International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 6 (2015) pp. 15165-15181

http://www.ripublication.com

RFSTTRM: Improving The Security Model To Protect Resource Allocation In Cloud Environment

[1]C.Kamalanathan, [2]Dr.S.Valarmathy and [3]S.Kirubakaran
[1]Assistant Professor (Sr.G), ECE Dept,Bannari Amman Institute of Technology,Sathy,e-mail:kamalanadhan@gmail.com
[2]Professor& Head, ECE Dept,Bannari Amman Institute of Technology,Sathy,e-mail:atrmathy@rediffmail.com
[3]Assistant Professor (Sr.G), ECE Dept,Bannari Amman Institute of Technology,Sathy,e-mail:skirubame@gmail.com

Abstract

Deliberation of security in resource allocation is a major part of the research on cloud computing. In the previous paper, we developed a fuzzy logic based trust and reputation model for secure resource allocation in cloud computing. To promote the security process of the previous technique in this paper we design and develop a technique for hybridization of rough and fuzzy set for trust and reputation model (RFSTTRM) for secure resource allocation. Initially, the rough set algorithm applied on the trust and reputation values of existing entries of user to make the rule base. In next, the system selects the genuine entries and it calculates the trust and reputation factors of each resource center, which is given to the fuzzy logic system to get the security, score of a resource center. With the help of the security score value scheduling manager can select the secure resource and the rules generated from existing user's knowledge and the efficient decision making system makes the proposed algorithm become effective. The rule base system evaluates entries from the new user and it decides the whether mthe entries are capable to calculate the trust and reputation factor. Finally, the experimentation is carried out and we compare our proposed algorithm with the previous algorithm and we proved the efficiency of the proposed algorithm is not changing the security score value of the resource center even the user provides wrong values of trust and reputation.

Keywords: Trust Factor, Reputation Factor, Fuzzy Logic System, Security Score, Resource Center, Rough set theory

Introduction

Computing possessions have happen to be cheaper, more dominant and more ubiquitously accessible than ever before, with the express expansion of dispensation and storage technologies and the achievement of the Internet. This technical tendency has enabled the understanding of a new computing model called cloud computing [1]. As an understanding of efficacy computing, Cloud computing aims to afford computing resources to clients like community utilities such as water and electrical energy. In a cloud-computing environment, an Infrastructure-as-a-Service (IaaS) contributor packages its physical resources (e.g. CPU, memory disk) into different types of virtual machines (VMs) in terms of their sizes and characteristics, and offer them as services to the universal public [2]. It delivers an infrastructure, platform, and software (applications) as services that are made accessible to clients in a pay-as-you-go model. In industry, these services are represented Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) correspondingly. In various locations around the globe to distribute Cloud computing services many computing service providers as well as Google, Microsoft, Yahoo, and IBM are quickly deploying data centers [3]. At the equivalent time, computing and information dispensation requests a range of public organizations and private corporations have been rising speedily. Ranging from developing to housing, from moving to banking, for instance it includes digital services and functions essential by the different industrial sectors [4].

To supply inexpensive and simple access to computational resources cloud computing is a fashionable trend in current computing. To the best of our knowledge recently, most existing researches just focus on the optimized characteristic of the source distribution in their Gird/Cloud platforms for simplicity, but none of them guaranties the autonomous dynamic outcome [5]. The dynamic and autonomous source management are in a data centers. The previous research is usually approved out through a centralized architecture, in this procedure. The research focuses on the use of efficacy functions to proclaim the preferences of AEs over a variety of resource levels in terms of utilities. On behalf of the entire data center, the efficacy values are then communicated to a global arbiter that computes and performs the source management [6]. To cut down energy utilization particularly, when the total demand is short, it is desirable to decrease the data center faculty. To ensure resources allocated to those clients who value them the most, the entire demand exceeds data center capability, which is desirable to encourage mechanism. In Cloud computing environments, we call this difficulty the *dynamic capacity control* difficulty for mark markets [7, 2].

Even if the advantages of cloud computing is accurate the cloud computing desires to construct an appropriate safety for cloud implementations [8]. A main concern that requires particular attention is safety of clouds where the trust management is a necessary module for cloud security [9]. To maintain the users to identify the consistent and reliable providers; for example: eBay, Amazon, and application markets for mobile applications trust and reputation systems [10] are effectively used in various applications. To assist the customers to choose the suitable responsible cloud providers related techniques are essential. Without bearing in mind previous

sources and extraction of information existing trust and reputation, system depends on client response. In addition, it requires additional parameters [11] that assist the clients in choosing providers in a cloud marketplace. To assist the clients in creating apparent assessments before selecting regular trustworthy cloud providers, confidence and reputation systems have to change into the trust management system [12]

In this paper, we develops an efficient algorithm for Hybridization of rough and fuzzy set theory for trust and reputation model to secure resource allocation in cloud computing. Initially, we generated rule base from the existing user entries of the trust and reputation values. Once the system constructs the rules, subsequently the system calculates the trust and reputation factor for each resource center by considering the genuine entries. The calculated trust and reputation factor is given to the fuzzy system to calculate the score value of each resource center. The score value represents the security level of the resource center and this value helps the scheduling manager to select most secure resource center. With the help of the generated rules, the proposed system achieved more security. The rule base system evaluates entries from the new user and it decides the whether the entries are capable to update the score value of the corresponding resource center. This make sure efficiency of the proposed algorithm is not changing the security score value of the resource center even the user provides wrong values of trust and reputation.

This paper is organized as follows: the second section shows some of the related works and the third section shows the need for security in resource allocation of cloud computing and the fourth section represents the motivation of the research. The section five explains our proposed technique and the sixth section discuss our experimental results and the seventh section concludes our technique.

Related Works: A Brief Review

In this section shows some of the researches available in the literature for trust based secure model and trust reputation system in cloud computing and grid computing environment.

Mohamed Firdhous*et al.* [13] for different distributed system, has suggested trust models. With exacting emphasis on their capability, applicability in reasonable heterogonous cloud environment and implementability, the trust management systems suggested for cloud computing had been investigated. For forming the trust scores throughout the appraisal of those systems, it was found that none of the systems was derived from solid theoretical foundation and it does not take any distinction of package attribute. Hence, for constructing trust models for cloud computing, solid theoretical foundation was necessary.

Shanshan Song et al [14] have anticipated safety declaration at all resource sites that trusted Grid computing stress robust resource allocation. From distant resource sites large- scale Grid applications were being late due to the lack of security assurance. They have produced a security-binding system in the course of trust integration across grid sites and site reputation measurement. They did not indulgence the trust factor deterministically; as a replacement, they have applied fuzzy theory to agree with the fuzziness or reservations behind all confidence attributes. By common

replace of site security information and matchmaking to assure user job demands, the binding was attained. PKI-based trust organization helps grids in multi-site confirmation and particular sign-on operations. However, at grid sites, cross certificates were not sufficient to consider local precautions conditions. For disseminated trust aggregation through fuzzification and addition of security attributes, they have recommended a fuzzy-logic trust system. They have introduced the trust guide of a Grid site, which was determined by site reputation from its record of accomplishment and self-defines probable attributed to the risk conditions and hardware, software defences deployed at a Grid site.

Vivekananth. P [15] has suggested that grid system was an energetic environment where all units shared the resources issued by the previous entities. For solving large-scale issues in science and engineering, the organization allows the coordinated and aggregated use of geologically distributed resources, regularly owned by independent organizations. However, application composition, resource management, and scheduling in those surroundings were a complicated process. Before initiating any operation, the resource provider as well as the consumer should be influenced. Mutual confidence must be recognized amid the user and the provider, where the trust was generated on reputation. The impression of reputation was attractive in peer-to-peer networks, but still it was not faultless in grid computing. For resource selection, they have offered an impression of accessible reputation based systems.

Need For Security In Resource Allocation of Cloud Computing

To improve the quality there is a vital requirement to progressively accumulate, manage, distribute, and analyse huge amount of composite data to generate the patterns and trends. It is essential that the clouds to be protected due to the essential nature of the applications. The main protection issue with the cloud system is that the possessor of the data may not have the influence of where the data is located. We need to protect the data in the middle of distrusted process, the reason is that if one needs exploiting the advantages of cloud computing, one should also use the resource allocation and development presented by clouds. The transpiring cloud computing classification attempts to concentrate on the fast expansion of web-associated devices and handle huge quantity of data. For dealing vast extent of data on commodity hardware Google has now offered the Map Reduce framework. For cloud computing united with integrated parts such as Map Reduce, Apache's Hadoop distributed file system (HDFS) is transpiring superior software component. The requirement to augment human reasoning interpreting and decision making capabilities have resulted in the appearance of semantic web which is an proposal that endeavorsto transform the web from its current human readable form to machine process able form. With huge amount of data to be shared and managed, this in turn has resulted in quite a few social networking sites.

Conveniently there are quite a few security issues for cloud computing as it covers a lot of technologies including networks, databases, load balancing, operating systems, transaction management, virtualization, resource scheduling, concurrency control and memory management. Significant to cloud computing there are lots of

security issue for numerous of these systems and technologies. For example, the networks that interconnect the systems in a cloud have to be protected. Furthermore, the virtualization paradigm in cloud computing consequences a numeral security concerns. For representing, mapping the virtual machines to the physician machines has to be approved steadily. In cloud, computing the secured resource allocation can afford the user to browse securely, where the user is able to maintain their data securely. By means of the user agreed characteristic value in this work, we locate the security score of a resource in cloud computing. Using this new user about a resource one can judge whether it is protected or not based on the security count.

Motivation of My Research

In our earlier work [22], we have developed a fuzzy logic based trust and reputation model in cloud computing for secure resource allocation. The security of the resource center is evaluated based on the trust and reputation factor of the resource center. After access the resource block, the each user gives the attributes value for the trust factor and the reputation factor since the values of trust and reputation factors are depends on user given values. In this case, some of the users may enter wrong values purposely to violating the score value of the resource center. As a result, the score value of secured resource may decrease and score value of insecure resource may increase. By referring the wrong score value, the scheduling manager may take wrong decision, this leads violating the user's privacy. Meanwhile we have to avoid the wrong entries in the future.

Proposed Technique For Hybridization of Rough and Fuzzy Set Theory For Trust and Reputation Model To Secure Resource Allocation In Cloud Computing

This section describes our proposed model for secure resource allocation in cloud computing through hybridization of rough and fuzzy sets. The following figure 1 represents the sample structure of the proposed algorithm. In this paper, initially the experts take the history of trust and reputation values of existing users and evaluates each entry and add decision variables in decision attributes whether entry is valid or not. Then, we adapt the rough set theory on the historical data to construct the rules for trust and reputation. Followed by the generation of rules, the system calculates the trust and reputation factor for each resource center through the valid entries of the user. The values of trust and reputation factor of every resource center is given to the fuzzy logic system, which calculates the score value of each resource center through the trust and reputation factor values. The highest score value of the resource center represents the reliable in terms of security since the calculated score value of resource center helps the scheduling manager to selects the most secured resource center from the available. When the user enter, the new values that will be matched with the rules base to evaluate the entries are trustworthy or not. If the entered values determined as

reliable subsequently those values are considered for update the score values of the resource center else, the entry is abandoned.

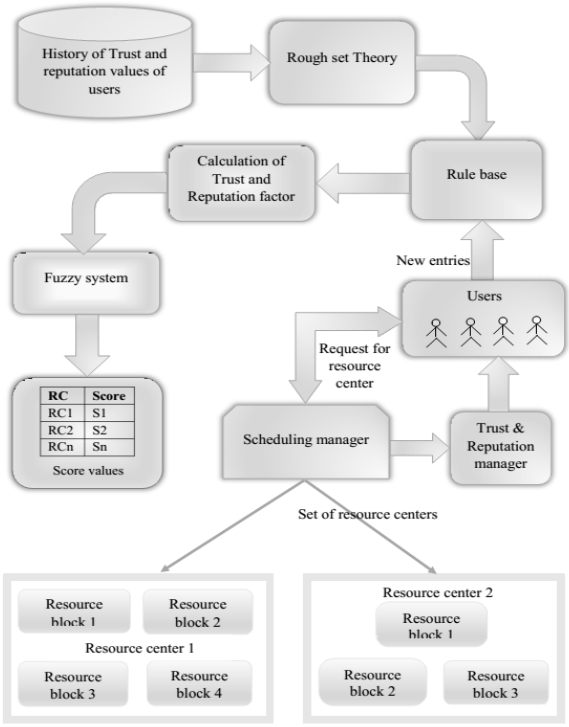

Figure 1: represents the sample structure of the proposed algorithm.

To perform the task the user sends the request to the scheduling manager then it selects any resource center from the set of resource center, which is represented as $RC = \{rc_k\}$ where $1 \le k \ge K$, the value of K represents the total number of available resource center to perform the task of the user. The each resource center has set of resource blocks, which is represented as $rc_k = \{rb_s\}$ where $1 \le s \ge S$, the value of S represents the total number of available resource block to perform the task of the user in the resource center rc_k. Since the scheduling manager assigns the resource block to the user for perform their task by accessing the resource block. Once the user finished their accessing of resource block, the scheduling manager sends the report to the trust and reputation manger subsequently, they sends a form to the user to evaluate the security of the resource block in terms of trust and reputation. The attributes in the trust and reputation are given in below sections 5.1 and 5.2.

Trust Factor of Resource Center

Definition: The entire sum of trust factor of each resource block in the resource center is the trust factor of resource center.

Trust is an important thing equally in human society and cyberspace security. Every one of us is responsive of the importance of trusting somebody. The

environment of trust is usually decentralized because of the fact that the parameters of the trust are normally personal. Despite monitoring or controlling the party, trust can be tagged as confidence where a specific party would work in a probable manner. Trust is measured as positive and gives good result, in uncertain environments. Generally, there has a grey area in conveying the reliability of a computer site [13]. Trust is demonstrated by a linguistic term rather numerically, which is related to the human relationship. Derived from time and environment trust would differ. Farag Azzedin and Muthucumaru Maheswaran [12] gave the description for the trust and it is as follows: Trust is a strong opinion in competence of an entity to act as anticipated and the strong opinion is not a fixed value associated with the entity but rather it is subject to the entity's attitude and applies only within a specific context at a given time. The strong opinion can be defined as a dynamic value that is found to span over a set of values differ from extremely trustworthy to extremely untrustworthy. Derived from the earlier experience, the trust factor is produced and is provided for a particular context. The trust factor is derived from the given time instance, as the trust level describing two entities is not significant to be same for today when compared to a year ago. Some of the attributes we measured for the trust factor are as follows:

- *Anti-virus Capability:* The capability of the resource to defend against viruses and malicious codes.
- *Firewall Capability:* The capability to guard the resource from additional network accesses.
- *Secured Job Execution:* The capability of the resources to assure the secure implementation of a job.
- *Copyright date:* Users trust shopping with frequently updated websites. For example, if the copyright of the website says 2000, subsequently it would be a large red flag for users.
- *Corporate logos:* Comprise the company logos on your website. Therefore, those users will trust your product and services.
- *About Us:* The about us page shows the complete history of the company and the user may trust relaying on the history.
- *Privacy Policy:* The privacy policy adds an important degree of trust since it shows that you care and respect the customer's individual information.
- *Business Address:* The business address on webpage shows that you have a physical location that adds a significant level of trust among the users.

Reputation Factor of Resource Center

One of the most important methods, which form the foundation for the circulated application and system safety, for its improved scalability and flexibility is the reputation mechanism. Since one can trust one more on basis of good reputation. Reputation is stated as a measure of trustworthiness in the sense of reliability. For generating trust during social control lacking of trusting third parties, reputation system [14] offers a proposal. For generating trust through social control using the community-based feedback about the previous experience of entities the reputation mechanism provides a proposal. FaragAzzedin and Muthucumaru Maheswaran [12] stated that reputation of an entity is an anticipation of its approach derived from other

entities observations or data about the entity's past attitude at a known time. Some of the reputation approaches we measured for reputation feature are as follows:

- *Consistency:* The capability of the resource to achieve the expected function under declared circumstances for a particular phase of time.
- *Confidentiality:* The capability of concealing information from illegal users.
- *Robustness:* The capability of the system to endure from the attacks proposed towards that system.
- *Contents look current:* If the website is in old arrangement, the users will pay no attention to it. So the website should be updated regularly with present trends, content and images.
- *Rapid Response:* The rapid reaction of a webpage will enlarge the reputation of the webpage since users would like to get to complete their job swiftly.
- *Trust symbols:* By means of trust symbols in the web page, it proves to the users that the web page is protected towards the hackers and viruses.
- *Return Policy:* This actually shows that you stand behind you products and it gives the users the satisfaction of expressive that they can return the product if it is malfunctioning or they are discontented with it.

While giving the values of trust and reputation factors, the user might enter the wrong values intentionally. The result of these wrong entries affects the score value of the secure resource center may be reduced this makes the secure resource center into insecure resource center, on the contrary, the score value of the insecure resource may be increased this makes the insecure resource center into secure resource center. To solve this problem in this paper, In this paper, initially the experts considers the history of trust and reputation values of existing users and evaluates each entry and add decision variables in decision attributes whether entry is valid or not. Once we evaluated the every existing entries subsequently adapt the rough set theory to construct the rules.

Rough Set Theory For Rule Generation

Rough set theory is emergent as an influential theory dealing with imperfect information. Rough set theory is a mathematical tool for the investigation of an imprecise report of objects [19, 26, and 28]. Here, we make use of the rough set theory for rule generation process. Let HDB denotes the historical database of the trust and reputation values with the decision attributes. The historical database contains two main parts which is separated by their parameters $HDB = T, R$ where the symbol T represents "trust" which contains the set of parameters $T = t_i$ where $1 \le i \ge n$ and the value of n represents the maximum number of parameters to evaluate the trust factor of the resource center. The symbol R from HDB represents "reputation" which contains the set of parameters $R = r_j$ where $1 \le j \ge m$ and the value of m represents the maximum number of parameters to evaluate the reputation factor of the resource center.

Construction of indiscernibility matrix for trust and reputation

The indiscernibility matrix also known as similarity matrix, which represents the relation between the common entries of the users. To construct the indiscernibility matrix, the experts add the decision attribute in the trust and reputation factors of the historical user entries for differentiate the valid and invalid entries. The following table 1 represents the sample historical user entries of the reputation factor for the resource block rb_s in the resource center rc_k .

Table 1: Sample Historical Data of Reputation Factor For Single Resource Block

	r_1	r_2	r_3	r_4	r_5	r_6	r_7	Decision r_m
U_1	1	1	1	1	1	2	1	1
U_2	1	2	2	2	1	2	2	1
U_3	3	2	3	1	2	2	3	2
U_4	1	2	2	2	2	1	2	2
U_5	2	2	2	3	2	3	2	1

The each column from the above table represents attributes of the reputation factor (r_1 to r_7) and each row represents the user. The inside values from the above table represents the user given entries to evaluate their used resource block in terms of reputation factor. The final attribute represents the decision attribute, which gives the entries of the user become valid, or not. The decision value 1 indicates that the valid decision and the value 2 represents the invalid decision. The following table 2 represents the indiscernibility matrix for the above table 1.

Table 2: Indiscernibility Matrix of Reputation Factor For Single Resource Block

	U_1	U_2	U_3	U_4	U_5
U_1	---	r_1, r_5, r_6	r_4, r_6	r_1	-
U_2		---	r_2, r_6	r_1, r_2, r_3, r_4, r_7	r_2, r_3, r_7
U_3			---	r_2, r_5	r_2, r_5
U_4				---	r_2, r_3, r_5, r_7
U_5					---

Computation of logical rules

The logical rules can mine from the indiscernibility matrix, which is represented in the above table 2. Let consider the entries of U_2 and the procedure to find the logical rules is given in following.

Step1; R2: $\left(r_2 \cup r_6\right) \cap \left(r_1 \cup r_2 \cup r_3 \cup r_4 \cup r_7\right) \cap \left(r_2 \cup r_3 \cup r_7\right)$

Step 2; R2: $\left(r_2 \cup r_6\right) \cap \left(r_2 \cup r_3 \cup r_7\right)$

Step 3; R2: $\left(r_2\right)$

The above rule R2 represents that if the value of r_2 is 2 then the decision is 1. Likewise, we generate the rules from all users and we plotted the constructed rules in the following table 3.

Table 3: Logical Rules of Reputation Factor For Single Resource Block

	r_1	r_2	r_3	r_4	r_5	r_6	r_7	Decision r_m
R_1	*	*	*	*	*	*	*	1
R_2	*	2	*	*	*	*	*	1
R_3	*	2	*	*	2	*	*	2
R_4	*	2	2	*	2	*	2	2
R_5	*	*	*	*	*	*	*	1

The above table 3 is the representation of logical rules of reputation factor for single resource block. The same procedure is followed to calculate the logical rules for the trust factor. Every resource block has two sets of rules one is for trust factor and the another one is for reputation factor because the every resource block has not have the same capacity since each resource block need unique rules for trust and reputation factor.

With the help of generated rules, the system can validate whether the newly received entries from the users are appropriate or not also, the system allows only the suitable entries from the user. Since the construction of rules in is a significant part of the proposed algorithm.

Computation of Trust and Reputation Factor

Once the rules are generated for each resource block, the next step is computation of trust and reputation factor only with the selected number of valid entries of the user. The valid entries are elected based on the decision attribute. In previous paper [22], the computation of trust and reputation factor considers all kinds of entries of the user including the wrong entries this will make the wrong evaluation of the resource block and the corresponding resource center since our proposed algorithm confirms that the computation of trust and reputation factor is trustworthy by selecting the valid user entries.

Computation of trust factor

With the intention of calculating the value of trust and reputation factor for resource center, initially we evaluate the trust factor for each resource block in the resource center. The calculation of trust factor of each resource block is as follows:

$TF_k(rb_s) = p_s \sum_{i=1}^{n} \left(\sum_{u=1}^{U} \frac{A_{ij} w_i}{TW} \right)$; *where*, $k = 1,2,3,.....$ The equation given below is used to calculate the total weight value of the attributes. It is the sum of the weight values of each attribute.

$$TW = \sum_{i=1}^{m} w_i$$

Where, $TF_k(rb_s)$ denotes that the trust factor of resource block rb_s in the resource center rc_k, the symbol p_s denotes that the probability of the user used the resource block rb_s in the resource center rc_k. The symbol t_{iu} represents the trust factor value for the 'ith' attribute is given by the user 'u' and the symbol w_i represents the weight value of the attribute. The total number of attributes is represented by n and the total number of user is represented by U.

After find the trust factor value for each resource block in a resource center, we need to calculate the trust factor for the resource center. For instance, in Fig.1, the first resource center has four resource blocks and to find the trust factor of the first resource center, we should know the trust factor value of all the four resource blocks. The trust factor for the resource center is calculated as follows:

$$TF(rc_k) = \sum_{s=1}^{S} TF_k(rb_s)$$

Where, $TF(rc_k)$ is represents the trust factor of a resource center rc_k and S denotes that the total number of resource blocks in a resource center rc_k.

Computation of Reputation Factor

The reputation factor of a resource center is also calculated by the same procedure used to calculate the trust factor of the resource center. The formula to calculate the reputation factor for the resource center is denoted by an equation given below:

$$RF(rc_k) = \sum_{s=1}^{S} TF_k(rb_s)$$

Where, $RF(rc_k)$ is represents the reputation factor of a resource center rc_k and S denotes that the total number of resource blocks in a resource center rc_k.

To find the reputation factor for the resource center, we ought to find the reputation factor for each resource block in the resource center. The formula to evaluate the reputation factor for each resource block in a resource center is as follows:

$$RF_k(rb_s) = p_s \sum_{j=1}^{m} \left(\sum_{u=1}^{U} \frac{r_{ju} l_j}{L} \right)$$

Where, $RF_k(rb_s)$ denotes that the reputation factor of resource block rb_s in the resource center rc_k, the symbol p_s denotes that the probability of the user used the resource block rb_s in the resource center rc_k. The symbol r_{ju} represents the trust factor value for the 'j[th]' attribute is given by the user 'u' and the symbol l_j represents the weight value of the attribute. The total number of attributes is represented by m and the total number of user is represented by U.

The calculation of total weight value L of the attributes for the reputation factor is given below.

$$L = \sum_{j=1}^{m} l_j$$

Fuzzy Logic System

In our method, this part delineates the usage of fuzzy logic system. To discover the security score of the resource center the trust factor value $TF(rc)$ and the reputation factor value $RF(rc)$ of every resource center are specified as input to the fuzzy logic system.

In our method, the Fig.2 shows the block diagram of the procedure of fuzzy logic system.

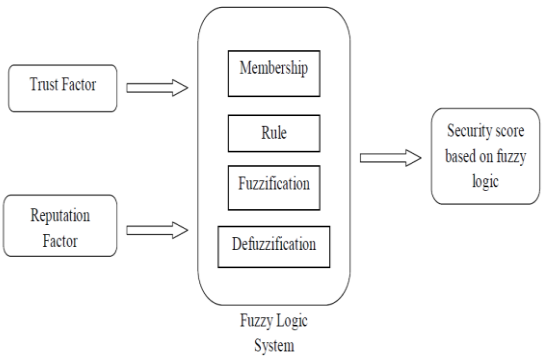

Figure 2: Input and Output of Fuzzy Logic System used in our technique

The input variables are mapped by set of membership functions in fuzzy logic system. Fuzzification is identified as the performance of converting the input value to fuzzy value. The fuzzification in the fuzzy logic system would be derived from the rule and whereas defuzzification is based on rule. We will get a single output for the specified number of inputs, after defuzzification. In Fig.2, as input to the fuzzy logic system, we present the trust factor and the reputation factor. The fuzzy logic system originally applies the input values in the membership functions and the fuzzification and defuzzification will be completed derived from the rule. The ultimate output we obtain from the fuzzy logic system is the security count. It is illustrated by an equation below:

$$I = TF(rc) \otimes RF(rc)$$

Where, the value of I represents the security score we obtained as output from fuzzy logic system and $TF(rc)$ represents the trust factor we give as input to fuzzy logic system finally $RF(rc)$ denotes that the reputation factor we give as input to fuzzy logic system.

Result and Discussion

This section shows the result of our proposed work. This section contains experimental setup, analysis the score value of the resource center and we compare performance our proposed algorithm with the previous work [22].

Experimental Setup

Our technique is implemented in java (jdk1.6) that has the system configuration as i5 processor with 4GB RAM. We have used three different datasets, which are Financial, Medical, and RDB for our technique. In our technique, we used four different resource centers that have three different resource blocks. The datasets we used are as resource blocks. We analyse the performance of our technique with different number of users because; the users will give the attribute values for the trust factor and the reputation factor after they used the resource.

Performance Analysis

This section delineates the performance of our recommended technique. To check the performance, we use two secure resource centers and two insecure resource centers. The first and second resource centers are insecure and the third and fourth resource centers are secure and let us see how our system works based on the feedback of the users. The performance of our system is checked with different number of users.

The following figure 2 represents the values of trust factor for the previous algorithm and the proposed algorithm for the various number of users. From the above figure 2 we conclude that the proposed algorithm has less numbers trust factor when compared with the previous algorithm. The reason behind this is, our proposed algorithm only considers the valid user entries since the many of the entries are not considered for calculating the trust factor also if the user has valid trust factor and invalid reputation factor means then the system disallow the corresponding entry to evaluate the resource blocks.

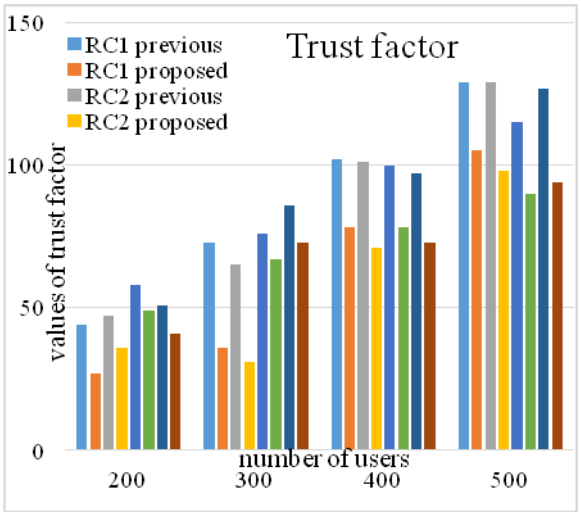

Figure 2: Represents The Evaluation of Trust Factor For Different Number of Users

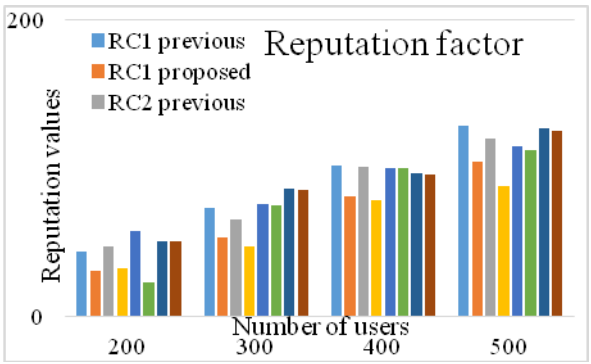

Figure 3: represents the evaluation of reputation factor for different number of users

The above figure 3 represents the values of reputation factor for the previous algorithm and the proposed algorithm for the various number of users. From the above figure 2 we conclude that the proposed algorithm has less numbers trust factor when compared with the previous algorithm. The reason behind this is, our proposed algorithm only considers the valid user entries since the many of the entries are not considered for calculating the trust factor also if the user has valid trust factor and invalid reputation factor means then the system disallow the corresponding entry to evaluate the resource blocks.

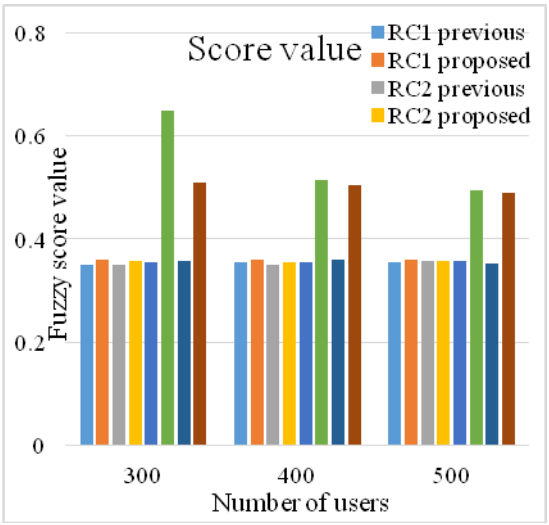

Figure 4: Represents The Evaluation of Score Value For Different Number of Users

The above figure 4 represents the evaluation of security score value for the previous algorithm and the proposed algorithm for the various number of users. From the above figure 2 we conclude that the proposed algorithm has more security score value when compared with the previous algorithm. The reason behind this is our proposed algorithm only considers the valid user entries since the fuzzy logic system get the proper values of the trust and reputation factors for every resource blocks. The proposed algorithm more security score value than the previous algorithm for the resource center3 and resource center4. Since we can confirmed that our proposed algorithm has worked properly.

Conclusion

We have developed the efficient algorithm for Hybridization of rough and fuzzy set theory for trust and reputation model (RFSTTRM) to secure resource allocation in cloud computing. Initially, we generated rule base from the existing user entries of the trust and reputation values. The system utilized the genuine user entries for calculate the trust and reputation factor. The result of the trust and reputation factor given to fuzzy system and it calculated the security score value. This makes the scheduling manager to select the most secure resource center. With the help of the generated rules, the proposed system achieved more security. The rule base system evaluates entries from the new user and it decides the whether the entries are capable to calculate the trust and reputation factor. Finally, the experimentation is carried out and we compare our proposed algorithm with the previous algorithm and we proved the efficiency of the proposed algorithm is not changing the security score value of the resource center even the user provides wrong values of trust and reputation.

References

[1] Qi Zhang, Lu Cheng and RaoufBoutaba, “Cloud computing: state-of-the-art and research challenges”, Journal international service Applications, vol.1, no.6, p p. 7-18, 2010.

[2] Qi Zhang, Quanyan Zhu and RaoufBoutaba, “Dynamic Resource Allocation for Spot Markets in Cloud Computing Environments”, Utility and Cloud Computing (UCC), pp.178-185, Dec 2011.

[3] AntonBeloglazov, JemalAbawajy and RajkumarBuyya, “Energy-aware resource allocation heuristics for efficient management of data centers for Cloud computing”, Future Generation Computer Systems, vol. 28, p p. 755-768, 2012.

[4] HadiGoudarzi and MassoudPedram, “Maximizing Profit in Cloud Computing System via Resource Allocation”, International Conference on Distributed Computing Systems - ICDCS, vol.12, no. 40, pp. 1-6, 2011.

[5] Sheng Di, Cho-Li Wang, Luwei Cheng and Ling Chen, “Social-optimized Win-win Resource Allocation for Self-organizing Cloud”, International conference on cloud and servicing, p p.15-18, 2011.

[6] Chandra MouliVenkataSrinivasAkana, Sundeep Kumar K, C.Divakar and Ch. Satyanarayana, “Social-optimized Win-win Resource Allocation for Self-organizing Cloud”, International Journal Advanced Networking and Applications, vol. 3, no. 2, p p. 1060-1069, 2011.

[7] Zhen Xiao, Weijia Song, and Qi Chen, “Resource Allocation Algorithms for Virtualized Service Hosting Platforms”, IEEE Transaction on parallel and distributed systems(tpds), vol. 2, no. 1, p p. 1-11, 2010.

[8] AlokTripathi and Abhinav Mishra,“ Cloud Computing Security Considerations”, IEEE International Conference on Signal Processing, Communications and Computing, Vol.4, no.7, pp.1-5,2011.

[9] Mohamed Firdhous, Osman Ghazali and Suhaidi Hassan,“ Trust Management in Cloud Computing: A Critical Review”, International Journal on Advances in ICT for Emerging Regions, Vol.4, no.2, pp.24-26,2011.

[10] A. Jsang, R. Ismail, and C. Boyd, “A survey of trust and reputation systems for online service provision," Decision Support Systems, vol. 43, no.2, pp. 618-644, 2007.

[11] S. M. Habib, S. Ries, and M. Muhlhauser, “Cloud computing landscape and research challenges regarding trust and reputation," Symposia and Workshops on ATC/UIC, vol. 0, pp. 410-415, 2010.

[12] A. Josang, C. Keser and T. Dimitrakos,”Can we manage trust?" in iTrust,” Springer, pp. 93-107, 2005.

[13] Mohamed Firdhous, Osman Ghazali and Suhaidi Hassan,“ Trust Management in Cloud Computing: A Critical Review”, International Journal on Advances in ICT for Emerging Regions, Vol.4, no.2, pp.24-26,2011.

[14] Shanshan Song, Kai Hwang and Yu-Kwong Kwok,“ Trusted Grid Computing with Security Binding and Trust Integration”, Journal of Grid Computing,2005.

[15] Vivekananth.P, “Trusted Resource Allocation in Grid Computing by Using Reputation,” International Journal of Computer Science & Communication, Vol.1, no.2, pp.23-25,2010.

[16] Shanshan Song and Kai Hwang, “Dynamic Grid Security with Trust Integration and Optimized Resource Allocation”, in Proceedings of the International Symposium on High- Performance distributed computing, Honolulu, 2004.

[17] Farag Azzedin, Muthucumaru Maheswaran, "Towards Trust-Aware Resource Management in Grid Computing Systems," in Proceedings of the 2nd IEEE/ACM International Symposium on Cluster Computing and the Grid, Washington, USA, pp: 452, 2002.

[18] R. A. Malaga. “Web-based reputation management systems: Problems and suggested solutions”, Journal of Electronic Commerce Research, Springer Netherlands, Vol: 1, No: 4, pp: 403-417, 2001.

[19] A. Pawlak, Rough Sets: Theoretical Aspects of Reasoning about Data, Kluwer Academic publishers, Dordrecht, The Netherlands, 1991.

[20] J.W. Grazymala-Busse, Rough Sets,Advances in Imaging and Physics 94,PP. 151-195,1995.

[21] A. Pawlak, J.W. Grzymala-Busse,R. Slowinski, W. Ziarko, Rough sets,Communications of the ACM 38 (11) 1995,89-95.

[22] C.Kamalanathan, S.Valarmathy and S.Kirubakaran, "Fuzzy Based Trust and Reputation Model for Secure Resource Allocation in Cloud Computing", International Review on Computers and Software, Vol.8, No.9, 2013.