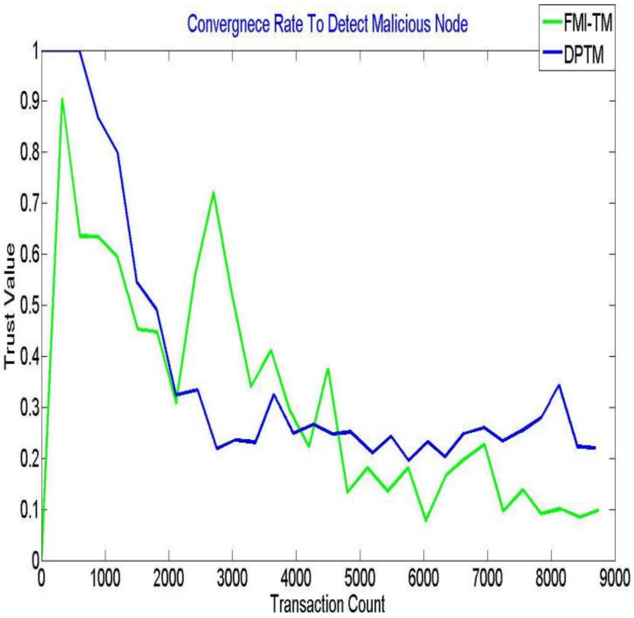

Fig. 9. Malicious node Convergence based Comparison for Black hole Attack.

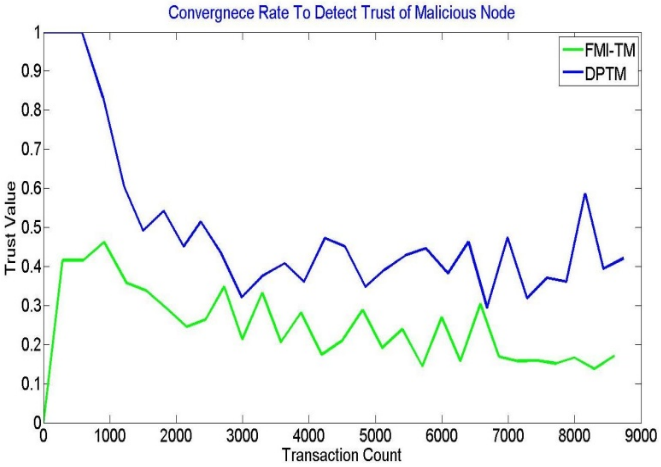

Fig. 10. Malicious node Convergence based Comparison for Group Attack.

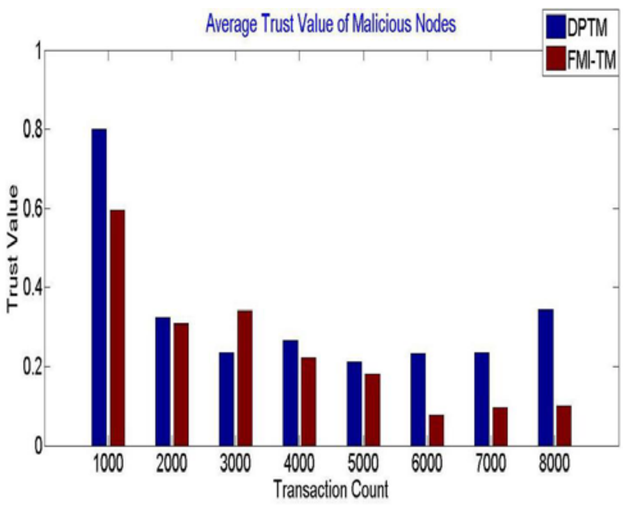

Fig. 11. Malicious node Convergence based Comparison for Black Hole Attack.

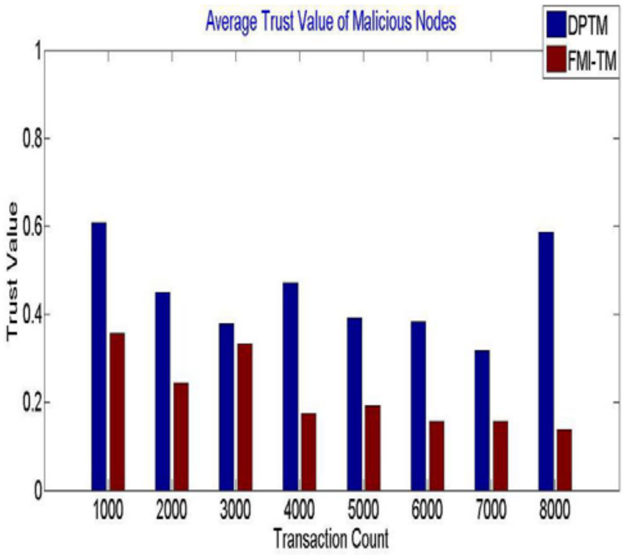

Fig. 12. Malicious node Convergence based Comparison for Group Attack.

TABLE III. CONVERGENCE RATE VALUE IN DIFFERENT CONDITIONS

Environment	DPTM	FMI-TM
Ideal	0.0078	0.0597
Black Hole	0.00086	0.0012
Group Attack	0.000796	0.0028

V. CONCLUSION

Cloud computing provide dynamic adaption of service sharing for company, individual, etc. So effective working of proposed model is highly required which directly depends on trust evaluation. This paper proposed a trust evaluation model by using Fuzzy Max Interval with multiple secure access for various role based access control users. Concept of centralized data updation was also enhances in this work as hierarchical cluster of nodes were developed, which was as per resource requirements for different data owners. Access of the resources was secured by involving AES encryption algorithm as well. Here model has increase the trust score of nodes with every successful transaction while its behavior with other nodes also affect the score value. Proposed model has reduced the malicious node trust score by identifying its working pattern with other nodes. Experiment and analysis was carried out on three environmental conditions ideal, black hole and group attack. Results were compared with existing method and it was obtained that proposed model has improved the malicious node convergence value by 58.6% and Trusted Node convergence value by 86.93%. In future researcher can adopt genetic algorithm for clustering of nodes into real and malicious nodes.

REFERENCES

[1] Talal H Noor, Quan Z Sheng, Abdullah Alfazi, Jeriel Law and Anne HH Ngu, Identifying fake feedback for effective trust management in cloud environments in Service-Oriented Computing, pp.47-58(2013 b).

[2] Talal.H.Noor, Sheng, Q.Yao, L.,Dustdar, S. and Ngu, A.H.H, CloudArmor: Supporting Reputation-based Trust Management for Cloud Services, IEEE Transactions on Parallel and Distributed Systems,99(2014).

[3] WanitaS ,Surya Nepal and Cecile Paris ,A survey of trust in social networks in Journal of ACM Computing Survey ,45(4),pp.1- 33(2013).

[4] Sheikh MahbubHabib, Max Mühlhäuser, Sebastian Ries**.** "Towards a Trust Management System for Cloud Computing".Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on, At Changsha, China.

[5] M. Alhanahnah, P. Bertok, and Z. Tari, "Trusting cloud service providers: Trust phases and a taxonomy of trust factors," *IEEE Cloud Computing*, vol. 4, no. 1, pp. 44–54, Jan./Feb. 2017.

[6] Satish Kumar and Anita Ganpati, "Multi-Authentication for Cloud Security: A Framework," International Journal of Computer Science & Engineering Technology (IJCSET),Vol. 5, Issue 4, pp. 295-303, Apr. 2014.

[7] V. Sulochana and R. Parimelazhagan, "A Puzzle Based Authentication Scheme for Cloud Computing," International Journal of Computer Trends and Technology (IJCTT), Vol. 6, Issue 4, pp. 210-213, Dec. 2013.

[8] Peiyun Zhang, *Senior Member, IEEE*, Yang Kong, AndMengchu Zhou. "A Domain Partition-Based Trust Model For Unreliable Clouds". IEEE Transactions On Information Forensics And Security, VOL. 13, NO. 9, SEPTEMBER 2018.

[9] Azad M.A., Bag S., Hao F., Salah K. M2m-rep: Reputation system for machines in the internet of things. Comput. Secur. 2018;79:1–16. doi: 10.1016/j.cose.2018.07.014.

[10] Rafey S.E.A., Abdel-Hamid A., El-Nasr M.A. CBSTM-IoT: Context-based social trust model for the Internet of Things; Proceedings of the 2016 International Conference on Selected Topics in Mobile & Wireless Networking (MoWNeT); Cairo, Egypt. 11–13 April 2016; pp. 1–8.

[11] Chen Z., Ling R., Huang C.M., Zhu X. A scheme of access service recommendation for the Social Internet of Things. Int. J. Commun. Syst. 2016;29:694–706. doi: 10.1002/dac.2930.

[12] Yubiao Wang School of Big Data and Software Engineering, Chongqing University, Chongqing, China ; Junhao Wen ; Wei Zhou ; Bamei Tao ; Quanwang Wu ; Zhiyong Tao. "A Cloud Service Selection Method Based on Trust and User Preference Clustering" IEEE Access Volume 7, 12 August 2019.

[13] L. Minh Dang , Md. JalilPiran, Dongil Han, Kyungbok Min and Hyeonjoon Moon. "A Survey on Internet of Things and Cloud Computing for Healthcare". MDPI, journal/electronics 6 July 2019;

[14] Xiuqin Ma, Hongwu Qin, NorrozilaSulaiman, TututHerawan, and Jemal H. Abawajy . "The Parameter Reduction of the Interval-Valued Fuzzy Soft Sets and Its Related Algorithms". IEEE Transactions On Fuzzy Systems, Vol. 22, NO. 1, FEBRUARY 2014.

[15] Mahdi Ghafoorian, DariushAbbasinezhad-Mood, and Hassan Shakeri. "A Thorough Trust and Reputation Based RBAC Model for Secure Data Storage in the Cloud". IEEE Transactions On Parallel And Distributed Systems 2018.