TRUST MODEL FOR CLOUD AND GRID ENVIRONMENT USING FUZZY LOGIC AND ARTIFICIAL NEURAL NETWORK

G Mahesh Kumar

Assistant Professor, Department of Computer Science, Bhavan's Vivekananda College, Sainikpuri, Secunderabad, Telangana-500094, India
maheshkumar.cs@bhavansvc.ac.in

Dr. S. Ramachandram

Professor of CSE and Vice-Chancellor, Anurag University, Venkatapur, Ghatkesar, Hyderabad-500088, India
schandram@gmail.com

Dr. Jayadev Gyani

Assistant Professor, Department of Computer Science, CCIS, Majmaah University, Saudi Arabia
je.gyani@mu.edu.sa

Abstract

Cloud Computing is a technology which offers various on-demand services such as software, platform, and infrastructure required by the clients. Grid Computing is a process of allotting the resources required to solve complex problems. In cloud or grid environment the service providers provides the services/resources to the clients. In this regard the service providers need to maintain and manage trust for further proceedings. This research article proposed a trust model using Fuzzy Logic and Artificial Neural Network (ANN) applicable for both cloud and grid environment. The Fuzzy Logic is used to remove the impreciseness of the data. The decision derived by using Fuzzy Logic lies between zero (0) to one (1) that represents the continuous values, where 0 is the lowest and 1 is the highest value in decision making. In this article Fuzzy Logic is used to generate the trust value based on the fuzzy rules by accepting the given inputs of six parameters namely reliability, response time, fault tolerance, security, elasticity, and service level agreement (SLA). Then based on the generated trust value the service provider is allotted to the clients. Artificial Neural Network is a prediction model used to predict the trust value of the service provider based on the same six parameters mentioned as input for Fuzzy Logic. Based on the predicted trust value the service provider is allotted to the client. This article shows the experiments and results based on the Fuzzy Logic Model and Artificial Neural Netwok Model for the process of service provider allottment. The experiments and results worked on the dataset of 20000 instances collected from the authenticated source.

***Keywords*: Cloud Computing; Grid Computing; Fuzzy Logic; ANN; Service Providers; SLA.**

1. Introduction

In the present era all the transactions are digitized and done online from various remote locations. The transactions done by the client may vary in size. There are many start-ups coming into the market and also the existing industries require the quality services at less cost. The cloud computing is such a technology where the services are offered on-demand and at less cost. The cloud computing process offers the services such as storage, software, hardware, execution platforms, operating systems, and many more through virtualization concept. The industries need not purchase very high-end systems for their tasks by investing a lot of cost. The industries can connect to the cloud for all varieties of services at any point of time throughout their subscription period. The cloud computing possess the characteristics such as multi-tenancy, service-oriented, universal access, self-organizing, dynamic resource provisioning, pricing based on utility consumption, resource pooling, etc. The cloud holds the service models such as IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service). The IaaS basically works through Severs, Virtual Machines, Storage, Networks, etc. The PaaS provides access to Database, Web Server, Application Development, Deployment

Tools, etc. The SaaS provides on-demand software such as Electronic Mail, Games, Virtual Desktops, etc. The cloud computing technology has the deployment models such as a Private Cloud, Public Cloud, and Hybrid Cloud. The Private Cloud is restricted to only one company and that company only can use the services of Cloud. The Public Cloud is used by every one and requires a lot of security. The Hybrid Cloud is the combination of private and public clouds, so that more flexibility is available in using the services.

Grid Computing is a technology used for allotting the resources required to compute complex problems. As few applications especially in medical field requires a lot of computational power to process the result. As a normal user they may not have a very huge set of resources to compute the complex problems. To overcome this problem the grid service providers allocates the resources required to solve a complex problem. The grid computing process pools the resources from the systems which are idle at a certain point of time and takes the permission of the concerned user to use their CPU cycles to compute the problem. The payment is done to the resouce provider based on the utilization of resouces.

The Cloud Computing or Grid Computing technology makes the communication posssible with the service providers/resource providers and the clients. The major problem among these entities is the Trust establishment. Trust is the belief on the other entity that they are genuine and they don't misuse the allotted services or resources. The trust is classified as Direct Trust and Indirect Trust. Direct Trust is a process in which the service/resource providers and the client know each other very well since they are working from many days. In direct trust no recommendation is required from third party about the client for other business entities. The indirect trust is the process where the client and service/resource providers don't know each other and they want to do the communication for business. Since there was no already existing communication between them, compulsorily a third party is required to give an assurance on behalf of the client. The indirect trust can be converted to a direct trust if the client and resource provider does fair transactions every time.

There is a need to build a robust trust model which helps to establish trust among the service providers/resource providers to perform genuine and authenticated transactions perfectly and improve their trust score. This article focuses on the Fuzzy Logic and Aritificial Neural Network to build a robust trust model. The Fuzzy Logic basically works with the continuous values where a certain range of values is considered between zero and one. This is used to remove the impreciseness of the data. The Artificial Neural Network model is a prediction model used to predict the trust value based on the input given by the client. The predicted trust value is mapped to the service providers trust value which was already predicted for the past transactions and then a suitable service provider is allocated. These two models work on the service parameters such as reliability, response time, fault tolerance, security, elasticity and service level agreement (SLA). Finally the experiments and results are shown based on the six parameters mentioned above with a dataset of 20000 instances from authenticated source.

2. Literature Survey

Abhishek Kesarwani and Pabitra Mohan Khiler (2022), [1] have proposed the development of trust based access control models using fuzzy logic in cloud computing. In this model the trust value is calculated for both cloud users and cloud service providers. The proposed model is divided into three sections i.e. user, service entity and trust management module. In the user section the user makes the request to access the cloud or to find out the trust value of cloud providers. The component named, behavior monitoring component checks whether the request is bogus, bad or unauthorized. All the user requests are stored in user behavior database. The user trust evaluation component finds the trust value of a user and their trust value is stored in user trust database. All service providers need to register the free resources such as memory, storage, processor speed, etc. Service Level Agreement component checks the response time, workload, availability and scalability of a cloud. The feedback component holds the information for security and usability of cloud. The elasticity component uses the fuzzy logic to find about the elasticity of cloud and also the performance component uses the fuzzy logic to find the performance of the cloud.

Syed Rizvi et al., (2020), [2] have proposed a fuzzy inference system (FIS) to evaluate the security readiness of cloud service providers. This model helps the cloud users to find the appropriate cloud service providers for communication. This model has incoporated the fuzzy inference rules which are feeded into the fuzzy inference system to generate a security index for the cloud users. This has considered the uncertainities and ambiguites to measure the trust value. This is used for both cloud users and cloud service providers to make a reliable communication.

Mona Soleymani et al., (2021), [3] have presented a research article on fuzzy-rule based trust management model for the security of cloud computing. This article highlighted the design of a new framework which identifies the fake feedback values. This trust management model works in multicloud environment that

supports multidimensional parameters to generate trust values. The new framework responsibilities are to select appropriate cloud service provider and also to verify their reliability apart from detecting fake feedbacks.

Rajganesh Nagarajan et al., (2017), [4] have proposed a fuzzy logic based trust evaluation model for the selection of Cloud Services. This model focused on feedback of the cloud users and it is accepted in linguistic terms of fuzzy logic. For every feedback there is a weight associated. The linguistic feedback values and their weights are feeded to the fuzzy inference system and the trust values are generated.

Mary-Jane Sule et al., (2017), [5] have presented a research article on fuzzy logic approach to modelling trust in cloud computing. In this article a multi-layer security trust model is designed which demonstrates the security features applicable for each layer of cloud computing such as IaaS, PaaS and SaaS. Each layer is holding some security measure and the final trust values are derived from the aggregation of all the layers security measure values. The fuzzy logic has been incorporated to find the final trust value.

Manish Mishra et al., (2014), [6] highlighted a view of artificial neural network. This article focused about the introduction to neural network, architecture of artificial neural network, applications and limitations of artificial neural network.

Mario Krenn et al., (2020), [7] highlighted on predicting research trend with semantic and neural networks with an application in quantam physics. They proposed an idea to build semantic network SEMNET of publications in the field of science. Whenever there is a need of publications in research then those publications to be made available to the people without any trouble. In this the neural network is to be trained by using the semantic network past to predict the future development in quantum physics.

Xu Yang et al., (2021), [8] presented a review paper on research and applications of artificial neural network in pavement engineering: A state-of-the-art review. In this paper the ANN architectures such as multi-layer perceptron neural network, convolutional neural network and recurrent neural network used for one-dimensional and multi-dimensional data were highlighted.

3. Fuzzy Logic

Every activity requires a decision making and earlier to fuzzy logic the Boolean logic was given the highest priority i.e. true or false/ 1 or 0/yes or no. The fuzzy logic is used to map the input space with output space and this mapping is mainly done by the specified rules. A crisp set holds the values of 0 or 1/no or yes. This crisp set holds only two values either true or false i.e. it has definite boudaries. But as we consider a human brain incase of decision making, it may not be able to decide exactly yes or exactly no. There will be some dilemma to decide on any activity exactly and accurately. To overcome such problem the fuzzy set was introduced in which values range from 0 to 1 and with 0, 1 inclusive. Fuzzy set contains elements with partial degreee of membership. The fuzzy logic identifies the uncertainity and impreciseness in the data and tries to remove the uncertainity and impreciseness of the data. The fuzzy logic works on the concept of individual perception where as all peoples perception is not same. The fuzzy logic defines the linguistic variables and is rule based i.e., it holds if-then rules. Each rule has one or more antecedents and consequents. Based on the rules the input space is mapped to the output space by deriving the result.

3.1. *Membership Functions*

A Membership Function of fuzzy set A on the universe of discourse X is defined as μ_A: X → [0, 1], where each element of X is mapped to a value ranges from 0 to 1. This value is called as degree of membership or a membership value. There are few types of membership functions such as Sigmoid Curve, Piecewise Linear Functions, Quadratic and Cubic Polynomial Curves, and Gaussian Distribution Function. Apart from the mentioned membership functions, there are straightline membership functions such as Triangular Membership Function uses trimf function, Trapezoidal Membership Function uses trapmf function, Linear z-shaped membership function open to the left uses linzmf function, and Linear s-shaped membership function open to the right uses linsmf function [12] as mentioned below in Fig.1.

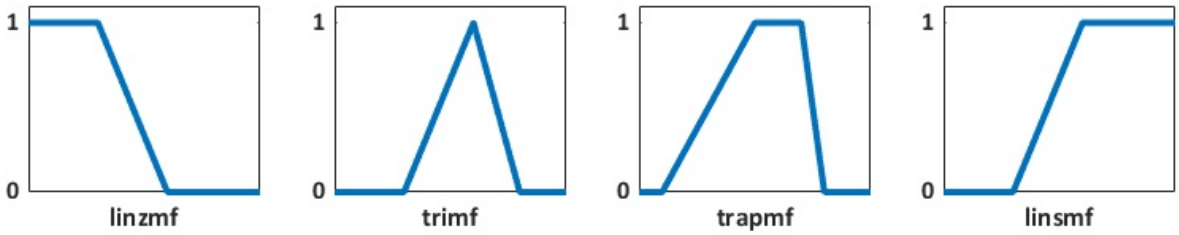

Fig.1. Membership Functions

3.2. *Logical Operations*

In fuzzy logic there are three logical operations such as AND, OR, NOT. In this if two fuzzy sets namely A and B holding truth values of (0,0) (0,1) (1,0) (1,1) respectively then the output values while using the AND logical operator is (0,0,0,1). The fuzzy logic uses min(A,B) function when AND logical operator is used. When the OR operator is used on the above mentioned values then max(A,B) function is used and the resultant output is (0,1,1,1). If there is a fuzzy set A with (0,1) values then output is (1,0) when NOT operator is used. These logical operations are basically used in the if-then rules of the fuzzy logic to derive the proper output. These operators are used among more than one antecedents and consequents.

3.3. *If-Then Rules*

The fuzzy logic is rule-based i.e. any decision to be made is done through the rules specified. Every rule is having an antecedent and a consequent section. The linguistic variables need to be assigned for the membership function and used in specifying the rules. The linguistic variables hold the value between zero (0) to one (1). The 0 value is the least value and 1 is the highest value where the performance value is good. The If-Then rule accepts the current value of a variable as the input i.e. a fuzzy set input and generates the appropriate fuzzy set output based on the rules. If the rules are designed properly then the generated output will have accuracy otherwise not.

3.4. *Fuzzy Inference System*

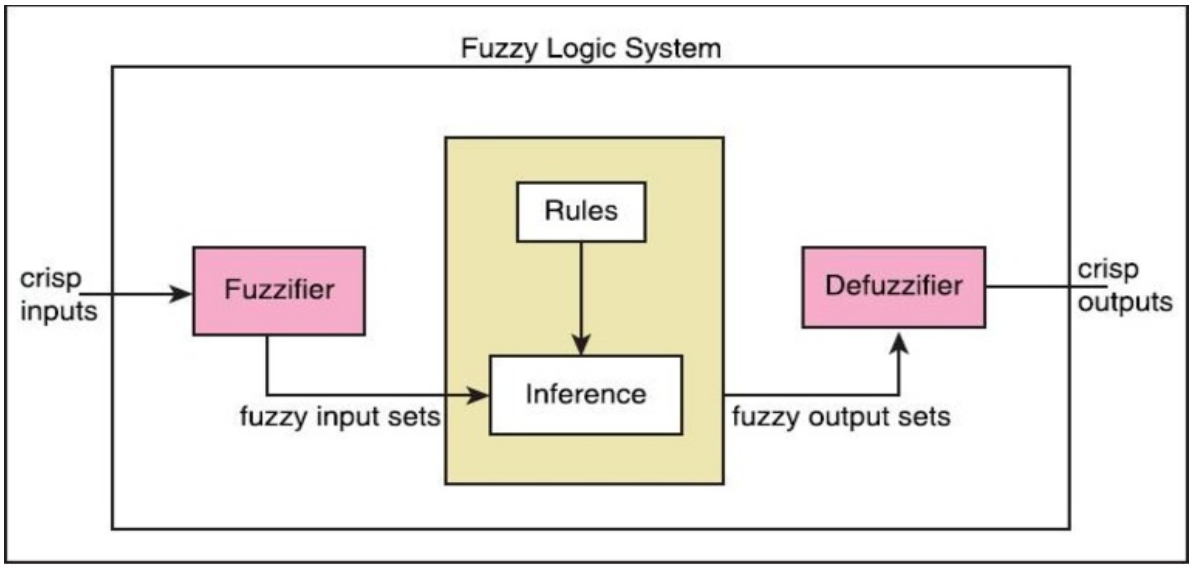

Fig.2. Fuzzy Inference System

The above Fig.2 depicts the architecture of Fuzzy Inference System [1] which accepts the crisp inputs and generates the crisp outputs with a lot of internal processing. The Fuzzifier component accepts the crisp inputs and converts it into the fuzzy input sets and is passed to the inference engine. The inference engine accepts the fuzzy input sets and based on the rules designed extracted from Rules component at the time of computation. The inference engine generates the fuzzy output sets after the computation is over. The fuzzy output sets are sent to the Defuzzifier component for convertion into crisp outputs.

4. Proposed Trust Model using Fuzzy Logic

In the modern era every transaction need to be performed very carefully and perfectly since the transactions arre performed online. To achieve this there should be a proper communication between the Cloud Service Providers and Cloud Users. The major problem faced by the stakeholders is Trust. Every entity involved in communication should be a trusted entity and that entity is responsible to do any task very genuinely and reliabily. The trust is classified as Direct Trust and Indirect Trust. If a Cloud Service Provider and Cloud User know each other and believe each other then the direct trust is established among them and no third party recommendation is required. If a Cloud Service Provider and Cloud User don't know each other then compulsorily a third party recommendation for Cloud User is required. In this proposed trust model namely Fuzzy Trust Model (FTM) six key parameters such as reliability, response time, fault tolerance, security, elasiticity, and service level agreement (SLA) are considered for trust value generation. There are totally 20 service providers namely SP1 (Service Provider 1) to SP20 (Service Provider 20) respectively. Each service provider is holding 1000 records for all the six parameters. Totally 20000 instances for all 20 service providers are considered from authenticated source [9] [10] [11]. This trust model uses the fuzzy logic approach to generate the trust value based on the rules specified.

4.1. *Experiments and Results of the Proposed Trust Model using Fuzzy Logic*

The experiments and results of proposed trust model using fuzzy logic are done using MATLAB software. The fuzzy logic toolbox is a graphical user interface tool consists of components such as Fuzzy Logic Designer, Membership Function Editor, Rule Editor, Rule Viewer, and Surface Viewer. The fuzzy logic designer component is used to depict and configure the input and output variables and the processing element. The membership function editor is used to assign membership functions to each input variable and an output variable. The rule editor describes the behavior of the system and allows to frame rules and also to edit the rules. The rule viewer shows the inference diagram and also depicts the rules which are active and the membership functions which are affecting the results. The surface viewer is used to generate the surface map of the system and shows the dependency between two input variables and one output variable.

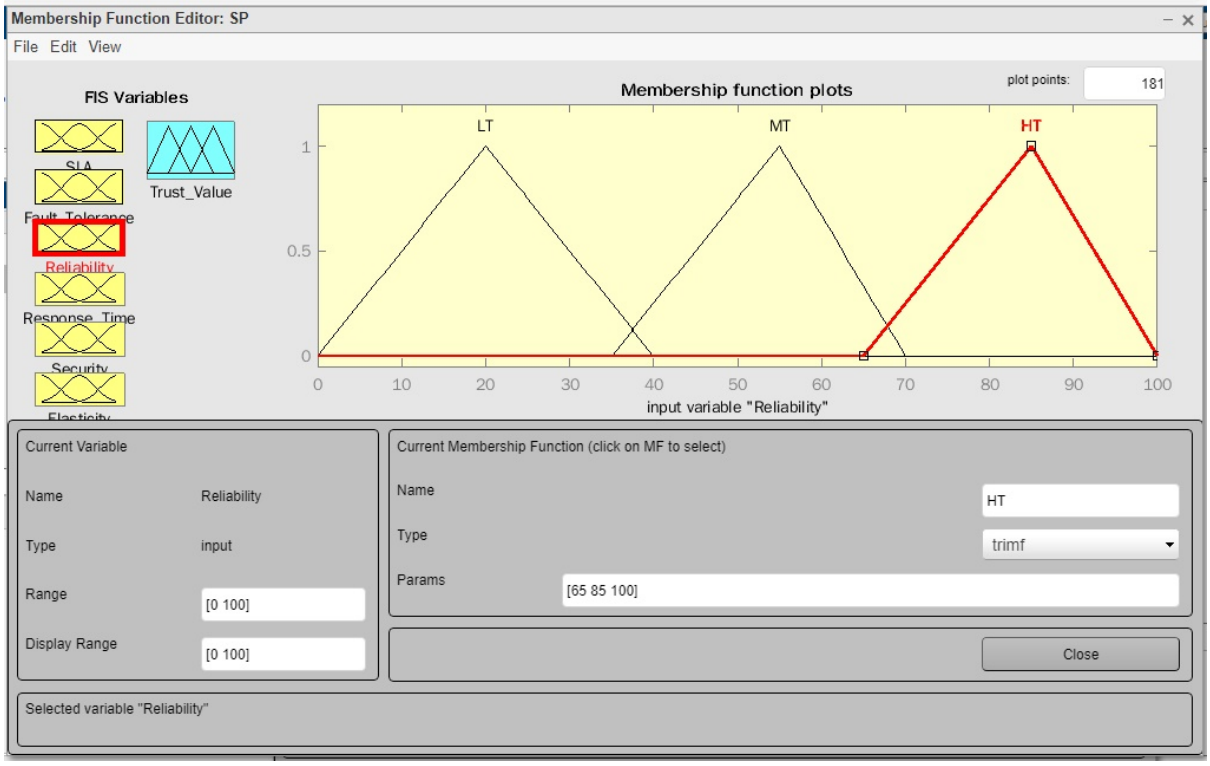

Fig.3. Membership Function of Reliability

The above Fig.3 depicts the membership function of Reliability input variable in the membership function editor. The linguistic variables are classified as Low Trust (LT), Medium Trust (MT) and High Trust (HT). The LT value is in the range of [0, 20, 40], the MT value is in the range of [35, 55, 70] and HT value is in the range of [65, 85, 100]. The membership function used is trimf function namely triangular membership function.

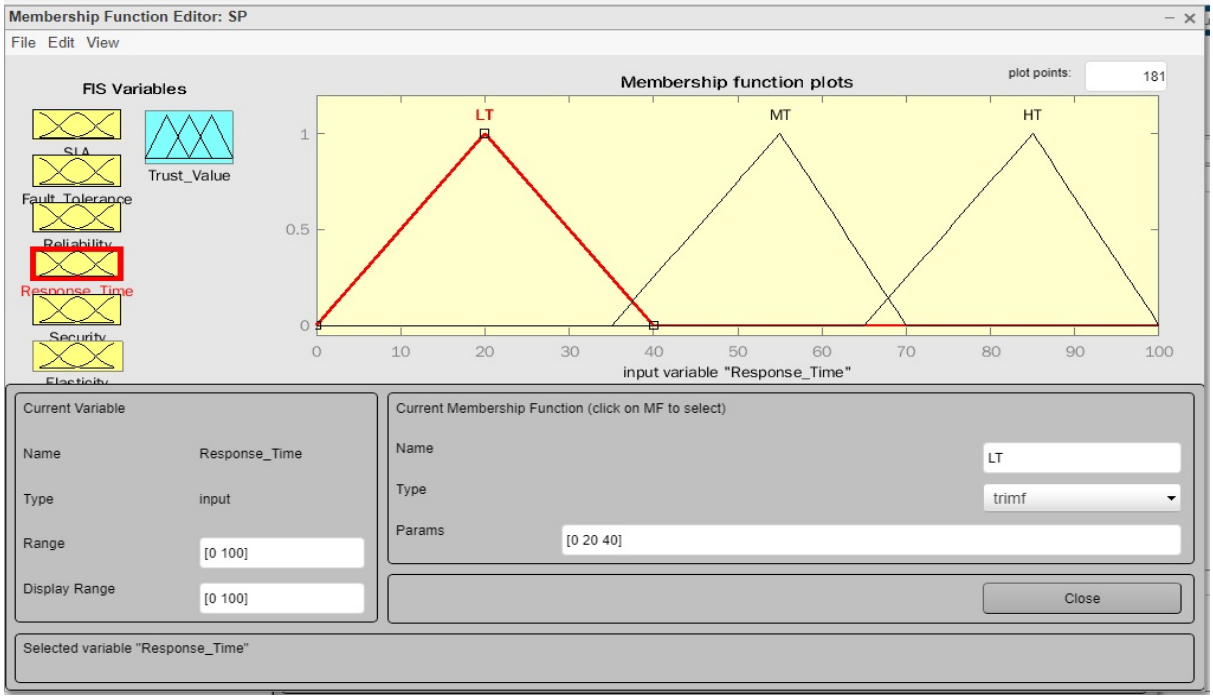

Fig.4. Membership Function of Response Time

The above Fig.4 shows the membership function of Response Time input variable in the membership function editor. The linguistic variables are classified as Low Trust (LT), Medium Trust (MT) and High Trust (HT). The LT value is in the range of [0, 20, 40], the MT value is in the range of [35, 55, 70] and HT value is in the range of [65, 85, 100]. The membership function used is trimf function namely triangular membership function.

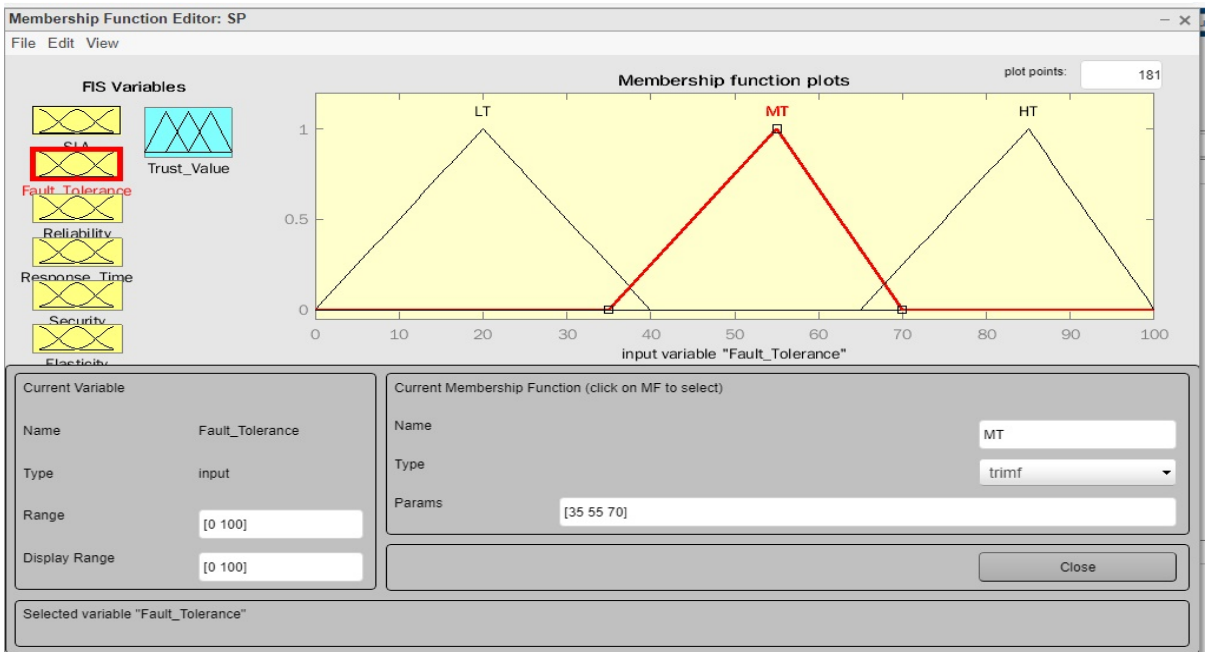

Fig.5. Membership Function of Fault Tolerance

The above Fig.5 represents the membership function of Fault Tolerance input variable in the membership function editor. The linguistic variables are classified as Low Trust (LT), Medium Trust (MT) and High Trust (HT). The LT value is in the range of [0, 20, 40], the MT value is in the range of [35, 55, 70] and HT value is in

the range of [65, 85, 100]. The membership function used is trimf function namely triangular membership function.

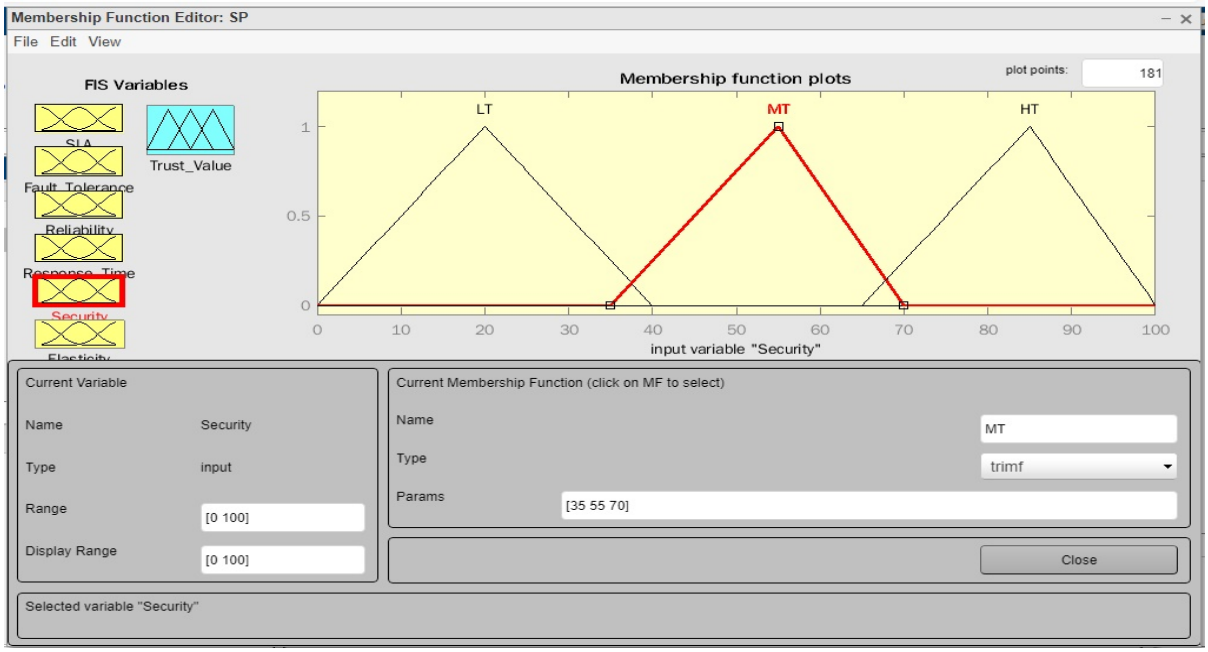

Fig.6. Membership Function of Security

The above Fig.6 depicts the membership function of Security input variable in the membership function editor. The linguistic variables are classified as Low Trust (LT), Medium Trust (MT) and High Trust (HT). The LT value is in the range of [0, 20, 40], the MT value is in the range of [35, 55, 70] and HT value is in the range of [65, 85, 100]. The membership function used is trimf function namely triangular membership function.

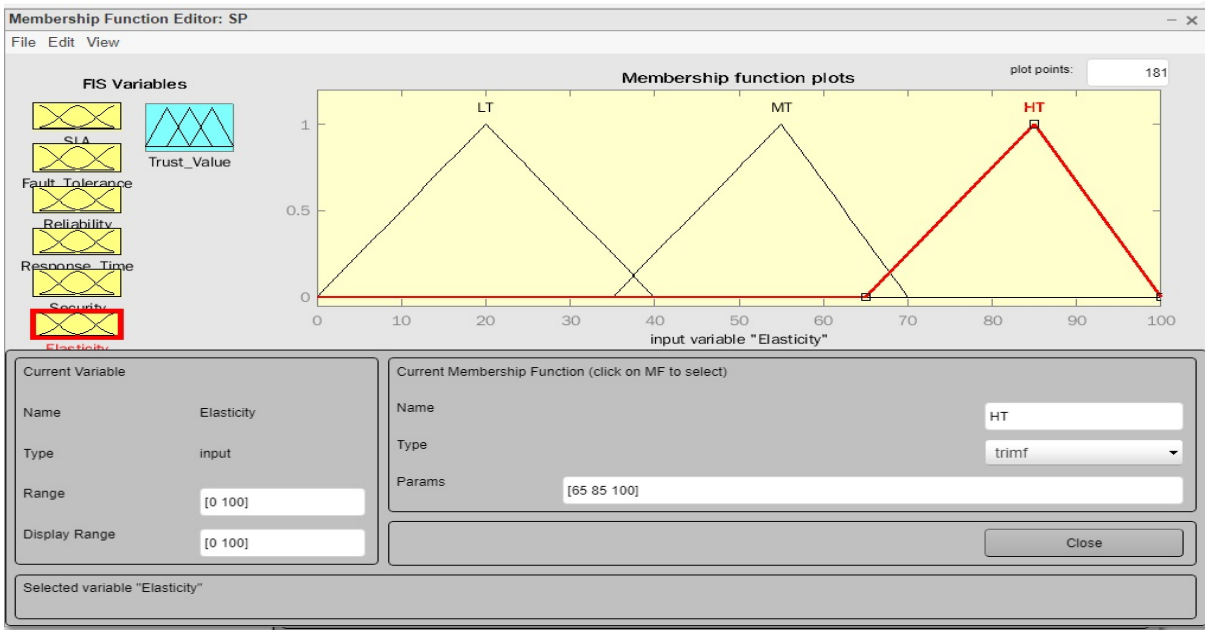

Fig.7. Membership Function of Elasticity

The above Fig.7 shows the membership function of Elasticity input variable in the membership function editor. The linguistic variables are classified as Low Trust (LT), Medium Trust (MT) and High Trust (HT). The LT value is in the range of [0, 20, 40], the MT value is in the range of [35, 55, 70] and HT value is in the range of [65, 85, 100]. The membership function used is trimf function namely triangular membership function.

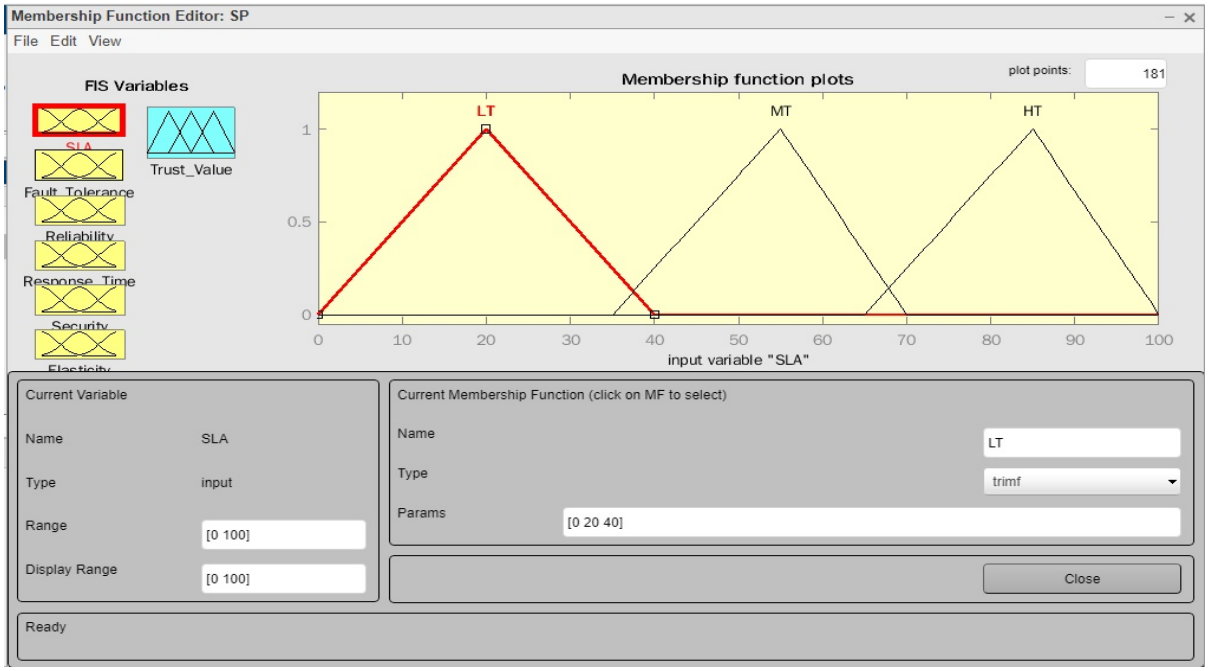

Fig.8. Membership Function of SLA

The above Fig.8 represents the membership function of Service Level Agreement (SLA) input variable in the membership function editor. The linguistic variables are classified as Low Trust (LT), Medium Trust (MT) and High Trust (HT). The LT value is in the range of [0, 20, 40], the MT value is in the range of [35, 55, 70] and HT value is in the range of [65, 85, 100]. The membership function used is trimf function namely triangular membership function.

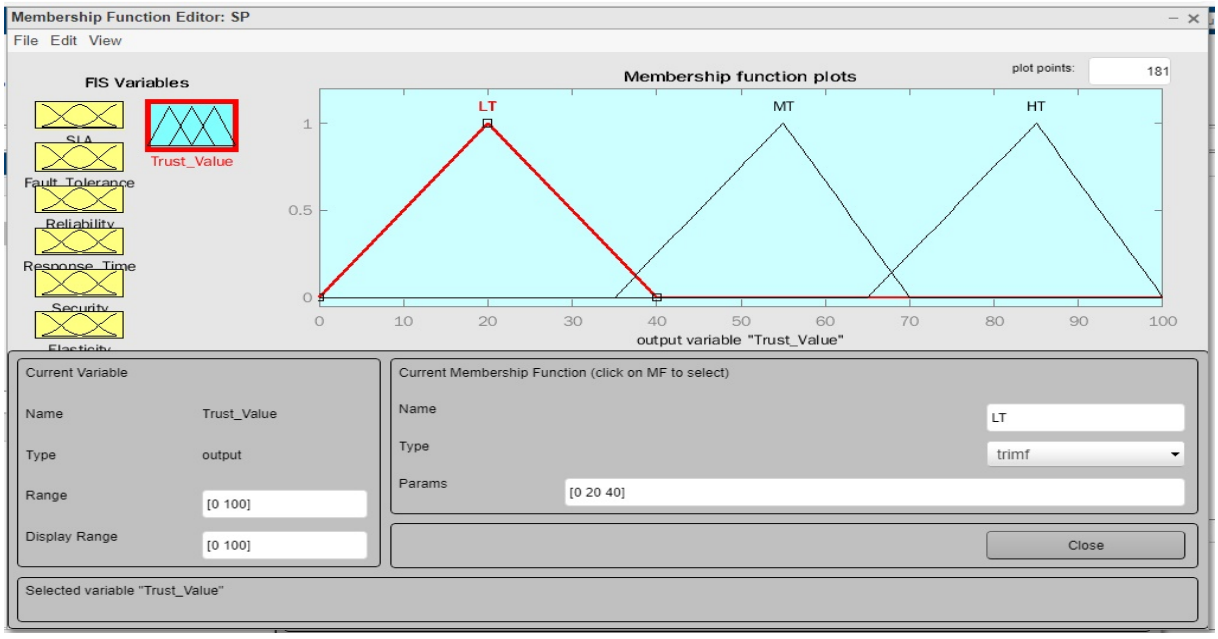

Fig.9. Membership Function of Trust Value

The above Fig.9 depicts the membership function of Trust Value output variable in the membership function editor. The linguistic variables are classified as Low Trust (LT), Medium Trust (MT) and High Trust (HT). The LT value is in the range of [0, 20, 40], the MT value is in the range of [35, 55, 70] and HT value is in the range of [65, 85, 100]. The membership function used is trimf function namely triangular membership function.

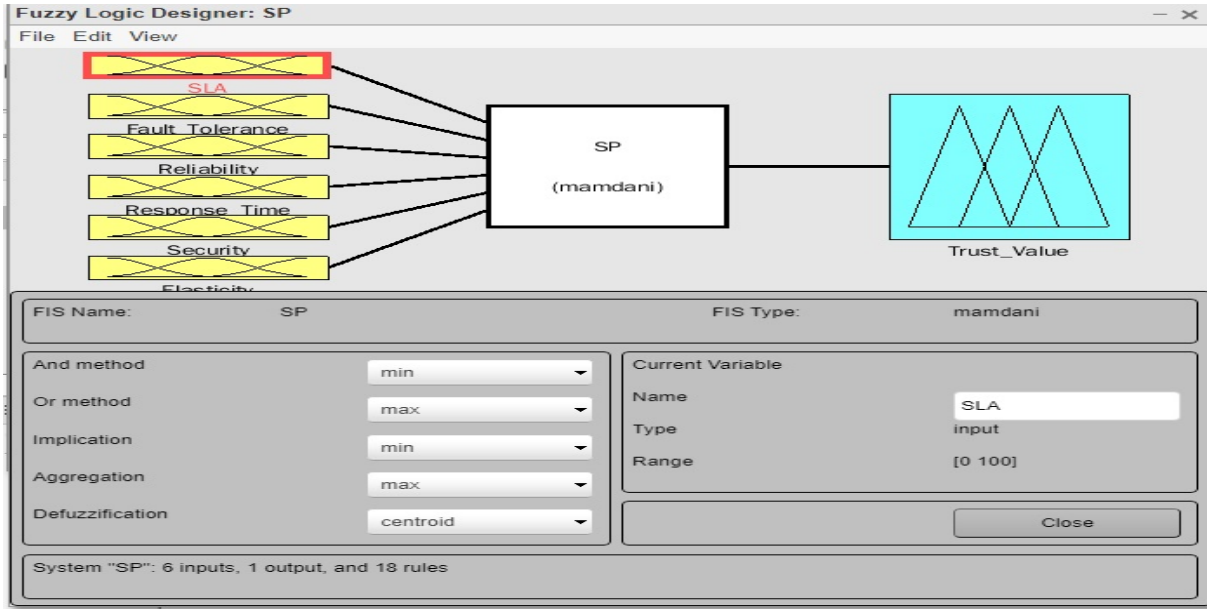

Fig.10. Fuzzy Inference System of Fuzzy Trust Model

The above Fig.10 represents the fuzzy inference system of fuzzy trust model (FTM) in the fuzzy logic designer. This shows the six input variables feeding their fuzzy value to the Mamdani Fuzzy Inference System which acts as an inference engine to accept the input variables and process the input based on the rules specified. Finally the trust value is generated.

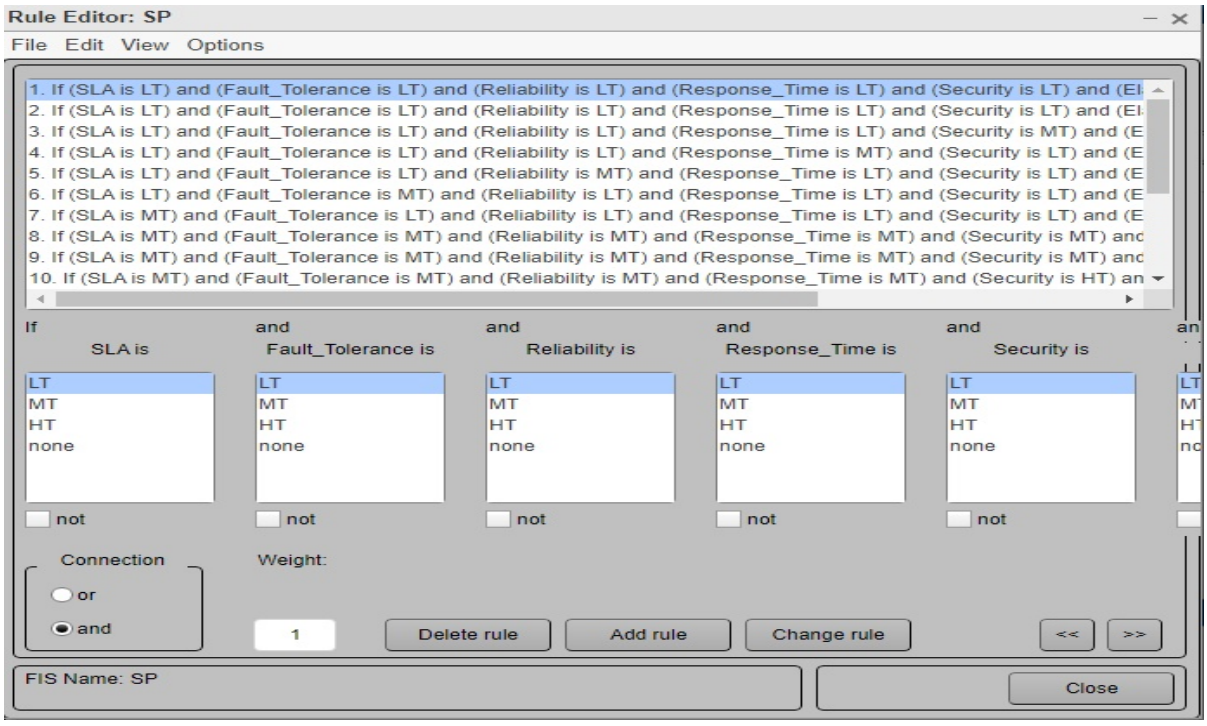

Fig.11. Rules of Fuzzy Trust Model

The above Fig.11 represents the rules of fuzzy trust model (FTM) in the rule editor. This rule editor is used to frame rules and edit rules. The rules are framed on six parameters using if-then rules. For every antecedent a linguistic variable is assigned and also the logical operators such as AND, OR, and NOT can be used. But in the above scenario only AND operator is used. Based on these rules the trust value is generated automatically.

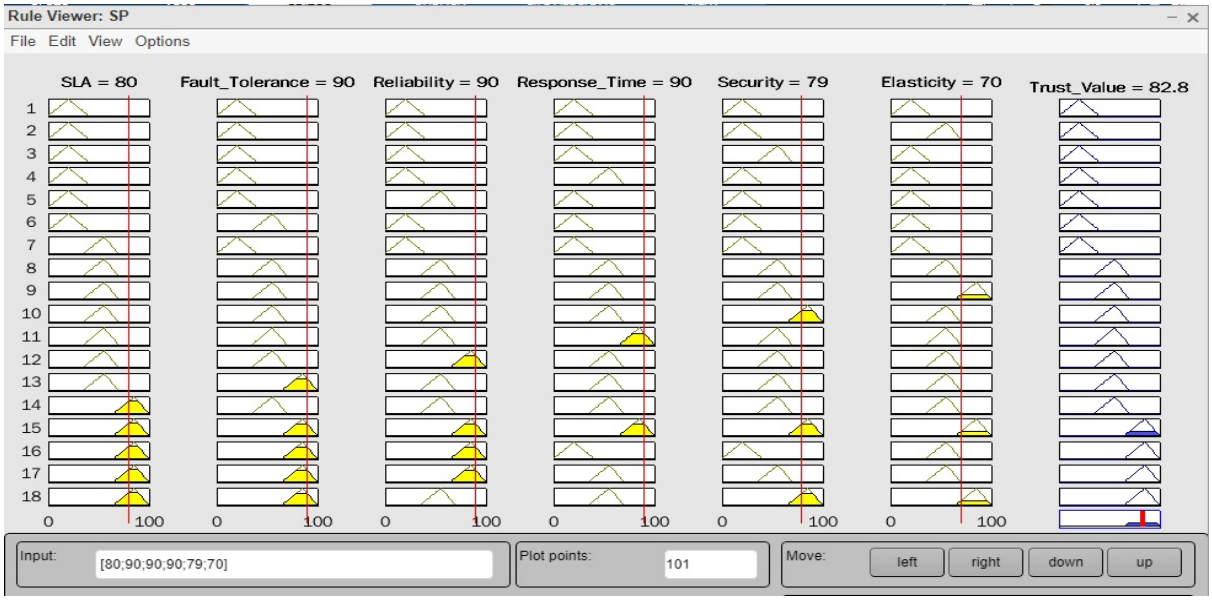

Fig.12. Complete Fuzzy Inference Process of Fuzzy Trust Model

The above Fig.12 represents the complete fuzzy inference process of fuzzy trust model (FTM) in the rule viewer. This rule viewer is a graphical user interface used to show the complete information of all the six parameters individually. On top of every column the name of the parameter is specified. The rules specified are considered with respective to the linguistic variables. The red line is used to adjust the parameter values. The yellow color is respresenting for input variables and blue color is representing for the output variable. There is a provision to enter the input for all six parameters and based on that the trust vlaue is generated. As and when the input values are changing the trust value is also changed. Once the trust value is derived then based on this trust value the service provider is mapped and allotted for communication. We have already proposed a generalized trust model for computational grids & clouds. This paper highlighted the working of T-CGE trust model which helps to find the top service providers [13].

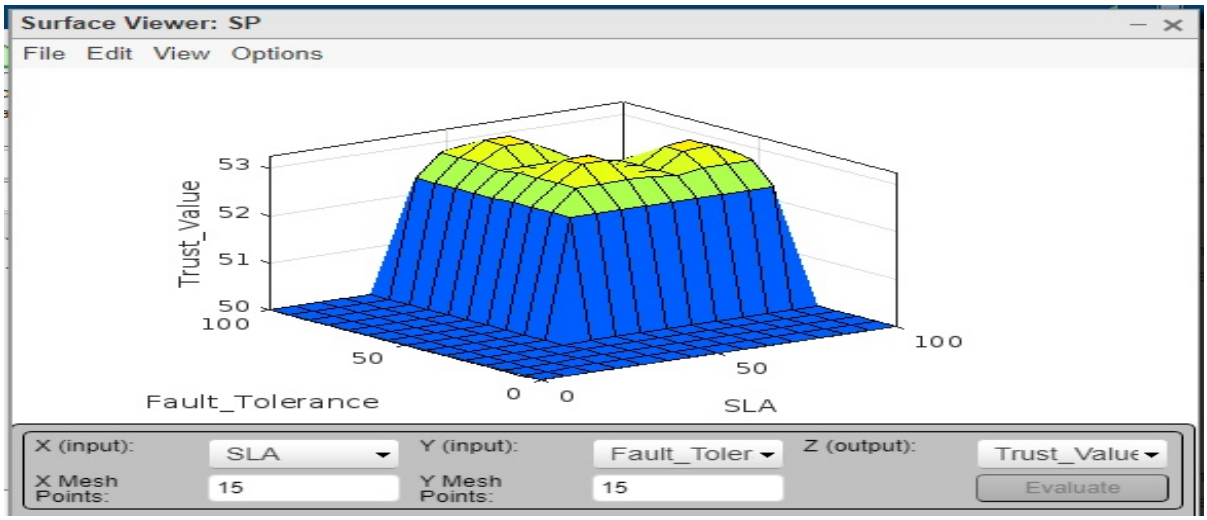

Fig.13. Surface View between Fault Tolerance and SLA

The above Fig.13 represents the surface view between fault tolearnce and SLA. This will accept two input variables and one output variable. As of this figure x input is SLA and y input is Fault Tolerance and z output is Trust Value. This demonstrates the multi-dimensional view.

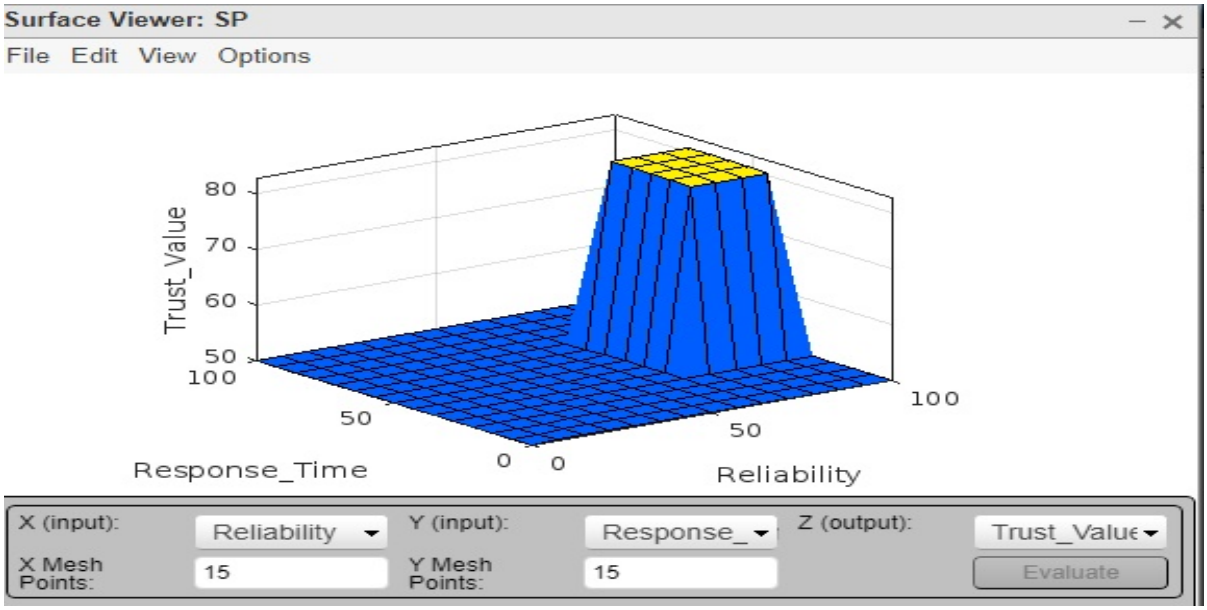

Fig.14. Surface View between Response Time and Reliability

The above Fig.14 represents the surface view between response time and reliability. This will accept two input variables and one output variable. As of this figure x input is Reliability and y input is Response Time and z output is Trust Value. This demonstrates the multi-dimensional view.

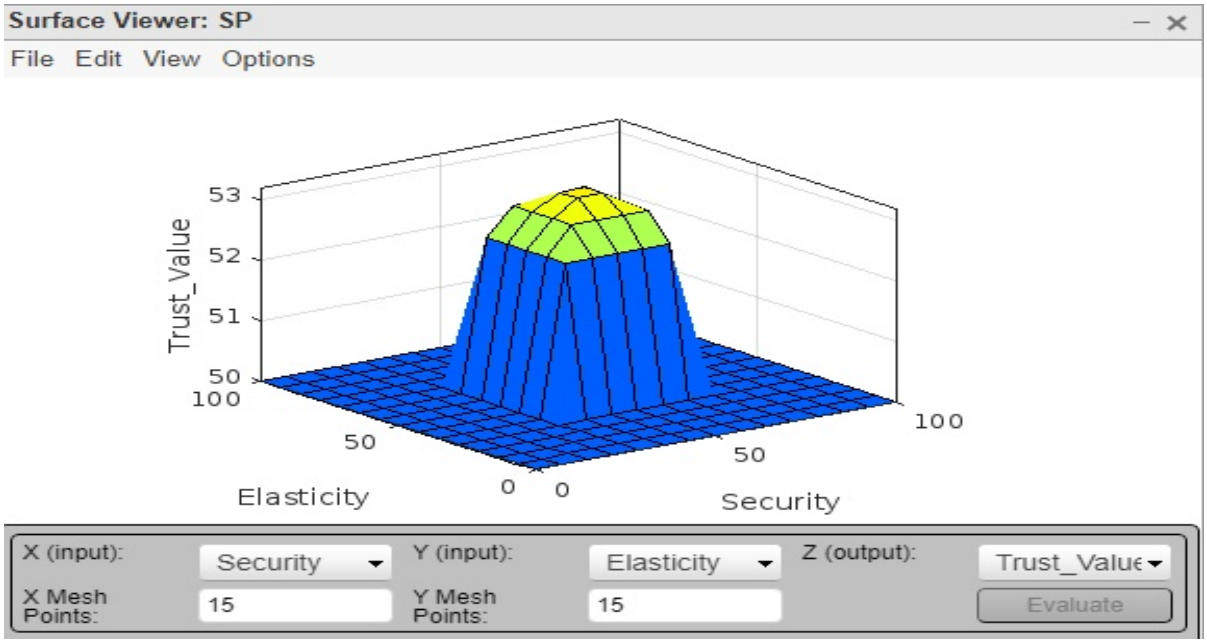

Fig.15. Surface View between Elasticity and Security

The above Fig.15 represents the surface view between elasticity and security. This will accept two input variables and one output variable. As of this figure x input is Security and y input is Elasticity and z output is Trust Value. This demonstrates the multi-dimensional view.

5. Proposed Trust Model using Artificial Neural Network (ANN)

The artificial neural network was designed based on the communication between neurons in a human brain. The ANN has multiple layers of abstraction i.e. it has one input layer, one or more hidden layers, and one output layer. Every input node in the input layer will be associated with a weighting factor. The output of one layer will

become the input of another layer. The hidden layers responsibility is to get trained with the data from which the ANN recognizes the patterns, classify data and predict the future events.

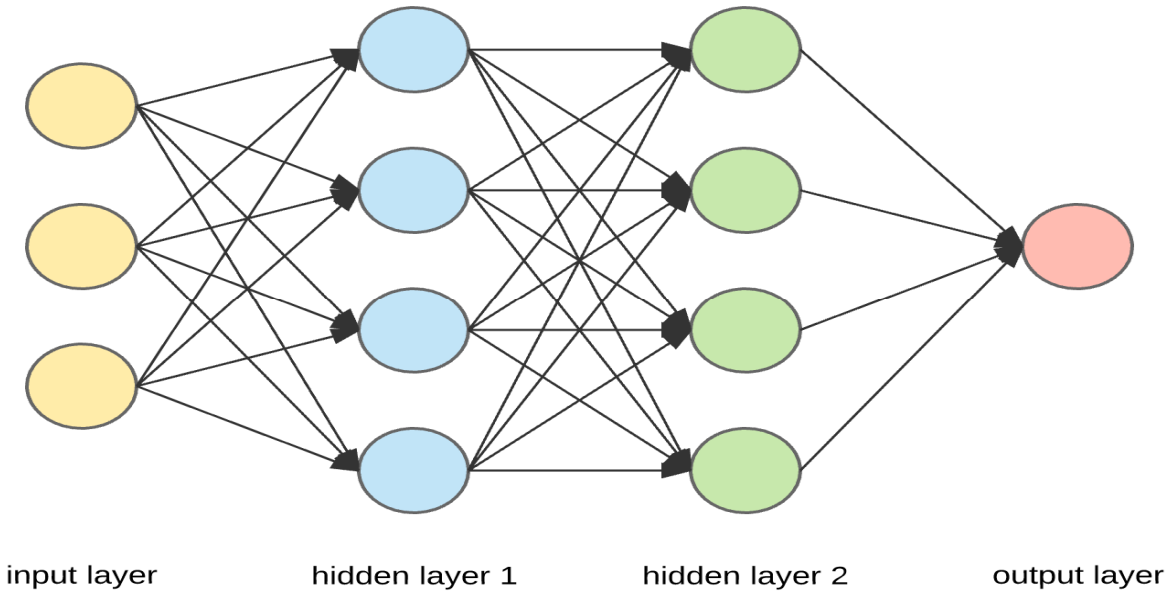

Fig.16. Artificial Neural Network [6]

The above Fig.16 depicts one input layer and two hidden layers namely hidden layer 1, hidden layer 2, and one output layer. The hidden layers do the complete processing of inputs and generate the output. The proposed trust model in ANN is named as ANNTM (Artificial Neural Network Trust Model).

5.1. *Step by step working procedure of Artificial Neural Network*

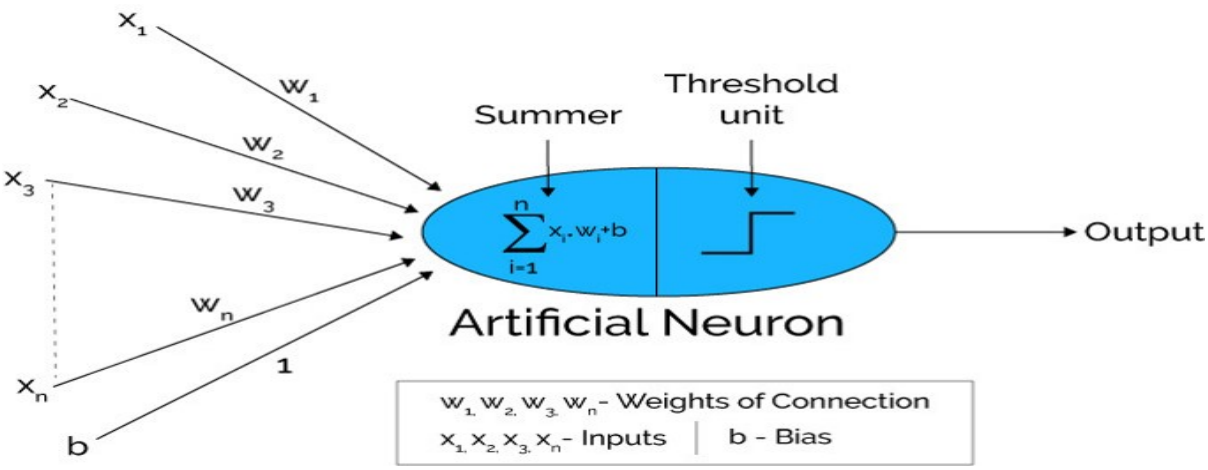

Fig.17. Artificial Neuron

The above Fig.17 shows the structure of artificial neuron and the working procedure of ANN is as follows:

1. The artificial neuron is accepting inputs x_1, x_2, x_3, x_4, ..x_n, weights w_1, w_2, w_3, w_4, ..w_n, and b is for bias.
2. The hidden layer consists of neurons and all neurons are interconnected.
3. The processing of nodes is done by the hidden layer as follows:
   - Initially all inputs are multiplied by their weights assigned and at last the bais b is added to it. The bias is a constant that helps the model to fit in the best manner.

$$z1 = w1 * x1 + w2 * x2 + w3 * x3 + w4 * x4 + ... + wn * xn + b \qquad (1)$$

- The activation function is applied to the Eq. (1) mentioned above.

4. Once the process in hidden layer is over then it goes to the output layer to generate output.
5. After generating the predictions the error is calculated by checking the difference between the actual output and predicted output.

5.2. *Experiments and Results of the Proposed Trust Model using Artificial Neural Network*

In ANNTM 20000 instances are considered. The service providers are 20 namely SP1 to SP20 respectively holds 1000 instances each. The ANNTM takes six parameters as input namely reliability, response time, fault tolerance, security, elasticity and service level agreement (SLA) and generates the output in output layer.

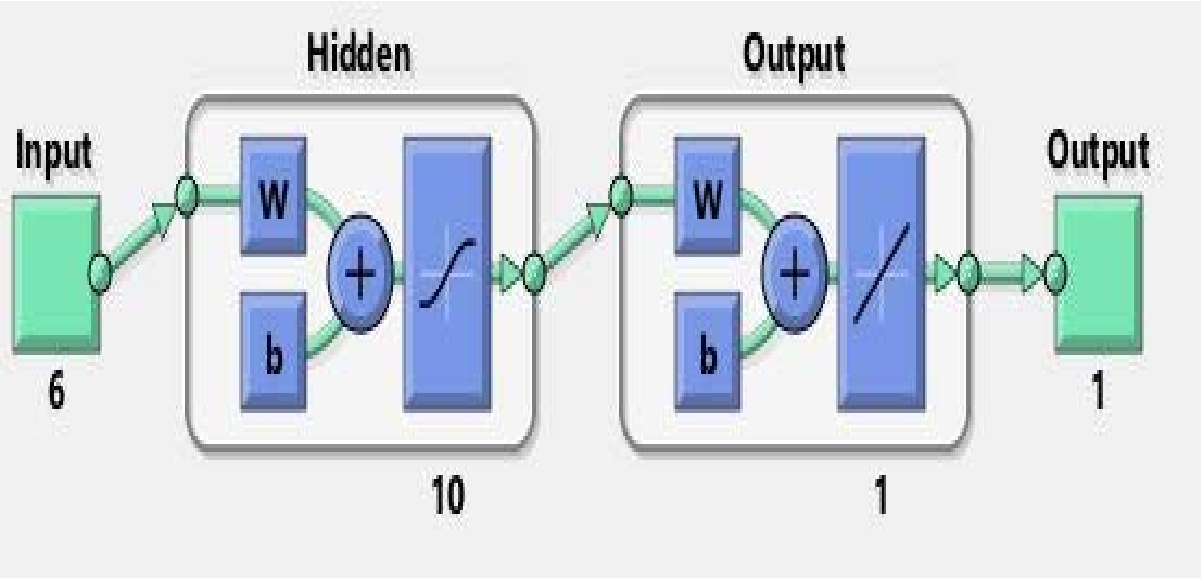

Fig.18. Artificial Neural Network Trust Model (ANNTM)

The above Fig.18 depicts the ANNTM which accepts the six service parameters mentioned above and ten hidden layers are created for processing which basically includes the weights and bias. The hidden layers output is fine tuned by the one output layer and finally produces the output. In this model for all 20000 instances which are already available with the generated trust value and the prediction is done by fitting the ANN model. Inorder to check whether the model is working fine or not we have taken 500 instances and predicted the trust value of it based on the client requirement. If the predicted trust value is mapping with any of the service providers already predicted value or within the range of predicted values then that service provider is allotted to that client. In this way the proposed model is helping out the customer to select the best service provider according their requirement.

The below Fig.19 shows the results of ANNTM Best Validation Performance. This figure has number of epochs on x-axis and mean squared error (mse) on y-axis. The best validation performance is 0.045663 at epoch 898 i.e. the optimum number of epochs required is 898 to get the best validation performance of the model. There is no large error difference between Training, Testing, and Validation of data. The best fit line is also demonstrated in the below figure.

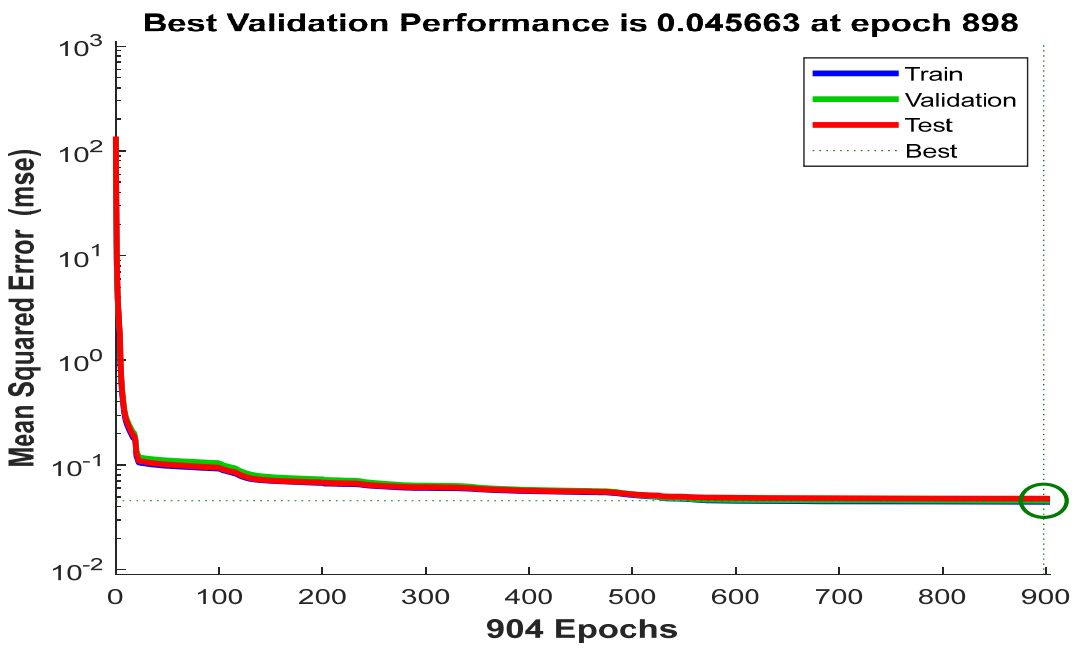

Fig.19. Artificial Neural Network Trust Model (ANNTM) Best Validation Performance

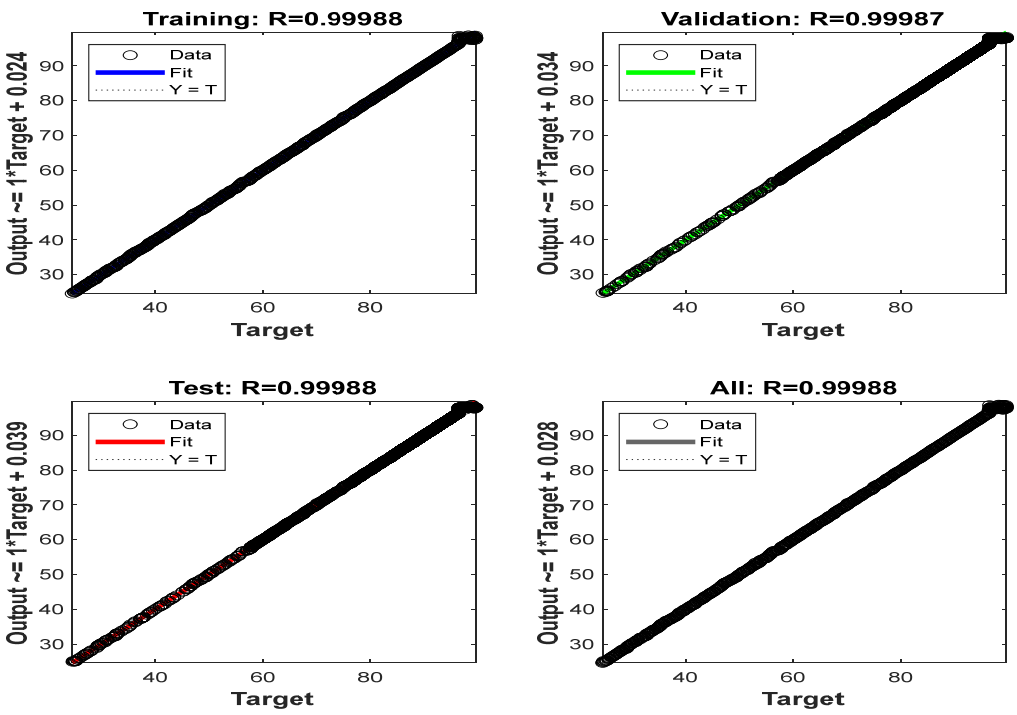

Fig.20. R Value of Training, Validation, Test and All of ANNTM

The above Fig.20 depicts the results of R value regarding Training, Validation, Test and All of ANNTM. The R value of Training is 0.99988, Validation is 0.99987, Test is 0.99988 and including all is 0.99988. By observing the results of the above in which R value is very near to one and also the Mean Square Error (MSE) value is 0.05927705, Root Mean Square Error (RMSE) value is 0.24346878 and Mean Absoulte Percentage Error (MAPE) is 0.00123471 which is very much less error and calculated for 20000 instances, we conclude that this model is very good.

6. Conclusion & Future Scope

The proposed Fuzzy Trust Model (FTM) and Aritificial Neural Network Trust Model (ANNTM) assist the clients to select the best service provider. The Fuzzy Trust Model basically works with Fuzzy Logic and its rules to define a trust value based on the client requiements. The impreciseness of the data is removed by using Fuzzy Trust Model. Once the trust value is generated based on rules then we need to check that the generated trust value is suitable to which service providers among the existing service providers. The list of top service providers are extracted based on the trust model for computational grids & clouds which was proposed in our previous research article. From this list of top service providers the clients are assigned to service providers based on their trust value generated. The ANNTM is used to predict the future for clients to select a service provider. If the predicted trust value based on the client requirement is mapped to the actual trust value which was already predicted and if it lies within the range then the service provider is selected. Both the trust models worked on 20000 instances of service providers namely SP1 to SP20 respectively and each service provider is allotted with 1000 instances. Based on the experiments and results shown for FTM and ANNTM we conclude that both are very good and according to the scenario either of the models can be used for service provider selection by the client. The proposed two models can be used for both cloud and grid requirements. In future this model can be further extended where the cloud users/clients also need to be monitored properly so that no misuse of resources will occur from clients.

7. Conflicts of Interest

The authors declare no conflict of interest.

References

[1] Kesarwani, A.; Mohan Khiler, P. (2022), Development of trust based access control models using fuzzy logic in cloud computing. Journal of King Saud University – Computer and Information Sciences, **34**, pp. 1958-1966.
[2] Rizvi, S.; Mitchell, J.; Razaque, A.; Mohammad Rizvi, R.; Williams, I. (2020), A fuzzy inference system (FIS) to evaluate the security readiness of cloud service providers. Journal of Cloud Computing – Advances, Systems and Applications**, 9**:42, pp. 1-17.
[3] Mona, S.; Navid, A.; Elham, T.; Safieh, S.; Rasoul, K. (2021), Fuzzy Rule-Based Trust Management Model for the Security of Cloud Computing. Mathematical Problems in Engineering, pp. 1-14.
[4] Rajganesh, N.; Ramkumar, T.; Selvamuthukumaran, S. (2017), A Fuzzy Logic Based Trust Evaluation Model for the selection of Cloud Services. IEEE International Conference on Computer Communication and Informatics, pp. 1-5.
[5] Mary-Jane, S.; Maozhen, L.; Gareth, T.; Clement, O. (2017), Fuzzy Logic Approach to Modelling Trust in Cloud Computing. IET Cyber-Physcial Systems: Theory & Applications, **2**(2), pp. 84-89.
[6] Manish, M.; Monika, S. (2014), A view of Artificial Neural Network. IEEE International Conference on Advances in Engineering & Technology Research, pp. 1-3.
[7] Mario, K.; Anton, Z. (2020), Predicting research trends with semantic and neural networks with an application in quantum physics, PNAS, **117** (4), pp. 1910-1916.
[8] Xu, Y.; Jinchao, G.; Ling, D.; Zhanping, Y.; Vincent, C.S.L.; Mohd Rosali; Mohd Hassan; Xiaoyun, C. (2021), Research and applications of artificial neural network in pavement engineering: A state-of-the-art review. Journal of Traffic and Transportation Engineering, (6), pp. 1000-1021.
[9] Source: ftp.pdl.cmu.edu/pub/datasets/hla/
[10] Source: http://fta.scem.uws.edu.au/index.php?n=Main.DataSets
[11] Source: www.uoguelph.ca/~qmahmoud/cgi-bin/display.pl
[12] Source: https://in.mathworks.com/help/fuzzy/foundations-of-fuzzy-logic.html
[13] Mahesh Kumar, G.; Ramachandram, S.; Jayadev, G. (2019), A Generalized Trust Model for Computational Grids & Clouds. International Journal of Innovative Technology and Exploring Engineering, **9** (2), pp. 4074-4080.

Authors Profile

G Mahesh Kumar holds the position of Assistant Professor, Department of Computer Science, Bhavan's Vivekananda College, Sainikpuri, Secunderabad, Telangana, India. He is currently pursuing his Ph.D. in Computer Science & Engineering from JNTU Hyderabad. He has done his Masters in Infromation Systems, M.Tech (CSE) from Osmania University. He has presented & published papers in national and international conferences. He has published research papers in international journals. He teaches subjects such as Java Programming, Advanced Java Programming, Python Programming, Mobile Computing, Software Engineering, Information Security, Big Data Analytics for both undergraduate and post-graduate students. His research areas include Grid Computing, Cloud Computing, and Internet of Things, Blockchain Technology.

Dr. S. Ramachandram received his bachelor's degree in Electronics and Communications Engineering (1983), M.Tech(CSE) (1985) and Ph.D. in Computer Science & Engineering (2005). He is presently working as a Professor, Department of Computer Science & Engineering, University College of Engineering, Osmania University, Hyderabad, Telangana, India. His research areas include Cloud Computing, Mobile Computing, Grid Computing, Server Virtualization, Software Engineering and, Big data Analytics. He has authored several books on Software Engineering, Operating Systems, handled several national & international projects and published several research papers at international and national level. He is currently the Professor of CSE and Vice-Chancellor of Anurag University, Hyderabad and was the former Vice-Chancellor, Osmania University. He also held several positions in the university as a Principal, Vice-Principal, University College of Engineering, Osmania University, Chairman Board of Studies, Nodal Officer for World Bank Projects and chair of Tutorials Committee. He is a member of Institute of Electrical and Electronic Engineers (IEEE), Computer Society of India (CSI) and Institute of Electronics and Telecommunication Engineers (IETE).

Dr. Jayadev Gyani, currently holds the position of Assistant Professor in Majmaah University, Al-Majmaah, Kingdom of Saudi Arabia. He received his Doctoral degree in Computer Science from University of Hyderabad in 2009 and Master of Technology in Computer Science and Engineering from Osmania University, INDIA in 1994.He worked at several levels such as Lecturer, Assistant Professor, Professor & Head of CS department. His overall teaching experience is 26 years. He handled several subjects such as Software Engineering, Algorithm Analysis and Design, Programming Languages, Assembly Language Programming, Software Evolution, Software Architectures, Low-Level Design of Software, Design Patterns, Artificial Intelligence, Parallel Architectures and Parallel Programming. He taught students at Undergraduate and Post- Graduate Levels. He has been guiding research students from JNTU, Hyderabad and JNTU, Kakinada. His research interest includes Software Engineering, Bigdata Analytics, Distributed Computing, Machine Learning Algorithms and their applications.