Sidharth Mohan, 2021, 9:1
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

Jaccard Coefficient Based Cloud Malicious Node Detection by Mutual Trust Feature

Sidharth Mohan, Asst. Prof. Jayshree Boaddh
Dept. of Computer Science &Engineering
Mittal Institute of Technology Bhopal,
Madhya Pradesh, India
jayshree.boaddh@gmail.com

Asst.Prof. Jashwant Samar
Dept. of Computer Science & Engineering
UIT-RGPV
Madhya Pradesh, India
jashwantsamar.samar2@gmail.com

Abstract- Cloud environment increases flexibility for various application, organization, implementation, monitoring, etc. Cloud feasibility raises many issues that attracts researcher to provide solutions. This paper has work on unreliable cloud where nodes can provide service to users. Reliability of nodes in a cloud depends on services offered, job completion, etc. So a mutual trust value was evaluated in a specific time period for each node. Based on jaccard coefficient mutual trust value selection of node class either real or malicious was evaluated. Time period based node classification reduces the data storage hardware and increases the working efficiency of cloud, as malicious node removed timely. Experimental values of proposed model were compared with existing model and result shows that proposed model detect malicious node in less session.

Keywords:- Cloud Computing, Decision Tree, Resource Management, Attack Detection.

I. INTRODUCTION

Cloud computing is a compilation of the virtual servers that allows any user to view, store and retrieve data virtually [1].These tasks are mainly based on data outsourcing and securing such data is an essential task of all the cloud providers as cloud computing is an internet-based platform and works on accessing soft ware's, data, and resources from any part of the world.

Distributed nature is one of the vital characteristics of a cloud environment. These cloud providers can easily de-allocate and allocate resources based on usage and availability. They can also use free resources at the time of computation of bulk data. This feature provides good computation speed for the users but also generates the risk of data being exposed in an unknown network and thus the safety of the data is the main concern here. There are several issues regarding safety in a cloud environment. One model of Iaas provides services like multiple computers, virtual machines, and users while the other provides the users with document Information, etc. Attackers are regularly developing the latest Software to attack cloud infrastructure and their malware can easily enter within the cloud infrastructure without the knowledge of anyone. We need that some hosts should detect such malware and so that we can take care of that particular host and pre vent the malware from spreading into the entire cloud environment. A profile should be made of all the groups of a host when malware is detected and action needs to be performed on such a host as they play a vital node in the spread of the malware.

II. LITERATURE SURVEY

Chen et al. [6] performed an investigation related to sensitivity and problems related to safety in the structure of the cloud by covering all the statistics. He emphasized records separation, securing the information and cloud, cloud calculating, and privacy safety. They found out that the problems were basic ally on SAAS, IAAS, and PAAS LEVEL. He concludes that the main aim is to recognize and separate the information for it safety for getting a well-planned cloud infrastructure.

Cloud computing [7] provides us a wide platform to perform several data transactions and helps in business events to its users. But these providers have also provided TTP (trust third party) to assure the safety of the user's data but still many users are not sure about the safety of their data. In his study, he demon started an approach called DM (Identity management) that can be used to build the trust of users in cloud computing. This can be done by using multi association computation and other vigorous method and approaches over a set of information. The package will follow a defense plan and inspection and comp raises PII to reach its results. It will lead to involvement of IDM solicitation on such clouds that are not trustable. The success of the cloud atmosphere depends on the ability to recover the data and defend it from being misused.

In [8] the paper demonstrated a model and suggested some trust management techniques by recognizing nodes based on the division of domain. He showed that if we detach the nodes into the domain it will decrease the trust load related to computation and storage of data. All the fresh conventional values were planned to be collected by running cross-domain and domain sliding windows. After this, an algorithm was run to calculate the trust value of these nodes and thus hateful nodes were determined after a filter process and removed from the domain.

Azad et al. [9] gave the idea to use the planned mechanism to check the dependability of IoT equipment. He collected some applicants and asked them to rate their machines and their experience with them. He later collected all the faith values and put them on board. After that, he used a multiparty calculating technique to calculate the universal trust value often machine s.

Rafey et al. [10] allotted a faith score based on the performance of the node. He calculated the node community characteristics such as friendship, and connection and node operation qualities such as, node power calculation, assurance, significance of context, and the response. At the time of trust calculating he also laid emphasis on its support and proposals on the further nodes. He also measures background contacts of the nodes to determine the faith value. There was also some problem related to suggestions from the false nodes which have pro vided higher values to their associates than expected.

Chen et al. [11] believe in mutually Quality trust metrics, energy grade systems, communal faith data that were based on the likeness of the community to calculate the trust-related data. His study does not lay much emphasis on faith.

III. PROPOSED MODEL

Proposed model Jaccard Coefficient Trust Model JCFM was detained in this section of paper. It was assumed that all nodes transactions related information was managed by Cloud Bridge represent as CB. Trust value calculation was done by bridge periodically. Life cycle of CB updation was shown in fig.1. Flow chart of trust model was shown in fig.2. Various elements of the model were explained below.

1. Nodes: In cloud nodes come to provide and take services. Trust evaluation of each node was done by the work as per transaction behavior done by nodes in the cloud.

2. Transaction: A node in cloud request for a service and other node who accept request to provide that service is transaction. If requesting node acknowledge as service received successfully then traction get successful otherwise count as unsuccessful transaction.

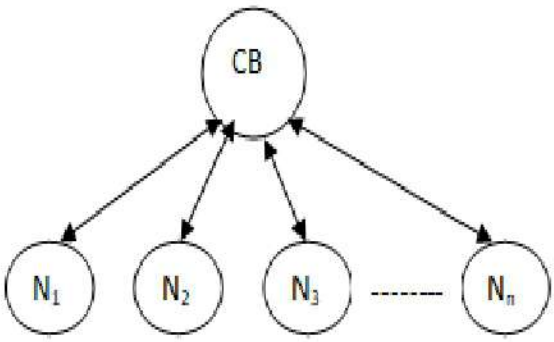

Fig 1. Cloud node and bridge model.

3. Cloud Bridge: its centralized data storage in cloud where each transaction related information was maintained. Cloud bridge store node specific transaction count, successful transaction count, failed transaction count and transaction nodeI D. This bridge store data as per clock. After completion of clock cycle trust value of the nodes were evaluate as per the transaction behavior done by node in past clock cycles.

4. Clock Cycle: Cloud defines a fix size time range as a clock. So in one clock cycle more than one node may initiate a transaction. Clock cycle (CC) is definite number of clock count for updating a trust value of nodes at cloud bridge table.

5. Node Trust value Each node in the cloud has a trust value range from 0 to 1. This value may increase or decrease as per the behavior of the nodes in form of transaction success. Cloud bridge storage tables were used to evale this value of work. First was evaluation of node direct trust value where number of successful transaction counts was dividing by total number of transaction.

So let successful transaction count between i, j node is represent by Tsij and total number of transaction represent by Ttij. Estimation of direct trust value was done Eq.1

$$D_{ij} = \frac{Ts_{ij}}{Tt_{ij}} \text{----Eq. 1}$$

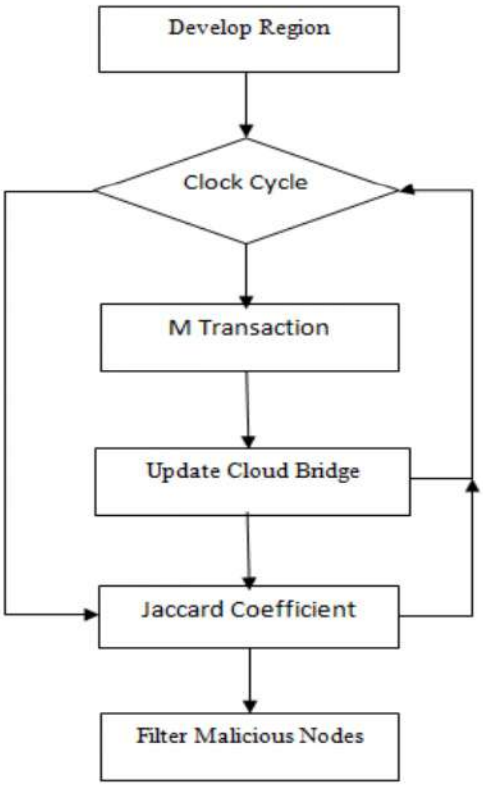

Fig 2. Proposed work training module.

Above eq. 1 gives n number of direct trust value for each node, but behaviors of node with node may be different. As malicious node provide good service to some node and poor service to others. So this trust value needs to be further process by jaccard coefficient function. This function takes all direct trust value of a node and generates a single value of the node as per different behaviors operations done by node with other nodes.

6. Jaccard Coefficient:

Jaccard function was proposed by [] whereas per various observed features between two element a trust value was generate by Eq. 2.

$$JC = \frac{A \cap B}{A \cup B} \text{----Eq. 2}$$

In above eq. A, B are nodes in the cloud and features are direct trust value between them. A∩B is obtained by getting lower direct trust value between A and B for same nodes like A•C, B•C. A∪B is obtained by getting higher direct trust value between A and B for same nodes like A•C, B•C.

7. Proposed JCFM Algorithm:

Input: n, CC // n: number of nodes in cloud
Output: T, M // T: Trust of nodes, M: Malicious nodes

- T•Initial_Trust(n)
- CB•Initial_Cloud_Table(n)
- Loop 1:CC
- Loop 1:m//m:Number of transaction in one clock.
- i•Rand()
- i•Rand()
- [Tt Ts]•Transaction(i, j)
- CB•Update_Cloud_Bridge(Tt, Ts)
- EndLoop
- Loop 1:n
- JC[n]•Jaccard_Coefficient(CB)
- If T<threshold
- M•T
- End if
- End Loop
- T•JC
- End Loop

Detail steps of the proposed algorithm shows that after each CC Jaccard coefficient values were update and nodes which performed malicious activity in cloud are filtered and removed.

IV. EXPERIMENT AND RESULTS

Proposed algorithm was developed on MATLAB 2016 version software. Experimental work was performed on machine having configuration of 4GB RAM and i3 processor 6th generation. Comparison of proposed model was done with DPTM algorithm proposed in [8].

International Journal of Science, Engineering and Technology

An Open Access Journal

1. Evaluation Parameter;

1.1 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.

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

1.2Trusted 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.

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

2. Result:

Experimental results were evaluate in two different section first was ideal condition where no nodes were doing any malicious activity and other was attack condition. In attack condition gray and friend attach was performed on the cloud environment by inserting malicious nodes.

2.1 Ideal Condition Trust Variation Values Comparison:

In this ideal condition sixty nodes were takens for 100 clock cycle. These 60 nodes were observed for 14289 transactions. As all nodes are fair and provide services nicely, so trust value of nodes get increases in short number of transaction.

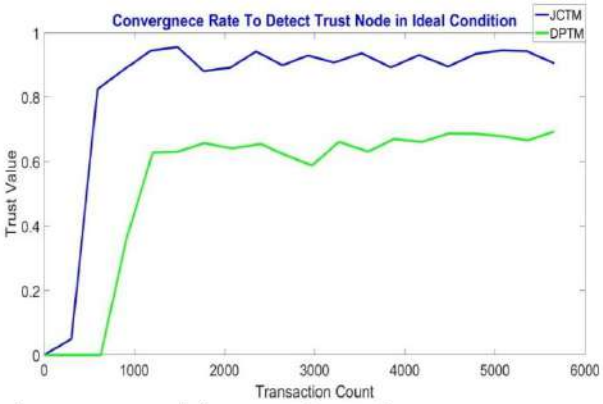

Fig 3. Trust model comparison of convergence rate detection.

Fig3 shows that proposed model has increase the trust value of nodes in less number of transaction as compared to DPTM model [8]. This was achieved by involving the centralized transaction storage.

Fig4 shows that proposed model has increase the trust value of nodes in less number of transaction as compared to DPTM model [8]. Use of jaccard coefficient value has raise the trust value as good performing nodes were promote by JC, in the model.

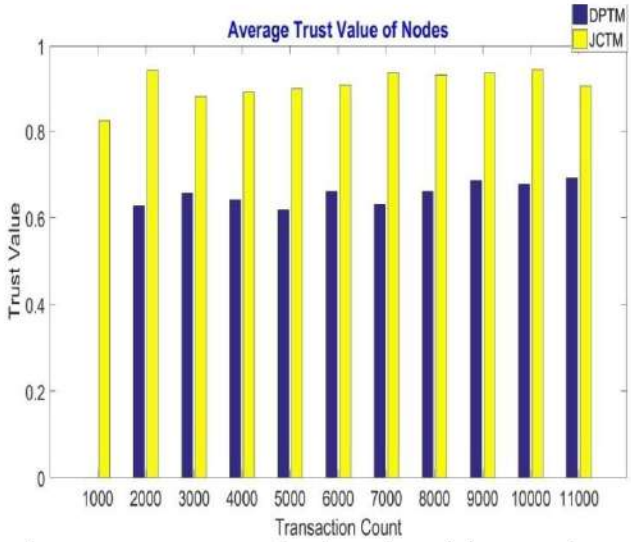

Fig 4. Average Trust value based model comparison at different transaction count.

Fig5 shows that proposed model has increase the trust value of nodes in around 700 number of transaction as compared to DPTM model [8]. This was achieved by involving the centralized transaction storage.

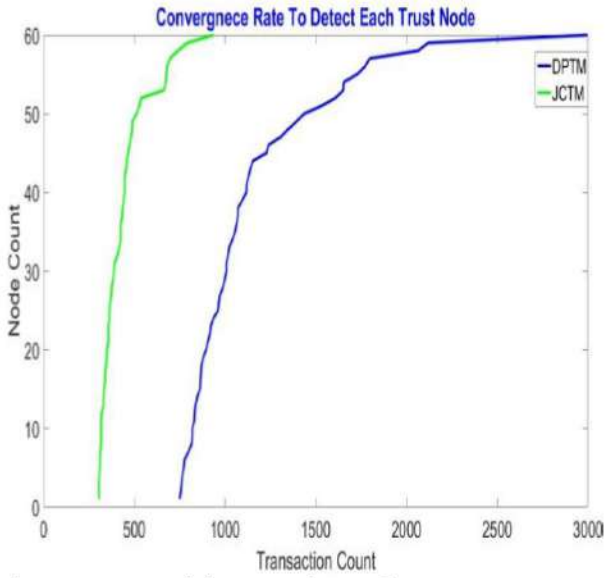

Fig 5. Trust model comparison of convergence rate detection of node.

International Journal of Science, Engineering and Technology

An Open Access Journal

2.2 Gray Attack Condition Malicious Node Detection:

In this condition of cloud have two types of node first was true node and other was malicious node. In gray attack malicious node may drop or complete a transaction intentionally. So detection of such node was done by both models.

Fig. 6 shows that under gray attack proposed model has increase the trust value of true nodes in less number of transactions as compared to DPTM model [8]. Use of Jaccard coefficient value has raises the trust value as good performing nodes were promote by JC, in the model.

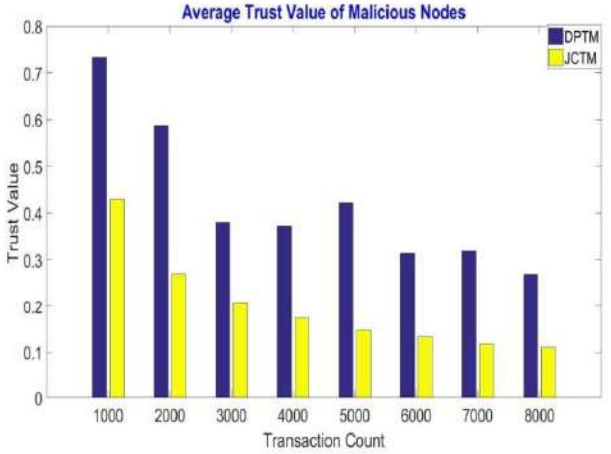

Fig 6. Average Trust value based model comparison at different transaction count.

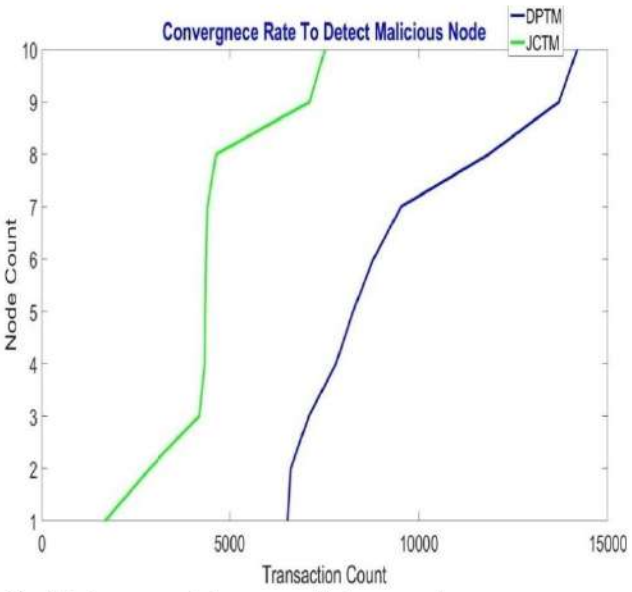

Fig 7. Trust model gray malicious node convergence rate at different transaction count.

Fig7. Shows that proposed model has increase the trust value of nodes in less number of transaction as compared to DPTM model [8]. Use of jaccard coefficient value has raised the trust value as good performing nodes were promote by JC, in the model.

2.3 Friend Attack Condition Malicious Node Detection:

In this attack two or more malicious node communicates with other malicious node and increase successful transaction count of each other. Malicious node drop packets of true nodes and direct trust values get failed to detect such node. Hence Jaccard trust value that was evaluated by various other nodes transaction performance play a important role to detect such kind of friend malicious attacked node.

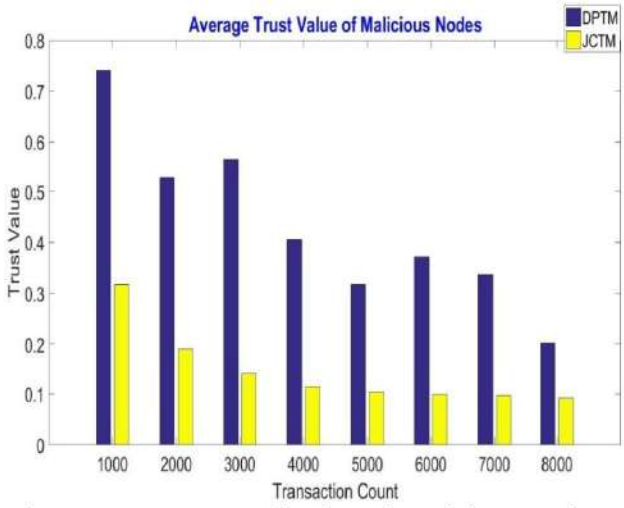

Fig 8. Average Trust value based model comparison at different transaction count.

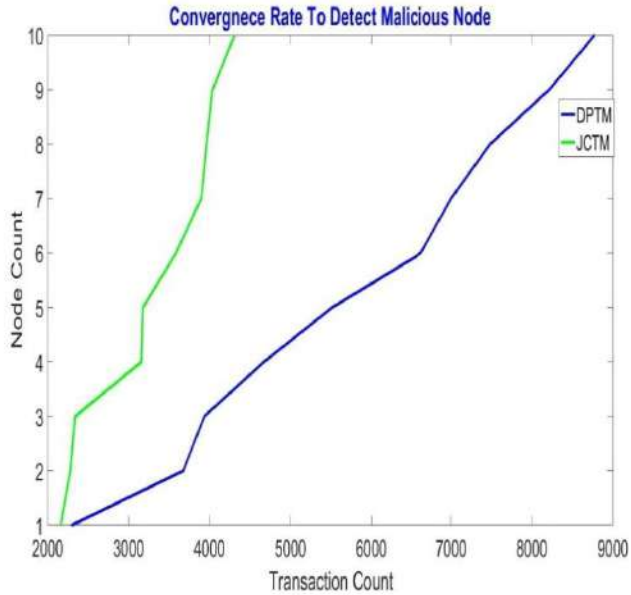

Fig 9. Trust model friend malicious node convergence rate at different transaction count.

V. CONCLUSIONS

Cloud computing is an Internet-based computing and the next stage in evolution of the internet. It has received significant attention in recent years but security issue is one of the major inhibitors in decreasing the growth of cloud computing. However, this sole feature of cloud computing introduces many security challenges that need to be resolved and understood clearly. So a mutual trust value was evaluated in a specific time period for each node. Based on jaccard coefficient mutual trust value selection of node class either real or malicious was evaluated.

Time period based node classification reduces the data storage hardware and increases the working efficiency of cloud, as malicious node removed timely. Experiment was done on three environmental conditions ideal, gray hole and friend attack. Results shows that proposed model has decrease the trust value of malicious nodes in less number of transaction as compared to DPTM model [8] under friend and gray attack. It was also found that proposed model has increase the trust value of real working nodes in less number of transaction. Use of jaccard coefficient value has raise the trust value as good performing nodes.

REFERENCES

[1] Talal HNoor, Quan Z Sheng, Abdullah Alfazi, Jeriel Law and Anne HHNgu, 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] 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).

[4] Sheikh Mahbub Habib, Max Mühlhäuser, Sebastian Ries. "Towards a Trust Management System for Cloud Computing".Trust, Security and Privacy in Computing and Communications (Trust Com), 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 Comput., 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, Issue4, 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, Issue4, pp.210-213, Dec. 2013.

[8] 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.

[9] Azad M. A., Bag S., Hao F., Salah K. M2m-rep: Reputation system for machines in the internet of things. Comput. Secure. 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 (MoW NeT); 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 Interne 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; Quan wang Wu; Zhiyong Tao."A Cloud Service Select ion Method Based on Trust and User Preference Clustering" IEEE Access Volume 7, 12 August 2019.

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

[14] 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.