Agent Based Information Security Threat Management Framework for Hybrid Cloud Computing

***Muhammad Imran Tariq*[1]*, Shahzadi Tayyaba*[2]*, Muhammad Usman Hashmi*[1]*, Muhammad Waseem Ashraf*[3]*, Natash Ali Mian*[4]**

[1]Department of Computer Science, Superior University, Lahore, Pakistan
[2]Department of Computer Engineering, the University of Lahore, Pakistan
[3]Department of Electronics, Govt. College University, Lahore, Pakistan
[4]School of Computer Science, National College of Business Administration and Economics, Lahore, Pakistan

Abstract

Cloud computing is an effective, fast growing, and low cost way for today's businesses organizations to provide professional and IT services over the Internet. Cloud computing has variety of service and deployment models providing both solid support to organizations to secure their business interests and flexibility to deliver new services. Security threats are associated with each service and deployment model, vary and depend on wide range of factors including the sensitivity of information, resources and architectures. Over time, business and cloud organizations tend to tight their security posture. For effective threat management, cloud service provider must perform threat assessments on regular basis. Threat Agent is an individual or group that exploit vulnerabilities, manifest a threat and conduct damaging activities. An alerting position arises when threat agent breach security and leaks confidential and sensitive information of organization. To cater this situation, we have proposed Agent Based Information Security Threat Management Framework that ensures threat mitigation in Cloud environment. The core objectives of this article is to present Agent based information security threat management framework for better understanding from threat identifying process to apply countermeasures. We also introduced software and intelligent agent concepts that gather appropriate, relevant, variety of information relates to Information Security to use in proposed framework and to develop system that facilitates organization to define, update, propose, validate and apply measure against each threat agents. The proposed framework validated using fuzzy logic inference system and simulated and tested through MATLAB®. The proposed framework covers all cloud services and deployment models. Cloud organizations can apply this framework to their organizations to mitigate threats.

Keywords:

Information security Framework, Cloud computing, Fuzzy logic, Threat management, Risk management, Self-Adaptive Systems

1. Introduction

Cloud has always become a computer / communication paradigm that has the potential to change the way our systems and services are used. Thanks to the rapid provision of cloud computing resources with minimal management effort or interaction between service providers, we are now forced to reconsider the core technology of information (IT) data elements [1].

For small and medium enterprises (SMEs) and sectors such as e-health and eGoverment are using benefits of Cloud Computing but unfortunately security issues are bigh conern as noted by the ENISA and. The importance of creating reliable and secure cloud services has led to a central issue [3]. Other IT ecosystems (eg Critical Infrastructure) are alwasys opt well-designed security measures that not only useful to increase the security guarantees provided by a system but also awareness of its sensitivity and even also assess the effectiveness of the various security mechanisms being implemented. Unfortunately due to the special features of the Cloud Computing, there are only a few attempts to target a common framework.

The primary purpose of information security (IS) is to ensure the business interests against threats and ensure success in daily operations by ensuring confidentiality, integrity and availability. Best Practice Information Security (IS) is highly dependent on well-functioning risk management (RM) processes, and RM is often regarded as the cornerstone of IS. Risk Management for Information Security (ISRM) is a continuous process wherein we start from identification of risk, mitigation techniques, reviewing and monitoring risks to obtain and maintain risk acceptance [4].

ISRM is a complex arena with many unsettled problems; some claims that the current risk management situation is that it is broken and not functioning, while others take a step further and claim that current quality risk management practices are worse than failing have nothing [5]. We believe that understanding the risk causes that are causing problems is essential for the research community to be able to make progress. Due to the complexity and linkages in the research field, researchers should avoid tackling an isolated problem at one time while ignoring the remaining challenges.

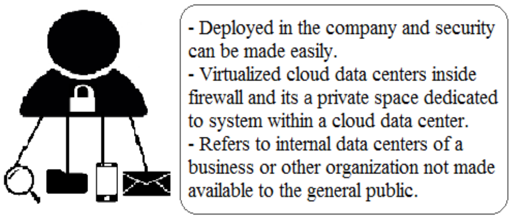
In past, various authors used agent technology in security frameworks. The authors opted agent techniques in additon to symmetric and asymemetric keys to more secure cloud infrasture [6]. The said proposed framework using agent technology will enhance reliability of cloud without effecting performance. The authors redress security issue of Denail of Service by adopting agent Novel and mixed agent based techniques [7]. In order to secure open cloud, authors under refernce [8] introduced multi-agent techniques and proposed framewrok that communicate with other clouds reliably. The results of the framewrok shows that perforamance of the newtwork has been increased after the implementation of proposed multi-agent techniques [8]. Another researchers performed such types of experiments and propsoed three-tier agent based framework by using agent techniques to reduce complexity of the system [9]. For cloud storage security, agent based techniques are also used in Cloud Computing to increase the reliability and peformance of the cloud storage [10]. Multilevel agent technology also uses in Cloud computing to increase security and privacy. Authors under reference [11] used protocols to increase reliable communication between two unreliable storage clouds. During symentic literature review, it is revealed that same agent based techniques can be used to redress the issues relates to threats and malicious attacks. Foregoing in view, the authors planned to club software agents techniques with threat management to proposed information security frameworks for Cloud computing.

2. Cloud Architecture

The system architecture has been suggested by NIST for cloud computing. Architectural model presents three deployment models listed below:

2.1 Private Cloud

In this model the user/organization can make its own infrastructure and manages it as well.

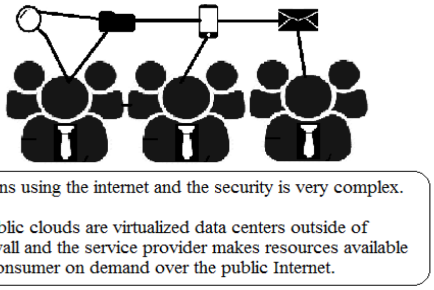


- Deployed in the company and security can be made easily.
- Virtualized cloud data centers inside firewall and its a private space dedicated to system within a cloud data center.
- Refers to internal data centers of a business or other organization not made available to the general public.

Fig. 1. Private Cloud

2.2 Public Cloud

The services are delivered to the client via the Internet from a third party service provider [2]. Services are available to general public over the internet. The Public Clouds are configured in a public data center, shared container services, non-guaranteed resources, variable cost for additional capacity, in secured shared network, No dedicated proactive support



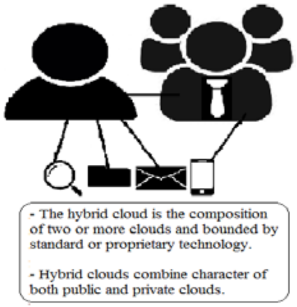
- Runs using the internet and the security is very complex.

- Public clouds are virtualized data centers outside of firewall and the service provider makes resources available to consumer on demand over the public Internet.

Fig. 2. Public Cloud

2.3 Hybrid Cloud

Hybrid Cloud is basically combination of above sated two cloud deployment models. In Hybrid model, you can purchase the use of a mix dedicated physical servers and virtual servers. Tailor mix to suit capacity and security requirements and it may still pay for unused resources [12].



- The hybrid cloud is the composition of two or more clouds and bounded by standard or proprietary technology.

- Hybrid clouds combine character of both public and private clouds.

Fig. 3. Hybrid Cloud

2.5 Software as a Service (SaaS)

It is a way to provide applications over the internet. The organizations do not required to purchase license, install, upgrade, and maintain applications in their own organizations. The customers simply access applications over the internet, feeling free from maintenance and its hardware management. Such types of services are also referred as web based software and hosted software. It always installed on the servers of the Cloud Service Providers and it is the sole responsibility of the Cloud Service providers to maintain software, keep it secure from threats, risks, vulnerabilities, make sure its 24/7 availability and increase performance.

2.6 Infrastructure as Service (IaaS)

It consists of Applications, Data, Runtime, Middleware and Operating System. Servers and Store are made available in a scale way over a network. For example EC2, Rackspace, CloudFile, OpenStack, CloudStack and OpenNebula.

2.7 Platform as Service (PaaS)

The PaaS is a cloud computing service model that offers a policy and environment for developers to create applications and services on the Internet. The PaaS services are available over the internet and users can access it via any one of the web browser.

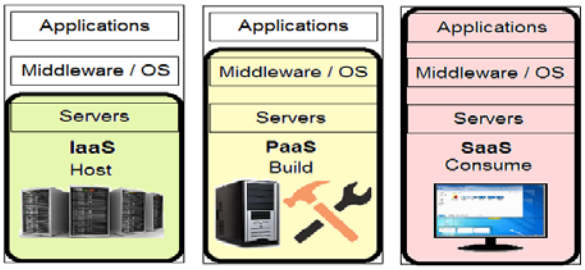


Fig. 4. Comparison of Service Models

Cloud demand for computer clouds is a daunting task for security patrons. The virtual environment must be protected so that all of them can provide flexible services to their customers [12]. Clouds have been undertaken in order to identify the security problems of the cloud. The most important security issues in cloud computing are loss of control, recovery, backup failures, loss of encryption keys, unauthorized access and attacks.

Many models uses different methods, including the inclusion of Agent. It is easy to use, light and portable program that can be used to extract security related information from other agents [13]. The agent based technology is also used to solve the cloud related issued like resource management, transfer of data from one cloud to another and solve service composition. The renowned Cloud Service Providers uses NIST, ISO / IEC 27000, FISMA, CSA, COBIT and others based upon their service and deployment model [14].

3. Software Agent

Software Agent (SA) is an advanced technique that could be opted in different security frameworks with unlike knowledge [15]. During the review of the literature it has been revealed that it is a new field and its acceptance will take time. The agent is an autonomous entity that has the ability to act in certain areas on a continuous basis. environment for his host to perform a specific task or a number of tasks. In addition, during the process of executive tasks, the intervention of his creator / host does not require [16] The software agents are very similar to real life agents who are experts in a particular field negotiating with their clients and the established interests of their hosts / organizations. [17] Software agents are programmed and require only specific and specific information to work in a given environment. [18] When the software The agent can observe information from their environment and make decisions based on the information collected, then it can be called Intelligent. Agent software agents are designed to act in a given environment and communicate with other agents to complete a specific task. [16] Various authors and researchers introduced a series of definitions of agent independence and interaction with other agents and demonstrated the ability of enthusiasm for the concept. The ability of these concepts means that the software agent is constantly working on the basis of the set of available actions, select the task base in its priority coordinates with other agents collecting information responses and make decisions in the best interests of the host without their involvement. [19] Agents are usually independent programs that can interact with the environment and act accordingly to achieve their tasks. The binding features of agents include autonomy, temporary continuity, decision-making, goals and mobility. These features are mainly for distributed computer models. In multi-agent distributed computers, they share very common features with other distributed systems. It is fundamental to realize that each agent has a certain number of attributes distinguishing it from another agent [16]

4. Agent in Cloud Computing

Software Agent is a very advance technique that uses applications uses complex information that is required to superior frameworks and mass storage. Along with these lines, Cloud computing gives flawless and perfect foundation as a result of its elite wide range of assets on an expanded scale and memory accessibility for operators to reach their chosen messages [20]. On the other hand the independent agents are used as part of Cloud computing for sharing asset and managing resources, organize resources and secure network [13].

Software Based Agents having intelligent characteristics are used in large scale data centers to maintain their extractable large data [21]. These agents could be used in data centers to monitor the services, provide access to legitimate users to cloud infrastructure, energy efficient as possible and develop strategies based on collected information. The most important benefits of agent based systems are:

1. Network load will be expressively reduced
2. The network delay is significantly reduced
3. The system becomes robust
4. Apply dynamically and fault tolerantly

In the event that the cloud and software agent work together, it can create imaginative outcomes. During literature survey, it has been observed that so far many scientists have not suggested the possibility of combination of these two innovations [21]. In the cloud computer we need to plan and implement system for familiarity with the dynamic behavior of Cloud computing. To address these above mentioned challenges, multi agent techniques can be used as they have heterogeneity and volatility [22]

5. Agents Based Information Security Framework

The most important block in the expansion of cloud are security and privacy restrictions. Although all distributors claim that they provide their customers with adequate security, several research were conducted to meet the security needs in cloud, but it remains a big challenge for organizations in the cloud. The risks and threats to security always directly diminish the critical, technical and organizational processes of an organization. During the review of the literature, it is noted that there are several information security frameworks that tried to redress the issues of Cloud Computing, but unfortunately none of the frameworks used Software and intelligent agents to redress the issues of information security.

In this document, we present software agents to build IS Framework and we used information security metrics techniques that are a valuable tool for measuring the performance of the information security system. These Information Security Metrics are used in the proposed framework to generate security threats through the use of threat modeling techniques. In addition, risk management techniques are used to identify and mitigate the risk. In order to provide IS to customers and distributors in the cloud, a six-level approach has been proposed, as shown in Fig. 5.

5.1 Threat Agent Identification Process

The purpose of Threat identification process is to determine what may have happened to cause a potential loss, and to obtain information on how, where and why the loss can occur [23]. Threats are also identified for future assessment. Threat identification stage often identify many threats scenarios some of which are worse than others. The evaluation team often confirms the specific scenarios for the monitoring process where the main outcome is the threat scenarios that assessment teams find realistic.

5.1.1 Identify Threat Source / Event

The best active threat identification technique focuses on the root problem which says organization why an incident occurs. The cause of the threat reveals the information about what causes the loss and where the organization is vulnerable [26]. It gives meaningful feedback to the root categories, what measures have to be taken to effectively reduce threats, determining the outcome or result based risk leads to ineffective mitigation measures. Discover potential impulses that can cause a threat event. One threat event may have a specific one cause or might be one threat have many cause.

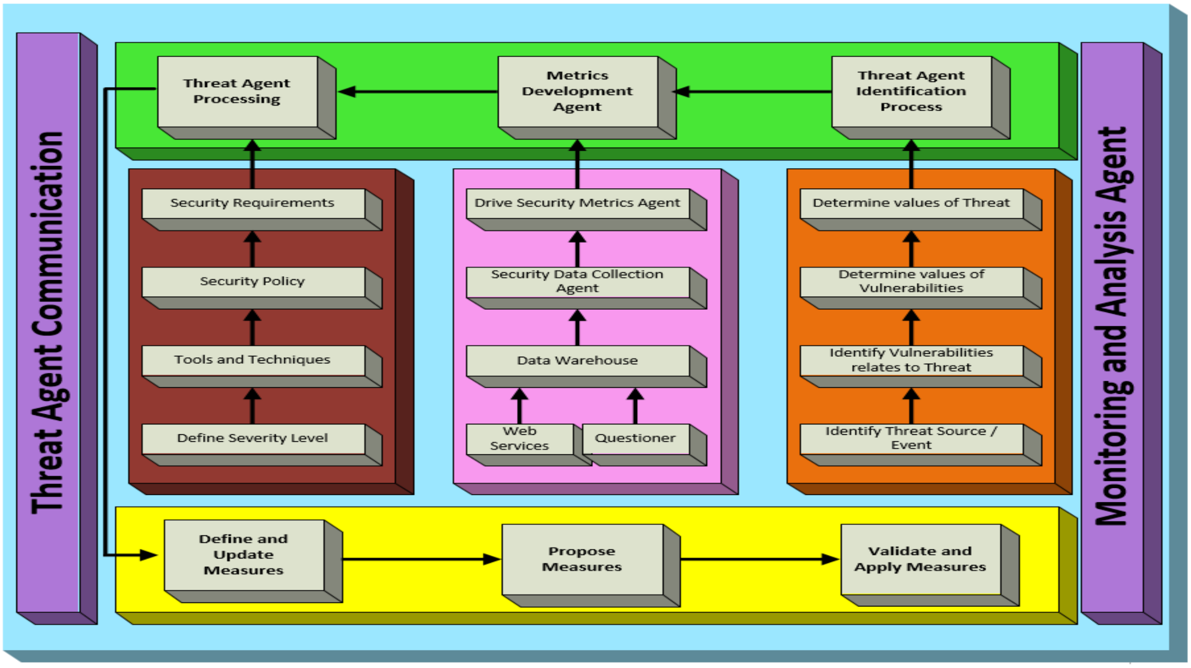

Threat Agent Communication
Threat Agent Processing
Metrics Development Agent
Threat Agent Identification Process
Security Requirements
Security Policy
Tools and Techniques
Define Severity Level
Drive Security Metrics Agent
Security Data Collection Agent
Data Warehouse
Web Services
Questioner
Determine values of Threat
Determine values of Vulnerabilities
Identify Vulnerabilities relates to Threat
Identify Threat Source / Event
Define and Update Measures
Propose Measures
Validate and Apply Measures
Monitoring and Analysis Agent

Fig. 5. Agent Based Information Security Threat Management Framework (ABISTMF)

5.1.2 Identify vulnerabilities relates to Threat

This second process is composed off to define all vulnerabilities in cloud computing environment and the second one identify particular vulnerabilities relates to threat identified in the first stage. This process will be very helpful to makes the decision to define the adequate corresponding measures protection and vulnerability value.

5.1.3 Determine values of Vulnerabilities

When potential threats have been identified vulnerability assessment should be undertaken. It assess the impact of loss after a successful attack and it also indicate the assets that were targeted. The impact of the loss is that the agency's mission hampers the successful attack on that particular threat. The key component of the vulnerability assessment limits the vulnerability and vulnerability assessment.

5.1.4 Determine values of Threat

The third step in a threat management is a threat assessment. A threat assessment considers the full spectrum of threats (i.e., natural, criminal, terrorist, accidental, etc.) for a given facility/location. The purpose of this layer is to determine how much loss will cloud organization face after successful threat attack against each Cloud Actor. This layer will be helpful in the decision making process of the framework wherein before implementing measures, we assess the cost of the measures and compared it with the threat values.

5.2 Metrics Development Agent

The key responsibility of the Metric Development Agent (MDA) is to build solid and useful Information Security (IS) Metrics. The process of Metrics development is based upon multi agent technique wherein other agent will facilitate the future development of the Metric Development Agent (MDA). The MDA is facilitated by 03 sub layers to formulate comprehensive metrics that facilitate organization in decision making.

5.2.1 Security Data Collection Agent

The Security Data Collection Agent (SDCA) is depends upon the inputs from Data Warehouse which further depends upon web services and Questionnaire to solicit requisite information.

5.2.2 Data Warehouse

Data Warehouse is basically a security log which store and maintain information security related data derived from different sources. This layer consist of two sub-layers i.e. Web services and Questioner to gather all requisite information.

5.2.2.1 Web Services

Web services are advanced way to collect data relates to information security from the internet but the collected data must be meaningful to store in Data warehouse. In order to make collected information more accurate and valuable data, it must be linked to Key Indicators KPIs, existing Information Security Guidelines, Frameworks, Standards and advanced metrics [24]. Security Information Management SIM is an excellent source and tool for collecting information security information from different Web sites and preparing reports for future research. The collected data must be merged, standardized and link with each other.

5.2.2.2 Questioner

The questionnaire is a method used by the information security agent. SANs has issued checklists for internal and external audits of the organization and it may also be used to obtain any of the Key Point Indicators (KPI) [24].

5.2.3 Drive Security Metrics Agent

The output of the Security Data Collection Agent will act as input of the Drive Security Metrics Agent. The purpose of the layer is to develop further metrics that measure the effectives of the implemented Security controls derived from the security standards.

5.3 Threat Agent Processing

The outcomes of the previous sections that are Threat Agent Identification and Metrics Development Agent is the input of this layer This layer is comprising of multi agent techniques that interact with other agents share data with each other and work together to accomplish a task This layer is very important and requires full attention of the organization to solve the threat agent.

5.3.1 Define Severity Level

This is continuous process wherein layer defined severity level of each identified threat and also on the base of the preliminary analysis of the threat. The severity level is always gauged in terms of high, moderate, low and insignificant against likelihood of occurrence that is frequent, probable, occasional, remote and improbable. This layer also defines that which threat is required to be mitigated immediately, as soon as possible, within reasonable time and management review has required.

5.3.2 Tools and Techniques

Analytical tools and techniques used to implement security policies against each threat agent, these provides sufficient solutions against threat agents. We may use various websites newsgroups forums and research docs to generate the most important tools. Although not all the devices and techniques used for the cloud are the same but in this section the proposed framework will find the most appropriate and acceptable tools for the mitigation of the threats. For example HyTrust Virtual Machine and CohesiveFT.

5.3.3 Security Policy

Once you have secured the security obligations, it is important to establish a security policy. Each security policy will be based on mitigation techniques against each threat agent and also relied upon security tools and techniques also must be taken into consideration while framing security policy. Policies must be precise, clear and applicable to mitigate the threat.

5.3.4 Security Requirements

To reduce the potential dangers you must determine the threat agent's safety goals and security requirements. Before defining security requirements against each threat agent, organization have to consider severity level of the threat and policy defined to mitigate the risk. One threat might be requires certain requirements or might be based on one requirement but whatever the case is, security requirements must be precise and clear. Cloud Security Alliance (CSA) has introduced Cloud Control Metrics V3.01 which introduced controls and requirements against each threat / risk [25].

5.4 Define and update Measures

The major functionalities of 4th layer is to define measures against each threat. The first step in this layer is to define measure against each threat agent and asset. There are various techniques to design measures which may be taken into consideration. If the measure is already available against threat agent then it is required to be reexamined to check whether measure is completely capable to remove the threat or it has partial capabilities and again if the measure has not complete capability then it requires to be redesign to make it full capable to remove the threat. The newly design measure is also required to be updated in the existing measures database to use it in future.

5.5 Propose Measures

The 5th layer is about to propose measures against each threat agent and cloud actor. One measure may be used to solve multiple threats and one threat may be solved by multiple measures. So identifying suitable measure or a set of measures is a tricky and critical task.

5.6 Validate and Apply measures

Before applying measures, it is mandatory for the organizations to validate the measures. Without validating measures either may not mitigate the threat or partially mitigate. Therefore, for effective threat agent mitigation, validation is the measures is required before implementation.

5.7 Threat Agent Communication

The second last step in threat management is to communicate the assessment results and share threat related information. The main purpose of this step is to make sure that all the decision makers of the organization have identified threat and its associated measures related information for their future requirement. Cloud organizations may communicate threat assessment results to other stakeholders in a variety of ways. Such communication may be formal or informal.

5.8 Monitoring and Analysis Agent

After successful implementation of treatment and communication of threat agent, it is necessary to initiate continuous monitoring program. Under this program, all treat assessment activities are reexamined and if there is a need to change or update in framework then immediately take necessary measures to make framework more accurate. Every organization have to revisit their threat agent mitigation activities on regular basis described in the threat management framework and update currently security requirements, policies, tools and techniques and measures accordingly.

6. Evaluation of Framework

Fuzzy Logic is a method for the handling of data that is inaccurate and inexact. Fuzzy Logic is a powerful design philosophy that describes and develops control systems that provide designers with simple and intuitive methods for implementing complex systems.

Imprecise
Inaccurate
Fuzzy Logic System
Decisi

Fig.6. Fuzzy Logic System

Fuzzy logic system can be modeled with less number of data of even without data. Fuzzy Logic Technique has many advantages over other software. One of them is less dependable in previous values. Fuzzy Logic Controller and its applications: Fuzzy Controllers classical as different to other classical controllers, have the capability to utilize the knowledge solicited from human decision. Inaccurate data and unclear statements are used as inputs to the fuzzy logic system which resultantly produced decision values on outputs. The Fuzzy model gives you the output against corresponding inputs. The Fuzzy model is shown in **Fig. 7**, with four main modules. The first module, fuzzification, accepts crisp values from the users and converts them into fuzzy values. Based on the knowledge base, fuzzy values are obtained, processed using inference engine, processed the data and transformed into crisp values by Defuzzification.

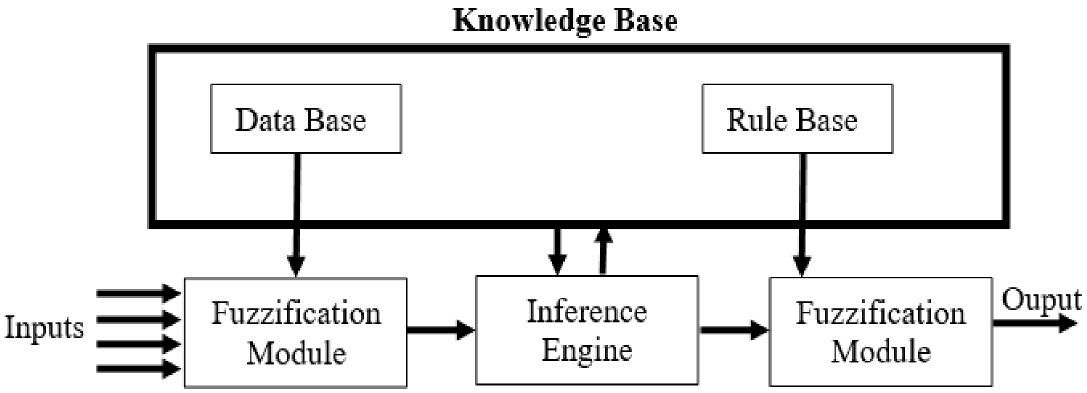


Fig.7. Fuzzy Model

For the implementation of fuzzy logic consists of many different fuzzy sets. The values of membership functions are always lies between 0 and 1. Fuzzy logic has eleven membership functions that are available in MATLAB®. To evaluate proposed framework, we have considered only 3 Membership functions i.e. Triangular, Trapezoidal and Gaussian.

To evaluate Proposed framework for threat management, a fuzzy inference system is required to be design based upon fuzzy set theory. In first instance, we had set input and output variables which are shown in **Fig. 8**. The second step was to collect data for the input variables. Every input variable has further feeding input variables as given in **Fig. 5** but in this fuzzy model we are not going towards cascading.

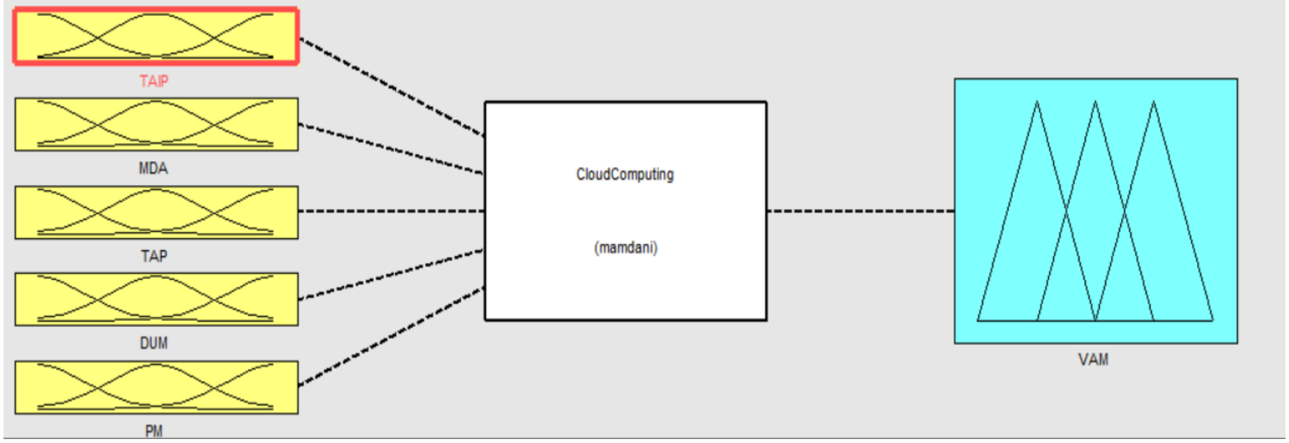


Fig. 9. Fuzzy Logic Controller using fuzzy based logic inference system editor for cloud system.

There are three membership functions against each input. The model has one output i.e. Validate and Apply Measure. Output VAM has also comprised of three membership functions. **Fig.9** depicts selected input and output variables. The ranges of membership functions are taken as 0 to 10 for each input.

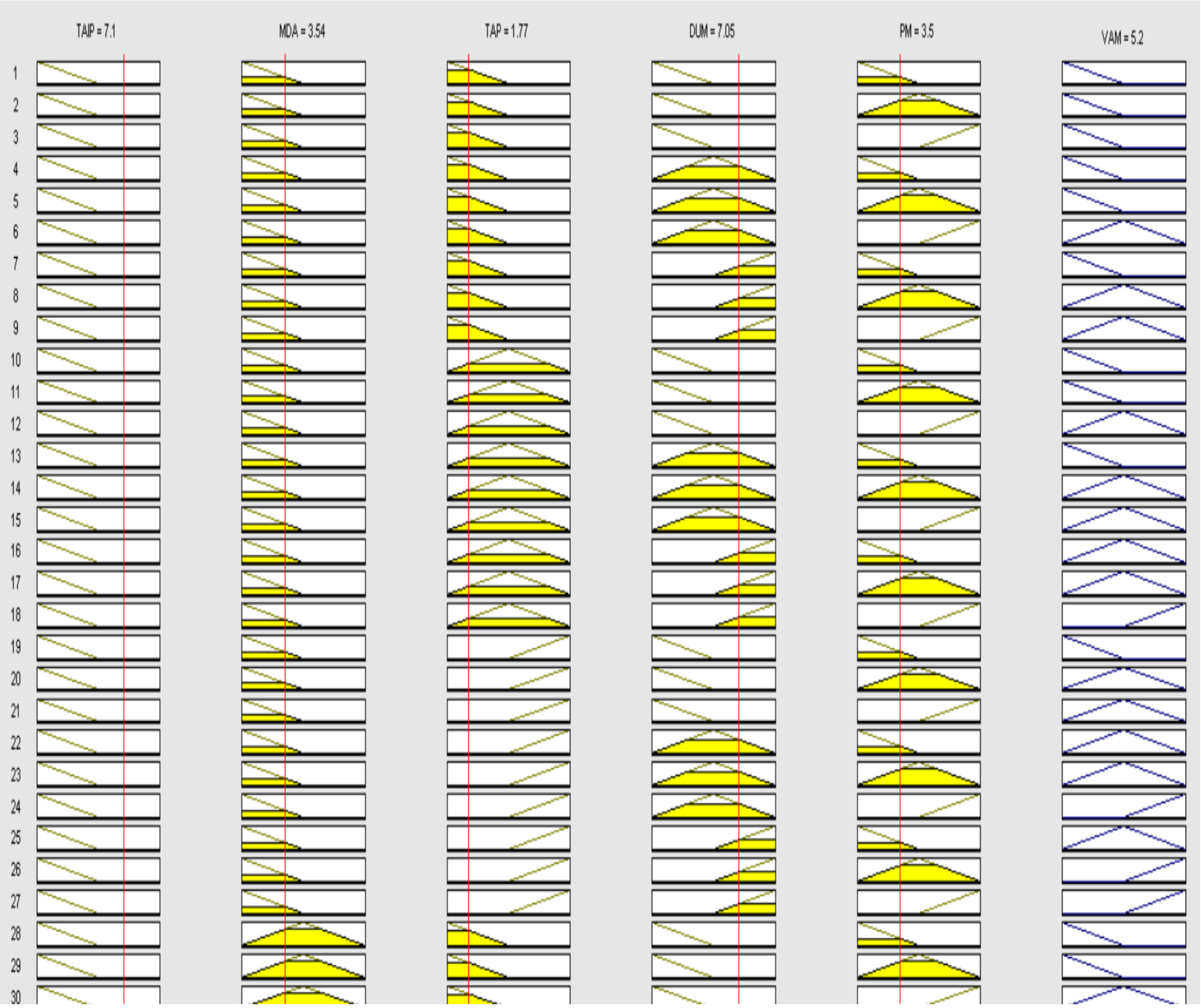


Fig. 10. MATLAB Rule view

Here the 3D graphs of surface viewer for the TAIP, MDA, TAP, DUP, MP and output Validate and Apply Measure (VAM) are presented in the **Fig. 11** (a, b, c, d, e, f, g, i and j). **Fig. 11(a)** shows the dependency of output decision on MDA and TAP. **Fig. 11(b)** shows the dependency of output decision on TAIP and TAP. **Fig. 11(c)** shows the dependency of output decision on DUP and TAP. **Fig. 11(d)** shows the dependency of the output decision on the TAP and the MP. **Fig. 11(e)** shows the dependency of output decision on TAP and MDA. **Fig. 11(f)** shows the dependency of output decision on DUP and MDA. **Fig. 11(g)** shows the dependency of output decision on MDA and PM. **Fig. 11(h)** shows the dependency of output decision on TAP and DUM. **Fig. 11(i)** shows the dependency of output decision on TAP and PM and **Fig. 11(j)** shows the dependency of output decision on DUM and PM.

A user was intended to validate and apply measure on the identified threat. Therefore, output Validate and Apply Measure was taken on the values of TAIP = 7.1, MDA = 3.54, TAP = 1.77, DUP=7.05, PM = 3.5 and according to Mamdani's model output was obtained 5.2. We found that Mamdani's model is interesting, appropriate and useful for crisp values of Fuzzy Logic system. The results obtained through MATLAB ® for Mamdani's model are given in **Table 1.**

With the great precision and greater output performance, Fuzzy Logic based Threat Management Framework for cloud computing established satisfactory. The dynamic and complex system has been successfully analyzed, developed and solved. The rules formulated to get output decision are found correct. Therefore, the proposed framework for threat agent mitigation has confirmed with the precise values of all the inputs.

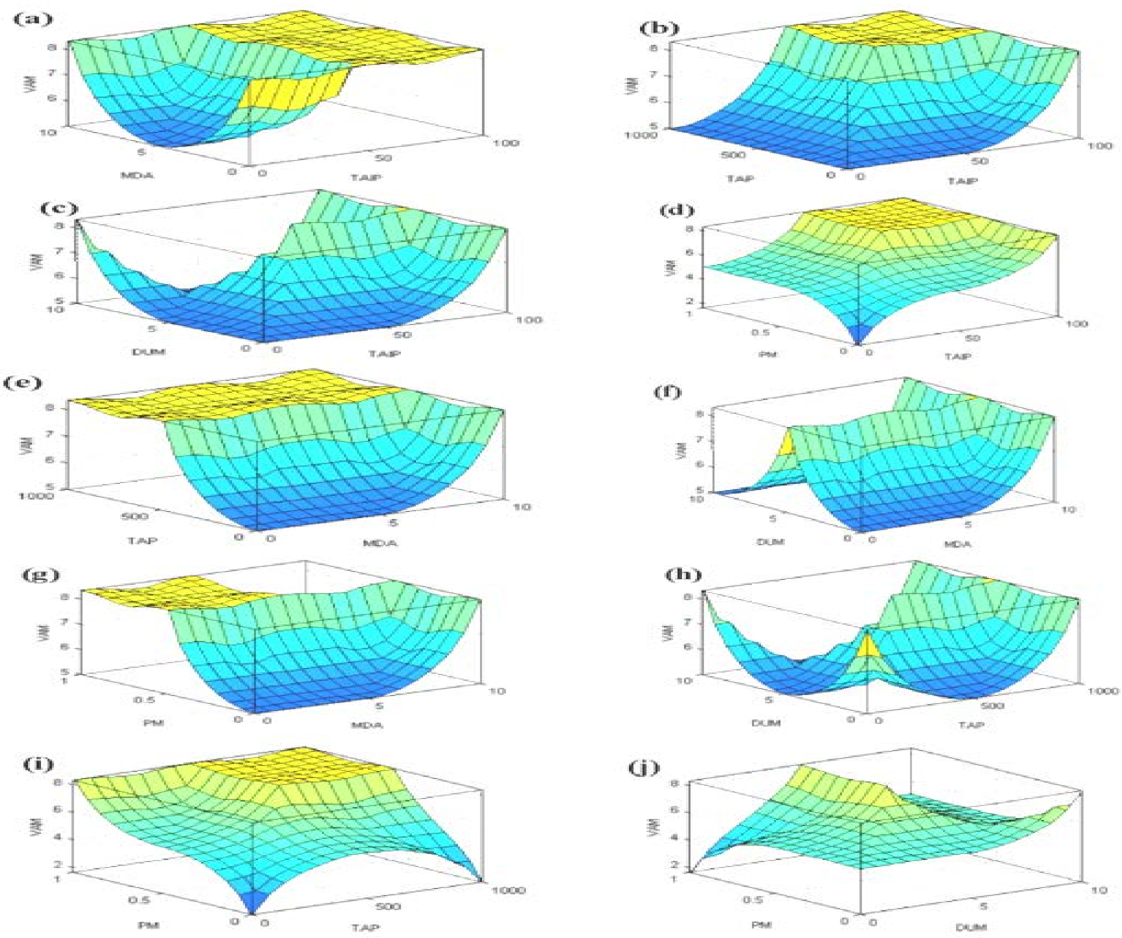


Fig. 11. 3D Graphs of Sample Solution

Table 1. Result Comparison

Category	Decision
Mamdani’s value	7.45
MATLAB simulation	7.48
Difference	0.03
Error percentage	0.54%

After simulation and applying Mamdani model, we observed very insignificant difference in the designed and simulated values i.e. just 0.54%. It confirms that that our proposed Agent based Information Security Threat Management Framework could be used to successfully apply measures to mitigate security threats.

6. Conclusion

The cloud computing architecture in which scalable and virtualized resources are provided over the Internet. The acceptance of cloud computing becomes vulnerable by the appearance of security problems. Therefore, we are interested to target cloud related threats in this paper. In order to accomplish our goal, we have developed six layered approach for framing information security framework by introducing software and intelligent agent problem solving techniques. During systematic literature review, we studied various risk management, threat management and vulnerabilities management related techniques and even studied literature relates to agents in information technology and after considering their pros and cons, we developed threat management framework wherein information security metrics, threat elicitation, threat assessment, threat evaluation, security policy, threat mitigation tools and techniques and measures were taken into consideration. After implementation of proposed framework, organizations will be able to use agent techniques from threat agent identification to threat agent mitigation.

Although, proposed Agent Based Information Security Threat Management Framework (ABISTMF) is expected to redress security issues relates to Information Security threats, but even then we don’t claim that users, who will use ABISTMF, would not undergo any attack thereafter. The aims and objectives of the proposed framework (ABISTMF) is to reduce level of damages from the threat agent.

Even though, we faced many different types of constraints in the development and testing of proposed framework, even then we have planned to develop algorithm for simulation of agents. We also intended to implement proposed framework in real time, create various scenarios to check validity and reliability of proposed framework and extend proposed framework if we feel requirements to ensure more security.

We hoped that our research will open new dimensions for researchers and cloud organizations to enhance security of their security system.

References

[1] A. Sajid, H. Abbas, and K. Saleem, "Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges," IEEE Access, vol. 4, pp. 1375–1384, 2016.

[2] R. Sharma and R. K. Trivedi, "Literature review: Cloud Computing –Security Issues, Solution and Technologies," International Journal of Engineering Research, vol. 3, no. 4, pp. 221–225, Jan. 2014.

[3] P. Samarati and S. D. C. D. Vimercati, "Cloud Security," Encyclopedia of Cloud Computing, pp. 205–219, 2016.

[4] V. Chang, Y.-H. Kuo, and M. Ramachandran, "Cloud computing adoption framework: A security framework for business clouds," Future Generation Computer Systems, vol. 57, pp. 24–41, 2016.

[5] A. Boukerche and Y. Ren, "A trust-based security system for ubiquitous and pervasive computing environments," Computer Communications, vol. 31, no. 18, pp. 4343–4351, 2008.

[6] V. Arora and S. Tyagi, "Analysis of Symmetric Searchable Encryption and Data Retrieval in Cloud Computing," International Journal of Computer Applications, vol. 127, no. 12, pp. 46–51, 2015.

[7] M. R. Islam and M. Habiba, "Agent based framework for providing security to data storage in cloud," 15th International Conference on Computer and Information Technology (ICCIT), 2012, pp. 441–451.

[8] A. Mehmood, H. Song, and J. Lloret, "Multi-Agent based Framework for Secure and Reliable Communication among Open Clouds," Network Protocols and Algorithms, vol. 6, no. 4, p. 60, 2014.

[9] M. Kuo, "An intelligent agent-based collaborative information security framework," Expert Systems with Applications, vol. 32, no. 2, pp. 585–598, 2007.

[10] A. M. Talib, R. Atan, R. Abdullah, and M. A. A. Murad, "Towards a Comprehensive Security Framework of Cloud Data Storage Based on Multi Agent System Architecture," Journal of Information Security, vol. 03, no. 04, pp. 295–306, 2012.

[11] S. Khatua, N. Mukherjee, and N. Chaki, "A new agent based security framework for collaborative cloud environment," in Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research - CSIIRW 11, 2011.

[12] M. R. Islam and M. Habiba, "Agent based framework for providing security to data storage in cloud," in 15th International Conference on Computer and Information Technology (ICCIT), 2012.

[13] M. I. Tariq, "Towards Information Security Metrics Framework for Cloud Computing," International Journal of Cloud Computing and Services Science (IJ-CLOSER), vol. 1, no. 4, 2012.

[14] M. I. Tariq and V. Santarcangelo, "Analysis of ISO 27001:2013 Controls Effectiveness for Cloud Computing," in Proceedings of the 2nd International Conference on Information Systems Security and Privacy, 2016, pp. 201–208.

[15] A. Boukerche and Y. Ren, "A trust-based security system for ubiquitous and pervasive computing environments," Computer Communications, vol. 31, no. 18, pp. 4343–4351, 2008.

[16] D. Talia, "Clouds Meet Agents: Toward Intelligent Cloud Services," IEEE Internet Computing, vol. 16, no. 2, pp. 78–81, 2012.

[17] A. M. Talib and N. E. M. Elshaiekh, "Multi Agent System-Based on Case Based Reasoning for Cloud Computing System," Academic Platform Journal of Engineering and Science, vol. 2, no. 2, pp. 34–38, 2014.

[18] V. Rybakov, "Multi-agent Non-linear Temporal Logic with Embodied Agent Describing Uncertainty," Advances in Intelligent Systems and Computing Agent and Multi-Agent Systems: Technologies and Applications, pp. 87–96, 2014.

[19] M. Hafiz, P. Adamczyk, and R. E. Johnson, "Organizing Security Patterns," IEEE Software, vol. 24, no. 4, pp. 52–60, 2007.

[20] J. Yang, J. Wang, H. Wang, and D. Yang, "Agent-based provable data possession scheme for mobile cloud computing," Journal of Computer Applications, vol. 33, no. 3, pp. 743–747, 2013.

[21] I. Lopez-Rodriguez and M. Hernandez-Tejera, "Software Agents as Cloud Computing Services," Advances in Intelligent and Soft Computing Advances on Practical Applications of Agents and Multiagent Systems, pp. 271–276, 2011.

[22] R. Aversa, B. D. Martino, M. Rak, and S. Venticinque, "Cloud Agency: A Mobile Agent Based Cloud System," International Conference on Complex, Intelligent and Software Intensive Systems, 2010.

[23] F. Masmoudi, M. Loulou, and A. H. Kacem, "Formal Security Framework for Agent Based Cloud Systems," International Workshop on Advanced Information Systems for Enterprises, 2014.

[24] S. N. Foley and W. M. Fitzgerald, "Management of security policy configuration using a Semantic Threat Graph approach," Journal of Computer Security, vol. 19, no. 3, pp. 567–605, 2011.

[25] X. H. Le, S. Lee, P. Truc, L. T. Vinh, A. Khattak, M. Han, D. V. Hung, M. Hassan, M. Kim, K.-H. Koo, Y.-K. Lee, and E.-N. Huh, "Secured WSN-integrated cloud computing for u-Life Care," 2010 7th IEEE Consumer Communications and Networking Conference, 2010.

[26] R. Derr, "Threat Identification and Rating," Threat Assessment and Risk Analysis, pp. 37–54, 2016.