IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact Factor: 6.078

(Volume 7, Issue 3 - V7I3-1157)

Available online at: https://www.ijariit.com

The intelligent agent-based information security model for cloud

Milind Deshkar
deshkar.miliind@gmail.com
Department of CEA,
GLA University, Mathura, Uttar Pradesh

Dr. Manoj Kumar
manoj.kumar@gla.ac.in
Department of CEA,
GLA University, Mathura, Uttar Pradesh

ABSTRACT

Today's era is the era of cloud computing and agent-based processing. Data security and integrity are achieved by information security systems, which ensure the continuity of business and protect organizations against potential risks. Information security systems are used to estimate the risks and search the place of the occurrence of the risks. It should also be able to measure the risk consequences associated with cloud organizations. The cloud organizations must analyse the information system processes and they should develop their own information systems based on the analysis. This paper proposes a comprehensive Agent-Based Information Security framework for Cloud Computing. We have considered risk assessment methods for calculating consequences by focussing on potential threats, assets, vulnerabilities, and their associated measures. A decision system for the organizations is created by taking the help of intelligent (smart) and software agents that are used to fetch and group the relevant information used in a framework that decides against threats based on information provided by the security agents. We have used a fuzzy inference system based upon fuzzy set theory for creating a decision system.

Keywords— *Information security, Risk Management, Agent-based Computing, Multi-agent systems, Cloud Computing, Grid computing, Fuzzy logic, Fuzzy set theory.*

1. INTRODUCTION

Cloud computing is an internet-based on-demand service that uses a shared computer resource environment. The resources are provided as services to the users. The cloud computing environment can and in case of increased load, the system can increase the capacity by adding more hardware.

Cloud computing is an internet-based on-demand service that uses a shared computer resource environment. he resources are provided as services to Security concerns have been the primary obstacle for organizations considering cloud services, particularly public cloud services. The security and privacy issues are always misused by the agents of threat. Hence vulnerability is a major risk factor. The interaction between various complex entities like Cloud Service Providers / Venders, Cloud Consumers and the brokers governs the streamlined services of cloud computing[2].

In the recent past, a new novel method of handling security threats has arisen which is known as Agent-based security measures. These measures are used to provide the highest level of security to the cloud computing processes. The proposed agent-based schema will surely increase the security of the Cloud without affecting the system's overall performance. For example, the Authors adopt multi-agent-based techniques and a privacy assurance framework that uses comprehensive cryptographic techniques against security threats like Denial of Service (DOS) [3]. The multi- agent-based framework secures reliable communication between open Clouds networks. The test results show that performance-enhanced after the implementation of the agent. A multi-tier agent-based framework can increase the abilities of agents to minimize the complexity of the system [4]. The agent-based approach also used to provide security to Cloud networks, infrastructure, and storage [5]. After checking reviews, it is revealed that agent-based techniques do not use risk management techniques to offer defense against malicious attacks and threats. Therefore, the authors merged software agent techniques with risk management techniques to propose information security schema for Cloud Computing.

2. CLOUD COMPUTING

The term Cloud is a web-based system. Cloud is something, which is present at remote location, and provides the services over some public and private networks. Since the information can be found and accessed remotely in the virtual space, the name given to is Cloud computing. It offers various services like hardware, software, firmware and interfaces like OS and applications online. The data stored can be accessed through Internet. This system of data processing and access provides mobility due to which the work can be performed remotely and the processes can be executed on any devices, anywhere in the world. The Cloud Computing is making our business applications mobile and collaborative, by offering platform independency. All the basic and advanced applications such as e-mail, web conferencing, customer relationship management (CRM) can be executed on cloud.

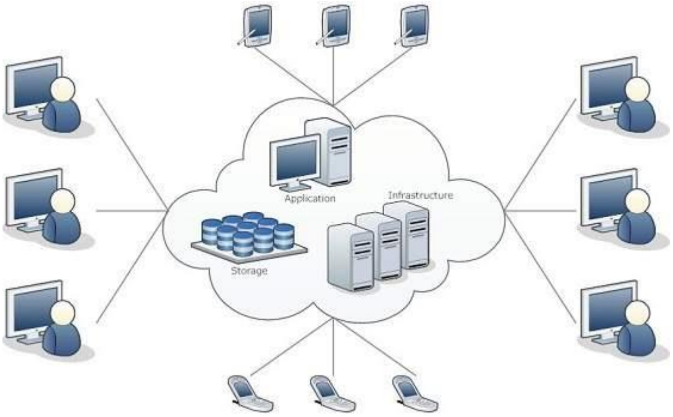


Fig. 1. Cloud Computing

2.1 CLOUD ARCHITECTURE

Various cloud components are joined to create Cloud Computing architecture, which are loosely coupled. The cloud architecture comprises of:

- Front End
- Back End

Both are connected through a network.

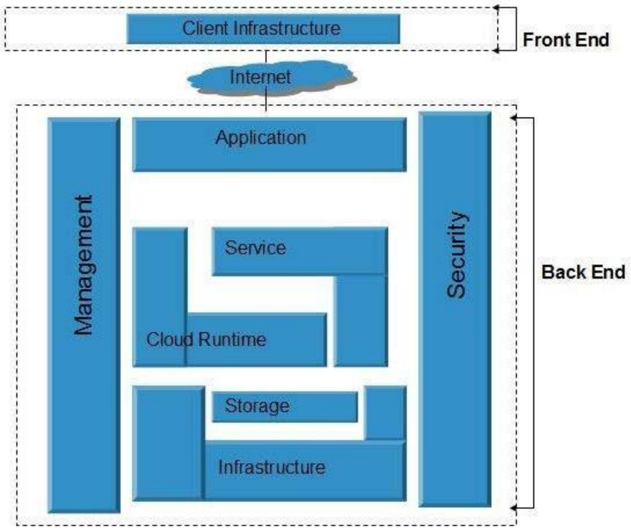


Fig. 2. Cloud Computing Architecture

Front End- It is the client part of cloud computing system. It consists of interfaces and applications that are required to access the cloud computing platforms, Example - Web Browser.

Back End- It is the cloud itself, which consists of all the resources required to provide cloud computing services. It comprises of hardware like data storage, virtual machines, servers, and software like security mechanism, services, deployment models, etc. The middleware is used to provide an interface between hardware, software and client's devices.

For making the cloud computing feasible and accessible to end users, certain models and services work in the background. The most mandatory are:

- Deployment Models
- Service Models

2.1.1 Mandatory cloud computing characteristics

- *On-demand self-service:* Automatic computing capabilities as and when needed without human interaction.
- *Broad network access:* Facilities and capabilities are available over the web and can be accessed through heterogeneous thin or thick client platforms.
- *Resources pooling:* The resources are assigned dynamically on-demand using a multi-tenant model of service providers.
- *Rapid elasticity:* Scaling is rapid depending on the demands of the customers.
- *Measured service:* The services are metered automatically to get control and optimize resources.

2.2 Deployment Models

NIST has suggested following four deployment models based on the business needs of the customers:

(a) Public Cloud
(b) Private Cloud
(c) Community Cloud
(d) Hybrid Cloud

2.2.1 Public Cloud

It handles B2C (Business to Consumer) type interactions. Here the computing resource is owned, governed and operated by government, an academic or business organization.

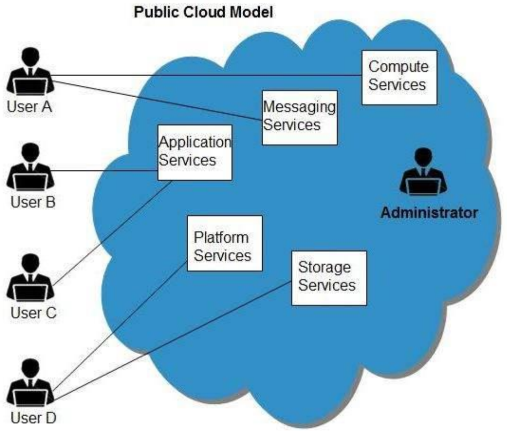


Fig. 3. Public Cloud

2.2.2 Private Cloud

It handles B2B (Business to Business) type interactions. It is deployed for one particular organization. This type of cloud is used to handle interactions between various departments of an organization. The computing resources is governed, owned and operated by the same organization.

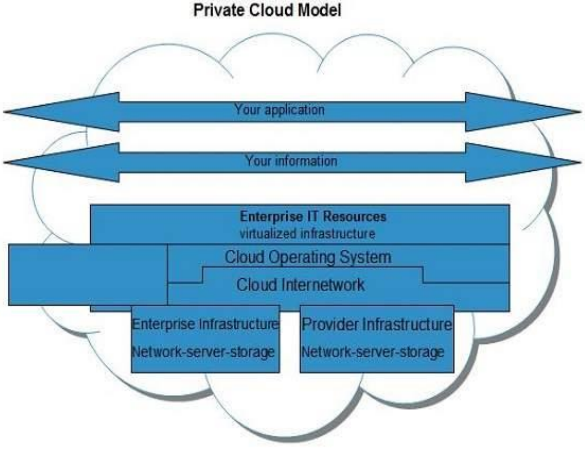


Fig. 4. Private Cloud

2.2.3 Community Cloud

It manages computing resources for a community and organizations.

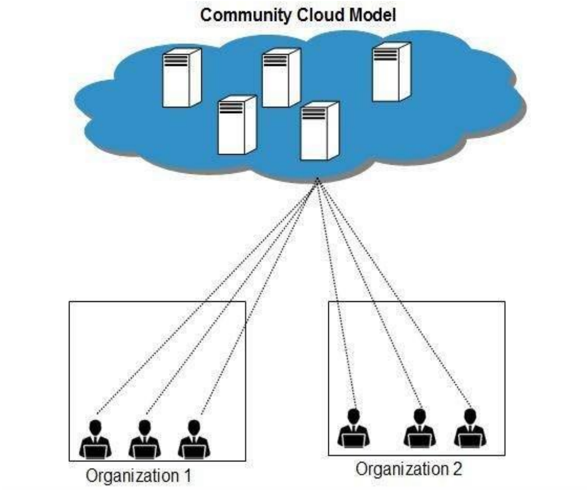


Fig. 4. Community Cloud

2.2.4 Hybrid Cloud

Since it can handle both B2B (Business to Business) and B2C (Business to Consumer), hence the name.

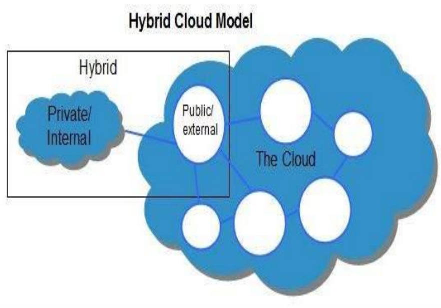


Fig. 6. Hybrid Cloud

2.3 Service Models

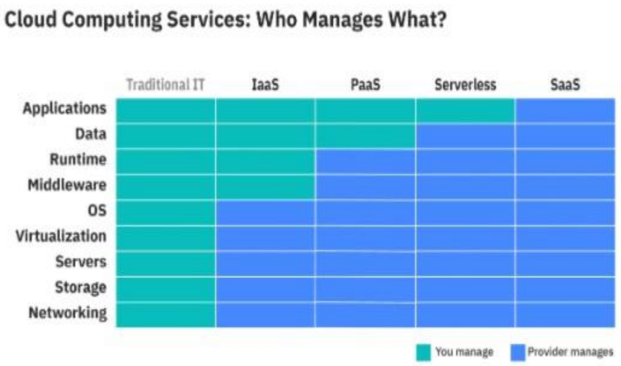
Some of the services provided by cloud computing are:

- Email
- Storage, backup, and data retrieval
- Developing and testing apps
- Analysing data
- Audio and video streaming
- Delivering software on demand

These services are grouped into following three major cloud computing service models:

(a) Infrastructure as a Service (IaaS)
(b) Platform as a Service (PaaS)
(c) Software as a Service (SaaS)

Different business use some or all of these components according to their requirement.



Cloud Computing Services: Who Manages What?

	Traditional IT	IaaS	PaaS	Serverless	SaaS
Applications	🟩	🟩	🟩	🟩	🟦
Data	🟩	🟩	🟩	🟦	🟦
Runtime	🟩	🟩	🟦	🟦	🟦
Middleware	🟩	🟩	🟦	🟦	🟦
OS	🟩	🟦	🟦	🟦	🟦
Virtualization	🟩	🟦	🟦	🟦	🟦
Servers	🟩	🟦	🟦	🟦	🟦
Storage	🟩	🟦	🟦	🟦	🟦
Networking	🟩	🟦	🟦	🟦	🟦

🟩 You manage 🟦 Provider manages

Fig. 7. Cloud Computing Services

2.3.1 Infrastructure As A Service

IAAS provides access to hardware resources such as physical and virtual machines, virtual storage, etc. These resources are made available to the customers by **server virtualization.** It offers Virtual machine disk storage and VLANs, Load balancers, IP addresses and Software bundles.

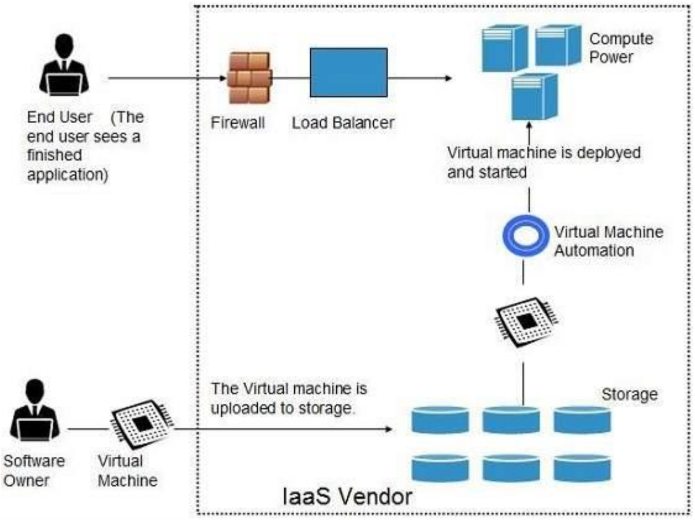

End User (The end user sees a finished application)
Firewall
Load Balancer
Compute Power
Virtual machine is deployed and started
Virtual Machine Automation
The Virtual machine is uploaded to storage.
Storage
Software Owner
Virtual Machine
IaaS Vendor

Fig 8. Infrastructure as a Service

Example of IaaS: Digital Ocean, Linode, Amazon Web Services (AWS), Microsoft Azure, Google Compute Engine (GCE), Rackspace, and Cisco Metacloud.

2.3.2 Platform As A Service

PAAS offers the runtime environment for applications. It also offers languages and tools for application development and deployment. PaaS has **drag-and-drop** tools that enables non-developers to create web applications.

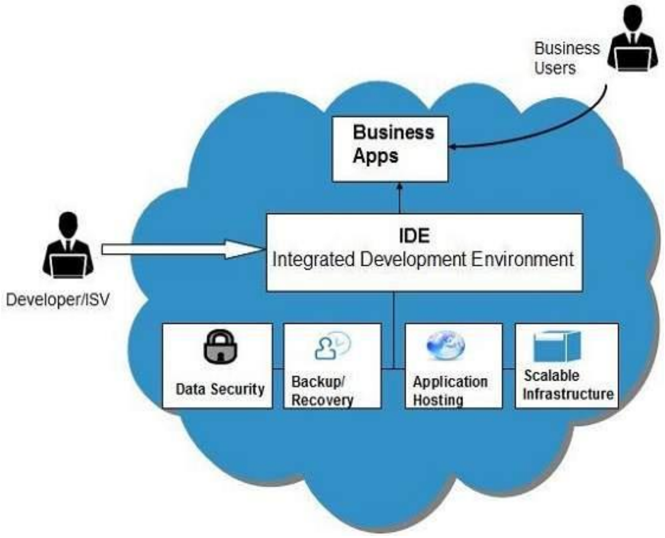


Fig. 9. Platform as a Service

Example of PaaS: AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, Magento Commerce Cloud, and OpenShift.

2.3.3 Software As A Service

SAAS provides the end users with **Application Programming Interface (API),** which allows to develop a customized application software application as a service. It refers to a software that is deployed on a host service and is accessible via web.

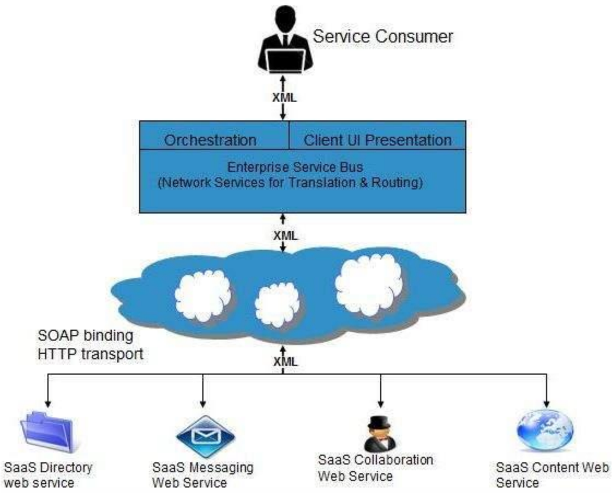
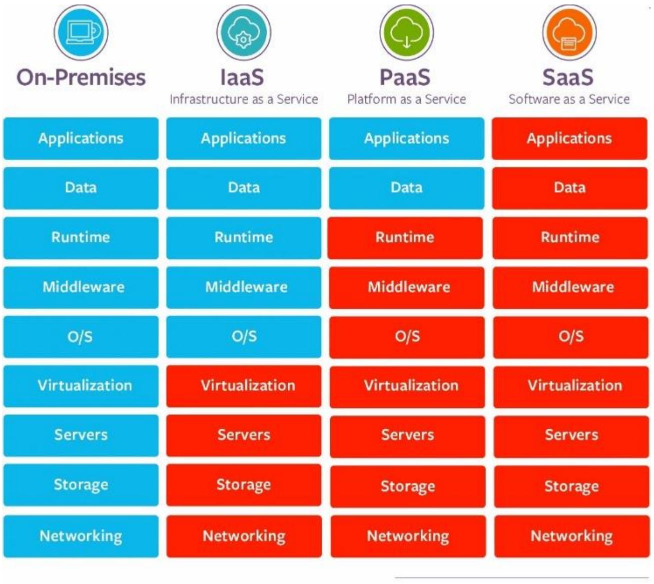


Fig. 10. Software as a Service

Example of SaaS: BigCommerce, Google Apps, Cisco WebEx, Salesforce, Dropbox, ZenDesk, ZenDesk, Slack, and GoToMeeting.



On-Premises	IaaS Infrastructure as a Service	PaaS Platform as a Service	SaaS Software as a Service
🟦 Applications	🟦 Applications	🟦 Applications	🟥 Applications
🟦 Data	🟦 Data	🟦 Data	🟥 Data
🟦 Runtime	🟦 Runtime	🟥 Runtime	🟥 Runtime
🟦 Middleware	🟦 Middleware	🟥 Middleware	🟥 Middleware
🟦 O/S	🟦 O/S	🟥 O/S	🟥 O/S
🟦 Virtualization	🟥 Virtualization	🟥 Virtualization	🟥 Virtualization
🟦 Servers	🟥 Servers	🟥 Servers	🟥 Servers
🟦 Storage	🟥 Storage	🟥 Storage	🟥 Storage
🟦 Networking	🟥 Networking	🟥 Networking	🟥 Networking

Fig. 11. Responsibilities of Cloud Service Models

3. SOFTWARE AGENT

Software Agent is a novel technique that can be used in different fields with different knowledge domains. The agent is an autonomous entity that can accomplish a specific task or number of tasks that are assigned to it. Furthermore, no external intervention is needed during the task accomplishment process [6].

Software Agents are very much like real stake holders that are expert in a particular field, that negotiate with their customer and secure the interests of their hosts/organization [7]. The software agents are programmed according to certain environments to communicate with other agents to complete a specific task and they require only specific and particular information. When the Software Agent is able to identify information from its environment and if it takes decisions on the basis of collected information then it can be called an Intelligent Agent.

Agent is normally independent program, which interacts with environment and act upon it accordingly to achieve its tasks. The binding properties of Agents are Autonomy, Temporal Continuity, Decision Making, Goal Oriented and Mobility. The above said qualities are mostly for distributed computing models. In fact, in distributed computing, multi-agent share many common features with other distributed systems. It is paramount to add that every agent possess certain number of properties that distinct it from other agent [6].

4. AGENT IN CLOUD COMPUTING

Software Agent is a novel technique that requires mass storage and high-performance systems to handle complex data/information. Cloud computing resources uses high performance systems and fast memory access methods to handle different resources at a large scale and thus provides ideal infrastructure to agents to accomplish their assigned tasks.In Cloud Computing discovery and composition of services, resource sharing, and authentication is performed by autonomous agents. The agents in Cloud Computing work autonomously and thus improves the security, privacy, resource management, discovery of new services, storage management, processing management and negotiation with venders [8].

These autonomous intelligent agents are used in large-scale data centers to manage and control the huge extracted data and are used to develop strategies based on collected information, monitor the services, grant access to authenticated users, and make Cloud infrastructure more energy efficient. The main advantages of the agent-based systems in cloud computing are:

1.The network load is reduced significantly.
2.The network latency is reduced greatly.
3.The system becomes robust and fault tolerant.

If we combine the technologies associated with Cloud Computing and software agents together then it may produce innovative and encouraging results. In Cloud Computing, we have to plan and implement a system for familiarization with the dynamic behavior of Cloud Computing environment. For this to work, intelligent multi-agent techniques can be used, which can take decisions dynamically without the intervention of any human resources. Hence, for effective Information Security Framework for Cloud Computing, agent-based models can be used.

5. ESSENTIAL PARTS OF INFORMATION SECURITY RISK ASSESSMENT PROCESS

Following are the two methods for performing risk assessments:

1. Quantitative
2. Qualitative

There are four parts that must be understood before performing the Information Security Risk Assessment process.

5.1 Threats

Threats can be posed to an organization by a variety of bad actors. In a cybersecurity context, bad actors can range from nation states, organized criminal syndicates, random hackers, hacktivists, business competitors, insiders, and more.

5.2 Vulnerabilities

Vulnerabilities on any network can be exploited, which provides the means or capability to a threat actor to achieve whatever bad thing they have in mind. Some of possible vulnerabilities, includes:

- Software vulnerabilities.
- Hardware vulnerabilities.
- Virtualization vulnerabilities.
- Vulnerabilities in the supply chain.
- Weaknesses in your hiring, training process.

5.3 Consequences

The list of consequences an organization could face without the proper information security risk assessment methodology in place can range from small annoyances to potentially catastrophic events. The ISRA team must consider the following:

- How do we value the data, systems, or assets that an organization owns?
- What proprietary information about or from a company could be stolen or compromised (like trade secrets, intellectual property, loss of network uptime, etc.)?
- What are the most serious consequences that can arise from a cybersecurity incident?

5.4 Likelihood

What is the chance of a security incident happening in an organization? This is the final (and tricky) piece of the information security risk assessment methodology to understand. An organization have to examine if the value of its data has particular significance to a group of bad actors.

6. INTELLIGENT AGENT BASED INFORMATION SECURITY MODEL

The biggest obstacles in Cloud Computing development are data security and privacy constraints. Every service provider claims that adequate security is provided to the customers and various research efforts are taken to satisfy the needs of security in Cloud computing, but still the organizations have to work a lot. The threats and risks related to security often decrease the operational processes of the organization. After so many advancements in the Cloud computing environment and Intelligent agent-based systems, still, none of the Information Security framework use Software Agents and Intelligent Agent's technology to meet the challenges of Information Security.

In this paper, we have introduced Software Agents to formulate Information Security framework and used Information Security Metrics tool to measure the performance of the Information Security System. In order to provide Information Security to the Cloud customers and venders, a four stages approach is proposed, as shown in Fig.11.

6.1 Risk and Assets Identification Agent

The preliminary assessment is performed by agent by identifying business processes, goals and objectives. It analyse stakeholders, risk effected assets, owner and container of the assets estimates the cost of damage. It then evaluates each and every asset that can be targeted by the threats and vulnerabilities. Agents then identifies potential risks through negotiation and collaboration with other agents over the network. Assess and evaluates associate risks with cloud service provider. The detailed task of each agent is as follows:

6.1.1 Context Establishment: Context establishment means defining the scope of all processes involved in the risk management and also sets the criteria to assess the tasks for the reduction of risk.

6.1.2 Preliminary Assessment: The target is to identify business processes and objectives, identify and enlist the stakeholders that are affected by risk, initially analyse the stakeholders to secure their interests, identify the risk factors, risk documentation,, and risk protection measures.

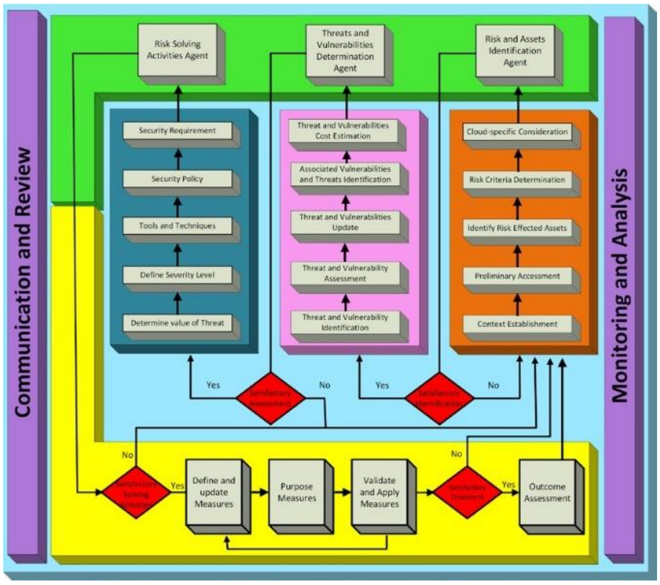

Communication and Review
Monitoring and Analysis
Risk Solving Activities Agent
Threats and Vulnerabilities Determination Agent
Risk and Assets Identification Agent
Security Requirement
Security Policy
Tools and Techniques
Define Severity Level
Determine value of Threat
Threat and Vulnerabilities Cost Estimation
Associated Vulnerabilities and Threats Identification
Threat and Vulnerabilities Update
Threat and Vulnerability Assessment
Threat and Vulnerability Identification
Cloud-specific Consideration
Risk Criteria Determination
Identify Risk Effected Assets
Preliminary Accessment
Context Establishment
Yes
Satisfactory Assessment
No
Yes
Satisfactory Identification
No
No
Satisfactory Solving Activities
Yes
Define and update Measures
Purpose Measures
Validate and Apply Measures
No
Satisfactory Treatment
Yes
Outcome Assessment

Fig. 11. Intelligent Agent Based Information Security Model

6.1.2.1 Business Process and Objective Identification: Here the documented operational activities, policies and rules of a business organization are identified. During risk reduction process, the objectives of the owner or organization is concerned and secured.

6.1.2.2 Analysis and Identification of Stakeholder: In this step, stakeholders are analyzed and identified thoroughly. Their interest and influence is checked based on defined criteria, since they are the main part of risk identification and reduction process.

6.1.2.3 Personal Data Identification and Mapping: Security and recovery of personal data of the personnel associated viz., employees, employer and stakeholders is next important step. During, the introductory part of assessment, this identification is the part of the risk management and map the same.

6.1.3 Identify Risk Effected Assets: During the process of risk reduction, assets of an organization play a very important role. These assets facilitate the identification of less important assets and helps to manage and evaluate the assets and its effects on the information system of an organization.

6.1.3.1 Evaluation of assets: The Assets are evaluated on the basis of importance in the information system, cost, timeline of utilization, assets user, and its priority.

6.1.3.2 Identification of Asset's owner and Container: There are two points of identification. First is, asset's owner, who decides the rules, principles, scope and target for the risk assessment. Second is, asset's container, who is responsible for storage, processing and transportation of asset's owner, who decides the rules, principles, scope and target for the risk assessment. Second is, asset's container, who is responsible for storage, processing and transportation of assets.

6.1.4 Risk Criteria Determination: The Information Security Risk Assessment decision-maker team takes decisions on the basis of risk criteria. The risks are categorized on the basis of assets type, assets stakeholders, reduction cost, area of attack, and severity. Following are the steps:

a. Risk Elicitation.
b. Key Risk Indicators.
c. Risk Level Determination.

d. Risk Aggregation.
e. Risk Prioritization.

6.1.5 Cloud specific consideration: To study the risks associated with cloud computing, the Information Security Risk Assessment (ISRA) process has included the cloud related considerations are. The proposed framework can handle the risk assessment for both traditional IT and cloud specialization organizations.

6.1.6 Assessment of Cloud Service Provider: This task will include Cloud Service Provider's existing security controls and compliance.

6.1.7 Software Agent Consideration: This task will expedite risk mitigation process by collaborating with other agents over the internet.

6.2 Threats and Vulnerabilities Determination Agent

Once the Risk and Assessment Agents have documented and identified the risks and threats, these agents shall identify previous and new threats and vulnerabilities, assess each of them in detail, update document them, thoroughly assess each of them, find associated threats and vulnerabilities by coordinating with other agents over the network, update the document and estimate threat damage and reduction cost.

6.2.1 Threat and Vulnerability Identification and Assessment

It is the process of identifying relevant threats and vulnerabilities of an asset and for organizations that exploit information security. The said task identifies each threat and vulnerability, and prioritizes them on the basis of their severity and affects. During the assessment process, the capability of each threat and the capacity and potential of each threat are assessed to compare with the risk reduction capability of the information security system. The document is updated.

6.2.2 Associated Vulnerability and Threat Identification: In this step, different threats and associated vulnerabilities are identified and updated. The required to be assessed with the mechanism used for associated threats and vulnerabilities are the same as that for main threats and vulnerabilities.

6.2.3 Threat and Vulnerability Cost Estimation: There are many threats that have high mitigation and damage cost and low severity. Such threats are assessed and their cost is evaluated. The system, then, accordingly set their mitigation priority as very low and often don't mitigate them due to their high cost.

6.3 Agent of risk solving activities

After all the detailed identification of assets, threats, risks, vulnerabilities, stakeholders, owners and business processes, the risk solving activities are performed. Before moving to the next step, the agent must find the related problems like, severity level, cost of threats, policies, current security requirements and tools and techniques to address potential risks and threats. Then perform the next step of finding solutions to resolve the issues.

6.4 Measures Agent

It is the final stage of the Information Security framework, where the framework performs the following operations:

- Redefine existing measures in the system.
- Assess the effectiveness of controls.
- Re-identification of controls to apply on risks.
- Use one measure against one risk or may use more than one measure (Purpose).
- Update the measures.
- If the risk, threat, and vulnerability are completely removed, then the event shall be documented along with the details of the concerned risks, assets, threats, and vulnerabilities, etc., otherwise the whole process will be repeated.

6.5 Communication and Review Agent

Communication and review are the continuous task in the entire information security risk assessment method, where the information related to risk, assets, threats, vulnerability, is shared with other agents. The sharing of the information and details with other agents of the organizations helps the agents in updating their system methods to reduce such types of risks in the future [13]. If each cloud organization shares the risk and threat assessment results with other stakeholders, it would be helpful for all the agents to know well in advance about the threats and vulnerabilities and the methods to reduce it beforehand.

6.6 Monitoring and Analysis Agent

Monitoring and analysis is a continuous process, which the Information Security Risk Assessment team should perform to keep track of the assessment tasks of all threat and risk activities are observed and examined minutely, and if the team feels necessary, make changes and update the method and security requirements, tools & techniques, policies and applicable measures to make it more comprehensive.

7. EVALUATION OF THE PROPOSED MODEL

The main goal to develop any model for Information Security is to design complex control systems which will help the designers and developers using intuitive and simple methods to identify and hence control the threats and vulnerabilities. Fuzzy logic is an important method that is used to handle raw, inexact data. It can be used to describe and implement complex control systems. Fig. 12 shows the Fuzzy Logic System.

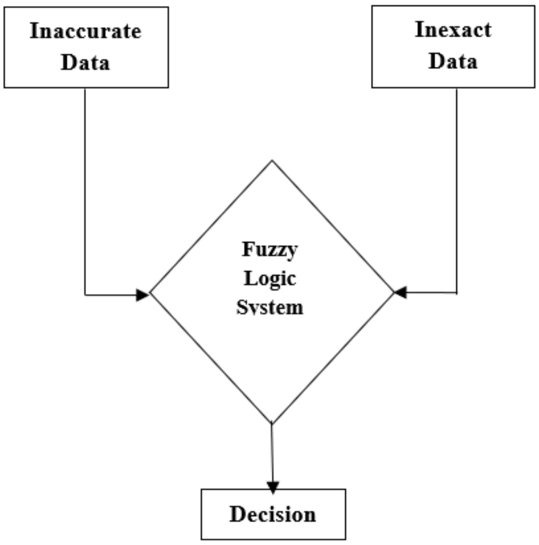


Fig. 12. Fuzzy Logic System

We can develop a model using Fuzzy logic allows which uses a smaller number of inputs. Fuzzy Controller is one of the applications, which uses human decision as its knowledge base. We can give inaccurate or imprecise input and still get a valid decision. The **FIG. 13** is presenting fuzzy model comprises of four input modules. The first stage fuzzification, accepts fragile values and convert them to fuzzy values. Fuzzy values are obtained on the knowledge base of users, processed by the inference engine, and it is then converted into fragile values by Defuzzification. Fuzzy logic uses fuzzy sets and membership functions for intelligent decision-making. For the evaluation of the Intelligent Agent-Based Information Security Model, we can use Triangular, Trapezoidal, and Gaussian functions in the fuzzy-wuzzy library of Python. We can use the Numpy library as well of Python to create sets of inputs and outputs and Fuzzy Interference System of Mamdani type.

The Mamdani scheme is a type of fuzzy relational model where each rule is represented by an IF– THEN relationship. It is also called a linguistic model because both the antecedent and the consequent are fuzzy propositions.

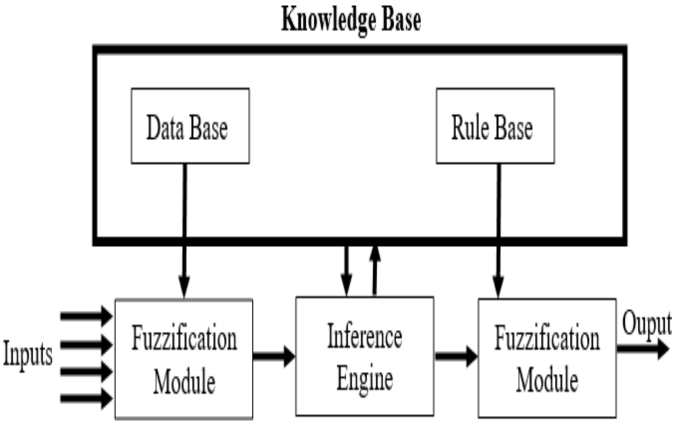


Fig. 13. Fuzzy Model

First, we have to design a Fuzzy Interference System of the Mamdani type. First step is to determine input and output variables, given in Fig. 11 and then the second step is data collection for input variables is performed. All the input variables have further input feeding variables that are mentioned in Fig. 11. The third step is to propose FBISM - Fuzzy Based Information Security Model. FBISM has forward and backward chaining. The model – is given in **Fig. 14.** Fuzzy rules are used to form the inference.

The fourth step is Defuzzification, in which the Mamdani method is used for regular Defuzzification. It acts as an interface between fuzzy control and inference system.. The fifth and final step is the Python implementation of fuzzy rules. The FBISM has been implemented to get the decision. Fuzzy norms are used for implementation. Membership functions are assigned to both, input and output values using Python. Different Information Security risks and threats can be recorded and processed.

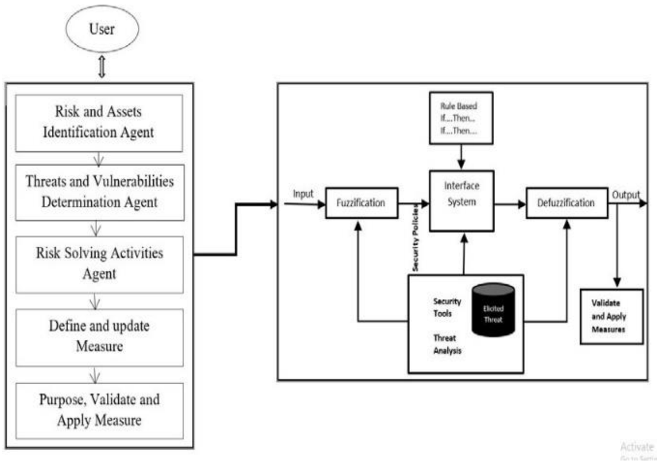

User
Risk and Assets Identification Agent
Threats and Vulnerabilities Determination Agent
Risk Solving Activities Agent
Define and update Measure
Purpose, Validate and Apply Measure
Rule Based If....Then... If....Then....
Input
Fuzzification
Interface System
Defuzzification
Output
Security Policies
Security Tools
Threat Analysis
Elicited Threat
Validate and Apply Measures

Fig. 14. Fuzzy Based Information Security Model (FBISM)

A fuzzy Logic cloud computing system can be developed, with a higher output performance and accuracy. We can create a system that has dynamic control and hence complexity can be successfully analysed, developed, and solved. Thus, for the output decision, the rules can be obtained using this system. This unique novel system can produce the precise values of all the inputs.

8. CONCLUSION

The main obstacle in Cloud computing development is the challenges faced due to its security and privacy due to the scalable and virtualized resources of cloud computing architecture. In this paper, we have targeted cloud-related threats and hence proposed the use of intelligent agents for the development of an Information Security model, for Cloud Computing wherein Information Security Metrics, threat agent elicitation, analysis, and reduction techniques were used and a decision was taken based on the information collected by the agents. During a detailed literature review, we studied various risk, threat, and vulnerability management-related techniques and studied literature related to agents in information technology.

The proposed agent-based model can facilitate the organizations to use multi-agent techniques in the identification of a threat, develop security metrics through agents and analyse threat agents, but even then we don't claim that users, who will use IABISM, would not undergo any attack thereafter. The aims and objectives of the proposed model (IABISM) are to reduce the level of damages from the threat agent. This model can be extended by adding new layers of authentication, virtualization and the privacy in the model. The proposed model can be implemented using the fuzzy-wuzzy library in Python and evaluated by fuzzy set theory and can prove to be a viable solution. We hoped that our research will open new dimensions for researchers and cloud organizations to enhance the security of their security systems.

9. REFERENCES

[1] 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.

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

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

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

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

[6] 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.

[7] M. I. Tariq, "Towards Information Security Metrics Framework for Debenham JK, Henderson-Sellers B (2002). Full lifecycle methodologies for agent-oriented

systems – the extended OPEN process framework, In Proceedings of Agent-Oriented Information Systems (Eds. Giorini P, Lespreance Y, Wagner G, Yu E), Toronto pp. 87-101.

[8] 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.

[9] T. K. Damenu and C. Balakrishna, "Cloud Security Risk Management: A Critical Review," in Proc. of 2015 9th International Conference on Next Gen. Mobile Applications, Services and Technologies, 2015.

[10] A. Rot and B. Olszewski, "Advanced Persistent Threats Attacks in Cyberspace. Threats, Vulnerabilities, Methods of Protection," in Proc. of Position Papers of the 2017 Federated Conference on Computer Science and Information Systems, 2017.

[11] D. Mortimer and S. T. Mortimer, "Quality and risk management tools, "Quality and Risk Management in the IVF Laboratory, pp. 118–134, 2015.

[12] Information technology: security techniques: information security management systems: requirements. Sydney, NSW: Standards Australia, 2006.

[13] A. Singhal and X. Ou, "Security risk analysis of enterprise networks using probabilistic attack graphs," 2011.