Security Issues and Challenges in Cloud Computing

Shantanu Sarkar, Vimal Kumar Bharadwaj, Priya G
School of Computer Science, VIT University, Vellore

---***---

Abstract – *Cloud computing is a latest technology that has gathered the attention of the IT industry and has revolutionized the computing world. A lot of people using internet are utilizing the features of cloud computing also known as on-demand computing [2]. The usage of this technology is growing exponentially because it helps the users to utilize the services using the shared pool of virtualized resources. It provides scalability, flexibility, reliability, high performance and lower cost. Cloud computing stores information i.e data and its distributed resources in the environment, so the main problem is cloud computing is regarding the security of the data stored in the cloud [1]. A lot of users store personal data in cloud and so it is necessary to secure the data. In this paper an effort is made to shed some light on the security issues faced in cloud computing and provide the cloud users with solutions and some encryption algorithms for securing cloud data*.

Keywords: Cloud computing, SaaS, PaaS, IaaS, Security Issues, Challenges, Encryption

1. INTRODUCTION

Cloud computing is the term used for hosting and delivering services over internet. It is the latest technology in IT industry. This computing is based on internet, where shared resources, software and information can be accessed on demand from any location using computers or any other device [5]. Researchers define cloud computing as "a computing paradigm where a highly capable IT enabled services are provides to the customers through internet technologies."

A cloud is a pool of easily accessible virtualised resources, such as development services, hardware and software. In cloud computing, the user need not store the data on their system as they store the data on cloud or remote server [7]. According to forbes, the leading private cloud company in the world is Slack, with almost 3 million users and $3.8 million valuation. Some other leading cloud companies are Dropbox, Docusign, Stripe and Cloudera.

2. SECURITY ISSUES

Issues in Service Methods:

Software as a Service (SaaS)

Application is utilized as an on request benefit. As it is provided by the internet frequently it diminishes the need to introduce and run the application on the client's own particular physical machine [4]. Exercises that are overseen from focal areas not from every client's webpage, empowering clients to benefit the applications remotely through the web. Application conveyance that commonly is same as a one-to-numerous model (multi-inhabitant engineering) than to a balanced model, including design, cost, cooperating, and administration trademark.

Hackers are increasingly considering no longer most effective breaking into your community but the price of the info they will to find there. If the SaaS supplier is compromised, information encryption is a good proposal to aid guard organizational data; however, it will no longer safeguard in opposition to phishing and malware assaults launched to steal person consumer entry credentials. Encryption should be viewed a "ought to have" technology; however organizations will have to bear in mind that it, with the aid of itself, will not be a panacea.

Despite the fact that SaaS vendors must provide assurance that they're taking steps to mitigate breach dangers, the accountability for protection cannot discontinue there. Corporations that opt for SaaS options ought to additionally share safety responsibility and enforce internal tactics and methods [8]. This involves schooling tactics to teach staff the right way to determine and reply to phishing campaigns, as well as surroundings organization policies round what knowledge should be placed in the cloud and what is higher stored within the firewall. Just due to the fact that an institution can retailer their information within the cloud doesn't mean that they will have to. Organizations have got to have a conversation with a depended on, knowledgeable companion to recognize what (if any) knowledge is high-quality served on premise, in a hybrid atmosphere, or completely "in the cloud" to recognize the business and safety penalties of doing so. Setting insurance policies and fine practices round what data could or may not have to be stored within the cloud can store numerous complications, and abilities knowledge publicity and loss, later.

Platform as a Service (PaaS)

PaaS permits for firms to construct, run and ultimately manage web applications while not the infrastructure that is very often needed [4]. When you contemplate that PaaS is established in the thought of constructing use of shared resources (corresponding to hardware, network, and safety provisions), questions of safety are historically fascinated mission relevant understanding that hackers will acquire throughout Associate in Nursing data breach. If the PaaS customers have Administrator privileges, or shell access to the servers walking their circumstances, any questions of safety might arise if hackers are equipped to realize an unauthorized entry and alter configurations. To boot, safety controls and self-carrier entitlements equipped by suggesting that of the PaaS platform would create an obstacle if not fitly organized. Vendors can got to be ready to give clear insurance policies, educational materials, and cling to business approved satisfactory practices. Once again, security cannot be completely the PaaS provider's responsibility. Once distinctive a PaaS vender, take into consideration these very important disorders before final selection.

Infrastructure as a Service (IaaS)

IaaS provides virtualized computing resources over the web hosted by employing a third party. The protection issues of IaaS are just like the issues of your own data [4]. Are you shielding the important data or intellectual property? Are there compliance standards or service level agreements that are need to be met and the way are these requisites evaluated? Does one need the necessity to audit your cloud supplier to satisfy those service level agreements requisites? What procedure will the cloud marketer take in monitoring? With IaaS environments, management is that the predominant hindrance that you simply just have gotten to alter. Only if you're utilizing a virtualized atmosphere and assets that are not technically yours, weaknesses at intervals the dealer's security will influence your cluster dramatically.

Issues in Deployment Methods:

Public Cloud

In public cloud system 3rd party data centre provide both memory space and computing power for all the application software [9]. Applications, stockpiling, and different assets are made accessible to the overall population by an administration supplier. Open cloud administrations can be free of cost or it might be offered on a compensation for every use show. Here Public Cloud is utilized to give utility registering. Illustrations like Amazon EC2: Amazon datacentres, Xen, EC2 APIs, Google AppEngine: Google server farm, GFS, AppEngine APIs, Batch handling software's: MapReduce, Hadoop.

Private Cloud

Private cloud- In this type of Deployment model you need to set up your own data centre and also bear all the installation & maintenance cost, and have complete control of all your data. Cloud Computing private to an enterprise. Datacenters are not available for rental. Advantages of Private cloud is it maximizes the utilization of computing resources and Provide more security and privacy. Example: Amazon Book Store.

Community Cloud

Cloud framework is shared by different associations it is a particular group that has shared concerns, for example, mission, security necessities, strategy, and consistence. It is kept up by an associations or an outsider. It is a multi-tenant model that is being used by several organization that belong to a particular group which have same computing needs. A community cloud can be internally managed or it can be managed by any third party organization. This is recommend for those organizations which works on joint business or research and requires a centralized data centre.

Hybrid Cloud

Cloud base is made out of two or more mists. A half breed cloud is commonly offered in one of two ways. i) A seller

has a private cloud and structures an association with an open cloud supplier, ii) An open cloud supplier frames an

organization with a merchant that gives private cloud stages [9]. For instance, for general processing venture could chooses to make utilization of outer administrations, and its own server farm's contains its own information Centre's. Half and half cloud display has number of points of interest (advantages) like it is exceedingly adaptable, it gives better security, cost effectiveness and adaptability.

3. SECURITY CHALLENGES IN CLOUD

A few security challenges in cloud are:

Data Protection: In cloud computing the personal data of a user is placed in the hands of a third party, so it is important to ensure the security of data. Data should be encrypted and the data encryption keys should be managed and owned by the client himself.

Contingency Planning: Since the cloud has a centralized repository for storing all important data, so there are risks for securing the data like the data getting breached or compromised. If the data gets disrupted in a cloud the people owning the data will be liable for it. Getting the security accessed from a third party will help in improving the security of the cloud.

Access Control: The cloud should have the policies for access control for ensuring the promotion of the legalized users.

Authentication: All over the internet the data stored in the cloud by the user is accessible to unauthorized people. To ensure the rectitude of data, the user should be able to view the data access logs to ensure that only the authenticated users are able to access the data. The user must ensure that the cloud provider is taking all the security measures for the protection of the data.

4. ENCRYPTION TECHNIQUES

Encryption techniques are used to ensure the security of the cloud and reduce the risk for the users storing their data in cloud. Bi-Directional DNA encryption algorithm [11], is a technique to secure data in the cloud. The drawback of this technique is that it uses only ASCII characters and ignores the non-english users of cloud.

Multilevel Encryption [12], is an encryption technique which is more secure as compared to other techniques. This type of encryption increases the strength of the algorithm by making use of 5 keys to encrypt each character. The values of the keys are not static, every time the encryption of a character is done the value of key changes leaving the intruder confused. Blowfish technique uses a symmetric-key block cipher, it provides good encryption rates. A combination of blowfish and RSA can also be used for security [13], the writer has explained various types of threats that can have an effect on cloud computing and its environment [14]. Various issues of security are explained in the paper which can have a serious affect on the infrastructure of the cloud.

5. CONCLUSION

Cloud computing is a most recent innovation in the field of web innovation and it gives a considerable measure of advantages to its clients. Cloud computing gives powerful execution at a low cost. The use of cloud computing will definitely increment in the forthcoming years. The primary worry in cloud computing is the security of the information put away in the cloud as the information is put away openly and the correct area of information is not known so there is a high danger of the information getting hacked or burglary amid capacity or amid transmission. In this paper, we have talked about the security issues in the service and deployment models of cloud computing, challenges faced during cloud security and the encryption techniques used to improve the security of the cloud.

6. REFERENCES

[1] Rajani Sharma, Rajender Kumar Trivedi “Literature review: Cloud Computing –Security Issues, Solution and Technologies” International Journal of Engineering Research Volume No.3, Issue No.4, pp: 221-225
[2] F. A. Alvi, B.S Choudary, N. Jaferry, E.Pathan “A review on cloud computing security issues & challenges”

[3] Nidal Hassan Hussein, Ahmed Khalid "A survey of Cloud Computing Security challenges and solutions" International Journal of Computer Science and Information Security (IJCSIS),Vol. 14, No. 1, January 2016
[4] Jaspreet Singh, Sugandha Sharma "Review on Cloud Computing Security Issues and Encryption Techniques" 2015 IJEDR | Volume 3, Issue 2 | ISSN: 2321-9939
[5] Jagjit Singh, Gurjit Singh Bhathal "A Review on Storage Security Challenges in Cloud Computing" International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 6, June 2015
[6] Anitha Y "Security Issues in Cloud Computing - A Review" Security Issues in Cloud Computing - A Review
[7] Sharma, Rajeev, and Bright Keswani. "STUDY& ANALYSIS OF CLOUD BASED ERP SERVICES."
[8] Juneja, Gurpreet K. "Use of Modeling Language to deploy applications in clouds."
[9] Chandrahasan, R. Kalaichelvi, S. Shanmuga Priya, and L. Arockiam. "Research Challenges and Security Issues in Cloud Computing." International Journal of Computational Intelligence and Information Security 3 (2012).
[10] Santos, Nuno, Krishna P. Gummadi, and Rodrigo Rodrigues. "Towards trusted cloud computing." Proceedings of the 2009 conference on Hot topics in cloud computing. 2009.
[11] Amit et al. "Enhancing Security in Cloud Computing Using Bi-Directional DNA Encryption Algorithm" Springer 2015
[12] Aized et al. "Encryption Techniques For Cloud Data Confidentiality", International Journal of Grid Distribution Computing Vol.7, No.4 (2014)
[13] Rachna et al. "Secure User Data in Cloud Computing Using Encryption Algorithms", International Journal of Engineering Research and Applications (IJERA), Vol. 3, Issue 4
[14] Dr.A.Padmapriya et al. "Cloud Computing: Security Challenges & Encryption Practices", Volume 3, Issue 3, March 2013
[15] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications (2011), pp. 1-11.
[16] Mohammed A. AlZain, Ben Soh, Eric Pardede, "A Survey on Data Security Issues in Cloud Computing: From Single to Multi-Clouds", JOURNAL OF SOFTWARE, VOL. 8, NO. 5, MAY 2013
[17] Meenu Bhati, Puneet Rani, "Review of Passive Security Measure on Trusted Cloud Computing", International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-3, June 2015.
[18] Ibikunle Ayoleke ," Cloud Computing Security Issues and Challenges", International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011
[19] Navneet Singh Patell," Software as a Service (SaaS): Security issues and Solutions ",International Journal of Computational Engineering Research (IJCER) ISSN (e): 2250 – 3005 || Vol, 04 || Issue, 6 || June – 2014
[20] Deepaklal. K. B, "fuzzy keyword search over encrypted data in multicloud ", Discovery, Volume 21, Number 67, July 3, 2014
[21] " A Reputation Based Trustworthy System For Cloud Environment" in International Journal of pharmacy and Technology,Vol 8,No 3 ,pp No: 16702-16708, September 2016