A Robust Model for Unreliable Cloud by Evaluating Trust Values

Sonanchal Singh **Prof. Sumit Sharma**
Vaishnavi Group of Institutions
Bhopal MP India.

Abstract - **Trust plays a crucial role in cloud environment to offer reliable services to the cloud customers. It is the main reason for the popularity of services among the cloud consumers. To achieve this, trust should be established between cloud service provider and cloud consumer. Trust management is widely used in online services, E-commerce and social networks. This paper focus on a model that can identify real nodes by its behavior in cloud. Here fuzzy max interval values were evaluate from the transactional behavior of the node in fix interval. By increase in transaction count real node trust value get increase and macilous nodes trust value get decreases. Experiment was done on ideal and attacked environment. Evaluation parameters values shows that proposed model of fuzzy interval trust is better as compared to other existing model of unreliable clouds, for identification of malicious nodes.**

Keywords- **Cloud Computing, Fuzzy logic, Trust Computing, Resource Management.**

I. INTRODUCTION

Cloud computing offers web supported services on an efficacy source to the trade development. The boarders split a band of assets that are scatter own and handled. Therefore safety is a chief apprehension in the cloud atmosphere. The clients will defeat the power of information in the cloud environment and therefore an appropriate faith system is necessary to guarantee records safety and security [1].

As the cloud computing is collected of diverse narrow systems and embraces the associates from various surroundings, consequently the safety in cloud is obscure. In one side, the safety machinery should offer warranty protected 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 honesty and elasticity of the PC and accepted commercial operating structures have been significant features sustaining their extensive 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 with the software such as Spyware, Trojans etc. while the client works with the client boundary in order to entrance the network services. The information in the contaminated PC is no longer secure. Thus even after taking every protection methods such as installing antivirus software as well, there exist the threats of our receptive information getting hacked when we utilize the internet service of cloud computing [3].An eff ectual trust management system assists cloud service suppliers and clients gather the advantage brought about by cloud computing equipments.

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 still require to be tackled. Customary trust organization approaches such as the exercise of Service Level Agreement (SLA) are insufficient for compound cloud atmospheres. The indistinct sections and uncertain scientific specifications of SLAs can guide cloud service clients to be incapable to recognize dependable cloud services [4, 5].

II. LITERATURE SURVEY

Chen et al. [6] 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 learning, the writers detailed privacy safety, information protection, records separation, cloud safety and cloud calculating. 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. Subsequent to the examination of information safety and confidentiality the inclusive key is to assemble the want of recognition and separation of information is main job at plan stage of cloud based functions.

Cloud computing [7] gives us a platform to utilize a 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 it's all benefit it also to boost the risk for safety when a TTP (Trusted Third Party) is concerned. By connecting a TTP (Trusted Third Party) there is still a possibility of heterogeneity of clients which effects safety on a cloud. In this investigation, the writers suggest a TTP (Trusted Third Party) autonomous approach for IDM (Identity Management) with the ability of utilising distinctive information on undependable information guard 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-dependability inspection of procedure, it comprise PII, defense mechanism, 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 abstract knowledge. Records recovery and safety of the defense of data is the major question in cloud building and atmosphere.

In [8] paper suggests a innovative conviction model and connected algorithm to reduce trust management transparency and progress spiteful node recognition capability based on domain division. 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 operate 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] planned mechanism to mechanism reputed system to appraise the dependability of equipment 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 analyze the universal status of machine by using the information cryptograms in the bulletin panel.

Rafey et al. [10] to improve collaboration among trusted nodes and regulate the faith scores vigorously based on the node performance. In this copy, node operation characteristics (e.g., node calculation power, assurance, context significance, 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 exaggerated by suggestions from false nodes that allocate superior trust values to their collection of associates.

Chen et al. [11] for effectual service composition and confrontation beside trust-related assaults. In their representation, they believe mutually QoS trust metrics as well as energy grade and excellence status and communal faith metrics based on communal likeness. Though, this learning doesn't believe the related and vibrant nature of faith.

III. PROPOSED MODEL

This section gives an brief review of the proposed model by block diagram of proposed model, with explanation of different section of blocks. Here proposed algorithm gives 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 term as transaction T. Information of each node and transaction count, with successful number of transaction was centralized. Hence trust evaluation of the nodes was also centralized. So table 1 shows various set of symbols:

1. **Window:** In this work m size window from moves to monitor the transaction behavior of various nodes in different domain of the network. Here after each m number of time frame trust value of the nodes was evaluate. This can be understood by below diagram where each block is mth time frame where more any number of transactions may occur between nodes. This transaction may be of same or different domain.

Table I:

1	2	…… ……	m	Update CB	1	2	…… …… …	M
m^{th} Window					$m+1^{th}$ Window			

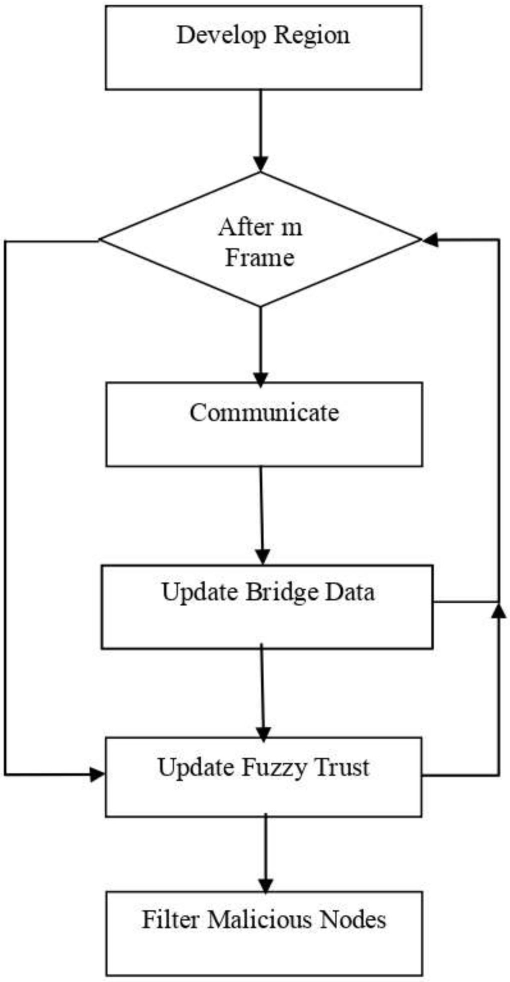


Fig.2. Proposed work training module.

2. Direct Trust

A node can generate its trust on other node from its previous set of transactions. Here if Node i request a service of node j than transaction happen between i□ j. Hence direct trust between them is evaluate as:

$$D_{ij} = \frac{S_t}{k}$$

$$D_{ij} = \frac{S_t}{k}$$

In above equation t_i is ith 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.

3. Centralized Bridge

In this model all set of information related to node activities were manage by this bridge [13]. Hence number of transaction between nodes, number of successful transaction S_t was manages by centralized bridge. This has trust value for the nodes as well. To evaluate trust of a node proposed model uses Fuzzy Interval approach.

4. Fuzzy interval

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

For generating interval following set of steps were followed.

$$I_{ik} = Max\, F_i - F_{ik}\, k = \{1,2, \dots \dots N\}$$

In above equation 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.

5. Trust Score

In this step one single value is calculate correspond to all set of fuzzy interval, so this term is called as Trust score. This is very simple as above step of interval values were sum up as per nodes.

$$T_i = \frac{1}{{}_{j=1}^{k} I_{ij}}$$

Hence trust value of above set of nodes were evaluate by the centralized bridge.

6. Proposed Algorithm

Input: CB, N, m, S // S: Services

Output: T // Trust

```
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
Otherwiseif Tj > 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.
```

7. Experiment and results

In order to implement above algorithm for intrusion detection system MATLAB is use, where dataset is use of different size. Neural Network Toolbox includes command-line functions and apps for creating, training, and simulating neural networks. This make it easy to develop neural networks for tasks such as data-fitting, pattern recognition, and clustering. After creating networks in these tools, it can automatically generate MATLAB code to capture work and automate tasks.

8. Evaluation Parameter

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

9. Malicious Node Convergence

This term is the ratio of number of malicious nodes to number transaction required to detect. Hence lower higher ratio value is better as it take low number of transaction.

$$MNC = \frac{Number\ of\ Malicious\ Node\ in\ Network}{Number\ of\ Transaction\ Need\ to\ Detect}$$

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

$$TNC = \frac{Number\ of\ Trusted\ Node\ in\ Network}{Number\ of\ Transaction\ Need\ to\ Detect}$$

10. Result

Comparison was done on three environmental situations first was Ideal (No attack), Second was Black Hole Attack and third was Group Attack. A. Ideal Condition: In this environment proposed model FMI-TM (Fuzzy Interval-Trust Model) has perform better as fig. 3 shown 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.

Fig.3. shows that proposed model has increase the trusted node trust value in less number of transaction and maintained the value for further transaction effectively. While previous approach DPTM has also increase 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 interval in FMI-TM.

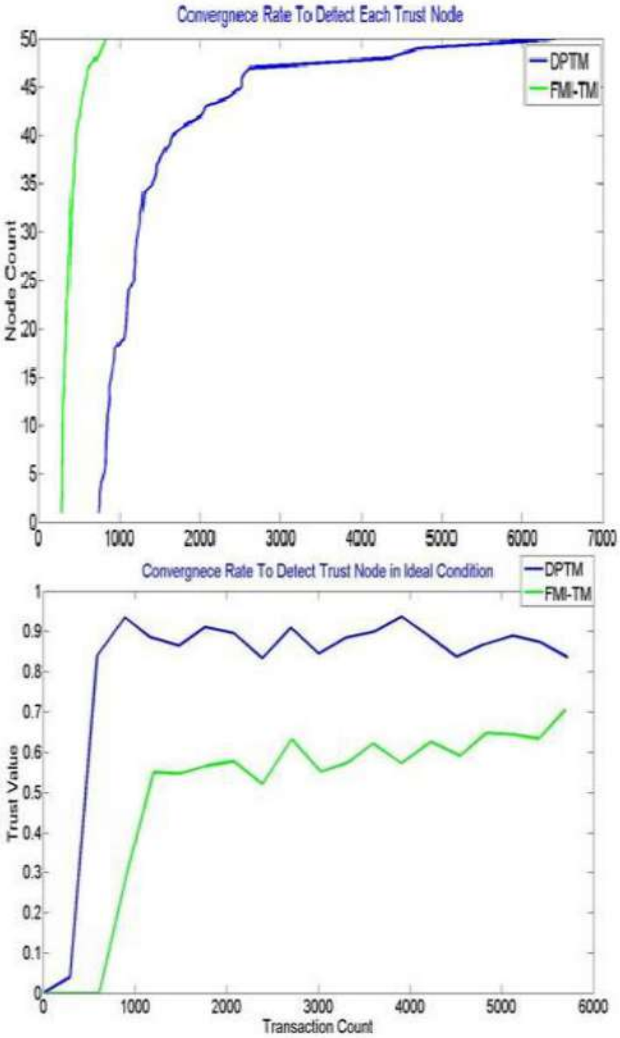


Fig.3. Trusted node convergence based comparison.

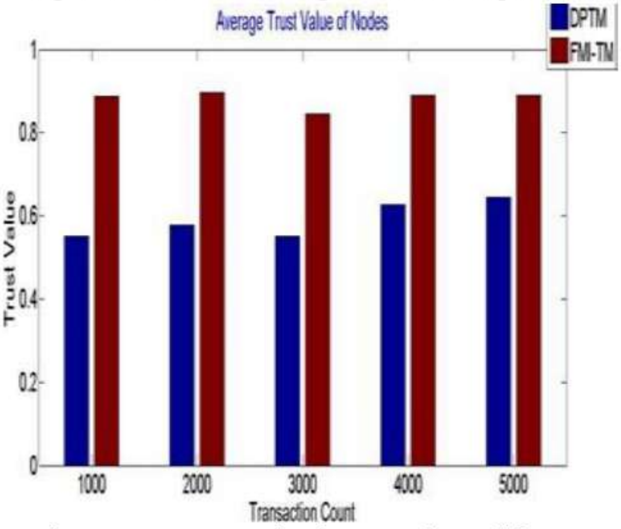


Fig.4. Average Trusted node trust value at different number of transactions.

Above fig. 5 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 Interval value updated regularly in each domain.

11. Black Hole and Group Attack:

In this environment proposed model FMI-TM (Fuzzy Interval-Trust Model) has perform better as fig. 6 shown that convergence of malicious node detection was done in less number of transaction 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 increase the trust value of other malicious

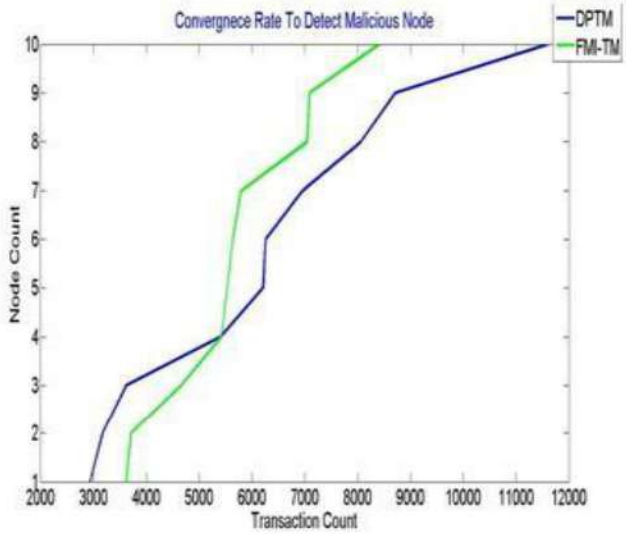


Fig.5.Malicious node convergence based comparison for black hole attack.

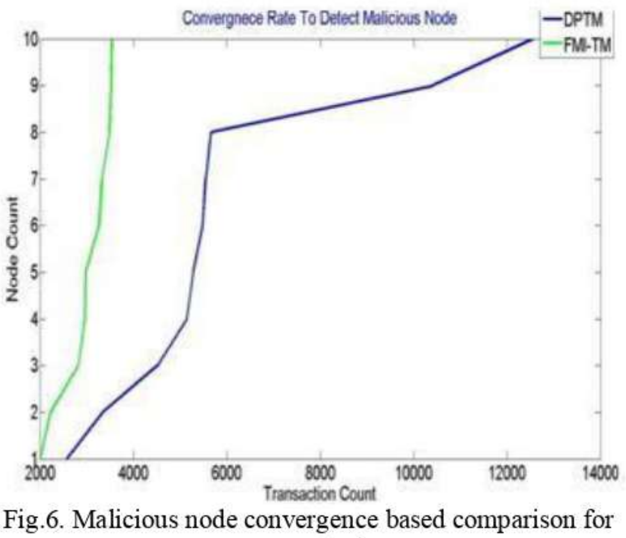
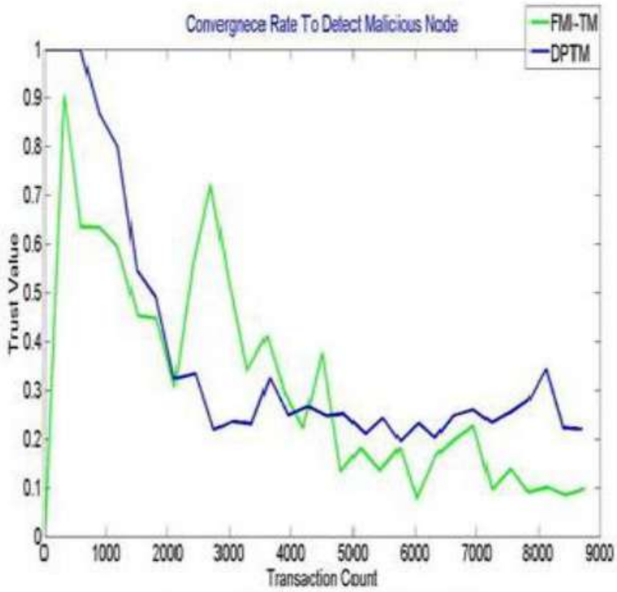


Fig.6. Malicious node convergence based comparison for group attack.



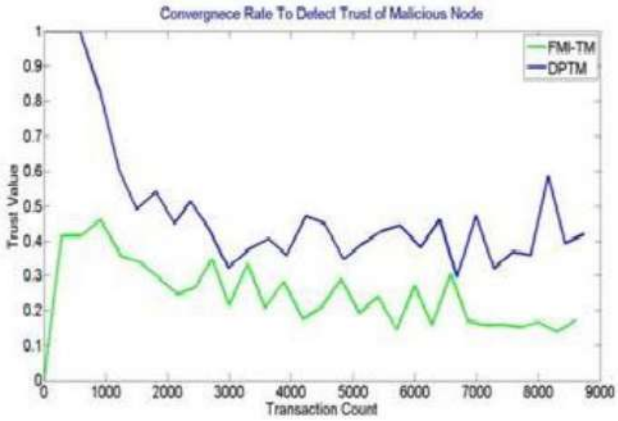


Fig. 8. Malicious node convergence based comparison for group attack.

Fig. 8 and 9 shows that proposed model has reduce the malicious node trust value in less number of transaction and maintained the value for further transaction effectively. While previous approach DPTM has also decrease 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 interval in FMI-TM.

IV. CONCLUSIONS

Cloud computing provide dynamic adaption of service sharing for company, individual, etc. So this paper proposed a trust evaluation model by using Fuzzy Interval. Here model has increase the trust score of nodes with every successful transaction while its behavior with other nodes also effect the score value. Proposed model has reduce the malicious node trust score by identifying its working pattern with other nodes. Experiment was done on three environmental conditions ideal, black hole and group attack. Results were compared with existing method and it was obtained that proposed model has improve the Malicious node convergence value and Trusted Node convergence value. In future researcher can adopt genetic algorithm for clustering of nodes into real and malicious nodes.

REFERENCES

[1]. 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).

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

[3]. Sheikh Mahbub Habib, 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.

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

[5]. 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.

[6]. 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.

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

[8]. 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.

[9]. 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.

[10]. 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.

[11]. 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.

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

[13]. Xiuqin Ma, Hongwu Qin, Norrozila Sulaiman, Tutut Herawan, 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.