A Review on Various Aspects of the Cloud Security

Komal Jeet Kaur
Sri Guru Granth
Sahib World University,
Fatehgarh Sahib

Sarpreet Singh
Sri Guru Granth
Sahib World University,
Fatehgarh Sahib

ABSTRACT
Cloud Computing plays a vital role in networking. All the applications nowadays shifted over the cloud as its easy availability of resources, sharing of resources, Virtualization makes the cloud computing popular. But with the immense growth of users over the cloud creates security issues that need to be resolved for the storage of data securely.The overall purpose of using the Mutual Authentication Algorithm is to detect the Malicious users over the network and avoiding side channel attack. Malicious user always try to grab the useful information of the authenticated user and makes the system vulnerable. The algorithm discussed in this paper for finding these types of users by using Mutual Authentication. Under this server and client authenticate each other credentials. Many researchers use various methods and techniques for secure the data i.e. AES algorithm, Deffie hellman algorithm, etc. This review paper proposed the algorithm for the authentication of user and provide a control the access by avoiding the untrusted entities.

Keywords
Cloud Computing, Side channel Attack, Mutual Authentication.

1. INTRODUCTION
1.1 Cloud Computing
Cloud Computing is the environment which provides on-demand and convenient access of the network to computing resources like storage, servers, applications, networks and the other services which are efficient. Cloud is a source of centralized data in which a user, who is actually the client in cloud, can retrieve and modifies the stored data. Cloud is a design, where

Cloud Service Provider (CSP) provides services to the user on demand. It means that the user or the client who is using the service of cloud has to pay for whatever he/she is using or being used and served. It is a technique which gives a huge amount of applications under different topologies and each topology gives some new specialized services.[1] The best feature mostly cloud service providers are providing is user can access the cloud from anywhere anytime in the world with the internet connectivity. Cloud Computing can enable a user to access applications and data from any computer to any time since they are stored on a remote server. It also minimize the need for companies to acquire top of the line servers and hardware or hire people to execute them since it is all maintained by a third party.[2]

1.2 Service Models
There are four deployment models in the cloud that provides software , platform, infrastructure as a service from these models infrastructure as a service is the most basic. The higher model abstracts the details of the lower models[1]

- **Software as a Service (SaaS):** This is the capability of using applications which are running on cloud infrastructure. The users access these applications through internet connections. These kinds of clouds offer the implementation of some specific business threads that gives specific cloud capabilities. For E.g. GMAIL, Facebook.
- **Platform as a Service (PaaS):** It gives the computational resources on which services and applications can be host and develop. For E.g. Online Photo Editing, Google Docs, YouTube.
- **Infrastructure as a Service (IaaS):** This is the capability of doing processing, storing and run software which is given to the consumer. It's also referred as the "Resource Code" which provides resources as the services to a user. This work is done by the service provider. For E.g. Host Firewalls.

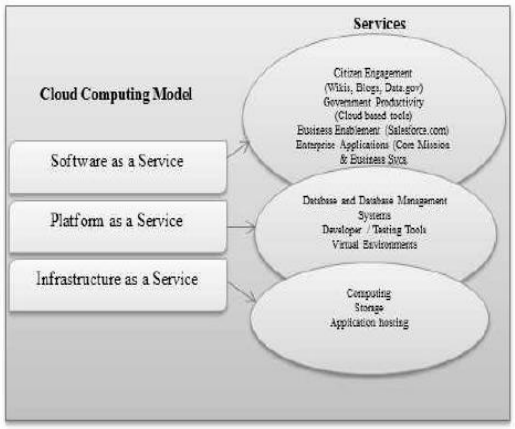

Figure 1.1 Service model of Cloud Computing

1.3 Deployment Models [1]
- **Public Cloud:** In this cloud, resources allocated are publically. Applications in this cloud are on pay-per-use basis. Public clouds can be managed by government organizations or business. For E. g. Sky Drive and Google Drive.
- **Private Cloud:** In this cloud, resources are limited and used within an organization. It is more secure as employees in an organization can access the particular data only. For E. g. Banks.
- **Hybrid Cloud:** In this cloud, there is a combination of both Public and Private cloud. The services within the organization are control by the customer and resources which need to be delivered externally are controlled by the service provider.
- **Community Cloud:** This cloud is used by those organizations which have same concerns like security requirements; mission or policy. This is managed by organizations within a community or by the third party auditor.

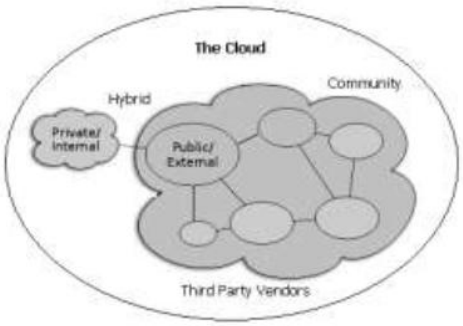

Figure 1.2 Deployment model of cloud computing

1.4 Characteristics of cloud computing[5]

- **On-Demand Self-Service:** It gives the "Graphical User Interface (GUI)" control panel to use the computing resources like Network bandwidth, Additional computers or the user account.
- **Broad Network Access:** It allow users to have the access on computing resources over the networks like the Internet from a wide range of devices such as tablet, PC, laptops.
- **Resource Pooling:** Cloud Computing has pool of resources that are then assigned to various clients according to the requirement..
- **Elasticity:** If the client get more resources from cloud then client or user can scale that resources back by discharging that resources.
- **Measured Services:** The measuring of the resource utilization called measured services. Monitoring the storage, CPU hours, bandwidth usage etc.

1.5 Cloud Computing Security Issues

- **Security issues in Saas :**In Saas provider is responsible for the security measures of the data. The service provider here needs to ensure the user about the security of the storage of data. Hence in this it is difficult for the user to assure about the security when needed[20]. Here the focus is not upon the application portability but to preserve the functionality of security and provide authentication to the applications and achieve the successful data migration.[21]
- **Security issues in Paas :**Paas provides the platform to the user for build their own applications on the top of the platform that are more extensible in case of Saas. Hackers are likely to attack code that are in readable form or easy to guess. The vulnerabilities of cloud are associated with machine to machine service oriented architecture applications.[5]
- **Security issues in Iaas :**In the Iaas has better security control than Saas and Paas. Even though reliability of data depend upon the storage within provider's hardware. Increasing the virtualization of cloud resources and hardware , get the control over the data to the owner of the data. To acquire maximum trust and security features on a cloud resources various technique have to applied.[23]

1.6 Threats in Cloud Computing

There are various types of threats that comprises with the storage of user data. The threats are as follows:

- **Brute Force Attack :** It is a technique in which hacker breaks passwords. The success of attack reliant on powerful computing capability because many possible passwords are needed to a targeted user account until the correct one to access.[21]
- **DOS Attack :** Denial of service attack disrupt the host and network resource to make the legitimate user unable to access the services. It has three categories consumption scarce limited or non renewable resources, destruction or alteration of configuration information and physical destruction alteration of network components.[21]
- **Man in Middle Attack :**In this type of attack, hacker grabs the crucial information, hacker is the third person that sits between client and server. He catches the information of the sender, reads it and then sends towards the receiver.[9]
- **Replay Attack :**In this attack attacker delayed the actual information and attacker copies a stream of messages between two parties and replay the stream to one or more parties.

1.7 Side Channel Attack

Cloud Computing has major issue regarding Security of the data that are stored by the user and transfer over the network from client to server and server to client. Side channel attack is most common attack in Cloud Computing. In this attacker deploy the malicious virtual machine for hacking the user credentials. The virtual machine moniter (VMM) is created to run multiple VM's that host operating system and applications on a single host computer [7]. The Attacker choose a targeted Virtual Machine to attack . First, get all the information and location of the targeted machine. The location of the targeted VM can be measured using NMAP (Network Mapping), Wget (website information) through network probing. Now the attacker finds the close ip address to target VM in the same region. when the malicious VM placed successfully then the attacker get all the useful information from targeted VM [8].

1.8 Mutual Authentication Technique

Mutual Authentication technique used here for isolate the side channel attack in the cloud computing. The main focus of this technique is to detect the malicious VM's. In this server and user authenticate each other's entity and creates the mutual trust before sharing any kind of information. Here client has to prove his/her own identity to the server and requires to prove his originality by providing his identity. Similarly, server has need to do the same [9]. Mutual Authentication is widely used as this helps to minimize the frauds and detect the malicious nodes and provides a secure connection between client and server. With this technique only legitimate users can sharing the data with each other that reduces the attacks and frauds like man in middle attack, data confidentiality etc.

2. LITERATURE REVIEW

Nimmy k., M. Sethumadhavan, et al (2014)[17]proposed scheme for secret sharing key between both the sharing parties for achieving the mutual authentication. In this steganography technique are used for the secure communication that are composed of four stages i.e. registration stage, login, authentication, and password change stage. on the

authentication all furthur messages are encrypted with the session key that are framed between user and server.

Mrudula Sarvabhala, et al (2014)[18] proposed the improved scheme over the nimmy at al scheme also has four stages but try to improve the security by enhancing the parameters. In this researchers proposed low cost steganography authentication scheme that are more secure. The algorithm used here are best for the asymmetric cloud computing. In this scheme load on the server are reduced that results fast response to users at server side. At the client side there are taken off the resource consuming stegano, encryption and decryption operation from client side.

Keiko Hashizume, et al (2013) [10] proposed the analysis of security issues of cloud computing.They worked up upon SPI model i.e. SaaS,PaaS,IaaS) vulnerabilities and threats .As when data is travelled

through internet or involvement of third party is there, at that time we have to ensure the security factors and provide proof of security to organization. Different types of virtualization technologies approach security mechanisms in different ways. Storage, virtualization, and networks are the biggest security concerns in Cloud Computing. They have focused on this distinction, where we consider important to understand these issues. They have made relationship between vulnerabilities and threats to identify what vulnerabilities contribute to the execution of these threats and make the system more robust. Virtual networks are also target for some attacks especially when communicating with remote virtual machines. In this paper they mentioned some counter measures for avoiding the threats i.e. counter measures for accounting or service hijacking, measures for data leakage, measures for data manipulation etc.

Jian Yu, et al(2013) [11] Proposed special issues and service computing of cloud computing. Cloud services include reliability model, service virtualization, and user-centric services. They have proposes a stochastic reliability model of atomic Web services. Some fault tolerance techniques have been proposed using recovery block adaptation to improve the quality of service. Fuzzy requirements and a two-level ranking algorithm are discussed and evaluated.

One of them have proposes a spreadsheet-like programming environment called Mashroom to support situational data integration by non professional users. This paper focus on key directions in this vibrant and rapidly expanding area of research and development. One important issue is that large-scale data centres must offer reliable and secure services with high quality standards to satisfy the on-demand needs of users, to develop service security.

Mohammed A. AlZain, et al (2012) [12]: Proposed the research related to security of single cloud and multi-cloud and solution regarding them. As dealing with single cloud became less popular, due to innovation of “multi-cloud”, “intercloud”, “cloud of cloud”. As its being described that multi-cloud infrastructure requires less security attention as compare to single cloud. Security techniques such as encrypting data using cryptographic hash function for maintaining data integrity and storing data on different servers to overcome the limitation of availability of data. For virtual storage Depsky data model which deals with different cloud provider is a being used with depsky library. In multi-cloud bottom layer is the inner cloud while the secondary layer is the inner cloud i.e. Byzantine protocol which deals with hardware and software faults called as byzantine faults.

Anas BOUA Y AD, et al (2012)[13]: Proposed the security challenges of cloud computing. While adopting the model for cloud computing, we consider the major impact of security issues in that. As due to model related problems such as architecture of cloud model, multi-tenancy, elasticity, it became more complicated to handle out security problems. Virtualization and SOA (service oriented architecture) are used for some of the security problems and on contrary multi-tenancy and isolation is being done for security of SaaS. They investigated the problem from different perspective such as cloud architecture, cloud services, characteristics and derive a detailed specification of the cloud security problem from this analysis. Elasticity engines and APIs (Application program interface) are some interfaces which provides flexible security interfaces.

Mohamed Hamdi (2012) [14]Proposed research of security, storage and networking of cloud computing. When services are delivered through network, security vulnerabilities are there because sometimes due to involvement of third party. Security requirements, security principles, testing mechanism are some of fundamental concepts of cloud discussed in this paper. Some attacks like HTTP Get flood attacks which effect basically resources of web application and then attach URL of that TCP connection flood on port 80 same as HTTP attack . Basis of cloud security techniques, tools, and countermeasures are discussed. The security challenges faced by cloud used and providers have been first highlighted. Attacks that can be conducted against cloud-based services are also reviewed.

Huaglory Tianfield (2012) [15] He proposed different issues regarding security of cloud computing i.e., confidentiality, integrity, availability, trust, and audit and compliance. Responsibility of cloud security by multi-stakeholder according to services is described in detail..Loop holes of public cloud are discussed as in public-cloud computing, we have multiple security issues that need to be addressed in comparison to a private cloud computing scenario. Virtualization and multi-tenancy are the big issues on using cloud computing to provide a better shared resources environment. Summarization of the security issues in cloud computing by a cloud security architecture and taxonomy for security issues in cloud computing are reviewed in this paper.

Wentao Liu(2012) [16] Proposed a paper which illustrates cloud concepts and demonstrates the cloud capabilities such as scalability, elasticity, platform independent, low-cost and reliability. The security problems in the cloud system are discussed. There are many customers who mistrust the security and privacy of cloud computing customers and they do not want to move the data into the cloud platform from the company or private system. These problems have hindered the development of cloud computing and the security issue is the core problem. The cloud computing provider must make variety of measures to protect the security in order to effectively solve these problems.

Joel Gibson, et al (2012) [3]: Proposed the challenges that are faced by the service models in cloud. The three pre dominant models that are present in the cloud computing are mainly infrastructure as service, platform as service and software as service. Infrastructure as service provides with the use of servers, storage and virtualization to enable utility like services for user.

This paper gives clear indication that services should be available at anytime and anywhere so that availability of services do not decrease. Main issue is lack of services and resource availability which leads to inadequacy.

Ravi jhawar, et al (2012) [6]**:** Proposed a approach which describes the implementation techniques of fault tolerance for users and application developers. However there are reliability, availability and security concern s to obtain fault tolerance properties from third party. They have adopted redundancy mechanism to create replicas of different resources for providing better fault tolerance .Long term fault tolerance is being provided to client application by service provider. Working of FTM (fault tolerance manager) is done, however work is not described.

Alexandru Iosup, et al (2010) [10]:Proposed the analysis of cloud computing services for multi-task scientific computing and analysis was being done on some clouds such as Amazon(EC2),GoGrid(GG)etc .Virualization,abstraction,resource level parallelism are factors describes impact on cloud infrastructure. In this paper they have checked the sufficiency of cloud performance that to Multi- Task Computing. They found out that performace for scientific solutions is not good but it provides instant resources and temporarily needed for scientific purpose.

Balachandra Reddy, et al(2009) [11]: Proposed a study regarding service level agreement(SLA) which is a security assurance provided to customers by vendors in order to provoke them for relying on security issues ,as when data travels through internet ,many security concerns arises. Present SLA's of cloud computing is discussed and standardization of SLA's followed by the proposed data security issues is also reviewed. There is a standardized way to prepare SLA in spite of everything to the providers like it has to define several security risks privileged user access ,regulatory compliance and this will also help in looking forward in using cloud computing services for enterprise Security policies and implementation of SLA is also discussed. However, if any customer will missus any cloud service then there is legal action for that too.

3. 3. SCOPE OF STUDY

Cloud computing incorporates on-demand deployment, virtualization, open source software, and Internet delivery of services . The Cloud Computing Architecture which contains on-premise and cloud resources, middleware, , services, and software components, geolocation, the externally visible properties of those and the relationships between them this is also refers as documentation of a system's cloud computing architecture. Due to this mobility increases and employees can access the information anywhere. There is capability of cloud computing to free-up IT workers who may have been occupied to performing factions like , installing ,updates and patches or involving in application support. As good services and benefit of Cloud Computing has to provided but there are security issues which make users unstable about the efficiency, safety and reliability in cloud computing. In this work, we will work on to isolate zombie attack in cloud architecture. The zombie attack will degrades the network performance to large extend. In this work, new technique will proposed which isolate zombie attack and detect malicious VM machines are responsible to trigger zombie attack.

4. CONCLUSION

This survey represents the various issues in the cloud computing. In this paper it is concluded that the different types of attacks affects over the secure storage of data. By using the mutual authentication protocol the data can be secured as it is used for sharing the secret information using the Stegnography proposed by Nimmy et al. There are attacks and threats that makes the system working vulnerable. Here security consider as a major issue. For avoiding the security issues the improved scheme of sharing data and resources needs to be deployed so that data shared securely by authentication of the server and client. Moreover Cloud Computing provided many features but there are security issues which make users unstable about the efficiency, safety and reliability in cloud computing. This paper provides review on mutual authentication for cloud computing. The attacks directly effects over the network performance and on the throughput of the system . So new technique will proposed which isolate these types of attack and detect malicious VM machines that are responsible for such attacks. In the future work there is need to isolate the side channel attack in cloud computing by using mutual authentication protocol

5. REFERENCES

[1] Bhavna Makhija, Vinit kumar gupta, Indrajit Rajput "*Enchanced Data Security in Cloud Computing with Party Auditor*" International journal of advanced Research in Computer Science and Software Engineering ISSN: 2277 128X Vol.- 3 issue no. -2 2013.

[2] Namita N. Pathak, Prof. Meghana Nagori "Enchanced Security for Multi Cloud Storage using AES Algorithm" 2015 International journal of Computer Science and Information Technologies ISSN: 0975-9646 Vol. – 62015

[3] Riddhi Ghevariya, Rajyalakshmi jaiswal *"Secure data forwarding in cloud using AES Algorithm"*International journal of Computer Applications (2395-4396) Vol.-2 issue no.-3 2016.

[4] Rajleen Kaur, Amanpreet Kaur*"A review on evolution of cloud computing its approaches and comparison with Grid computing"*International journal of Advances in Engineering Research ISSN: 2231-5152 Vol.-9 issue no.-4 2016.

[5] Deepak Puthal, B.P Sahoo, Sambit Mishra and Satyabrata Swain *" Cloud Computing Features, Issues and Challanges A Big Picture* " International Conference on Computational Intelligence and Networks 2015.

[6] Deyan Chen, Hong Zhao "*Data Security and Privacy Protection Issues in Cloud Computing*", International Conference on Computer Science and Electronics Engineering IEEE 2012.

[7] W.A. Jansen " Cloud hooks: Security and privacy issues in cloud computing" in 44th Hawaii International Conference on System Sciences IEEE pp. 1-10 2011.

[8] Md Bajlur Rashid, Nazrul Islam, Abdullah Al Mahedi Sabuj, Sajjad Waheed and Mohammad Badrul Alam Miah "*Randomly Encrypted Key Generation Algorithm Against Side Channel Attack in Cloud Computing* " 2nd International Conference on Electrical Engineering and Information and Communication Technology IEEE 2015.

[9] Harpreet Kaur, Usvir Kaur "*Mutual Authentication in Cloud Computing A Review*" International Journal of Computer and Technology ISSN: 2231-2803 Vol. - 34 2016.

[10] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez *"An analysis of security issues for cloud computing"*Journal of internet service and applications springer open journal 2013.

[11] Jian Yu, Quan Z. Sheng, Yanbo Han*"Introduction to special issue on cloud and service computing"*Springer-Verlag London26 April 2013

[12] Mohammed A. AlZain, Eric Pardede, Ben Soh , James A. Thom*"Cloud Computing Security: From Single to Multi-Clouds"*45th Hawaii International Conference 2012.

[13] Anas BOUA Y AD, Asmae BLILA T, Nour el houda MEJHED, Mohammed EL GHAZI "*Cloud computing : security challenges"*Sidi Mohamed Ben Abdellah UniversityIEEE 2012.

[14]Mohamed Hamdi(2012) "*Security of Cloud Computing, Storage, and Networking***"** School of Communication Engineering, Technopark El Ghazala, 2083 Tunisia IEEE 2012.

[15]Huaglory Tianfield(2012) *"Security Issues In Cloud Computing"*International conference On systems, Man, Cybemetics October 14-17, IEEE 2012.

[16]Wentao Liu" *Research on Cloud Computing Security Problem and Strategy"*International Conference on Consumer Electronics, Communications and Networks IEEE 2012.

[17] K.Nimmy, M.Sethumadhavan, "*Novel mutual authenticationprotocol for cloud computing using secret sharing and steganography*", Fifth International Conference on the Applications of Digital Information and Web Technologies feb,2014.

[18] Mrudula Sarvabhatla, M. Giri Chandra, Sekhar Vorugunti "A Secure Mutual Authentication Protocol for Cloud Computing using Secret Sharing and Steganography" Cloud Computing in Emerging Markets International Conference IEEE 2014.

[19] Subashini, S. and V. kavitha (2011) "*A survey on security issues in service delivery models of cloud computing."* journal of Network and Computer Applications, 34(1), pp.1- 11,2011.

[20] Vidyanand Choudary*" Software as a service: Implication for investment in software Development*" 40th Annual Hawaii International Conference on system Sciences, IEEE 2007.

[21] A Seccombe, et al. "*Security guidance for critical areas of focus in cloud computing* "Cloud Security Alliance in Cloud Computing, V2.1, 2009.

[22] Gajek , S., et al *"Breaking and fixing the inline approach"* Proceedings of 4thACM workshop on secure web services , November 2, 2007.

[23] Descher , M., et al. "*Retaining data control to the client in infrastructure clouds"*International Conference on Availability, Reliability and Security, IEEE, pp, 9-16 2009.

[24] Joel Gibson, Darren Eveleigh, Robin Rondeau and Qing Tan*" Benefits and Challenges of Three Cloud Computing Service Models"*4th International conference on Computational aspects of social networks IEEE 2012.

[25] Ravi jhawar, Vincenzo Piuri,Fellow,and Macro santanbrogio*"Fault tolerance management*" System Journal IEEE 2012.

[26] Alexandaru losup, Simon osterman, Nezih yigitbasi, Radhu Prodan, Thomas Fahringer and Dick epama "Performance Analysis of Cloud Computing Services for many tasks Scientific Computing" November 2010

[27] Balachandra Reddy Kandukuri, Ramakrishna Paturiv, Dr. Atanu Rakshit "*Cloud Security Issues*" International conference on Services Computing IEEE 2009.