Review and Evaluation of Security Issues on Cloud Computing

Vikram Gupta, Sarvjit S. Bhatia

Abstract**:** ***With globalization, blends and tremendous amount of electronic data usage, the consumer demands for the innovative techniques of data processing concerns. These issues require enterprises to rethink the strategies for utilizing the resources in an efficient manner. In order to gain and increase a competitive advantage, these enterprises are enforced to move accelerative to be more capable, flexible, efficient, and innovative. To meet the present generation demands for utilizing the resources of Information Technology, Cloud computing emerges the most important paradigm that provides on demand business services globally. In Cloud Computing, resources and applications are available on-demand on the internet. In this context the concept of third party is evolved which provides the services to the end users. By adopting the cloud computing, some social issues like trust, privacy, compliance and legal matters appears. On the adoption of cloud computing in the organizations, the outsourcing of data and trade as well as business applications to a third party causes the issues related to security and privacy critically. As a large amount of depository of the heterogeneous companies are placed in cloud, there is need to have the safety of the cloud environment. With the constant increase in the utility of cloud computing day by day, there must be a genuine effort to review and evaluate the current latest trends and evolutions in security. In this paper, a survey of different cloud computing models, different security risks, counter measures of security in cloud computing that affect the cloud environment in the area of confidentiality, integrity and computing on data are thoroughly reviewed.***

Index Terms**:** ***Cloud computing, CSP, DDoS, DoS, IaaS, PaaS, SaaS.***

I. INTRODUCTION

Cloud computing has been intended to be the most emerging and evolving paradigm in computation that provides IT and on demand business services globally. Cloud computing as per National Institute of Standards and Technology (NIST) is the term explained as, it enables global, very convenient, on-demand access of networks to a shared pool of computing resources that are configurable e.g. networking resources, virtual servers, storage space, computing application services, platform and software related services which can be quickly provisioned with service provider interaction or minimum efforts of management [1]. The resources are present in someone else's premises or network and these are accessed remotely from anywhere by any of the cloud users in cloud infrastructure.

Cloud computing environment provides hardware, software and application resources and services in the data centers and also different amenities to satisfy almost all the requirements of the users over the Internet. In this environment the concept of third party has been evolved in which service provider provides as well as manages all the services. The CSP (Cloud Service Provider) provides the entire services globally over the Internet. The users use these services for their industry, trade and business requirements and after using the required services, pay accordingly as per use. This concept can be considered as a new standard of computing which provides services as per the demands of the users and at a minimal possible cost. The Cloud Computing has three most commonly used service models and four deployment models. Service models are SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service). Deployment models are Public cloud, Private cloud, Community cloud, and Hybrid cloud.

A. Cloud Service Models

1. Software as a Service (SaaS)

In SaaS service model, the CSP provides and deploys software with the related data to the concerned organization and users can easily use the services through the web browsers.

2. Platform as a Service (PaaS)

In PaaS service model, the CSP provides platform for a set of software program services that can be used to solve the specific task for the organizations and users.

3. Infrastructure as a Service (IaaS)

In IaaS service model, the service provider provides infrastructural resources like virtual machines and storage space capabilities to improve the business and trade capabilities of the organizations and users.

B. Deployment Models of Cloud Computing

In cloud computing environment, as per NIST there exists four set of deployment models. These are:

1. Public Cloud – Public cloud means accessible by anybody. Therefore, infrastructure of this type of cloud represents an environment that can be very easily manageable and conveniently accessible publicly by the organizations, users or any other CSP.

2. Private Cloud – Private cloud means accessible privately by the organization for which it is meant. This type of infrastructure of cloud represents an environment that can be used and managed only by the private organization. The cloud model primarily provides consistency in maintaining comparatively greater extent of privacy as well as security in the organizations.

Revised Manuscript Received on 30 January 2019.
***** Correspondence Author

Vikram Gupta*, Research Scholar, Department of CSE, Uttarakhand Technical University, Dehradun, India.
Dr. Sarvjit Singh Bhatia, PG Department of Computer Science, GSSDGS Khalsa College Patiala, India

3. Community Cloud – In community type of cloud computing model, services and resources are managed by almost same community of organizations or others. Similar organizations or communities have common vision as well as target to achieve i.e. security, jurisdiction etc.

4. Hybrid Cloud – In this cloud computing model, two or more than two cloud computing models are combined and attached with each other while all of these combinations remain always a unique entity.

Cloud computing environment is currently the most promising trend to be used in the computations. The new and innovative concept has many prospective advantages as compared to traditional ERP and IT models, apart from these advantages, as per the customers' viewpoint, while adopting cloud computing, there are still some of the considerable problems for the organizations and users to store very important data, deploy and organize applications. The most significant issue in adopting cloud computing is data security concern along with some other issues like trust, privacy, compliance and legal matters [2].

Data security issue has been constantly a main barrier in the emerging field of information technology. Data is distributed and spread in different systems and storage space devices like personal computers, servers, mobile and internet devices like smart phones, sensor networks etc. Also the data is placed and located at many different places throughout the globe over the internet, so it becomes a very serious issue to secure this important data. Data security concern is still the major barrier and is definitely more complex in cloud environment than that of traditional ERP systems. While adopting cloud computing by the enterprises as well as users and making the cloud environment reliable, firstly the concerns related to security should be resolved.

To adopt such a latest technology, the reliability of environment is the basic and the prior necessity to win confidence of users [3]. As the utility of cloud computing is increasing day by day, there must be a genuine effort to review and evaluate the current latest trends and evolutions in security. The challenges for the users are to provide the basic building blocks for the security system i.e. trust, confidentiality, integrity and authenticity etc. This paper not only evaluates and reviews the security and privacy issues but also provides the adequate solutions for these issues.

II. SECURITY REQUIREMENTS FOR CLOUD COMPUTING

A. Data Confidentiality

Data Confidentiality means the ability to share sensitive data and information between specific communities of users. It grants the privileges to the prime owner of data only. It ensures that sensitive data remains invisible and confidential not only to the user but also to the cloud provider. The used data cannot be stolen or reused even though the provider data Centre has been attacked [4], [5]. Data privacy is considered to be a special case of data confidentiality, which means the data owned and retained by owner of data will never allow to be disclosed to any other individual. Data privacy is much easier to maintain than confidentiality as data sharing is not acceptable. Symmetric key algorithm i.e. Data Encryption Standard (DES) is the most simple and effective method for ensuring data privacy by encrypting the data of the user. In this algorithm, the prime user is the owner and holding the cipher key, therefore others are not able to access the actual data. Encrypted backups for personal data are proposed to be managed by some Storage Service Providers. These providers ensure the safety of data from unauthorized means of access even by their own staff about data encryption every time whenever data is transmitted to customer's computer from the server and back. Data privacy solutions are possible not for all applications but for a limited range of applications due to its internal sharing e.g. in hospitals, patient's medical history and records are discussed and shared by doctors, in e-commerce sites customer's information is shared etc.

Data Confidentiality in Cloud Computing can be assured by:

1. **Authentication:** This process gives surety that the authorized users are allocated user login and passwords which are confidential. Biometrics is other type of authentication process.
2. **Authorization:** This process ensures user authorization by employing role-based security methods. The specified staff may be allocated data authorization and access levels.
3. **Access controls**: It ensures access control to be allocated to the specified staff and user may take actions within their limit of roles. User who has access control to read data but not write data, defined controls may be integrated.

B. Data Integrity

Data integrity refers to keep the sensitive data in its original form. Integrity assures that the data stored in database cannot be amended by other than trusted individuals [6]. There are two dimensions of integrity i.e. Completeness and Correctness. Completeness means that the query results of the database are obtained by fetching all records and none of the record is excluded containing the predicate. Whenever a query is exposed on the database, the entire results are ensured to be obtained. Correctness means the query results obtained and generated by the original server are perfect. Therefore when the database is completely and correctly executed by the service provider or process with all matched predicates in query, the integrity is said to be maintained and assured. Data integrity in cloud computing can be assured by:

1. Provable Data Possession (PDP)

PDP technique is used on the remote servers for assuring data integrity in cloud computing. In this technique, client stores data in faithless server can be used to verify that this specific server holds the original data without being retrieved. PDP's working principle is: Client of the server uses probabilistic key generation algorithm and creates a pair of public and secrete matching keys. Public key is sent to the server along with the file for its storage by the client at its location and after that he deletes this file from its local storage. The client challenges and checks the response of the server as a proof of possession for the presence of subset of blocks in that file.

2. Proof of Retrievability (PoR)

POR technique is used to verify and acquire a proof that in cloud computing, the data stored by the user known as cloud storage archive is not amended by the archive therefore assuring data integrity.

The simplest POR technique can be created using a function known as keyed hash function
hk(F).

C. Access Control

Access control is a strategy or technique which generally controls or allows access to any defined system [7]. It can control the access and identify the unauthorized users who are trying to access a system. It may allow to access one application that can have faith in the identity of some other application [8].The application-centric access control model is not practicable in cloud based applications. It is the traditional one for accessing the control, in which every application has recordkeeping of a set of users and the method to manage the users [9]. This model requires large memory storage to store the required details like username and password. Whereas the cloud architecture needs user-centric control in which user has to request any CSP for controlling the access and is having user identification and other required information.

Access control in cloud computing can be assured by:

1. Secure fine-grained access control

In this technique there must be precise specification of the ability of dissimilar users for accessing the data and important information at different security levels. The users may decrypt cipher text only and only when the required attributes and fields fulfill the access control structure, whereas an unauthorized user cannot get permission to access the sensitive data and information[10].

2. Assured data deletion

After data deletion, it must not be accessible to the users permanently. Whenever the data is deleted, the non-recoverability of the data is ensured by assured data deletion. The key related to this data is encrypted with access control mechanism and the cipher text of key is encrypted again, cipher text cannot be decrypted back in accurate form by the private key of the user, and therefore the data is non-recoverable [10].

III. SECURITY ISSUES IN CLOUD COMPUTING

A. Security in service models

SaaS, PaaS and IaaS are the three cloud service models also named as SPI model. The cloud provider is accountable for security and privacy in SaaS model. It is mainly due to the degree and level of abstraction. The model has greater level of integrated functionality but lower level of customer control or extensibility. Conversely, comparatively lower level of abstraction, but higher level of extensibility and higher customer control is provided by PaaS model, whereas IaaS model offers higher range of consumer control over security and privacy than both SaaS and PaaS.

1. SaaS issues

SaaS is a service model that provides service applications online on demand and any time like electronic mail, audio video conference software, and commerce and trade applications etc. SaaS users have lower level of customer control over security out of all the three models of cloud.

2. PaaS Issues

In this service model service provider facilitates a reliable platform for set of software services which can be used to run and solve the programming related tasks for the users without spending money in hardware and software. It provides higher level of extensibility and higher consumer control and depends on reliable and secure network and web browser. There are two software layers of PaaS application security, first layer is the Security of PaaS platform itself provided by runtime engine and the other layer is Security of consumer related applications that are setup on the PaaS platform.

3. IaaS Issues

In IaaS service model, the service provider provides infrastructural kind of resources like virtualized or physical servers, storage media, computer networks, virtual machines etc. to improve the business capabilities of the users. It offers higher range of consumer control over security and privacy than that of both SaaS and PaaS. The users of these services are allowed to use, run and execute any kind of software with complete management and control on almost all allocated resources. The users are accountable for the configuration of security plans correctly, also control and govern the software running in the virtual machines. The probable threats that may be the outcome from creation, editing, observing, agility and communication, the providers of IaaS must carry out considerable efforts for providing the security to rectify and reduce these threats.

B. Security in Cloud Communication

The communication processes in cloud computing means that data or applications transmission between the consumers and Virtual machines (VMs). It generates cloud related challenges for cloud technologies and characteristics.

1. Communication infrastructure sharing

With the characteristic resource pooling, resource sharing of computing, storage and network related infrastructure components is sanctioned [11]. The resource sharing and communication of networking infrastructure modules provide to attacker the cross-tenant attack [12]. IaaS service model is affected by the vulnerability. As it is very difficult to differentiate between activity of the attacker and vulnerability scan of present network, these scans are disallowed by the CSPs. In the similar case IP centered segregation is not applied to network because these resources cannot be related to individual users and are non-statically provisioned. For managing the VMs, the cloud computing users are given an access known to be the super user access. The access capability allows acquiring system IP or MAC addresses of the malicious user and therefore making IaaS as malicious practice of network interfaces. Therefore it may promote different type of security attacks over the present network like sniffing and spoofing etc.

2. Virtualized network

Virtualized networks like other real networks are used to play very important part in the field of communication. Virtualized network means dynamic network and it is a type of logically organized network that has been made over a physical network. These take responsibility for communicating between VMs. The networking of VMs is supported by the network components like routers, bridges, network configurations over the same host. In cloud computing environment, the security challenges are generated by virtualized networks. The whole traffic over virtualized network cannot be observed by the mechanism of security, privacy and protection over the actual real network. Therefore due to such VMs malicious actions, security comes out to be the major concern. Because of the sharing among multiple VMs, there is definite possibility of some attacks like sniffing, spoofing, Denial of Service (DoS) etc.

in virtual networks. In malicious sniffing, spoofing, the cryptographic keys in virtual network become vulnerable to leakage [13].

3. **Misconfiguration of Security**

In the cloud network infrastructure, security configuration plays an importance role to allocate highly secure services for the users [14]. Whereas in contrast to this if misconfiguration occurs, it compromise and negotiate not only the security of users but also applications, complete system too. Consumers on the trust of cloud provider outsource data and applications aiming in mind the proper security of their assets in cloud. But little misconfiguration can act as a breach in the security. The most common and simple misconfiguration occurs while selecting a configuration tool by the administrator for the familiarity with security but it does not cover all security and privacy requirements. The data migration, applications on VMs through real nodes, traffic pattern modifications and their configuration topology can be used to generate diverse security policies. To ensure the cloud security in such case, the configuration should be dynamically managed. Similarly flaw in protocol and session configuration may be exploited to access very important sensitive data of the user by capturing the session.

C. Security in Application programming interface (API) and Web Application

The Web and other applications delivered by CSP are located globally at the cloud and users of the cloud can access it any time universally. Web and cloud applications are not at all attached with particular users. Same applications can be used and gained access at the same time period by some different users. Vulnerabilities reside as a part of not only traditional web applications but the cloud applications too. But due to more devastating vulnerabilities the security solutions for SaaS applications are totally unlike from web applications used traditionally. Security becomes vulnerable concern due to synchronized use of cloud applications by several different users and shared resources and data. The following are the web applications risks and threats identified in a project of 2013:

1. Injection (SQL, OS, and LDAP)
2. Insecure Direct Object References
3. Invalidated Redirects and Forwards
4. Security Misconfiguration
5. Sensitive Data Exposure
6. Using Known Vulnerable Components

These risks are considered to defend the web applications and other user resources. APIs bridge the gap of cloud application services and the user. Therefore APIs security and availability greatly impacts the security of the cloud computing services. Secure APIs directly secures and protects the services of cloud. The CSPs provides and publish APIs for extending the features of own cloud. Insecurity in APIs can give trouble up to great extent for both cloud and its users. APIs vulnerabilities are not sufficient authorization, weak credentials etc. There might be security holes in the applications produced by APIs frequent updates.

IV. COUNTER MEASURES OF SECURITY IN CLOUD COMPUTING

There are various ways that can be expanded on the vulnerable issue of security in cloud computing. Also different techniques are used to take the control of the security to an adequate level.

1. **Architecture security**

Security related challenges of Cloud can be practically controlled by the accomplishment of security assessment. Kelvin Jackson defined an approach known as architecture ontology for the security of cloud computing [15]. This architecture consists of different components of security i.e. Network and Storage space Security, Security API and Access Management. Embedding these types of components provide secure form of cloud computing.

2. **Communication issues**

To provide the security to the network and communication issues, the Cloud Security Alliance (CSA) strategies are used to recommend the mixture of virtualized LANs, IDS, firewalls etc. to protect the outgoing data. These strategies emphasize on consumer data leakage due to a virtualized computer network and the usage of similar infrastructure.

3. **Networking Concept**

3.1 SQLi attacks

Filtering techniques are the techniques that are used for user input to check type of Structured Query Language Injection attacks. For preventing these attacks which dynamically identifies user information inputs, proxy architecture for assumed SQL related control statements and commands are recommended [16].

3.2 XSS attacks

To prevent Cross Site Scripting type of attacks, one of the technology i.e. Active Content Filtering and the other i.e. Content Based Data Leakage Prevention technique has been recommended. These techniques agree to adopt different methods to detect and fix security flaws. These attacks can also be defended on the any type of web browser by adopting a sandbox kind of environment. A practical approach has been proposed which reduces web browsers dependency to identify non-trusted content over the network [17].

3.3 MITM attacks

To prevent Man in the Middle type of attacks in cloud computing, LockBox approach has been adopted with Digital Signature [18]. To defend these attacks, assessing SaaS security, virtualization in the network at end-point, different server and endpoint security processes have also been validated. Security processes implemented in the private network of enterprises are also applied to the private cloud. To implement security features, network topology may have to be changed in the implementation of public cloud.

3.4 DNS Attacks

The Domain Name System threats effects are decreased by the measure (DNSSEC)

Domain Name System Security Extensions but not made to be over and remains some inadequate security cases in which path in between sender source and receiver source gets redirected over certain infected connection.

3.5 Sniffer Attacks

In this attack the data and information i.e. non-encrypted is hacked through network. As an example, within the period of communication, password can be hacked by the attacker which is not appropriately encrypted. Round Trip Time and Address Resolution Protocol sniffing detection platform may be used for detecting malicious system which is executing on a network. To handle this type of attack, encryption method must have to be used by the parties for securing data.

3.6 DoS Attacks

To defend Denial of Service attack, the most popular method is Intrusion Detection System (IDS). For securing these attacks defense federation is used [19]. Every type of cloud has separate IDS that work on information exchange basis. The supportive IDS warn by alerting the entire system if a specific cloud is under attack. The major decision related to honesty of specific cloud is reserved with the help of voting method and the performance is not troubled at all for the system.

3.7 Cookie Poisoning

To defend and avoid this type of attack, regular cookie cleanup scheme can be performed or an encryption technique for cookie data can be implemented.

3.8 DDoS Attack

To defend Distributed Denial of Service attack, logic called as swarm based logic has been proposed. Similarly for protecting the cloud from these attacks, the use of SNORT IDS has been proposed in virtual machines for sniffing incoming and outgoing traffic.

3.9 CAPTCHA Breaking

To defend it, the multiple authentication integration schemes with CAPTCHA code credentials can be the right option i.e. adopted by Google, Facebook, and Tweeter. Different methods to avoid CAPTCHA breaking like variable fonts of the letters, increasing string length, letter overlap etc. can be used.

V. CONCLUSION

To deliver business services on demand globally, the cloud computing has been intended as the emerging and innovative technology which is supporting the third party services. The various researches are going on to address the issues like virtualization, attacks and threats, protection of the data and network security etc. To implement this innovative term Cloud Computing, it is utmost important to obtain user's confidence. The confidence can be achieved only when there is a guaranteed secured system. Data security helps in obtaining the confidentiality, integrity and access control. The counter measures help in implementing the cloud computing which will increase the performance, quality and security in the services that are provided by the CSPs. In this research paper, the overview of requirements, issues and counter measures related to vulnerable concern security has been analyzed. The Review and Evaluation is also performed on each category of the cloud service and deployment model.

REFERENCES

1. Mell P., Grance T., "The nist definition of cloud computing National Institute of Standards and Technology", 2011 Special Publication 800-145
2. Xiao Z., Xiao Y., "Security and privacy in cloud computing IEEE Communications Surveys & Tutorials", 2013 152 843 859 10.1109/SURV.2012.060912.00182 2-s2.0-84877272118
3. R. Latif, H. Abbas, S. Assar, and Q. Ali, "Cloud computing risk assessment: a systematic literature review in Future Information Technology", 2014, pp. 285–295, *Springer*, Berlin, Germany.
4. Hussain Aljafer et al., "A brief overview and an experimental evaluation of data confidentiality measures on the cloud", *Journal of innovation in digital ecosystems*, 2014, pp. 1– 11.
5. Sweta Agrawal and Aakanksha Choubey, "Survey of Fully Homomorphic Encryption and Its Potential to Cloud Computing Security", *In International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 4, Issue 7, 2014, pp.679 – 686.
6. The Cloud Services Measurement Initiative Consortium (CSMIC), "Service Measurement Index Framework Version 2.1", July 2014, Carnegie Mellon University Silicon Valley Moffett Field, CA USA.
7. A.R.Khan, "Access Control in Cloud Computing Environment", *ARPN Journal of Engineering and Applied Sciences*, Vol. 7, no 5, MAY 2012.
8. B.Sosinsky, *Cloud Computing Bible*, Ed.2011, United States of America: Wiley.
9. Y.G.Min, Y.H.Bang, "Cloud Computing Security Issues and Access Control Solutions", *Journal of Security Engineering*, vol.2, 2012.
10. Yong Yu et.al, "Assured Data Deletion with Fine-grained Access Control for Fog-based Industrial Applications", *IEEE Transactions on Industrial Informatics*, Volume: 14, Issue: 10 , Oct. 2018.
11. D. AB. Fernandes, L. FB. Soares, J.V. Gomes, M.M. Freire, P. RM Inácio, "Security issues in cloud environments: a survey", *International Journal of Information Security*, 13 (2) (2014) 113–170.
12. K. Hashizume, D.G. Rosado, E. Fernndez-Medina, E.B. Fernandez, "An analysis of security issues for cloud computing", *J. Internet Services Appl.*, 4 (1) (2013) 1–13.
13. N. Gonzalez, C. Miers, F. Redgolo, M. Simplcio, T. Carvalho, M. Nslund, M. Pourzandi, "A quantitative analysis of current security concerns and solutions for cloud computing", *Journal of Cloud Computing*, 1 (1) (2012) 1–18.
14. Morsy MA, Grundy J, Müller I., "An analysis of the Cloud Computing Security problem", *In Proceedings of APSEC 2010 Cloud Workshop* APSEC, Sydney, Australia.
15. Kevin Jackson, "Secure Cloud Computing: An Architecture Ontology Approach",DataLine,2009, http://sunset.usc.edu/gsaw/gsaw2009/s12b/jackson.pdf
16. Singh N. et al., "SQL Injection Attack Detection & Prevention over Cloud Services", *International Journal of Computer Science and Information Security*, Vol. 14, No. 4, April 2016.
17. Gupta S., Sharma L., "Exploitation of Cross-Site Scripting (XSS) Vulnerability on Real World Web Applications and its Defense", *International Journal of Computer Applications* (0975 – 8887) Volume 60– No.14, December 2012.
18. Yadav S., Jaysawal A., "Prevention of MITM Attacks in Cloud Computing by Lock Box Approach Using Digital Signature", *International Journal of Advanced Research in Computer Science and Software Engineering* Volume 7, Issue 5, May 2017.
19. Ruiping Lua and Kin Choong Yow, "Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network", *IEEE Network*, vol. 25, no. 4, pp. 28-33, 2011.

AUTHORS PROFILE

Vikram Gupta is Associate Professor in PG Department of Computer Science at GSSDGS Khalsa College Patiala and registered Ph.D. scholar in Computer Science & Engineering at Uttarakhand Technical University Dehradun. He has 20 years of work experience in the field of teaching. He is an active member of IAENG. He has published over 8 papers in International and National Journals. His research area is Interfacing of Cloud Computing with ERP.

Dr. Sarvjit Singh Bhatia is a researcher and Senior Faculty in PG Department of Computer Science at GSSDGS Khalsa College Patiala. He has 21 years of work experience in the field of teaching and 10 years of research experience. He has published 15 books and 6 research papers in International and 5 in National journals. His major research area is Implementation of Cloud based ERP in SMEs.