JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Literature Review on Security Mechanisms for Cloud Data Applications

[1]CH.Madhavi Sudha, [2]Dr. D. S. R. Murthy.

[1]Research Scholar, [2]Professor.
[1]Computer Science and Engineering,
[1]Anurag University, Hyderabad, India

Abstract: This study has been undertaken to investigate the various security mechanisms for cloud environment and cloud data applications. In this paper recent standard papers considered and focused mainly on various security aspects. During 2021 and 2022, how various authentication levels considered for secure data access mentioned and threat specific risk assessment was calculated. The analytical framework contains.

Index Terms **– Security Mechanisms, Cloud environment, Threat specific risk assessment**

I. INTRODUCTION

Cloud Computing concept has emerged from the distributed software architecture. Cloud computed technology is aimed to provide hosted services over the internet. In recent years, cloud computing in Information Technology has given rise to various new user communities and markets. Cloud computing services are provided from data centers located in different parts of the world. Microsoft SharePoint and Google applications are general examples of cloud computing services. Security plays an important role in the wider acceptance of cloud computing services [1]. Existing literature is focused on different security solutions, including technology and security policy implementation. Threats, threat specific security level authentication [4] and different levels of security authentication the latter study introduced new attacks on the cloud environment from criminological perspectives. The proposed solution to these recent attacks. A study [1] identified several security issues affecting cloud computing attributes. The same research proposes to overcome the identified problems concerning the security of the cloud. A security guide, developed in this research, enables the cloud user organizations to be aware of security vulnerabilities and approaches to invade them. Security vulnerabilities and challenges arise from the usage of cloud computing services. Currently, cloud computing models are the primary source of these challenges and vulnerabilities. The intruders exploit the weakness of cloud models in accessing the users' private data, by attacking the processing power of computer systems [1]

II. LITERATURE SURVEY

In this chapter provides an overview of background knowledge and presents relevant existing literature for the proposed research problem

A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies This systematic literature review (SLR) is aimed to review the existing research studies on cloud computing security, threats, and challenges. This SLR examined the research studies published between 2010 and 2020 within the popular digital libraries.[1]. The outcomes of this SLR reported seven major security threats to cloud computing services. The results showed that data tampering and leakage were among the highly discussed topics in the chosen literature. Other identified security risks were associated with the data intrusion and data storage in the cloud computing environment. This SLR's results also indicated that consumers' data outsourcing remains a challenge for both CSPs and cloud users. Here in this survey paper identified the block chain as a partnering technology to alleviate security concerns. The SLR findings reveal some suggestions to be carried out in future works to bring data confidentiality, data integrity, and availability

Analytical Review of Data Security in Cloud Computing

Security challenges in services of cloud in the present scenario has explained, security of data is considered as a shared responsibility in cloud computing. As per the cloud service provider model, data security in cloud is divided under two parts: in this the provider will be responsible for the security of the cloud itself whereas data (inserted by the user) security concern will be looked after by the user itself. [2] Data security is one of the major concerns while considering the risk in using or implementing cloud computing. Some of the issues associated with the implementation of cloud computing are lack of data visibility, poor controlling of data, and many more. In this paper discussed the security issues layer wise, so that one can get clear visibility about the security in the cloud computing model.

Privacy and Security Issues in Cloud Computing: A Survey Paper

The reason why cloud computing is gaining in popularity is because of its ability to host applications that enable it to be offered to consumers at the lowest cost and great speed [3]. Among the forms of these applications are scientific applications. Biology: protein structure prediction Cloud computing is used extensively in biology applications. Such as predicting protein structure is an essential task for different types of research in the life sciences. Business and consumer applications: One of the sectors that can benefit the most from cloud computing technologies, and what makes the cloud interesting is the sense of pervasiveness it provides to access services and data. Moreover, cloud computing is the preferred technology for ERP systems, Customer Relationship Management (CRM), and social networks applications.

Threat Specific Security Risk Evaluation in the cloud

Existing security risk evaluation approaches (e.g., asset-based) do not consider specific security requirements of individual cloud computing clients in the security risk evaluation. In this paper, proposed a threat-specific risk evaluation approach that uses various security attributes of the cloud (e.g., vulnerability information, the probability of an attack, and the impact of each attack associated with the identified threat(s)) as well as the client-specific security requirements in the cloud. Our approach allows a security administrator of the cloud provider to make fine-grained decisions for selecting mitigation strategies in order to protect the outsourced computing assets of individual clients based on their specific security needs against specific threats. This is different from the existing asset-based approaches where they do not have the functionalities to provide the security evaluation of the cloud with respect to specific threats. On the other hand, the proposed approach enables security administrators to compute a range of more effective client-specific countermeasures with respect to the importance of security requirements and threats. The main contributions of this paper are summarized as follows: Threat-specific risk evaluation using vulnerability information: An evaluation of the security risk of specific threats to an asset based on security attributes of vulnerabilities in the network. Threat-guided counter measure selection: An optimal countermeasure selection given the pool of different applicable countermeasures, with respect to the specific threat(s) selected. Threat-specific security risk evaluation software tool: A prototype software tool is presented for evaluating the security risk of the cloud taking into account different categories of the threat. Experimental analysis of the proposed approach: We demonstrate the applicability, feasibility, and importance of our proposed approach via simulations. The key novelty of our approach is that it provides at it provides a principled formulation of the problem of evaluating threats in the Cloud by taking into account specific user security requirements. Depending on the nature of the security requirement of the specific Cloud client, some threats can be classified as more relevant than others. In order to differentiate the relevancy of threats, here assigned weighting factors to threats. The weighting factors differentiate the importance of one threat from another. Such differentiation helps in distinguishing the risks posed by each type of threat during security risk evaluation of the cloud. Through the assignment of weighting factors, our threat-based approach ensures that threats not relevant to the satisfaction of a security requirement are not considered in the risk evaluation—even if the risk evaluation indicates that those threats pose risk. This is one of the main features of our approach. However, in asset based approaches, such differentiation between threats is not possible as all threats are assumed to be of equal importance and relevancy, regardless of the security requirement. By considering the security requirement our approach makes it possible to distinguish between different threat types and eliminate risk due to those threats not relevant.[4]

Design of basic process of information security risk assessment in cloud computing environment

In this paper, the design of cloud computing system security risk assessment is to consider the performance degree of assets in each security attribute, and use the security attribute value to describe the asset from the five security attributes of confidentiality, integrity, availability, dependability and auditability. According to the relevant literature research, when the asset in the security attribute value is larger, it means that the asset in the face of malicious attacks, the impact of its specific security attributes on the system is higher. Generally speaking, the common asset identification methods mainly focus on the asset manifestation, business asset identification or information flow. The identification methods mainly include questionnaire survey, data search, on-the-spot investigation and so on. In the process of cloud computing system security risk assessment in this paper, referring to the traditional security attribute standards, we assign cloud computing assets from five aspects: confidentiality, integrity, availability, dependability and auditability. Then a reasonable evaluation standard of cloud computing assets value is established to ensure the accuracy and uniformity of the whole cloud computing system security risk assessment process. The evaluation criteria of cloud computing asset security attributes designedVulnerability identification of cloud computing systems will directly reflect the security status of the system, so vulnerability identification is an important part of cloud computing information security assessment. At present, the commonly used vulnerability detection methods include vulnerability scanning, code scanning, decompiling audit, fuzzy testing, etc

An Analytical Survey for Improving Authentication levels in Cloud Computing

Authentication is the process or action of verifying the identity of a user or process, who or what it declares itself to be. This technology checks the system against user credentials present in the database or in a data authentication server. Identification of the user is done with a user ID and authentication is done when correct credentials are provided. For example, a password that matches with that user ID. study of emotion detection from text pipeline primarily consists of three parts, choosing an emotion model to follow, identifying and aggregating relevant datasets for the emotion model chosen and applying a computational approach to perform the task of accurately determining emotions on given text. Machine learning can be broadly defined as inference of decision rules from a database of labelled training samples for the task of recognizing emotions..Knn and random forest are commonly used as models in this approach. We used a new approach as the emergence of deep learning in the recent past has motivated us to try it out in a variety of domains, including natural language processing (NLP).use a recurrent neural network architecture (LSTM in uni and bidirectional),with dropout and a weighted loss function, trained on word embedding's (GloVe). Note that these word embedding's do not take sentiment into account unlike works such as which attempt to incorporate sentiment features also into the embedding.

III. Methodology

A Systematic Literature Review (SLR) on Cloud Computing Security: Threats and Mitigation Strategies

Considered several papers related to Security issues in between the period of 2010 to 2020.

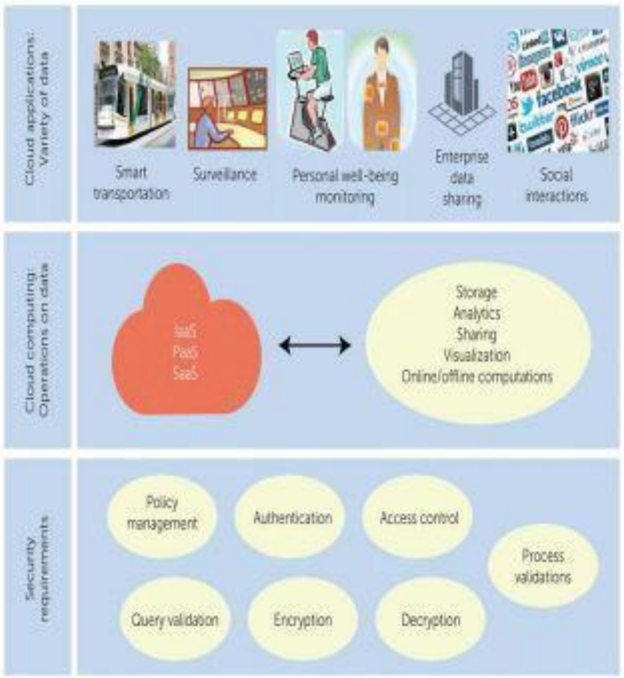
Formulated four research questions as below to cover aim and objectives of SLR [1]

RQ1: What are the cloud computing security threats and their mitigation strategies?

RQ2: What are the security problems that have not been addressed by commercial cloud providers?
RQ3: What are consumers' concerns from cloud computing standards and Policies implementation?
RQ4: What is the role of blockchain technology in the security of cloud data?

Analytical Review of Data Security in Cloud Computing

Initially explained about deployment models of cloud i.e., private,public,hybrid and community ,after that explained about service models and later on identified security requirements of cloud as shown in the [2] figure 3.1 security requirements of a cloud considered



3.1 Security requirements of a cloud [2]

and then focused on different security issues in layers such as Software as a service, platform as a service and Infrastructure as a service as follows [2]. Some common techniques that can be used by the provider or user for securing our data in cloud are as follows:

Firewalls: Firewalls are the core of security for cloud based systems. It is used to protect our data by making the network secure from intruders. It uses a feature called Access Control List" for making the restricted use of applications in cloud environment.

- VPN's (Virtual Private Network) This allows connecting our cloud or private network with other public networks for interchanging the data securely. Various mobiles or tablets can also connect through this network with our cloud system. Finally, we can say VPN allows our private network to connect with remote networks by making the use of internet in secured mode.
- Encryption: This is a process of message encoding in such a way that only authorized persons can get access to the message. It always denies the access of intelligible content from an unauthorized user. Therefore, such techniques can be used in cloud model so that we can secure our data from unauthorized access.
- Masking Is a process of message encoding. We can mask the message before transmitting into a network; this makes the content secure and accessible. In addition to above, some more measures could be taken which makes our data secure in cloud computing, one of them is data storage regulations. Most of the countries are having their own data regulations like storage of data within their country,this allows the development of secured data storage centers. So, one always needs to verify that the country has carried out such legal laws or not [2].

Privacy and Security Issues in Cloud Computing: A Survey Paper

In this privacy and security issues in cloud computing: a survey paper many aspects taken into consideration mentioned about applications of cloud as scientific application,biology and business applications ,considered challenges in cloud storage and threats in cloud computing.Data threats: One of the most important resources for any institution or company is data, so most customers transfer their personal files and data to the cloud [3]. The biggest challenge here is in maintaining data security. Among the problems that occur in data threats is that the customers do not know the location of their data Therefore, the service provider must be available to maintain the security of the main system and thus keep their data safe. Data security features must be available and must be available in the cloud, which are privacy, authorization, integrity, and confidentiality, and correct data processing must be required to avoid the occurrence of a data problem from the cloud service provider, and examples of data security threats are integrity violations, data loss and unauthorized access

Threat Specific Security Risk Evaluation in the cloud

There are many ways of specifying threats. In this paper, considered a well-defined threat model developed by Microsoft's Spoofing, Tampering, Repudiation, Information Disclosure, Denial of service, Elevation of Privilege (STRIDE) threat modeling framework for specifying different types of threats. Using the STRIDE model, proposed a threat-specific risk evaluation approach for cloud computing, this can evaluate the risk associated with each threat category in the STRIDE. This makes it feasible to measure the actual contribution of each threat category to the overall risk assessment more precisely. This approach evaluates the risk of the cloud at three levels: system, subsystem, and component as shown in Figure 3.2. The system risk level deals with the evaluation of risk of all components in the entire Cloud deployment. A subsystem consists of one or more components grouped together because of their contribution to the performance of a particular function or delivery of a given service in the system.

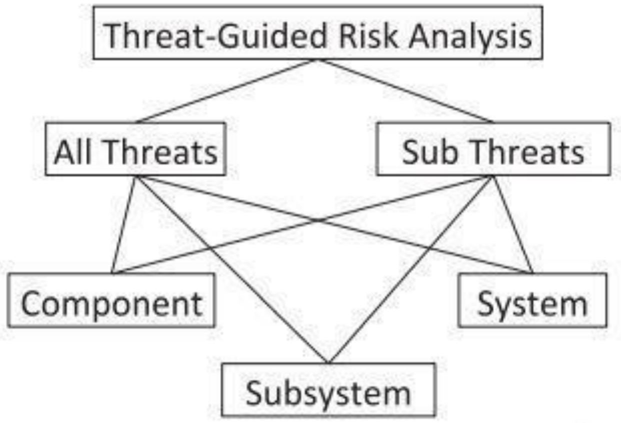


Figure 3.2 Relationship between system components and threats

Design of basic process of information security risk assessment in cloud computing environment

The identification methods mainly include questionnaire survey, data search, on-the-spot investigation and so on. In the process of cloud computing system security risk assessment in this paper, referring to the traditional security attribute standards, assigned cloud computing assets from five aspects: confidentiality, integrity, availability, dependability and auditability. Then a reasonable evaluation standard of cloud computing assets value is established to ensure the accuracy and uniformity of the whole cloud computing system security risk assessment process. The evaluation criteria of cloud computing asset security attributes designed

An Analytical Survey for Improving Authentication levels in Cloud Computing

The new system should provide easy-to-memorize secrets and should also be difficult for hackers to guess. The combination of recall,recognition,biometrics and token-based authentication patterns in this scheme can be used for authentication and survey taken into consideration for identifying frustration levels of users through direct and google forms in order to improvise the authentication levels in cloud computing. Only authenticated users should be given permission to change or remove passwords and this scheme must offer more authentication when it is compared to existing one.

IV TYPE OF DATABASE OR MATERIALS USED IN EXPERIMENTAL SETUP

The **A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies**
Considered several papers related to Security issues in between period of 2010 to 2020 Formulated four research questions as below to cover aim and objectives of SLR
RQ1: What are the cloud computing security threats and their mitigation strategies?
RQ2: What are the security problems that have not been addressed by commercial cloud providers?
RQ3: What are consumers' concerns from cloud computing standards and policies implementation?
RQ4: What is the role of block chain technology in the security of cloud data?
In this paper focused on search keywords, electric sources, reference management tool, and a search process and followed the studies' inclusion and exclusion criteria as listed as in Table 4.1 inclusion and exclusion criteria

Inclusion Criteria	**Exclusion Criteria**
Research Studies that discuss cloud computing	Studies that are published other than the English language
Research Studies that discuss cloud security issues	Papers with unidentified references
Research studies that examine the incidents of data intrusion in the larger organizations	Articles focusing on other than security topics of cloud computing
Research studies that include cloud security concerns mitigation strategies	Duplicated research papers
Research studies that include cloud security models	Papers published before 2010
Studies on Block chain technology with cloud computing services	Studies on block chain technology with other than cloud computing topics

Table 4.1 Inclusion and exclusion criteria

The Quality assessment criteria checklist is designed that depends upon the questions related to problems of the domain area. As given in Table 4.2, these questions aim to sort out the relevant studies to include them in the systematic literature review (SLR).

ID	Quality Assessment Criteria	Feedback Score
Q1	Does the study focus upon the domain's problem area?	Yes = 2, No = 0 and Partially = 1
Q2	Is a study explicitly focusing on cloud security issues?	Yes = 2, No = 0 and Partially = 1
Q3	Is the study about Cloud securely models or approach?	Yes = 2, No = 0 and Partially = 1
Q4	Does the study involve the cloud security mitigation strategy?	Yes = 2, No = 0 and Partially = 1

Table 4.2 Quality assessment criteria checklist

Analytical Review of Data Security in Cloud Computing

Some of the common security concerns associated with SaaS layer are as, No visibility for user data exists in cloud applications, Security concern due to malware attack(s), uncontrolled access to sensitive data, no proper monitoring of data during data transit. Lack of skills in IT staff for managing cloud security, lack of pre-assumption regarding cloud security, no proper framework for cloud regulatory compliance.Security of PaaS layer has been divided into two parts i.e. security of platform itself and security of applications deployed in the platform. The provider of PaaS layer is responsible for securing all the software's present or required during runtime of the application. Some of the key concerns associated with this layer are mentioned as [2] Dependency upon the security of web-hosted development tools and various third party providers, rapid changes in PaaS applications, Storage of data at different platforms may have security breach. Security concern with the development tools provided by the PaaS providers. Finally, one can say that for securing data at the PaaS layer we need the support from third party service providers.

Privacy and Security Issues in Cloud Computing: A Survey Paper

In this paper, Comparison among Public, Private, Hybrid and Community Cloud taken into consideration as shown in Table 4.3 comparison of Deployment models

Parameter/ Type	Public Cloud	Private Cloud	Hybrid Cloud	Community Cloud
Scalability	Very High	Limited	Very High	Limited
Reliability	Moderate	Very High	Medium to High	Very High
Security	Totally Depends on service provider	High class security	Secure	Secure
Performance	Low to medium	Good	Good	Very Good
Cost	Cheaper	High Cost	Costly	Costly
Examples	Amazon EC2,GoogleAppEngine	VMWare,Microsoft,KVM, Xen	IBM,HP,VMWare vCloud,Eucalyptus	SolaS Community Cloud,VMWare

4.3 comparisons of Deployment models

Cloud computing provides many benefits to users and organizations. However, challenges remain to be met in realizing the future generation of cloud computing. A list of possible challenges faced by cloud computing [3] is written below these the challenges, Scalability and flexibility, Resource management and scheduling, Reliability Sustainability, Heterogeneity, Interconnected clouds, Enable resource-constrained devices, Security and privacy, Economics of Cloud Computing ,Application development and delivery ,Data management, Networks, Ease of use apart from the benefits and services offered by cloud computing, there are a number of problems that impede its adoption.

Threats and vulnerabilities are discussed in detail about Data Breaches, Data loss,malicious insiders, Denial of Service, Weak Authentication and Identity Management, Account Hijacking, Denial of Service, Insecure Interfaces and APIs. An attacker can compromise the cloud data protection of many or all customers by exploiting a vulnerability or misconfiguration in a shared platform component, resulting in a data breach.

Threat Specific Security Risk Evaluation in the cloud

A case study: Medical records system taken into consideration for exploring this paper. Calculated risk computation using component impact Equation and exploitability Equation risk for all threats Equation and calculate impact, exploitability, risk for STRIDE threats, and overall component risk for each Virtual Machine (VM). The set of threats T associated with a component n_i is derived from the vulnerabilities of n_i. We, therefore, formulate the set of threats by taking each vulnerability v_i of the component n_i using the function V, and retrieve the threats T posed by each vulnerability vi using the function T. Since there can be an intersection between the threat sets of the vulnerabilities vi, we assume that the function G will generate a unique set of threats associated with the component n_i, i.e., members are not repeated. The possibility of an intersection between some threats may exist because a single threat can be posed by more than one vulnerability

Design of basic process of information security risk assessment in cloud computing environment

As the system vulnerability scanning and analysis software with the largest number of users in the world, Nessus has the characteristics of providing complete system vulnerability scanning service, performing vulnerability scanning and analysis in local / remote control, adjusting operation efficiency by itself, and customizing controls. Combined with Common Vulnerability Scoring System (CVSS), Nessus can score the vulnerability of current cloud computing system from six aspects: confidentiality, integrity, availability, attack path, attack complexity and security authentication

An Analytical Survey for Improving Authentication levels in Cloud Computing

Different methods to access cloud computing and authentication services are: i) Simple password ii) Third party authentication iii) Graphical password iv) Biometric and v) 3D password object. Textual passwords are easy to break and susceptible to dictionary or brute-force attacks. Smaller cloud deployment does not prefer Third party authentication. Graphical passwords have less memory space than textual password and it is based on the idea where users can recall and recognize pictures better than words [7]. The main drawback of using biometrics is it imprudence nature upon a user's personal characteristic. A special scanning device is used to authenticate users, which is not applicable for remote and Internet users. Multiple levels of authentication is not supported by 3D-password. Using one or a mix of the above methods in multi-level authentication, the possibility of breaking a password is reduced. Strict authentication has been achieved by introducing multi-level authentication technique in secure cloud transmission.

V. Results and Discussions

A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies

Data loss due to its leakage is a severe threat to cloud security. Data compromise and modifications occur without keeping the backup copy by altering or deleting the original information. Also, data storage on cloud media has less reliability because insiders and third parties can access the data. In irresponsible media, the companies' offering of cloud service are regarded as fraudulent. Utility based approach can be used to overcome the latter-mentioned challenge by detecting the malicious behavior of users

Analytical Review of Data Security in Cloud Computing

In this paper explored the methods through which we can make the data secure this helps model in the following ways. 1) Protecting important business data from threats. 2) It acts as a guard against internal security threats. 3) And, most important, it prevents the data loss. In analytical review of data security paper, described the various security issues concerned with cloud computing and also discussed that cloud computing is a new concept or a beginning of a new era which has some good benefits for its subscribers. But while making a study it has been identified that to know that security of data is a major concern in cloud computing which may slow down the process of its implementation. After discussing the issues or challenges in cloud based system it is easy for an organization to keep the watch while implementation of cloud system in their respective organization. Finally, discussed about the security challenges at each services (SaaS, PaaS, IaaS) of cloud computing. The paper has been ended by discussing the solutions like Encryption, Masking, VPN and Firewall in cloud enabled systems.

Privacy and Security Issues in Cloud Computing: A Survey Paper

Data privacy is an important aspect for some individuals and organizations because their sensitive data (like health, finance, personal information, etc.). Data privacy is of important value and any breach of privacy can harm them in terms of money and reputation, which may raise privacy concerns. In enterprise computing, data is stored within their organization and under the control of the entire organization. For cloud computing, the data is stored outside the customer's domain by Content Security Policy (CSP). Therefore, there is no guarantee that access to data is limited to authorized persons. Thus, it is preferred to provide a guarantee to the customer that stored data will be confidential and will not be compromised due to security weaknesses. There are six phases of the data life cycle: create, store, use, share, archive and destroy. Data must be secured throughout its life cycle, from its creation to its destruction. We refer to the storage and archiving stages with the sleep data and the usage stage to share the data and we refer to the data sharing stage and the last stage can destroy the data after deletion. These stages are self-explanatory [3].

With the great technological development, the cloud has become a major problem of security and there are many methods of preventing all types of these attacks. However, it is still not strong enough to face these attacks in all their forms. To achieve this, there is a necessity to build standards with all security policies between the CSP and the users. So that there can be a guarantee on data privacy in the cloud computing environment [3]. To detect this malware, a user may notice the following: (i) damages include the user's loss of data and information on the device and the violation of its privacy, or slowing down the operation of the device and creating many problems that lead to the breakdown of the device. (ii) Others, spy, send information that may be confidential, such as credit card numbers or passwords for postal accounts, and some can take pictures of the desktop, and some give full control of the device as if it was in front of it, so it can delete and modify files, and thus it may be harmful Much greater than virus harm. To achieve adequate security, there is a need to build standards with all security policies between the CSP and the users or it could be an assurance of data privacy in a cloud computing environment by using the National Institute of Standards and Technology (NIST) and also by using the data encryption method, which is also an information security requirement [3]

Threat Specific Security Risk Evaluation in the cloud

In this paper, Demonstrated that the existing asset-based risk assessment approaches may result in ineffective risk mitigation strategies because the selected countermeasures a likely to be coarse-grained (i.e., not specific to a threat posed to the security requirements of a specific client of the cloud computing).

The experimental evaluation results demonstrate that effective security solutions vary due to specific threats prioritized by different clients for an application in the cloud. Further, the proposed approach is not limited to only the cloud-based systems, but can easily be adopted to other networked systems and developed a software tool to support the proposed approach.

Design of basic process of information security risk assessment in cloud computing environment

Based on Nessus, referring to the evaluation standards, this paper evaluates the vulnerability of cloud computing system from five aspects: confidentiality, integrity, availability, dependability and auditability. The safety assessment criteria of the design are shown as follows vulnerability assessment in terms of N,P,C, where N stands for It has no impact. P for partially impact and C for complete impact on cloud environment Value -0 index -N description as It has no impact on the confidentiality of cloud computing system similarly value 0.275 for index P has description Some cloud computing data is leaked, but malicious attackers can't get control of cloud computing system. Value 0.660 and index is c for the description all cloud computing data is leaked, and malicious attackers can read all data of cloud computing system Take.

An Analytical Survey for Improving Authentication levels in Cloud Computing

Result for survey on improving authentication levels in cloud computing to cross all these levels of authentication are easy for authenticate user, but it creates user frustration. This user behavior is observed through the data gathering techniques like Google forms, questioners and interview. Respondents for this were working with Cloud Computing environment in Small, Medium and Large Scale industry. Some respondents send their views on different levels of authentication and it is observed that as security levels of Authentication increases user gets frustrated. Graphical representation shows that from level 3 that is graphical password user gets more frustrated and this frustration increase still last level that is 3D password object.

VI. Conclusions

The Systematic literature review paper reviewed the literature on cloud computing topics, including cloud security threats and their mitigation strategies and identified several security risks to cloud computing. Data tampering and leakage is one of the identified risks. Consumers' trustworthiness, data outsourcing, and its associated risks are significant challenges identified. Found one of the solution as using block chain technology and one limitation is it is specific to English literature [1]. Analytical review paper has been ended by discussing the solutions like Encryption, Masking, VPN and Firewall in cloud enabled systems [2]. In Privacy and Security issues in Cloud computing paper, the authors reviewed security and privacy problems, addressed the bottlenecks associated with cloud computing, identified security problems in the layers of cloud computing and loopholes, and how to avoid and control them [3].In threat specific paper, proposed threat-specific risk assessment can evaluate and identify more effective, fine grained countermeasures taking into account user-specified threats. Furthermore, the proposed approach can also be applied in other networked-based computing environments and demonstrated the applicability, feasibility and usability of proposed approach through experimental evaluation via simulations [4]. According to the characteristics of cloud computing systems, analyzes and designs the basic process of cloud computing information security evaluation [5]. This new authentication level will use some encryption techniques like color code generation for every sign in with data masking. This new technique will be completely smooth which will not irritate users for entry in cloud computing environments [6]..

REFERENCES

[1] Bader alouffi, muhammad hasnain, abdullah alharbi, "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies", IEEE ACCESS, Vol.9, Apr 2021.

[2] Mukesh Joshi, Satyam Prakash Sandeep Budhani, Naveen Tewari, "An Analytical review of data security in Cloud Computing", IEEE Explore, Second International Conference on Intelligent Engineering and Management (ICIEM), 2021.

[3] Doaa M. Bamasoud, Rudaina Abdullah, Al- Atheer Salem AL-Dossary, "Privacy and Security Issues in Cloud Computing: A Survey Paper", IEEE Explore, International Conference on Information Technology (ICIT), 2021.

[4] Armstrong Nhlabatsi, Jin B. Hong, Dong Seong Kim, Rachael Fernandez, Alaa Hussein, NooraFetais, and Khaled M. Khan, "Threat-Specific Security Risk Evaluation in the Cloud", IEEE Transactions on cloud computing, Vol. 9, No. 2, Apr-Jun 2021.

[5] Min Huang, "Design of basic process of information security risk assessment in cloud computing environment", IEEE Explore, IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE), 2021. 2021.

[6] Mrs. Devyani Patil, Dr. Nilesh Mahajan, "An Analytical Survey for Improving Authentication levels in Cloud Computing", IEEE ACCESS, International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2021 A. 2001.Macroeconomic variables as common pervasive risk factors and the empirical content of the Arbitrage Pricing Theory. Journal of Empirical finance, 5(3): 221–240.