A Review of Various Security Technique in Cloud

Aradhana Kaurav[1], LD Mahor[2]
[1, 2] Department of Computer Science Engineering
[1, 2] NITM, Gwalior, India

Abstract- *Cloud is a modern age computing paradigm which has potential to bring great benefits to information and Communication Technology (ICT) and ICT enabled business. The term Cloud comes from the image that was frequently used to exhibit the heterogeneous networks and complicated infrastructure. This image was once adopted to describe the numerous aspects of Cloud Computing. In this paper, we goal to determine the safety disorders in cloud computing. Here presenting an evaluation of protection issues in a cloud environment.*

Keywords- cloud computing; security; Authentication

I. INTRODUCTION

Now a days the Cloud Computing technology is rapidly developing and it was receiving attending the huge amount of attention from industrial and scientific communities. Gartner studies [1] considering Cloud Computing is first from the top ten vital technologies and with the best vision from last some years from companies and organizations. Cloud Computing allows easily availability, on-demand network access, global, to a shared pool of configurable computing resources (like as: - servers, storage, services, networks, and applications) and it was quickly facilitate and unconfined with little effort of management or interaction between service provider. Cloud Computing looks like a distributed architecture and a computational paradigm and the main purpose of it is to obtaining the quick, easily data storage, secure, and net computing service, by each and every computing resources considering as a services and supplied on the Internet [2, 3]. The cloud improves the agility, scalability, collaboration; availability, capability of adjusting the fluctuations by demand, fast-tracks the work of development, and offers possibilities for decreasing the cost via efficient and optimized computing [4-7].Cloud Computing is a pools configuration of amount of computing models and technologies like SOA (Service Oriented Architecture), virtualization, utility computing, Web 2.0and some another technologies with reliance on Internet, provides the public business application online via web browsers for satisfying the need of computing to the users, whereas their software and data is saved into the servers [5]. In some concept of Cloud Computing shows technology growing and the marketing term to represents its growing and about the services they provide [6].

There are many benefits and some significant problems for adopting Cloud Computing. One of the significant problems of adoption is security, privacy, legal matters and issues regarding compliance [8]. As we know Cloud Computing shows a newest computing model, there is nice deal of hesitation nearby in what way the security at each and every level (for e.g., application, data levels, network, and host) it will be realized and by what method applications security is moved to

Cloud Computing [9]. That doubt is constantly run to information directors about declaring their security is their number worries with Cloud Computing [10].Security worries related to risky fields like storage of external data, on "public" internet dependency, less control, multi-occupation and combination with internal security. By comparing with traditional technologies, the cloud technology have many unique feature like it is large scale and statistic that properties are belongs to the cloud providers and are totally distributed, and heterogeneous and completely virtualized. Traditional security functions like identity, authorization and authentication, are not so big for clouds in their present method [11].

II. CLOUD SERVICE DELIVERY MODEL

Three typical models and derivative combinations of there are mostly defines the delivery of cloud service. The specific three models are frequently mentioned as "SPI MODEL", where the "SPI" denotes to the Software, Platform and Infrastructure (as service) correspondingly (CSA Security Guidance, 2009).

Software as a Service (SaaS):

These is the ability which is given to the consumer for using the given applications which was executes on the cloud infrastructure and accessible from various client devices through a thin client interface such as web browser. In other words, in this model, a complete application is offered to the customer as a service on demand. A single instance of the service runs on the cloud and multiple end users are services. To the customers side there is not important to show the investment details to servers or the software licenses, while for the supplier side, the costs will be less, therefore only one

application have to be maintained and hosted. So in this model, the customers don't have to manage or control the essential cloud infrastructure, servers, network, storage, operating systems, and as well as the capabilities of even individual application, with the potential exclusion of some limited amount of user-specific application configuration settings. Presently, the SaaS was provided by business organizations like Google, Salesforce, Microsoft, Zoho etc.

Platform as a Service (PaaS):

In the PaaS model, it have a layer of software or the development environment which was encapsulated and provides as a service, on which some another higher stages of service are there. The user have right to create its own applications, which was executes on supplier's infrastructure. Therefore, the capability was provided to the user to utilize it on the cloud infrastructure the user-created applications by programming languages and the resources supported by the supplier (e.g., Java, Python, .Net etc.).Whereas the customer dosen't need to manage or controlling the infrastructure of underlying cloud, servers, network, storage, operating systems but user have the control on the utilized applications and feasibility on the application hosting environment configurations. To connect with controllable and scalable needs of the applications, the PaaS supplier provides a already known combo of the application servers and operating systems, like Linux, Apache, MySql and PHP (LAMP) platform, Ruby, restricted J2EE etc. Several PaaS example are such as: Google's App Engine, Force.com, etc.

Infrastructure as a Service (IaaS):

The IaaS model gives the simple storage and computing abilities as identical services on the network. Storage systems, Servers, data centre space, networking equipment etc. are pooled together and prepared it to handle workloads. The functions provides to the customer are storage, networks, rent processing, and some other fundamental computing resources where the customer is able to deploy and run arbitrary software, which can include operating systems and applications. The customer doesn't need to control or manage the main cloud infrastructure but the user or customer have the control on the, storage, operating systems deployed applications, and probably choose the networking constituents (like :-load balancers , firewalls etc.). Several examples of IaaS are: Amazon, GoGrid, 3 Tera etc. Understanding the relationship and dependencies between these models is critical. The base of all cloud services is IaaS therefore PaaS builds upon IaaS, and SaaS is built on PaaS. Architecture of cloud layer model

III. CLOUD SERVICE DEPLOYMENT AND CONSUMPTION MODEL

Irrespectively to the delivery model utilization (SaaS, PaaS, IaaS) there are four initial paths present by which the cloud services are utilized (CSA Security Guidance, 2009). Cloud combinations are an important part for finding the correct path of cloud for any particular organization.

Public cloud:

These clouds are offered by the particular service supplier and it will provides either multi-tenant (shared) or a single tenant (dedicated) , the environment of operating which provides complete profits and elasticity functioning and the utility/accountability cloud model. The physical infrastructure is generally owned by and managed by the designated service provider and located within the provider's data centers (off premises).

All user uses the one infrastructure and pooled with limited amount of configuration, availability variances and security protections, A benefit of public cloud is that it would big than a enterprise cloud, and also they gives the capability to scale flawlessly when required.

Private cloud:

These clouds are given via any organization or by their designated services and provide operating environment which was single-tenant (dedicated) and have whole benefits and elastic functionality an dutility/accountability model of a cloud. The purpose of private clouds is the address the problem on data security and provides a good control, which was usually missing in a public cloud. Private cloud is of two types:

a) Externally hosted private clouds and
b) on-premise private clouds.

The name shows about the externally hosted private clouds. These clouds are externally hosted and there was a cloud provider. The internal clouds are also known as on premise private cloud which was hosted into private data centre of one's. The model of on- premise private cloud model gives much protection and systematic process, but they have limited features of size as well as of scalability. The IT departments are also wants to earn the operational and capital costs on behalf of physical resources, and this was fits best for that application who wants the whole control and composition of infrastructure and the security.

Hybrid cloud:

This cloud is the combo of private and public cloud which helps in permitting the intransitive exchange of information and probably the compatibility of application and disparate cloud service offerings have portability and suppliers operating the proprietary or standard procedures irrespective to the possession or the location. By the hybrid cloud, provider of services will uses the third party cloud suppliers in the whole or fractional manner, thus there are increment in the flexibility of the computing. The hybrid cloud model so skilled for providing the externally provisioned scale, on-demand. The capability to boost a private cloud by the elements of public cloud will be used to control several unexpected streams of workload.

Managed cloud:

Through a selected service provider the managed clouds are delivered and it provides the operating environment of single-tenant (dedicated) or multi-tenant (shared) and also provides whole benefits and elasticity functionality with the model of utility/accountability to the cloud. The physical infrastructure is owned by and/or physically located in the organizations' data centres with an extension of management and security control planes managed through a provider of selected service. While defining about the services of cloud the concept of the public cloud, private cloud, managed and hybrid clouds will actually represents the management designation and the service accessibility to specific consumers of the services.

While calculating the effect by the services of any specific cloud will contains position of one's security and whole security architecture, and it was important to categorize the resource/service/assets inside into the settings not only its criticality and business impact even also into its location and it was also have to interconnected with management and the security. And by this we can understand that a risk calculation of risk at the particular level is easily performed for deliver it to notions of the cloud (CSA Security Guidance, 2009). In addition, it is important to understand various tradeoffs between the various cloud service models:

- Generally, SaaS provides a large amount of integrated features which was directly built with the lowest quantity of flexibility and with the high security (or may be security responsibility as a service provider).
- PaaS provides low combined functionalities which was designed to allow developers to develop specific applications on the platform, so, it is highly stretchable than SaaS features. This stretchable feature compromises with the security features and abilities.
- The IaaS gives few application-like features and deliver for huge stretch ability although have less security functionalities and abilities elsewhere protecting the themselves their infrastructure, so it wants that the applications, operating systems and contents is managed and protected by customers. The conclusion of it that for security perspective there are mainly three service models, less downcast the stack of cloud service supplier will halts, high security abilities and management and the customer is blame able for executing and managing.

IV. SECURITY ISSUES IN CLOUD

Cloud security is implemented, in part, via third party. They manages and more assertion in traditional expandable arrangements. Although there was not any common cloud computing security standard and there were some other challenges related with this. Several cloud suppliers have their own copyrighted standards and security technologies, and they have opposing security models, which was characterized on their own merits. In the vendor or supplier cloud model, for adopting the customer organizations is ultimately down and confirms the security of it and the cloud connects to their own security polices via requests or element gathering provider risk assessments, due diligence, and assurance activities (CPNI Security Briefing, 2010).

Thus, the security challenges faced by organizations wishing to use cloud services are not radically different from those dependent on their own in-house managed enterprises. The same internal and external threats are present and require risk mitigation or risk acceptance. In the following, we examine the information security challenges that adopting organizations will need to consider, either through assurance activities on the vendor or public cloud providers or directly, through designing and implementing security control in a privately owned cloud. Here we studied some the issues [13]

- The treats beside the properties of information which was present in cloud computing environments.
- The types of attackers and their capability of attacking the cloud.
- The security risks of the cloud, and in which attacks of applicable worries and there preventives.
- Cloud security risks which were developing.
- Cloud security incidents example.

Cloud Security Threats

The threats to information assets residing in the cloud can vary according to the cloud delivery models used by cloud user organizations. There are several types of security threats

to which cloud computing is vulnerable. For cloud customers the view of threats which was arranged according to its confidentiality, integrity and availability (CIA) in the security model and its significance according to the cloud service delivery model [13]

Types of Attackers in Cloud Computing

Several tasks and security threats in the cloud computing is strongly connected to organizations managing in house infrastructure and those involved in traditional outsourcing models. In the all delivery model of cloud computing service the threats are provided by the attacker and they are partitioned into two groups

As we know that the internal and external attacker is different from each other. The capabilities of perform a successful attacks is show the difference between them as a threat to the customers and the supplier similarity environment: weak, strong, substantial, and random (CPNI Security Briefing, 2010). All of these categories are dependent upon the capability to instigate a successful attack, quite different than arranged according to the type of threat in which they are present (i.e., terrorism, spying or criminal):

- Weak :

These kinds of attackers targets a particular supplier of servers or cloud via using new publicly available devices and particular targets. The techniques of this type of attackers are more advance as they effort to customize his attacks by using the explicitly available devices.

- Strong

In this category the well maintained, supported and experienced group of attackers are present. They internally concentrated on the particular target on some specific applications and the user of cloud. This group is good in high profile attacks and area well maintained crime group.

- Substantial

This category of attackers are motivated, the strong attackers is not found easily by the organizations, and by investigative organizations which was good in social crime or in cyber security. Justifying this threat needs good knowledge of attacks and specialized resources for responsible to detect a threat.

• Random

These category of attackers is common type of attacker. These type of attacker uses simple techniques and tools. They randomly scan the internet to find the vulnerable components. They utilize easily available tools and techniques which was found easily on internet.

Cloud Security Risks

The risk on security with every cloud delivery model and were dependent upon a huge amount of issues containing the sensitivity of information assets, cloud architectures and security control involved in a particular cloud environment. In the following we discuss these risks in a general context, except where a specific reference to the cloud delivery model is made.

V. VARIOUS SIDES OF AUTHENTICATION IN CLOUD

Authentication is a wide term that is used for authenticating the individual's identity. In cloud user authentication is required for enhancing security at different levels such as in logging, sending etc.

While logging in authentication can be applied by simply asking security related questions, by inserting captcha, palm images, iris identification etc. by using these options only authenticated users can log in.Other way of providing authentication is providing security to user's name and password. User's name and password can be in encrypted form. At the time of sending messages or receiving messages authentication can also be provided by using encryption algorithms like DES, AES etc.

The cloud-subscriber-person's should be able to authenticate themselves utilizing a typical headquartered protocol, corresponding to SAML, OpenID or Kerberos, to attain access to the cloud utility/service. Alternatively, the cloud-subscriber-user should be ready to transparently log in to the cloud software/carrier as soon as they're authenticated against any method that is a part of single-signal-on federation of techniques. The cloud-subscriber-consumer's account has been already provisioned within the cloud, see use case identification administration – consumer Account Provisioning. In the case of single-signal-on, prior believe relationships have been established (e.G., using depended on crypto keys) among the many identification supplier/authentication service and the cloud purposes/services which might be sharing the federated identification attributes of authenticated customers. (PaaS, SaaS): This scenario illustrates how a cloud-subscriber-user can authenticate in opposition to a cloud-established authentication carrier

making use of the appropriate credentials to attain access to the cloud-established purposes/services. The cloud-subscriber-person provides his/her credentials (e.G., utilizing password tokens or sensible card) to the cloud-provider's authentication carrier interface. The authentication request will get authenticated by means of the authentication service and an right authentication token is issued using a regular-centered protocol (comparable to a SAML authentication announcement). The cloud-subscriber-person then accesses cloud-deployed applications/offerings making use of the authentication token until the authenticated session expires or the person explicitly logs out making use of the authentication service' logout interface. Cloud-subscriber-person authenticates against an authentication carrier (identification provider deployed either in the cloud or within the organization's IT infrastructure) and transparently positive aspects entry to cloud purposes/services with out providing authentication credentials once more, attaining single-sign-on. The cloud-subscriber-user authenticates in opposition to the corporation's authentication service/identification provider, obtains an authentication token (akin to a digitally signed SAML authentication assertion); the cloud-subscriber-person accesses (through net browser) purposes/offerings deployed in the cloud with the authentication token; the authentication sub system furnished by using the cloud-supplier transparently trusts the authentication token and obtains the federated identity attributes for entry manipulate choices. Trust relationship amongst cloud-provider's offerings and the identity supplier is just not headquartered.

DES:

Data Encryption Standard is a symmetric-key block Cipher released through the national Institute of necessities and technological know-how (NIST). At the encryption website, DES takes a 64-bit plaintext and creates a sixty four-bit cipher textual content; at the decryption website, DES takes a 64-bit cipher textual content and creates a sixty four-bit block of plaintext. The same 56-bit cipher secret is used for both encryption and decryption. DES expects two inputs - the plaintext to be encrypted and the key key. The style wherein the plaintext is authorised, and the key association used for encryption and decryption, each check the variety of cipher it's. DES is for that reason a symmetric, sixty four bit block cipher because it makes use of the equal key for both encryption and decryption and best operates on sixty four bit blocks of information at a time5. The key dimension used is fifty six bits, however a 64 bit (or eight-byte) key is clearly input. The least massive little bit of every byte is both used for parity (bizarre for DES) or set arbitrarily and does not develop the security in any way. All blocks are numbered from left to correct which makes the eight bit of every byte the parity bit. Once a undeniable-text message is acquired to be encrypted, it's organized into 64 bit blocks required for enter. If the number of bits in the message shouldn't be evenly divisible by means of 64, then the final block will be padded. Multiple variations and substitutions are integrated in the course of in order to broaden the obstacle of performing a cryptanalysis on the cipher.

AES:

Like DES, AES is a symmetric block cipher. Which means it uses the identical key for each encryption and decryption. Nonetheless, AES is rather one of a kind from DES in a quantity of approaches. The algorithm Rijndael allows for for a sort of block and key sizes and not simply the sixty four and 56 bits of DES' block and key measurement. The block and key can in fact be chosen independently from128,a hundred and sixty,192,224,256 bits and need not be the same. Nonetheless, the AES typical states that the algorithm can best receive a block dimension of 128 bits and a option of three keys -128,192,256 bits. Depending on which variant is used, the name of the regular is modified to AES-128, AES-192 or AES-256 respectively. As good as these variations AES differs from DES in that it's not a feistel structure. Don't forget that in a feistel structure, half of of the information block is used to switch the opposite half of of the data block and then the halves are swapped. On this case the complete data block is processed in parallel during each circular utilizing substitutions and variations.

VI. LITERATURE SURVEY

P. Garbacki et al. [13] by presenting the cloud computing data security the cloud computing system fix the problem of data security. The Algorithm of fully homomorphism encryption is the innovative kind of solution for data security to secure the cloud computing. After some time this was constructed that's way they suggested the consequences of this application. For the furthermore processing or for the recovery of encrypted data there is a innovative security solution is totally interconnected leadingto the huge applicable storage of the cloud computing and the security of data transmission.

Prakash G Let al. [14] suggested about major data security challenge in cloud computing i.e. how to protect the outsourced sensitive data. To talk about these data security challenges, he proposed an effective data encryption for encrypting the sensitive data since sending it to the cloud server. It activates block level data encryption by utilizing 256 bit symmetric key and its rotation. And also the data users can regenerate the given data from the cloud server with the help

of shared secret key. They analyse about the protection of privacy of outsourced data using experiment is carried out the received data on the basis of text files and the variable size. The security and performance analysis shows that the proposed method is highly efficient than existing methods performance.

HanumanthaRaoet al. [15] gives a model of business which uses in the cloud computing for the security of data by utilizing the encryption and decryption algorithms of data. This method said that the cloud service provider is have the priority of storing the data and doing the data encryption/decryption tasks, and these takes extra computational overhead for execution of data in the cloud servers. A important drawback is that there is no control of data on the behalf of data owner that was data owner has completely trusted with cloud service provider and he has more computational overhead.

Swati Paliwal et al. [16] said in the paper about the Attribute Based Encryption (ABE) and the verifiable data decryption techniques for providing the data security in the cloud dependent system. And in the paper the data decryption algorithm designed by them which was based upon the attributes in which user requested for the out sourced encrypted data. This method has an important efficiency disadvantage i.e. supplier of cloud service have the more computational and above storage on the behalf of user attribute verification which contains the subcontracted encrypted data. When hosting the third party auditor the user have to reduce the overheads of the storage, computation, and communication in the cloud server, and by this the efficiency of the cloud data storage is increased.

Shiv Shakti et al. in [17] discussed in the paper about the environment of cloud computing, the six different symmetric key RSA data encryption algorithms how they works and its capability. They have proposed two separate cloud servers; one for data server and other for key cloud server and the data encryption and decryption process at the client side. The main drawback of this method is to maintaining two separate servers for data security in cloud, which creates a more storage and computation overheads.

J.Srivivasi et al. [18] proposes that the cloud Computing is a flexible technology which supports wide-range of applications and the different concepts which was present in cloud computing are searched and written in the paper. Cloud computing is application oriented as well as service oriented, it provides the virtualized resources when needed and it have assessable and billable tools. Because of the low cost and dynamic scaling in cloud computing, it reduces an innovation driver on behalf of small companies, mainly in the emerging world. Security, performance, availability, cost, regulatory requirements, quality of service, Bandwidth, and data limits is the basic issues of the cloud computing and he gives the overview of his survey on these.

VII. CONCLUSION

Any application relying upon an emergent science considers the various possible threats. Such an application with an inability to count on or control the threats may frequently result in failure. The classification of various security threats/problems presented on this paper would most likely improvement the cloud users to make out appropriate alternative and cloud provider vendors to manage such threats efficaciously. Authentication is required for providing enhanced security in cloud environment. In this paper presenting cloud related security issues and authentication for security.

REFERENCES

[1] Gartner Inc Gartner identifies the Top 10 strategic technologies for 2011. Online. Available: http://www.gartner.com/it/page.jsp?id=1454221. Accessed: 15-Jul-2011

[2] Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N (2009) Cloud Computing: A Statistics Aspect of Users. In: First International Conference on Cloud Computing (CloudCom), Beijing, China. Springer Berlin, Heidelberg, pp 347–358

[3] Zhang S, Zhang S, Chen X, Huo X (2010) Cloud Computing Research and Development Trend. In: Second International Conference on Future Networks (ICFN'10), Sanya, Hainan, China. IEEE Computer Society, Washington, DC, USA, pp 93–97

[4] Cloud Security Alliance (2011) Security guidance for critical areas of focus in Cloud Computing V3.0.. Available: https://cloudsecurityalliance.org/guidance/ csaguide.v3.0.pdf

[5] Marinos A, Briscoe G (2009) Community Cloud Computing. In: 1st International Conference on Cloud Computing (CloudCom), Beijing, China. Springer Verlag Berlin, Heidelberg, Centre for the Protection of National Infrastructure (2010) Information Security Briefing 01/2010 Cloud Computing. Available: http://www.cpni.gov.uk/Documents/Publications/2010/2 010007 ISB_cloud_computing.pdf

[6] Khalid A (2010) Cloud Computing: applying issues in Small Business. In: International Conference on Signal Acquisition and Processing (ICSAP'10), pp 278–281

[7] KPMG (2010) From hype to future: KPMG's 2010 Cloud Computing survey.. Available: http://www.techrepublic.com/whitepapers/from-hype-to-futurekpmgs- 2010-cloud-computing-survey/2384291

[8] Rosado DG, Gómez R, Mellado D, Fernández-Medina E (2012) Security analysis in the migration to cloud environments. Future Internet 4(2):469–487

[9] Mather T, Kumaraswamy S, Latif S (2009) Cloud Security and Privacy. O'Reilly Media, Inc., Sebastopol, CA

[10] Li W, Ping L (2009) Trust model to enhance Security and interoperability of Cloud environment. In: Proceedings of the 1st International conference on Cloud Computing. Springer Berlin Heidelberg, Beijing, China, pp 69–79

[11] JaydipSen; "Security and Privacy Issues in Cloud Computing".Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA.

[12] P. Garbacki and V. K. Naik(2007) "Efficient Resource virtualization and sharing strategies for heterogeneous Grid environments," inProc. IFIP/IEEE IMSymp., pp. 40–49.

[13] Prakash G L National Institute of Standards and Technology(2009), The NIST Definition of Cloud Computing, Information Technology Laboratory.

[14] Hanumantha Rao.Gallietc(2013 October)."Data security in cloud using hybrid encryption and decryption" International journal of advanced research in computer science and software engineering vol3.

[15] Swati Paliwal, RavindraGupta(2013 February),"A Review of Some Popular Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 2, ISSN: 2277 128X.

[16] ShivShaktietc(2013 January-Febuary)."Encryption using different techniques:A Review" international journal in Multidisciplinary and academic research (SSIJMAR) vol.2 No.1 -(ISSN 2278-5973).

[17] J.Srinivas, K.VenkataSubba Reddy, Dr.A.MoizQyser (2012 july)" Cloud Computing Basics" International Journal of Advanced Research in Computer and Communication Engineering ,Vol. 1, Issue

[18] Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N (2009) Cloud Computing: A Statistics Aspect of Users. In: First International Conference on Cloud Computing (CloudCom), Beijing, China. Springer Berlin, Heidelberg, pp 347–358