Agent Based Information Security Framework for Hybrid Cloud Computing

Muhammad Imran Tariq
Department of Computer Science, The Superior University
Punjab, Lahore 54700 - Pakistan
rukisimran@gmail.com
imrantariqbutt@yahoo.com

Received September 12, 2017; revised March 18, 2018; accepted August 15, 2018; published January 31, 2019

Abstract

In general, an information security approach estimates the risk, where the risk is to occur due to an unusual event, and the associated consequences for cloud organization. Information Security and Risk Management (ISRA) practices vary among cloud organizations and disciplines. There are several approaches to compare existing risk management methods for cloud organizations but their scope is limited considering stereo type criteria, rather than developing an agent based task that considers all aspects of the associated risk. It is the lack of considering all existing renowned risk management frameworks, their proper comparison, and agent techniques that motivates this research. This paper proposes Agent Based Information Security Framework for Hybrid Cloud Computing as an all-inclusive method including cloud related methods to review and compare existing different renowned methods for cloud computing risk issues and by adding new tasks from surveyed methods. The concepts of software agent and intelligent agent have been introduced that fetch/collect accurate information used in framework and to develop a decision system that facilitates the organization to take decision against threat agent on the basis of information provided by the security agents. The scope of this research primarily considers risk assessment methods that focus on assets, potential threats, vulnerabilities and their associated measures to calculate consequences. After in-depth comparison of renowned ISRA methods with ABISF, we have found that ISO/IEC 27005:2011 is the most appropriate approach among existing ISRA methods. The proposed framework was implemented using fuzzy inference system based upon fuzzy set theory, and MATLAB® fuzzy logic rules were used to test the framework. The fuzzy results confirm that proposed framework could be used for information security in cloud computing environment.

Keywords: Multi-agent systems, Information security, Risk Management, Cloud Computing, Grid computing, Fuzzy logic, Fuzzy set theory

1. Introduction

Cloud computing is a network-based environment that focus on sharing computation resources. Cloud resources are provided to users as a service on as needed basis. Resources in Cloud Systems can be pooled among a large number of users, and to deal with increased load, the system could advance its capacity efficiently through adding more hardware [1]. In computer security, risks and threat always exploits the vulnerability of the system to breach security and become harmful. The security and privacy issues are always misused by the threat agent. The threat agent acts as an anonymous attacker, malicious service agent, trusted attacker and malicious insider [2]. Therefore, vulnerability is a major risk factor. There are number of chances that an asset will be unable to resist the action of a threat agent [3]. Cloud computing has several advantages over the traditional computing but it has several constraints that acts as roadblock in the deployment of Cloud Computing [4]. The basic structure of Cloud Computing is characterized by an extremely strong interaction between the complex and different entities like Cloud Service Providers / Venders, Cloud Consumers and the brokers. These entities communicate and bargain with each other to provide better services to their customers [5].

In the recent past, a research was conducted in the area of agent based security. The authors used agent based techniques to make Cloud Computing more secure [6]. The proposed agent based framework will increase security of Cloud without effecting the performance of the system. Authors, by adopting Novel and mixed agent based techniques, introduced agent based security and privacy assurance framework which used cryptographic techniques against security threats like Denial of Service (DOS) [7]. To secure open Cloud networks, [8] introduced multi-agent based framework for reliable communication between open Clouds. The test results show that performance enhanced after the implementation of agent. The authors proposed a multi-tier agent based framework that leverage the abilities of agents to minimize the complexity of the system [9]. For Cloud storage security, agent based techniques were also applied [10] wherein the author proposed a three-tier security framework to increase the performance of the Cloud storage. Another agent based security framework was proposed that provides security at multilevel specifically for collaborative Cloud environment. The authors also proposed protocol that can be used for secure communication for non-trusted Cloud groups [11]. Agent based approach also used to provide security to Cloud network, infrastructure and storage [12]. After intensive review, it is revealed that agent based techniques have not been used with risk management techniques to offer defense against malicious attacks and threats. Therefore, authors clubbed software agents techniques with risk management techniques to propose information security framework for Cloud Computing.

The main contributions of the authors in this paper are summarized as below:

- We proposed an Agent Based Information Security Framework that secure organizations from potential risks and threats.
- We introduced Agent technique in Information Security Risk Assessment to effectively mitigate the risks and remove threats.
- We compared the proposed framework with existing seven renowned Risk Assessment methods to validate its novelty. Similarly, we evaluated ABISF by using fuzzy logic simulation techniques to validate its effectiveness.

The rest of the paper is ordered as follows, and section 2 is about Cloud Computing. In section 3, we discussed about Software Agent and subsequently, in section 4, we discussed the role of agents in cloud computing. In section 5, we presented the Agent Based Information Security Framework and in section 6, we implemented the proposed framework on renowned Information Security Risk Assessment methods and presented the results. We evaluated the proposed framework by using fuzzy logic in Section 7 and finally conclusion, limitations, and proposed future work in section 8.

2. Cloud Computing

Cloud is a new idea in the era of information technology. This concept gives new dimensions, ideas, techniques, and approaches to users. In cloud, data is stored, processed, and maintained virtually and only accessible through specific cloud's applications and infrastructure. Before the invention of cloud idea, organizations temporary rented out IT resources, human resources and software to cater their needs. Now, it is possible through cloud, wherein organizations rent the services of the cloud service providers to run their business processes and achieve their business objectives. The cloud service models and developments are as under:-

2.1 Cloud Architecture

The system architecture suggested by NIST for Cloud computing basically has three deployment models:

2.1.1 Private Cloud

The organization builds its own infrastructure and manages it as well.

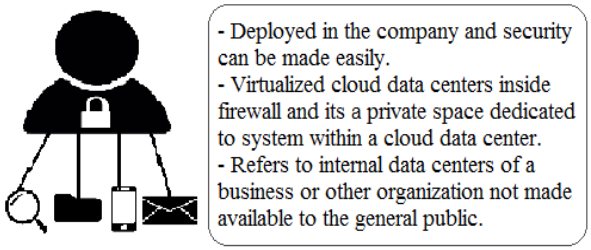

Fig. 1. Private Cloud

2.1.2 Public Cloud

The organization renders different services of Cloud Services Provider (CSP) as per its requirements and uses it as long as organization requires [2]. Private and Public Clouds are connected with each other through gateways to share data, applications and resources.

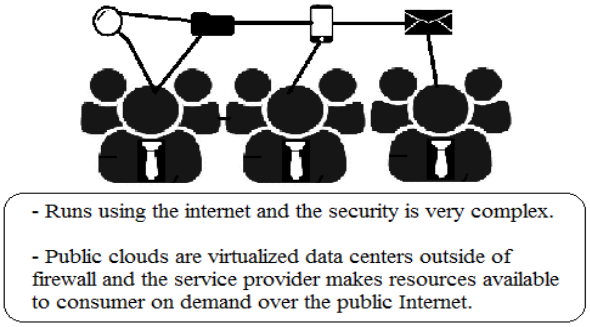

Fig. 2. Public Cloud

2.1.3 Hybrid Cloud

It is a combination of Private and Public Cloud models. It has characteristics of Public and Private deployment models. There is no location binding on hybrid cloud, it may located at private organization premises or Cloud Service Provider premises [12].

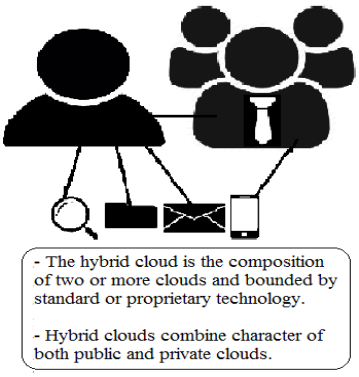

Fig. 3. Hybrid Cloud

2.1.4 Software as a Service (SaaS)

It is a software distribution model which gives the consumer ability to use the Cloud Service Providers' or a third-party provider application running in its cloud. It is the most likely candidate for SaaS application.

- Many competitors use the same products, such as Email.
- There is a significant peak demand, such as billing and payroll like this on a regular basis.
- The sales management software, such as mobile phone, as this the need for a mobile and web access.
- You need only short-term projects, such as collaboration software.

2.1.5 Infrastructure as Service (IaaS)

It provides hardware, storage and infrastructure related services to its users. Amazon EC2 and Rackspace are very famous examples of IaaS.

2.1.6 Platform as Service (PaaS)

It provides environment, tools, libraries to applications development framework, machines and operating system services to its customers.

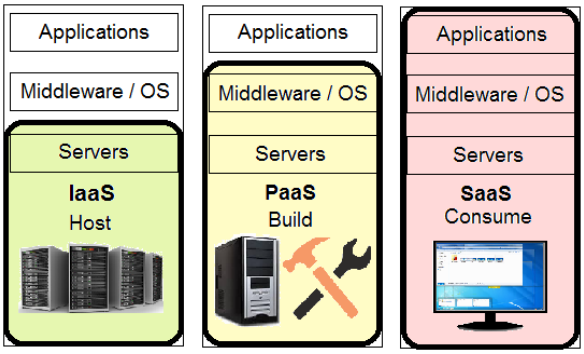

Fig. 4. Comparison of Service Models

Cloud computing has several advantages over the traditional computing but it has some constraints that are roadblock in the complete deployment of cloud computing. The rapid growing consumer demand of Cloud computing bring more challenges for the Information Security providers [12]. They must confirm that the virtual environment is secured, that they are able to provide distinct services to their customers. In this regard, several researches have been urged to identify the exact security issues of cloud computing [2]. The most critical security issues in Cloud computing are: Loss of Governance, Lock-in, Distributed Denial of Service, Vulnerabilities in backup system, Loss of encryption keys, unauthorized access and malicious insider.

During literature review, a number of models used various methods to achieve the agent involving system. Software agents that are easy to use, elastic and independent may be utilized for intelligence applications in the cloud computing. In addition, you can also consider using agent technology to solve service composition, management of resources, shifting of data from one Cloud Service Provider to another service provider [13]. However, no software agent work is standardized. The renewed Information Security standards, such as NIST, ISO/IEC 27001, FISMA, CSA and COBIT are used by Cloud organizations to implement Information Security in their organization according to their service and development model [14].

3. Software Agent

Software Agent is an innovative technique that may be used in different fields with distinct knowledge [15]. During literature review, it is revealed that it is new field and its acceptance will take time. Agent is an autonomous entity that has the capability to act continuously in certain environment on behalf of its host to accomplish a specific task or number of task that are assigned to it. Furthermore, during task accomplishment process, it does not need the intervention of its creator / host [16].

Software Agents are very much like real life agents that are expert in a particular field, that negotiate with their customer and secure the vested interests of their hosts/organization [17]. Software Agents are programmed and they require only specific and particular information to

be able to work in a certain environment [18]. When the Software Agent is able to perceive information from its environment it and take decisions on the basis of collected information then it can be called an Intelligent Agent. The Software Agents are devised to act in a certain environment and to communicate with other agents to complete a specific task [16].

Different authors and researchers have introduced a number of definitions for independence and interaction of agents with other agents, their ability and have shown great enthusiasm for this concept. The ability of these concepts means that the software agent continuously works based on available set of actions, selects the task base on its priority, coordinates with other agents, collects information, reacts on it and makes decision in the best interest of the host without its involvement [19].

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 [16].

4. Agent in Cloud Computing

Software Agent is an innovative technique that may Application that use complex data/information often required high performance systems and mass storage. Therefore, Cloud Computing provides perfect and ideal infrastructure due to its high performance, variety of resources at a large scale and memory availability to agents to accomplish their assigned tasks [20].

On other hand, the autonomous agents are used in the Cloud Computing for resource sharing, discovery and composition of services and authentication. The use of agents in Cloud Computing is new solution to improve the security, privacy, resource management, discovery of new services, storage management, processing management and negotiation with venders [13].

The software based intelligent agents are used in large-scale Datacenters to maintain their extracted huge data [21]. These agents are also used in Datacenters to monitor the services, grant access to legitimate users, make Cloud infrastructure as energy efficient as possible and develop strategies based on collected information. The main advantages of the agent-based systems are:

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

If Cloud Computing and software agent's technologies work together then it may produce innovative results. During literature review, it is observed that up till now, a very few researchers have proposed the idea of combination of both technologies [21]. In Cloud Computing, we have to plan and implement a system for familiarization with the dynamic behavior of Cloud Computing environment. In order to cater these challenges, multi-agent techniques can be used as they have heterogeneity and volatility capabilities [22]. Hence, Agent based models can be used to formulate effective Information Security Framework for Cloud Computing.

5. Agents Based Information Security Framework

The most critical roadblock in the development of Cloud Computing is its security and privacy constraints. Although every vender claims that it is providing adequate security to its customers and various research efforts have been made to cater the needs of security in Cloud computing, but still it is a great challenge for the Cloud organizations. Security risks and threats always directly decrease the operational processes of the organization. During literature review, it is extracted that various Information Security frameworks exist but none of the Information Security framework use Software Agents and Intelligent Agents technology to meet the challenges of Information Security.

In this paper, we introduced Software Agents to formulate Information Security framework and used Information Security Metrics that is a valuable tool to measure the performance of the Information Security System. Furthermore, risk management techniques are also used to define the severity level of the risk. In order to provide Information Security to the Cloud customers and venders, a four stages approach is proposed, as shown in **Fig. 5.**

5.1 Risk and Assets Identification Agent

The agent initially performs the preliminary assessment by targeting business processes, goals and objectives. Identifies and analyze stakeholders, identifies risk effected assets, estimates its damage cost, identifies owner of the assets, container of the assets, evaluates each and every asset that can be targeted by the risks, threats and vulnerabilities. It identifies potential risks through negotiation and collaboration with other agents over the network, internet, social contacts, security agencies, research portals, research laboratories, forums and groups etc. Segregate risks, define key factors, motivation of the risk, scope of the risk, targets of the risks, and identifies key risk indicators, risk aggregation and its prioritization. Assess and evaluates associate risks with cloud service provider. The details of each task of agent is given as under:

5.1.1 Context Establishment

Risks in context to Information Security are always uncertain and its mitigation process cannot be fully achieved until the objectives and strategies of the business are clear. Context establishment means to define the scope of all processes involved in the risk management and also sets the criteria to assess the tasks for the mitigation of risks [23]. The scope of risk management must be within limit of the organizational goals and objectives.

5.1.2 Preliminary Assessment

After defining context establishment, the next step is Preliminary Assessment. The target of preliminary assessment is to identify business processes and objectives, identify and enlist the stakeholders that are effected with risk, initially analyze the stakeholders to secure their interests, identify the risk factors, protective factors and document the gathered details about risk [24].

5.1.2.1 Business Process and Objective Identification

Business process identification is the part of preliminary assessment wherein all operational activities of the business are defined, applicable rules and policies are also documented [25].

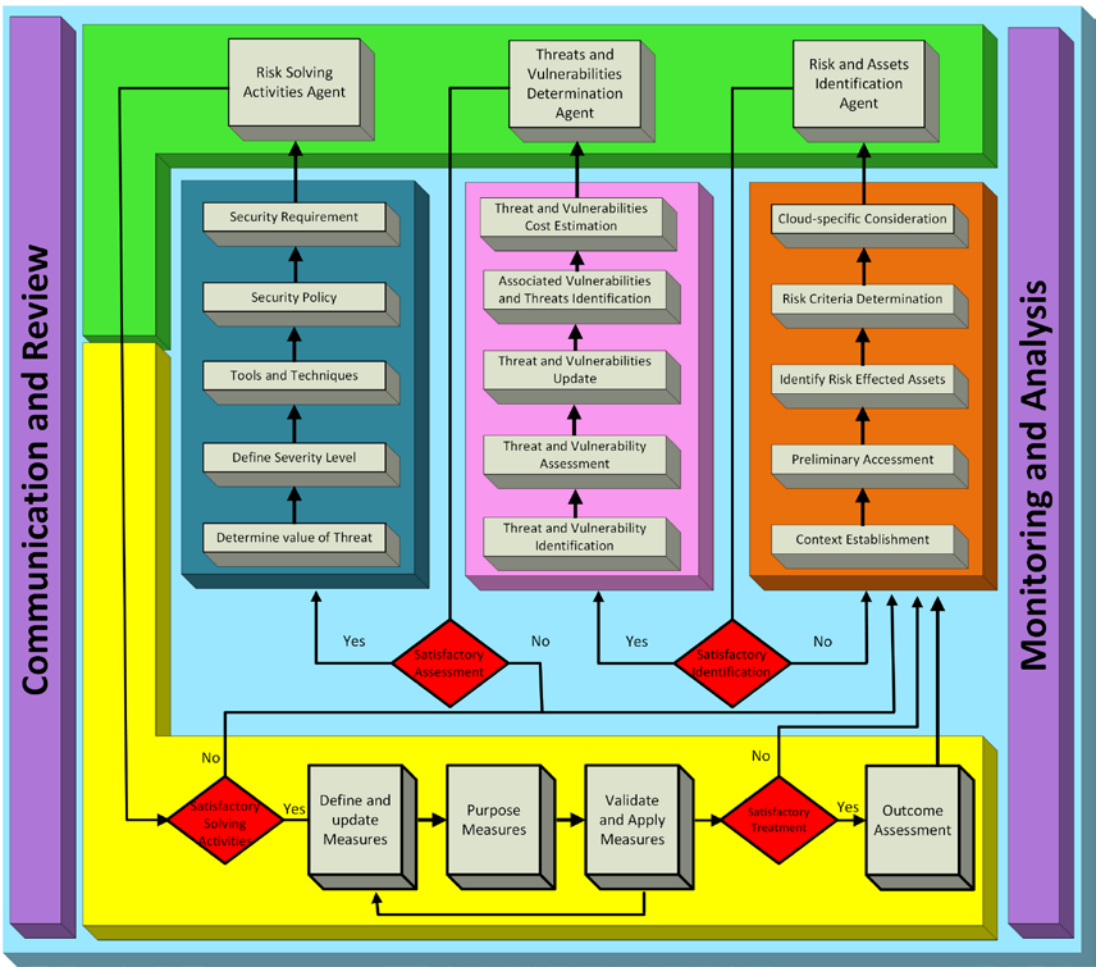

Fig. 5. Agent Based Information Security Framework

During risk mitigation process, it is necessary to consider and secure the objectives of the owner of organization.

5.1.2.2 Identification of Stakeholder

Identification of stakeholder is the process to identify the concerned stakeholders that are required to be contacted at the time of risk mitigation and also make sure their involvement in risk mitigation process to effectively identify and mitigate risks [26, 27, 28].

5.1.2.3 Analysis of Stakeholders

The analysis of the stakeholders is the essential part of the preliminary assessment wherein the stakeholders are thoroughly analyzed as per defined criteria of the risk management like their influence and interest in the risk mitigation process [25].

5.1.2.4 Personal Data Identification and Mapping

Personal data of the employees, employer and stakeholders is very important to be rescued, secured and recovered. During, preliminary assessment, it would be the part of the risk management to identify the personal data of the stakeholders, mapped the same and thereafter assessed whether it is according to law, policies and rules applicable therein or not? [29].

5.1.3 Identify Risk Effected Assets

Identification of assets is very critical process of the risk assessment and it always played a vital role in the risk mitigation [30]. During risk assessment and its mitigation, it is necessary to identify exact assets of the organization that are effected with risk and such record of the assets will further facilitate other tasks of the risk assessment [31].

5.1.3.1 Asset Evaluation

The Assets are required to be evaluated according to set criteria like their cost, worth, importance in the information system, who used the assets, timeline of utilization, and effectiveness of the asset in the information system and also its priority [32].

5.1.3.2 Identification of Asset's owner

The identification of asset's owner will facilities risk management process to frame its scope and focus target of the risk assessment [32].

5.1.3.3 Asset Container Identification

The asset container is the place where assets of the information system resides / stored / transported, and processed [32].

5.1.4 Risk Criteria Determination

The decision makers of Information Security Risk Assessment team takes decision on the basis of risk criteria. The risk criteria determines the significance of the risk and categorized the risks in the light of its severity, area of attack, types of assets, stakeholders, mitigation cost and other parameters [33].

5.1.4.1 Risk Elicitation

To define risk criteria, it is necessary to identify the risk. There are several ways to elicit the risk. There are several sources of Information security that enlist the current and past risks that can effect on information security [34]. Furthermore, the Information Security Risk Assessment team also elicit real time risks from the Information System.

5.1.4.2 Key Risk Indicators

After elicitation of risk, the next step is to identify and define key risk indicators. The key risk indicators are always build on the basis of predefined appetite and information security metrics [33]. If organization compromised these key risk indicators and risk appetite executed.

5.1.4.3 Determination of Risk Level

The third stage of risk criteria determination is to determine the level of the risk. For this, ISRA team builds risk scenarios, executes and compiles them, document the consequences and determine the value level of risk [35].

5.1.4.4 Risk Aggregation

Risk aggregation is a task that is performed to build link between rolled up risks and integration of high level and low level of risks [35]. ISRA team shall scan each risk according to its risk level and aggregate each individual risk. The purpose of this activity is to reinvestigate each risk and aggregate it according to its potential development.

5.1.4.5 Risk Prioritization

It is the task in which significance of each risk is evaluated, each risk mitigation process is prioritized in the light of its severity and cost [34].

5.1.5 Cloud-specific Consideration

Cloud related considerations are included in the Information Security Risk Assessment process to study the risks that are related to cloud computing. The proposed framework specialization is that it would be suitable for the cloud organizations in addition to traditional IT organizations. This task will make sure that during ISRA process, the ISRA team has considered the risks specific to cloud computing [29, 33].

5.1.6 Assessment of Cloud Service Provider

The purpose of assessing cloud service provider is to include methods and techniques in Information Security Risk Assessment related to Cloud Service Provider. This task will include Cloud Service Provider's existing security controls and compliance [33].

5.1.7 Software Agent Consideration

The Information Security Risk Assessment team shall consider software agent techniques during risk identification, assets elicitation, risk aggregation and prioritization. This task will expedite risk mitigation process by collaborating with other agents over the internet.

5.2 Threats and Vulnerabilities Determination Agent

The said agent shall identify potential and existing threats and vulnerabilities, document them, thoroughly assess each of them, update about threats and vulnerabilities by coordinating with other agents over the network, find out associated threats and vulnerabilities and also estimate threat damage and mitigation cost [36].

5.2.1 Threat and Vulnerability Identification

Vulnerability and Threat identification is the process of identifying relevant threats and vulnerabilities of an asset and for organizations that exploit information security. The said task identify each threat and vulnerability, quantify and rank each of them in the system. This task also covers relevant methods and approaches to find credibility and severity of potential vulnerability and threat [36].

5.2.2 Threat and Vulnerability Assessment

Vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system [35, 36]. The Information Security Risk Assessment methods further guided to expand the assessment techniques and tools to estimate each threat and vulnerability willingness and motivation to attack. During threat and vulnerability assessment, the capability of each threat is gaged to compare with risk mitigation capability of the information security system and furthermore, the capacity and potential of each threat is assessed in terms of the resources used by the risk to attack [37]. The assessment task documents the duration and consequences of each attack.

5.2.3 Threat and Vulnerability Update

The identified and assessed threats and vulnerabilities are required to be updated in the system so that the old information about these threats and vulnerabilities must not be used again [36, 38]. The software agents of the framework will communicate updates to other agents over the internet and receive updates from other agents to keep information to update.

5.2.4 Associated Vulnerability and Threat Identification

Various threats are interconnected with other threats and attack the system in collaboration with other threats. Therefore, it is necessary to identify and update all links and associated vulnerabilities and threats [38]. The associated threats and vulnerabilities are required to be assessed with the mechanism used for main threats and vulnerabilities.

5.2.5 Threat and Vulnerability Cost Estimation

Every threat mitigation is required to be assessed in such a manner that system should calculate its damage cost and the cost required to mitigate it. Various threats have high mitigation cost and very low severity level as compared to cost of the damage they do. The system, thereafter, accordingly set their mitigation priority as very low and often don't mitigate them due to their high cost [33, 34].

5.3 Risk Solving Activities Agent

The risk solving activities are performed after thorough investigation of risks, threats and vulnerabilities, associated assets, stakeholders, owners and business processes. The agent shall, before moving on to the next step, must first determine the value of the threat, define severity level of the risks and threats, find appropriate tools and techniques to address potential risks and threats, find applicable policies defined in the method, existing security requirements and then find alternate solutions to resolve the issues.

5.3.1 Determine Value of Threat

Threat value determination is actually the assessment of the damage done to the assets, personal information, organizational information and physical infrastructure [39]. Such value can be assessed through building scenario of potential threat and then assessing the damage it causes.

5.3.2 Define Severity Level

It is a continuous process which contains the defined/set severity of each threat agent based on the collected information, security requirements, established policies and tools required to mitigate the threat agent [40]. The severity level will facilitate the organization to set the priorities of action to be taken if more than two threat agents attack at the same time.

5.3.3 Tools and Techniques

In order to enforce the security policies against each threat agent, the analysis of tools and techniques lead towards the appropriate solution of threat agent. Different websites, news groups, dashboards, forums and research papers may be used to dig out the most suitable tools. Although the performance of all tools and techniques that are used for cloud are not equal, but in this section, the framework will find the most widely accepted and used tools for Cloud computing risks mitigation. For example HyTrust's virtual management and CohesiveFT sells cloud security tools [33].

5.3.4 Security Policy

After determining the security requirements, establishment of Security policy is necessary. Each security policy is established against each threat agent and its respective security requirements are taken care of. Security policies must be cleared and rectified for the threat agent [32, 35].

5.3.5 Security Requirement

In order to mitigate the threat agents, the security goals and security requirements of the threat agent should be determined [41]. The number of actions to be taken to reduce the severity of the particular threat agents have to be defined. Cloud Security Alliance (CSA) has introduced the Cloud Security Metrics V3.01 which is very useful for the Cloud organizations to define the security requirements against identified risks.

5.3.6 Agents to find out alternate solution

The agent shall find out alternate solutions available over the network, suggested by other organizations, gathers through collaboration and negotiation with other agents, research groups and forums, industry, research laboratories, discussion with information security expert, during communication and review task etc.

5.4 Measures

Measures is the final stage of this framework wherein framework update existing measures in system, identify controls to apply on risk, before applying appropriate controls, assess their previous effectiveness and finally purpose measure to mitigate risks, threat and vulnerabilities. The final outcome of the measures shall again be verified.

5.4.1 Define and update Measures

After intensive work out on risks and assets, threats, vulnerabilities, stakeholders, owners, business goals, process and objectives, find out relevant risk mitigation techniques, tools, policies, requirements and alternate solutions, it is necessary to define and update existing measures if necessary [42].

5.4.1.1 Control Identification

Before applying measures, identification of appropriate controls is very critical process. The system already has a number of relevant controls against the risks, but in case of newly identified risks, it is necessary to identify relevant controls from the existing control's database or otherwise agents will contact other agents to get controls for risks [33, 43].

5.4.1.2 Control Efficiency Assessment

This task is a tricky and very critical one as it assess the effectiveness of the already proposed controls for the mitigation of risk. If the control already applied on the same type of risk, then its previous effectiveness would be considered before its selection, otherwise agent would be activated to identify alternative controls for concerned risk [34].

5.4.3 Purpose Measures

After identification and assessing efficiency of the existing appropriate controls for the risk mitigation, measures shall be purposed. The Information Security Risk Assessment team shall use one measure against one risk or may use more than one measure and vice versa. Therefore, the ISRA team is required to keenly focus on this task.

5.4.4 Validate and Apply Measures

To validate the measures, it is required to identify the outcome of the measures, so first ISRA team must identify the likely outcome of the risks, threats, vulnerabilities and assets if security breaches and team also required to estimate the cost of damage if potential event occurs [44]. After assessing outcome of potential event and before applying measures, it is mandatory to validate the measures through reliable methods, and techniques. In case of measures not validated, the measures criteria is required to be evaluated again [36].

5.4.5 Outcome Assessment

This is the final stage of the Information Security framework. The outcome of the measures shall be assessed to check the effectiveness of the controls and applied measures [33, 45]. If the risk, threat and vulnerability is completely removed, then event shall be documented along-with concerned risks, assets, vulnerabilities, threat, applied measures, techniques, tools, methods, rules, policies, cost, severity level etc., otherwise the whole process will be repeated to accurately identify, validate and apply measures.

5.5 Communication and Review

The communication and review is the continuous task throughout information security risk assessment method. The risk, vulnerability, threat, concerned assets, outcome of the method and its outcome assessment shall be shared with other agents. The sharing of the said information and details with other agents of the organizations will update their system methods to mitigate such types of risks in future [46]. The other organizations will review the

outcomes of Information Security Risk Assessment and update their system if necessary. Each cloud organizations should communicate risk and threat assessment results with other stakeholders either formally or informally.

5.6 Monitoring and Analysis

Monitoring and Analysis is also a continuous process that keeps working from the pre-assessment to outcome assessment tasks. In this task, all threat and risk activities are observed and examined minutely, and if the team feels necessary, make changes and update the method to make it more comprehensive [47]. The Information Security Risk Assessment method should be reviewed, updated as and when new threat and risk identified or this method applied to mitigate the risk and threat. The ISRA team should keep update security requirements, tools & techniques, policies and applicable measures.

6. Information Security Risk Assessment Methods

During intensive literature review regarding Information Security Risk Assessment, we reviewed seven renowned Information Security Risk Assessment (ISRA) methods that have lot of common points and were developed specifically for risk assessment. These methods are well documented and currently, various organizations are following these methods to mitigate risks. The brief about these seven methods are as follow:

6.1 Conflicting Incentives Risk Analysis (CIRA)

It represents as method of risk assessment, wherein main focus is set on stakeholders, their conflicting incentives, and perceived output of these actions. It was developed on the base of game theory, economics and psychology. CIRA is developed by Rajbhandari [48] and Snekkeness [49]. There are two classes of owners in CIRA i.e. Risk Owner and Strategy Owner. The CIRA targets Risk Owner as Strategy Owner do its actions to increase perceived benefits.

CIRA framework while defining scope of the assessment, first identify the stakeholders, risk owner and other owners. For each stakeholder, CIRA define utility factors, establish scale and measurement policies and procedures, and also elaborate weight that assumed and assigned to each stakeholder. Game theory applied to each player of the game and finally, the risk is calculated by investigating strategy of each player.

CIRA does not discuss business related activities and also does not directly identify risks, vulnerabilities, but threats and stakeholders identified directly and they are part of its core action.

6.2 Factor Analysis of Information Risk (FAIR)

It is the only one international standard that provides quantitative model for operational risks and security as well as privacy. Its model provided an opportunity of understanding of information risks in light of its financial impact, analyze and quantify each risk. It also uses scientific approach for risk management instead of stereo type qualitative approach [50]. The FAIR approach is not concerned about how and from where organization gets prior information for use in the assessment as well as describe the value of information and how it contributes to establish risk [51]. First, FAIR applies preliminary assessment to identify assets and then identify the list of risks to generate scenario. This preliminary assessment is not sufficient for risk identification as it does not discuss vulnerability and threat even outcome of

each category are not addressed. The primary strength of FAIR is its risk estimation wherein it discussed about threats and vulnerabilities. During literature review, the FAIR is the second best method for information security.

6.3 ISO / IEC 27005:2011 — Information technology — Security techniques — Information security risk management

During literature review and after conducting comparison analysis, we found that ISO27005 is the most mature standard for risk management amongst selected 07 ISRM standards and frameworks. It secured highest completeness i.e. 59. ISO/IEC 27001:2011 provides a number of appendixes to users that support them to identify scope of the risk, risks, threats, and vulnerability assessment [52]. The standard does not support stakeholder identification and analysis, key risk indicators, and preliminary assessment task that other frameworks and standards support for risk management. The standards score highest in proposed 04 stages of Information Security Framework.

6.4 NIST Special Publication (SP) 800-30—Revision 1 Guide for Conducting Risk Assessments

The NIST SP 800-30 is guideline for Information Security Officers to assess the risks in their organizations. It amplify existing NIST SP 800-39 guideline. NIST SP 800-30 carried risk assessment in three steps i.e. prepare assessment, conduct assessment and maintain assessment [53]. In Risk and Assets Identification stage, the NIST SP 800-30 scored 21 marks whereas two other standards scored more than 21 marks i.e. 22 and 25. NIST SP 800-30 is based upon threat management without considering the primary and secondary factors of assets and other mandatory factors. NIST SP 800-30 performed well in the threat and vulnerabilities categories for risk identification but it does not support stakeholder assessment. It supports only subjective impact estimations without considering risk effected assets. NIST SP 800-30 secured third position in comparison table by getting 48 marks.

6.5 OCTAVE Allegro

OCTAVE Allegro (OA) mainly targets organizational risks and very light weight version with a large number of worksheets for the practitioner. OA was basically developed for large organizations having employees more than 300. It primarily focuses on information assets, how assets are being used and how threats attack on these assets. OCTAVE Allegro stated that assets identification is brainstorming activity and their experiences shows that users often face difficulty in the identification of risk effected assets. Therefore, OCTAVE Allegro focuses on how to identify critical assets and apply critical analysis to improve effected assets.

It registered each asset with the reason of its selection, custodian / owner of the asset and its security requirement. It also perform activities to identify and investigate critical areas of the concerned assets [54]. In Risk and Assets Identification, the OCTAVE Allegro scored 25 points as ISO/IEC 2700:2011 and FAIR whereas on the other hand, in Threats and Vulnerabilities Determination stage, OCTAVE Allegro scored only 8 points while ISO/IEC 27005:2011 perceived 14 points. OCTAVE Allegro also scores low on Risk Solving Activities Agent and Measures. OA uses risk metrics and risk treatment / mitigation as part of its execution.

6.6 The Risk IT framework and practitioner guide

The ISACA published RISK-IT Framework which states a comprehensive process model to manage IT risk. In this framework, RISK-IT performs risk analysis, establish scenario analysis, assign responsibilities, and highlight key risk indicators. It also contains practical scenarios and guide users on how to perform key activities described in the process model [55].

The RISK-IT framework is very distinguish framework and fill the gap between generic and detailed risk management IT related risk management's frameworks [56]. RISK-IT, due to its extensive documentation, scores fourth highest points which is really astonishing for the authors as it is least accessible framework. During literature review, we found that RISK-IT does not discuss about the activity of assets like identification and evaluation of assets which are the core requirement of the risk management. The RISK-IT mostly covers the business related aspects given in ISRA processes. Furthermore, the RISK-IT does not discuss about threat assessment and risk identification.

6.7 NSMROS

The Norwegian Security Authority Risk and Vulnerability Assessment has built special sequential approach that is relying upon the fundamental elements of ISRA methods. The NSMROS is mainly focuses on assets, vulnerabilities, threats and outcomes [57] [58]. The disadvantages of NSMROS are that it does not discuss business processes and tasks related to stakeholders, due to which, NSMROS scores very low as compared to other risk management frameworks / standards. Furthermore, NSMROS also does not discuss about threat assessment and risk-specific estimation. However, it suggests gathering of lost data to quantify impact estimation. The authors evaluated the NSMROS and found it at the bottom of the rank array.

7. Evaluation of Existing ISRA Methods with ABISF

During literature review, we studied different stereo-type criteria to compare existing Information Security Risk Assessment methods which uses only basic risk assessment techniques as benchmark and overlook the tasks that their proposed framework do not covers. The authors studied seven renowned Information Security Risk Assessment frameworks thoroughly and written down their common and distinguished risk assessment points to formulate a comprehensive criteria for the evaluations of existing ISRA methods. The authors critically analyzed each of the task covered under study method, collected the relevant tasks from other ISRA methods and thereafter, combined them to formulate one task that covers all approaches opted by other methods. The said approach is very comprehensive as the developed criteria is taken from surveyed ISRA methods. We have developed a simple criteria to quantify each ISRA method and the same criteria has been implemented on proposed ABISF to validate it.

A developed criteria is given in Table 1. Each method and its associated task will be selected and passed through criteria to get the results.

Table 1. ISRA Method Evaluation Criteria

Value	Description	Remarks
0	Not addressed	The method does not support task
1	Partially addressed	The method partially support task
2	Completely Addressed	The method completely support task

The developed criteria implemented on seven renowned ISRA methods and their scores compared with ABISF to validate its reliability and effectiveness. The given Table 2 is showing the comparison.

Table 2. Comparison of Agent Based Information Security Framework (ABISF) with seven information security risk assessment (ISRA) frameworks

Assessment Stage	Tasks	ABISF	NSMROS	CIRA	FAIR	ISO/IEC 27005:2011	NIST 800-30	OCTAVE A	RISK IT	Row Total
Risk and Assets Identification Agent	Context Establishment	2	2	2	1	1	2	2	2	**14**
	Preliminary Assessment	2	2	2	1	0	2	2	2	**13**
	Business Process and Objective Identification	1	0	0	2	2	0	2	2	**9**
	Identification of Stakeholder	1	0	2	2	2	0	1	2	**10**
	Analysis of Stakeholders	1	0	2	2	2	0	1	0	**8**
	Personal Data Identification and Mapping	2	0	1	1	1	1	1	0	**7**
	Identify Risk Effected Assets	2	2	2	1	2	2	1	1	**13**
	Asset Evaluation	2	2	2	2	2	2	2	2	**16**
	Identification of Asset's owner	2	0	2	1	2	0	2	0	**9**
	Asset Container Identification	2	0	0	2	0	0	2	0	**6**
	Risk Criteria Determination	2	1	2	1	2	1	2	2	**13**
	Risk Elicitation	2	2	1	2	2	2	2	1	**14**
	Key Risk Indicators	2	0	0	2	1	1	1	2	**9**
	Determination of Risk Level	2	0	0	2	2	2	1	2	**11**
	Risk Aggregation	2	1	0	0	2	2	1	2	**10**
	Risk Prioritization	2	2	2	0	2	2	2	2	**14**
	Cloud-specific Consideration	2	0	0	2	0	1	0	0	**5**
	Assessment of Cloud Service	2	0	0	1	0	1	0	0	**4**

Assessment Stage	Tasks	ABISF	NSMROS	CIRA	FAIR	ISO/IEC 27005:2011	NIST 800-30	OCTAVE A	RISK IT	Row Total
	Provider									
	Software Agent Consideration	2	0	0	0	0	0	0	0	**2**
	Sub-Total	**35**	**14**	**20**	**25**	**25**	**21**	**25**	**22**	
Threats and Vulnerabilities Determination Agent	Threat and Vulnerability Identification	2	1	1	1	2	1	1	1	**10**
	Threat and Vulnerability Assessment	2	0	0	1	2	1	0	0	**6**
	Threat and Vulnerability Motivation Strength	1	0	2	0	2	2	2	1	**10**
	Threat and Vulnerability Capability	1	0	1	2	1	0	0	0	**5**
	Threat and Vulnerability Capacity	1	0	1	1	1	0	1	0	**5**
	Threat Attack Duration	2	0	0	2	1	0	0	2	**7**
	Threat and Vulnerability Update	2	1	0	2	2	2	1	1	**11**
	Associated Vulnerability and Threat Identification	1	0	0	1	1	1	1	2	**7**
	Threat and Vulnerability Cost Estimation	1	1	1	1	2	2	2	2	**12**
	Agents to maintain Threat and Vulnerability	2	0	0	0	0	0	0	0	**2**
	Sub-Total	**15**	**3**	**6**	**11**	**14**	**9**	**8**	**9**	
Risk Solving Activities Agent	Determine Value of Threat	2	1	1	1	2	1	1	1	**10**
	Define Severity Level	2	0	1	2	2	1	1	1	**10**
	Tools and Techniques	2	1	2	1	2	2	1	1	**12**
	Security Policy	2	1	1	2	2	1	1	1	**11**
	Security Requirement	2	0	2	1	1	2	2	1	**11**
	Agents to find out alternate solution	2	0	0	0	0	0	0	0	**2**
	Sub-Total	**12**	**3**	**7**	**7**	**9**	**7**	**6**	**5**	
Measures	Define and update Measures	2	2	1	1	2	2	1	1	**13**

Assessment Stage	Tasks	ABISF	NSMROS	CIRA	FAIR	ISO/IEC 27005:2011	NIST 800-30	OCTAVE A	RISK IT	Row Total
	Control Identification	1	1	1	0	1	2	1	0	**7**
	Control Assessment	2	0	0	0	0	0	0	0	**2**
	Control Efficiency Assessment	2	0	1	0	2	1	0	1	**7**
	Purpose Measures	2	2	2	2	2	2	1	1	**14**
	Validate and Apply Measures	2	2	1	1	2	2	2	1	**13**
	Outcome Assessment	2	2	1	0	2	2	2	1	**12**
	Sub-Total	**13**	**9**	**7**	**4**	**11**	**11**	**7**	**5**	
Grand-Total		**75**	**29**	**40**	**47**	**59**	**48**	**46**	**41**	

After summing the score of four stages vertically, the results show that ABISF has obtained highest score whereas on the other hand, the ISO/IEC 27005:2011 is the second in rating.

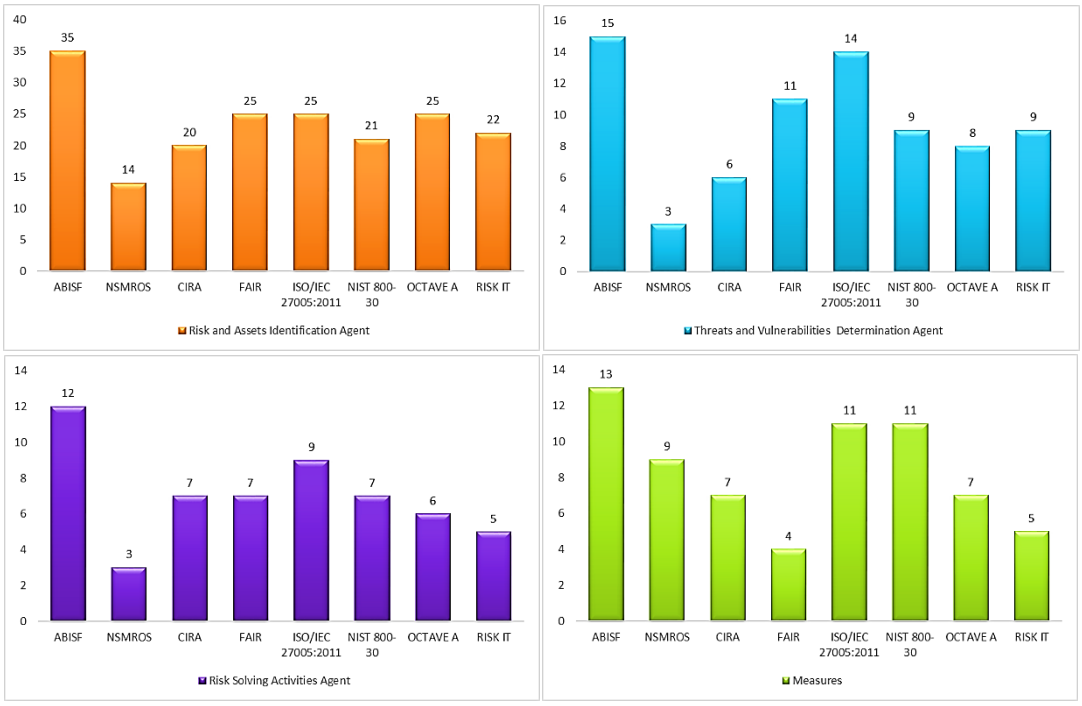

Fig. 6. Comparison of 4 stages of ABISF with other methods

The NIST SP 800-30, FAIR and OCTAVE A are on third, fourth and fifth position in rating with one point scoring difference. The results of ISO/IEC 27005: 2011 clearly states that it is a comprehensive method and Industry recommends it.

Although OCTAVE A has many citations, a number of researchers used this method in their research but results revealed that this framework still needs improvement. The results of NSMROS are not unexpected, during its study, we noticed its effectiveness and loopholes.

We also noticed that NSMROS is immature ISRA and it was built to cater the needs of specific areas not to cover all Information Security Risk Assessment areas that a comprehensive ISRA should have but even then, we included it in comparison to inform the readers about which areas still need improvement.

The **Fig. 6** presents the detailed comparison of 4 stages of Agent Based Information Security Framework with seven surveyed methods. The said figure clearly depicts that every stage of the ABISF has scored higher points than other methods. In Table 2, we summarized the scores of each task horizontally, to get a clear picture of which task is mostly addressed in the surveyed methods. In Risk and Assets Identification stage, Asset evaluation is the task that most of the methods included in their risk mitigation process. Thereafter, Context Establishment, Risk Prioritization, and Risk Elicitation scored equal marks in the Risk and Assets Identification stage. In the Threats and Vulnerabilities Determination stage, Threat and Vulnerability Cost Estimation scored 12 highest points which indicates that it is the task that most of the methods included in their list while addressing threat and vulnerability. Similarly, Tools and Techniques is the most preferred task while performing risk solving activities. Finally, purpose measure is the task that opt every method while mitigating risks from information system. The horizontal scores of the Table 2, helps the Information Security Officers and researchers determine which task is highly recommended by the surveyed methods and which task requires their attention on priority bases.

8. Evaluation of Framework

Fuzzy logic is a dominant method used to handle inaccurate and inexact data. It describes, develops and implements complex control systems that facilitates the designers to develop such systems with simple and intuitive methods.

Fig. 7. Fuzzy Logic System

Fuzzy logic allows us to develop model with less number of inputs or even without data. Fuzzy techniques have many advantages like lesser dependability on previous values as compared to other complex software. Fuzzy Controller classical is one of the applications, different from other classical applications, which has the ability to utilize human decisions as its knowledge. During fuzzification, users may use inaccurate and unclear statements as input, and it after Defuzzification, generates result to take decision. The **Fig. 9** is presenting fuzzy model comprises of four input modules. As stated earlier, fuzzification is the first stage of the model, it accepts crisp values and convert them to fuzzy values. Fuzzy values are obtained on the knowledge of users, processed by the inference engine, and then transformed into crisp values by Defuzzification.

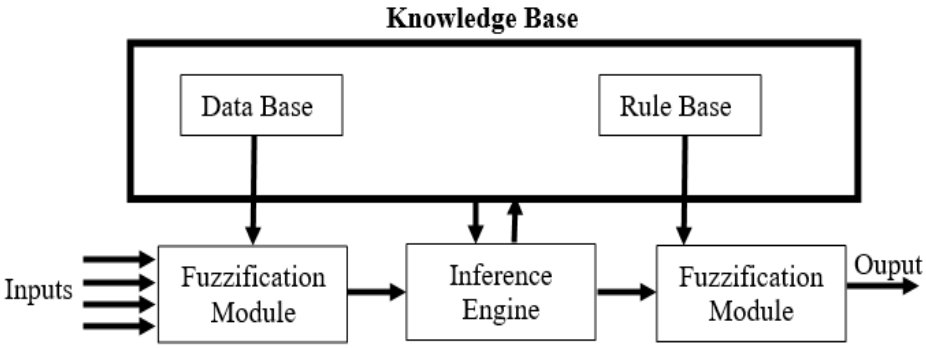

Fig. 8. Fuzzy Model

Fuzzy logic has different fuzzy sets and membership functions. Membership functions have values between 0 and 1. At this time, there are eleven membership functions available in MATLAB®. For the evaluation of Agent Based Information Security Framework, we considered only 1 membership function i.e. Triangular.

In 2011, Fuzzy inference has been used for risk assessment using risk matrix [59], whereas in the same year, authors focused on fuzzy logic for risk assessment [60]. The authors applied fuzzy logic for risk assessment and decision making [61]. Similarly, fuzzy logic opted and used by various researchers for risk assessment [62, 63, 64, 65].

Before evaluation of proposed framework, it is required to design a system using fuzzy inference system that is based upon fuzzy set theory i.e. if-then rules and logical reasoning. The first stage of the designed system is to determine input and output variables, given in **Fig. 9**. The second stage of fuzzy interface is the data collection for input variables. All the input variables have further input feeding variables that are mentioned in the **Fig. 5.**

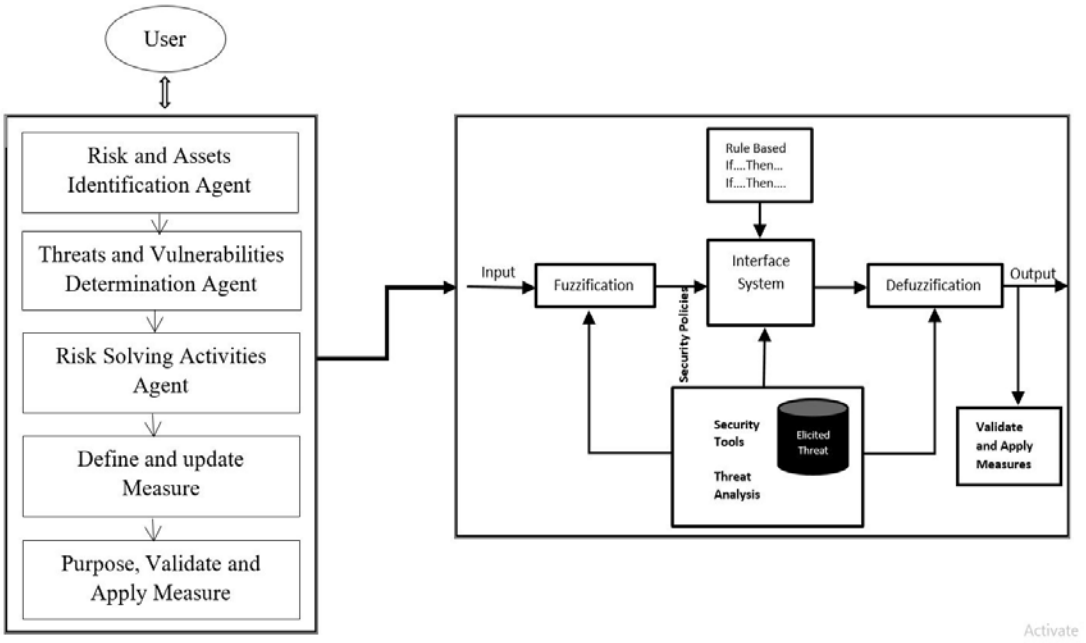

Fig.9. Fuzzy Based Information Security Framework (FBISF)

The third stage of fuzzy is to propose Information Security Framework. FBISF has forward and backward chaining. The model – is given in **Fig. 9** – has Risk and Assets Identification Agent (RAIA), Threats and Vulnerabilities Determination Agent (TVDA), Risk Solving Activities Agent (RSAA), Define and update Measure (DUM), Purpose, Validate and Apply Measure (PVAM) and Database consists of information about Threats and fuzzy rules, fuzzification, inference engine and defuzzifier.

The inference has been formed by grouping a number of fuzzy rules. 243 fuzzy rules were taken into consideration with the combination of linguistic variable values, and these rules are not mentioned in paper due to its length constraints. The second last step is Defuzzification which acts as mediator between fuzzy control and inference system. Regular Defuzzification methods (Mamdani) were opted. The last step is implementation of fuzzy rules through MATLAB®. In this study, four input variable and one output, are used as shown in **Fig. 10**. The FBISF has been implemented to get decision. Implementation is performed with the support of fuzzy norms. Membership function are assigned to both, input and output values using MATLAB®. Different Information Security risks and threats have been recorded and processed.

Total 3^5=243 rules are formulated and assessed by MATLAB Rule editor and viewer by using IF- AND- THEN logic. **Fig. 11** shows MATLAB Rule viewer for cloud computing.

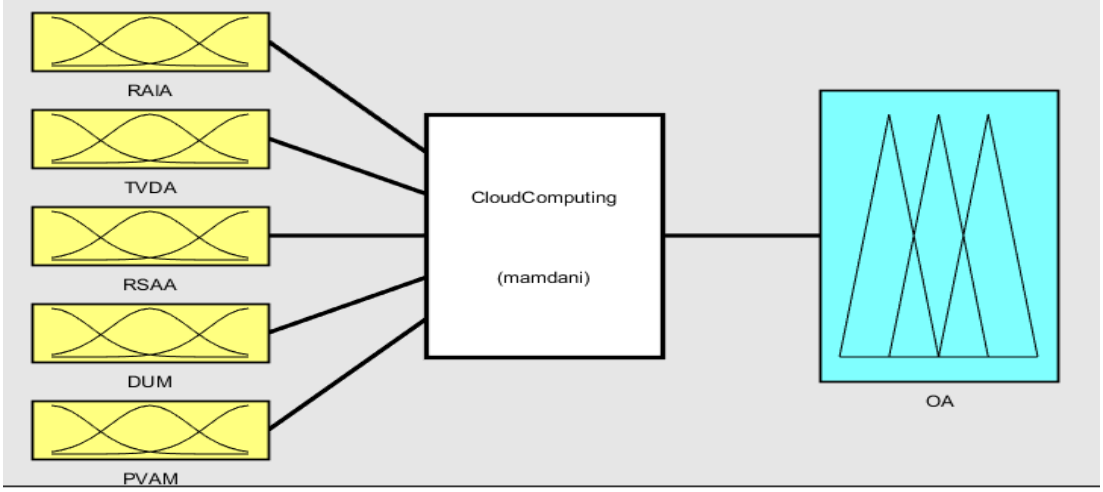

Fig. 10. Fuzzy Logic Controller using fuzzy based logic inference system editor for cloud system.

In this Fuzzy Logic cloud computing system, we have taken five variables as input variables and Outcome Assessment (OA) as output variable. There are three membership functions against each input .. Output outcome assessment has also three membership functions. **Fig. 11** shows these input and output variables. The ranges of membership functions are taken as 0 to 10 for each input.

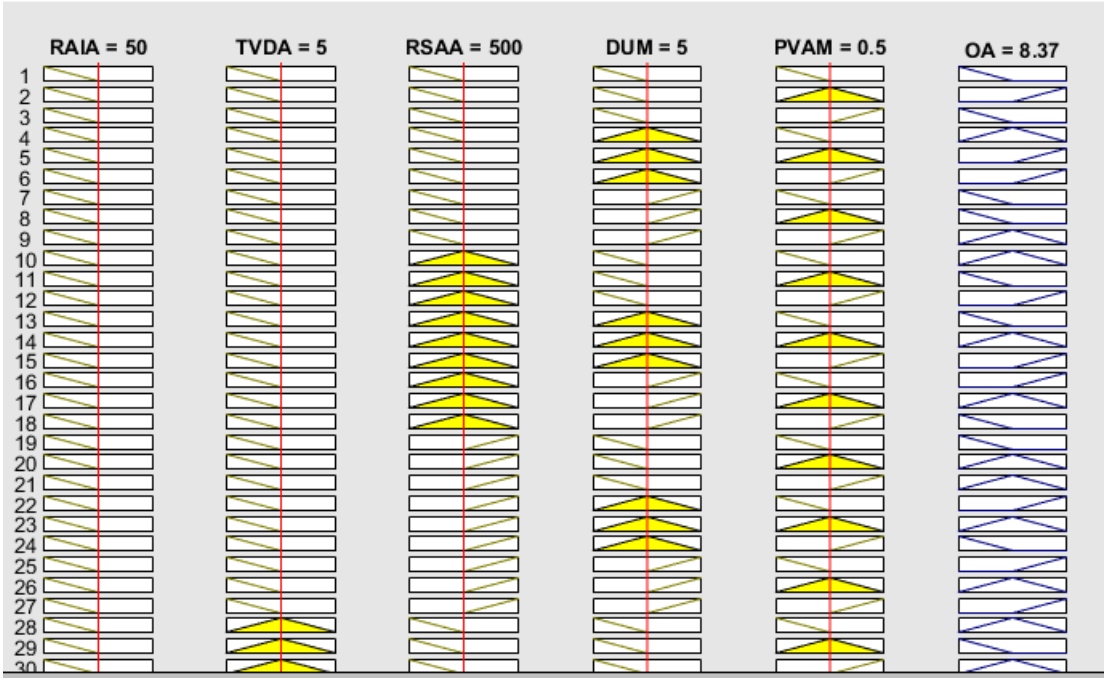

Fig. 11. MATLAB Rule view

Here the 3D graphs of surface viewer for the RAIA, TVDA, RSAA, DUM, PVAM and output OA are presented in the **Fig. 12** (a, b, c, d, e, f, g, h, I and j). **Fig. 12(a)** shows the dependency of output decision on DUM and RSAA. **Fig. 12(b)** shows the dependency of output decision on PVAM and RSAA. **Fig. 12(c)** shows the dependency of output decision on DUM and TVDA. **Fig. 12(d)** shows the dependency of the output decision on the RSAA and the TVDA. **Fig. 12(e)** shows the dependency of output decision on PVAM and RAIA. **Fig. 12(f)** shows the dependency of output decision on DUM and RAIA. **Fig. 12(g)** shows the dependency of output decision on RSAA and RAIA. **Fig. 12(h)** shows the dependency of output decision on TVDA and RAIA. **Fig. 12(i)** shows the dependency of output decision on TVDA and PVAM and **Fig. 12(j)** shows the dependency of output decision on PVAM and DUM. A user who intends to take decision on the identified threat may rely on identified dependencies. Therefore, output decision was taken on the values of RAIA = 50, TVDA = 5, RSAA = 500, DUM 500, PVAM =0.5 and according to Mamdani's model output was obtained 8.37. The Mamdani's model is very useful for these crisp values of Fuzzy Logic cloud computing system. The results of Mamdani's model and the MATLAB simulated value are in **Table 3.**

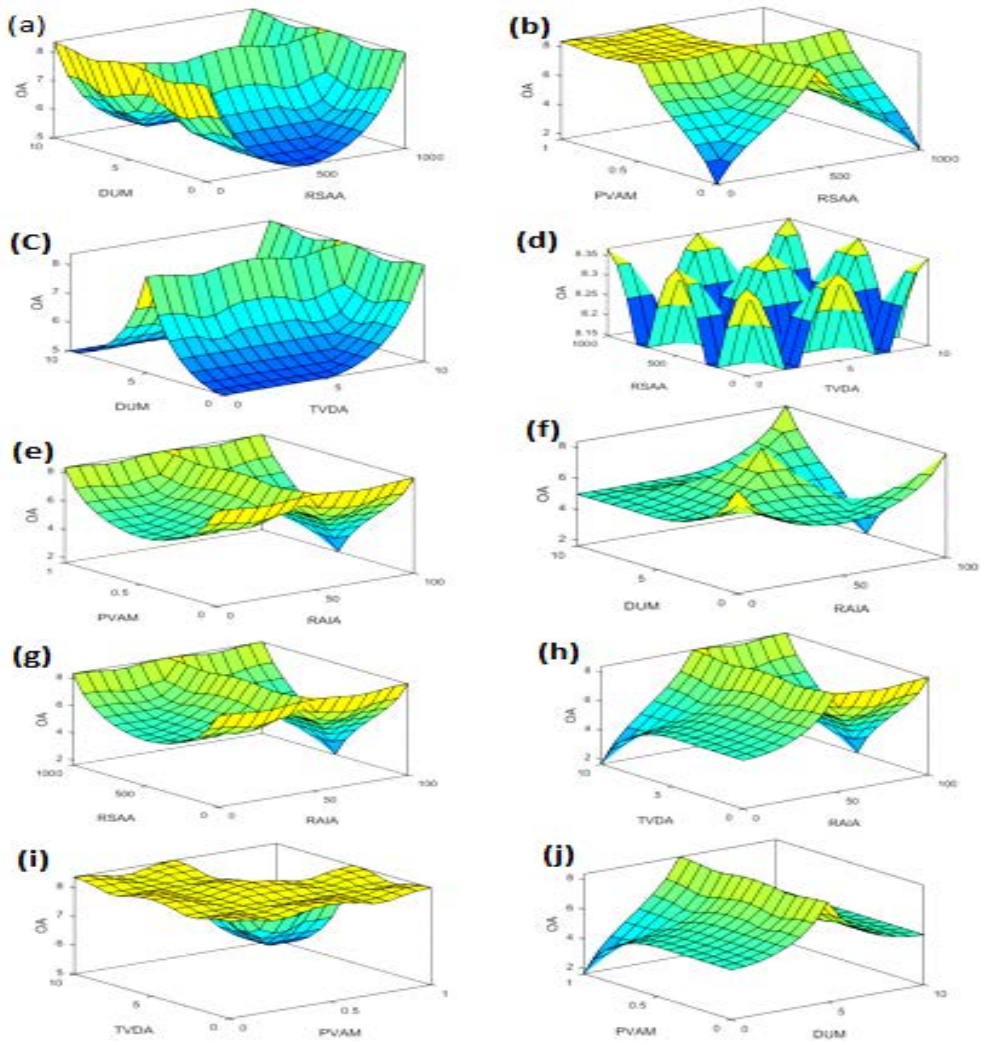

Fig. 12. 3D Graphs of Sample Solution

With a greater accuracy and higher output performance, Fuzzy Logic cloud computing system was established. Therefore, systems with dynamic control and complexity can be successfully solved, analyzed and developed. Hence, the rules were obtained through this system for the output decision. Therefore this novel system was confirmed for precise values of the all the inputs.

Table 3. Result Comparison

Category	Decision
Mamdani's value	7.46
MATLAB simulation	7.48
Difference	0.02
Error percentage	0.26%

The difference measured in the designed and the simulated value is just 0.26%, which is insignificant. It confirms that proposed framework could be used to take decisions on the security threats.

9. Conclusion

The core roadblock in the development of Cloud computing has its security and privacy challenges. The novelty and significance of this paper is to introduce software agents, intelligent agents and multi-agents problem solving techniques to formulate an Information Security framework for Cloud Computing. In this paper, a new methodology has been introduced for the development of Information Security framework, particularly for Cloud Computing wherein Information Security Metrics, threat agent elicitation, analysis and mitigation techniques were used with existing technology of agents and a decision was taken based on the information collected by the agents. The proposed agent based framework facilitates the organizations to use multi-agent techniques in the identification of a threat, develop security metrics through agents and analyze threat agents. The proposed framework could be extended by adding new authentication layer, virtualization layer and the privacy layer in the framework. The proposed framework was implemented in MATLAB® and evaluated by fuzzy set theory and found viable solution.

The study had several limitations that our future efforts can address. Let's say, we had studied seven Information Security Risk Assessment methods while during literature review, we found some other methods that we did not discuss in this paper. Furthermore, a number of researchers proposed their own ISRA methods that we did not consider. Second limitation is that the authors are novices, thus the ISRA experts may differ from the results. However, these results will be a guideline and prove useful for non-specialists and novices. The authors have diverse interests and skills, which can effect extracted results. Although, after drafting framework and its evaluation criteria, the authors contacted with available information security experts for their comments and thereafter, authors finalized framework. The comments of available information security experts might not be sufficient for final outcome of the framework. Despite of indicated limitations, our research is a key step to improve existing ISRA especially in the Risk, Threat and Vulnerability identification. We have plans to further refine and expand it to get more accurate results and to enhance its capabilities to mitigate risks, threats and vulnerabilities effectively and efficiently. Developing an effective application for the proposed Information Security framework. Furthermore, different scenarios can be created to check the validity and reliability of the proposed framework.

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. Article (CrossRef Link)

[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. Article (CrossRef Link)

[3] P. Samarati and S. D. C. D. Vimercati, "Cloud Security," *Encyclopedia of Cloud Computing*, pp. 205–219, 2016. Article (CrossRef Link)

[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. Article (CrossRef Link)
[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. Article (CrossRef Link)
[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. Article (CrossRef Link)
[7] 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. Article (CrossRef Link)
[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. Article (CrossRef Link)
[9] M. Kuo, "An intelligent agent-based collaborative information security framework," *Expert Systems with Applications*, vol. 32, no. 2, pp. 585–598, 2007. Article (CrossRef Link)
[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. Article (CrossRef Link)
[11] S. Khatua, N. Mukherjee, and N. Chaki, "A new agent based security framework for collaborative cloud environment," in *Proc. of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research - CSIIRW 11*, 2011. Article (CrossRef Link)
[12] 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. Article (CrossRef Link)
[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. Article (CrossRef Link)
[14] M. I. Tariq and V. Santarcangelo, "Analysis of ISO 27001:2013 Controls Effectiveness for Cloud Computing," in *Proc. of the 2nd International Conference on Information Systems Security and Privacy*, pp. 201–208, 2016. Article (CrossRef Link)
[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. Article (CrossRef Link)
[16] D. Talia, "Clouds Meet Agents: Toward Intelligent Cloud Services," *IEEE Internet Computing*, vol. 16, no. 2, pp. 78–81, 2012. Article (CrossRef Link)
[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. Article (CrossRef Link)
[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. Article (CrossRef Link)
[19] M. Hafiz, P. Adamczyk, and R. E. Johnson, "Organizing Security Patterns," *IEEE Software*, vol. 24, no. 4, pp. 52–60, 2007. Article (CrossRef Link)
[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. Article (CrossRef Link)
[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. Article (CrossRef Link)

[22] R. Aversa, B. D. Martino, M. Rak, and S. Venticinque, "Cloud Agency: A Mobile Agent Based Cloud System," in *Proc. of International Conference on Complex, Intelligent and Software Intensive Systems*, 2010. Article (CrossRef Link)
[23] T. K. Damenu and C. Balakrishna, "Cloud Security Risk Management: A Critical Review," in *Proc. of 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, 2015. Article (CrossRef Link)
[24] X. Yang, "Framework development in plant disease risk assessment and its application," *Plant disease epidemiology: facing challenges of the 21st Century*, pp. 25–34. Article (CrossRef Link)
[25] K. Sadgrove, *The complete guide to business risk management*. Abingdon, Oxon: Routledge, 2016. Article (CrossRef Link)
[26] A. Lehar, "Measuring Systemic Risk: A Risk Management Approach," *SSRN Electronic Journal*, 2003. Article (CrossRef Link)
[27] S. Klipper, "Information Security Risk Management," 2015. Article (CrossRef Link)
[28] R. K. Otto and K. S. Douglas, *Handbook of violence risk assessment*. New York: Routledge, 2010. Article (CrossRef Link)
[29] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, Jan. 2007. Article (CrossRef Link)
[30] "Methods," *Uncertainty in Risk Assessment*, pp. 27–28, Jul. 2014. Article (CrossRef Link)
[31] E. J. Riedl and G. Serafeim, "Information Risk and Fair Values: An Examination of Equity Betas," *Journal of Accounting Research*, vol. 49, no. 4, pp. 1083–1122, Jul. 2011. Article (CrossRef Link)
[32] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process," Jan. 2007. Article (CrossRef Link)
[33] S. Gregor and A. R. Hevner, "Positioning and Presenting Design Science Research for Maximum Impact," *MIS Quarterly*, vol. 37, no. 2, pp. 337–355, Feb. 2013. Article (CrossRef Link)
[34] S. Klipper, "ISO 27005 und BSI IT-Grundschutz," *Information Security Risk Management*, pp. 99–107, 2011. Article (CrossRef Link)
[35] S. Fenz, J. Heurix, T. Neubauer, and F. Pechstein, "Current challenges in information security risk management," *Information Management & Computer Security*, vol. 22, no. 5, pp. 410–430, Oct. 2014. Article (CrossRef Link)
[36] 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. Article (CrossRef Link)
[37] M. W. Harkins, "Emerging Threats and Vulnerabilities: Reality and Rhetoric," *Managing Risk and Information Security*, pp. 81–98, 2016. Article (CrossRef Link)
[38] M. Harkins, "Emerging Threats and Vulnerabilities," *Managing Risk and Information Security*, pp. 71–85, 2013. Article (CrossRef Link)
[39] S. Sridevi, "Wireless Lan Vulnerabilities, Threats and Countermeasures," *Indian Journal of Applied Research*, vol. 3, no. 9, pp. 123–126, Jan. 2011. Article (CrossRef Link)
[40] B. Karabacak and I. Sogukpinar, "ISRAM: information security risk analysis method," *Computers & Security*, vol. 24, no. 2, pp. 147–159, 2005. Article (CrossRef Link)
[41] J. Luna, H. Ghani and D. Germanus, "A Security Metrics Framework For The Cloud," *Proceedings of the International Conference on Security and Cryptography*, 2011. Article (CrossRef Link)
[42] K. J. Hole and L.-H. Netland, "Toward Risk Assessment of Large-Impact and Rare Events," *IEEE Security & Privacy Magazine*, vol. 8, no. 3, pp. 21–27, 2010. Article (CrossRef Link)
[43] P. Shamala, R. Ahmad, and M. Yusoff, "A conceptual framework of info structure for information security risk assessment (ISRA)," *Journal of Information Security and Applications*, vol. 18, no. 1, pp. 45–52, 2013. Article (CrossRef Link)

[44] M. S. Lund, B. Solhaug, and K. Stølen, "Risk Analysis of Changing and Evolving Systems Using CORAS," *Foundations of Security Analysis and Design VI Lecture Notes in Computer Science*, pp. 231–274, 2011. Article (CrossRef Link)
[45] S. R. Patil and H. C. Frey, "Comparison of Sensitivity Analysis Methods Based on Applications to a Food Safety Risk Assessment Model," *Risk Analysis*, vol. 24, no. 3, pp. 573–585, 2004. Article (CrossRef Link)
[46] D. Mortimer and S. T. Mortimer, "Quality and risk management tools," *Quality and Risk Management in the IVF Laboratory*, pp. 118–134, 2015. Article (CrossRef Link)
[47] H. Wang, J. Mylopoulos, and S. Liao, "Intelligent agents and financial risk monitoring systems," *Communications of the ACM*, vol. 45, no. 3, pp. 83–88, Jan. 2002. Article (CrossRef Link)
[48] G. Wangen, "Conflicting Incentives Risk Analysis: A Case Study of the Normative Peer Review Process," *Administrative Sciences*, vol. 5, no. 4, pp. 125–147, Sep. 2015. Article (CrossRef Link)
[49] E. Snekkenes, "Position Paper: Privacy Risk Analysis Is about Understanding Conflicting Incentives," *Policies and Research in Identity Management IFIP Advances in Information and Communication Technology*, pp. 100–103, 2013. Article (CrossRef Link)
[50] C. Yang, "Projects Bidding Decision Risk Analysis Based on Multi-factor Clustering Analysis," *Information Technology Journal*, vol. 12, no. 21, pp. 6164–6168, Jan. 2013. Article (CrossRef Link)
[51] P. Shamala and R. Ahmad, "A proposed taxonomy of assets for information security risk assessment (ISRA)," in *Proc. of 2014 4th World Congress on Information and Communication Technologies (WICT 2014)*, 2014. Article (CrossRef Link)
[52] Information technology: security techniques: information security management systems: requirements. Sydney, NSW: Standards Australia, 2006. Article (CrossRef Link)
[53] A. Singhal and X. Ou, "Security risk analysis of enterprise networks using probabilistic attack graphs," 2011. Article (CrossRef Link)
[54] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process," Jan. 2007. Article (CrossRef Link)
[55] B. G. Barnier, "The New ISACA Risk IT Framework and Best Practice: Filling a Gap, Making Risk Management Easier and More Effective," *Edpacs*, vol. 40, no. 1, pp. 1–7, 2009. Article (CrossRef Link)
[56] M. Fasanghari, A. Haeri, and S. M. Hatefi, "A slack analysis framework for IT risk processes management through risk IT framework," *International Journal of Industrial and Systems Engineering*, vol. 26, no. 1, p. 1, 2017. Article (CrossRef Link)
[57] D. Gritzalis, G. Iseppi, A. Mylonas, and V. Stavrou, "Exiting the Risk Assessment Maze," *ACM Computing Surveys*, vol. 51, no. 1, pp. 1–30, Apr. 2018. Article (CrossRef Link)
[58] H. Karlzén, J. Bengtsson, and J. Hallberg, "Assessing Information Security Risks using Pairwise Weighting," *Proceedings of the 3rd International Conference on Information Systems Security and Privacy*, 2017. Article (CrossRef Link)
[59] Y. L. Yang and Y. H. Zhou, "A Fuzzy Logic Based Information Security Risk Assessment Method," *Applied Mechanics and Materials*, vol. 130-134, pp. 3726–3730, 2011. Article (CrossRef Link)
[60] Y. Yang and Y. Zhou, "Fuzzy Logic Based Method for Network Information Security Risk Assessment," *2011 International Conference on Internet Technology and Applications*, 2011. Article (CrossRef Link)
[61] S.-T. Lu, "Risk Factors Assessment for Software Development Project Based on Fuzzy Decision Making," *International Journal of Information and Electronics Engineering*, 2012. Article (CrossRef Link)
[62] A. M. and T. Olivares, "Fuzzy Logic Applied to Decision Making in Wireless Sensor Networks," *Fuzzy Logic - Emerging Technologies and Applications*, 2012. Article (CrossRef Link)

[63] M. Fayaz, I. Ullah, D.-H. Park, K. Kim, and D. Kim, "An Integrated Risk Index Model Based on Hierarchical Fuzzy Logic for Underground Risk Assessment," *Applied Sciences*, vol. 7, no. 12, p. 1037, Nov. 2017. Article (CrossRef Link)

[64] Y. Yang and Y. Zhou, "Fuzzy Logic Based Method for Network Information Security Risk Assessment," *2011 International Conference on Internet Technology and Applications*, 2011. Article (CrossRef Link)

[65] I. Anikin and L. Y. Emaletdinova, "Information security risk management in computer networks based on fuzzy logic and cost/benefit ratio estimation," *Proceedings of the 8th International Conference on Security of Information and Networks - SIN 15*, 2015. Article (CrossRef Link)

Muhammad Imran Tariq is Deputy Director (Commerce) at Higher Education Department, Lahore, Pakistan, where he has been since 2006. He received a Bachelor of Computer Science from Allama Iqbal University, Islamabad in 2003, M.Sc. Computer Science in 2008 and Master of Science in Computer Science / M.Phil from University of Lahore in 2013. He is currently perusing Ph.D. degree in Computer Science from Superior University, Lahore. Moreover, he has MCSE, MCP+I, A+ and CCNA certifications. His research interests include Cloud Computing, Information Security, ISO, NIST, COBIT, Service Level Agreement, Information Security Metrics, Cloud Risks and its mitigation techniques, Wireless Networks Security and Risk Management. He is author of Many research papers and 02 books on Cloud Security. He is also reviewer of International renowned Journals. He is Associate Editor of IEEE Access Journal.