International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

Security Issues in Cloud Computing

Aayushi Tyagi[1], Aprajita Srivastava[2], Rachna Jain[3]
[1]CSE Department , BVCOE , New Delhi
[2,3]Assistant Professor , CSE Department , BVCOE , New Delhi

***Abstract:* Cloud computing allows companies to keep their resources online. This concept has helped lots of companies by reducing cost and providing flexibility. The biggest concern about cloud computing these days is its security i.ewhether the data put there is secured or not. This is the basic requirement of every company.All the cloud service providers are trying to solve this problem by trying different methods. In this article, the authors will drag your attention towards increasing risks of having security issues and measures that can be taken to prevent them and also the standards of security.**

Keyword: Cloud computing , IT , security , privacy , RSA algorithm

I. INTRODUCTION

Cloud computing is a delivery model which allows organizations to keep their resources online where they can be accessed by anyone. Cloud service providers provide platforms where users create their own web services. They rent out what company requires by taking care of hardware and software and their costs. With changing time, these service providers have evolved so that they can process with faster speed and provide more security. There are two major types of cloud computing, private cloud computing, and public cloud computing. In public cloud computing, many companies share the same infrastructure and this is given a term known as multitenant architectures whereas private cloud computing is considered as a proprietary architecture which provides services to a limited number of people. It offers 3 types of services:i) *Software as a Service (SaaS)* - It allows the users to applications available on the cloud instead of using applications of their own computer.ii) *Platform as a Service (PaaS)* - It manages lower level applications such as storage space available with the software i.e. in running of applications.iii) *Infrastructure as a service (IaaS)* -It is responsible for management of runtime, data, and applications. [9].Top Benefits of Cloud computing are as follows:i) *Speed* - In just a few mouse clicks you can get possibly all the information you require. It's extremely fast and time saving giving a lot of scope in the future to this much recent technological tool.ii) *Cost* - It eases out the user on renting out or buying hardware and software by proving it effectively at a preferably minor cost.iii) *Global scale* - It works at a global scale and is shared by people all over the world. Access rights are granted to the user.iv) *Performance* - The cloud servers are updated regularly and run on a secure and fast network of capable data centers all over the world. V) *Productivity* - For a cloud to produce desired results it must efficiently set up software, hardware and privacy should be checked on especially.vi) *Reliability* - It makes data backups a lot easier and doesn't let the client's data get lost anywhere because of very good disaster recovery. [5]Now a day's cloud has following main features: [8]

A. Resilience
B. Pay as you go
C. Multitenancy
D. Massive scalability
E. Self-provisioning of resources

II. RELATED WORK

SAML Technical Overview[1], 2008 was all of the security standard based on XML. The website discussed it in depth and provides a whole lot of information on the same. Ertaul et al in 2010[2] explained the services in cloud computing in a concise manner. It talked about various issues as well but focuses on the security standards like SAML, OpenID, OAuth, SSL/TLS. Hamlen et al in 2012 [3] provides an overview of cloud, its working and all the security issues including third party interferences which affect it. Goel et al in 2012[4] gives information about cloud security and privacy. It made the reader familiar with all the possible threats affecting your cloud system. Kadam et al in 2012[5] talked of cloud computing as a whole and lays emphasis on cloud problems but encryption as a strong tool to overpower security problems. The RSA algorithm was proposed and explained with a detailed flowchart. Dimitrios et al in 2012[6] talked about the issues that affect cloud computing nowadays, the prime ones being privacy, multi-tenancy, and availability. These issues and much more were researched in depth by the author. Hashizume et al in 2013[7] identified the various security issues encountered in the cloud environment, some of these being confidentiality, integrity, multi tenancy. Also, emphaisis was given on encryption as a secure technique to implement greater security measures. Jain et al in

2016[8] primarily focused on the privacy schemes that can help protect data in a more effective way. Kaur et al in 2017[9] gave all information on the security issues surrounding cloud computing, the author also gave a few solutions to tackle the same. OAuth - What does OAuth mean[10], told about this security standard in detail. Security issues in cloud computing by Microsoft Azure[11], explained all about the cloud , its types, services and also its brilliant characteristics that make it stand out.

III. VARIOUS SECURITY THREATS IN CLOUD COMPUTING

A. Data Confidentiality and Privacy

It states that sensitive data is not shared with persons who are not authorized, or who are unaware of various processes involved [7]. This is a huge threat in the branch of cloud computing and by deploying data to a cloud network we jeopardize the privacy of data to a huge extent [2]. It emphasizes the need to secure a user's data by applying various authentication measures. One of these is electronic authorization and if the cloud has no such security measures put up there is a high risk of a breach in privacy of the user. The user does not want every bit of data to be accessed by the service provider so some of it is kept confidential [2].

B. Multi-Tenancy

As an approach, it makes sharing of resources efficient but also poses a threat [2]. It can be referred as the synonym to multitasking. Multiple amounts of data are kept reserved for different tasks and make this prone to a major leakage of information. All the data is reused at some point and this is both a boon as well as a bane to the data vendors [1].

C. Data Integrity

Integrity is the authorization of data only by trusted parties and associates. This ensures data is protected on a much higher security level [6]. Organizations see authentication and authorization when dealing with security [2]. Cloud model maintains data integrity. The software is also integrated and its access is in the hands of the cloud administrator only. Everything from the hardware to the software needs to be defended and that is when it would achieve optimum accuracy [7].

D. Availability and Accessibility

When any authorized personnel try to access the cloud data it is termed accessible and it is made available if it exists in the cloud storage. Accessing applications is easier when you operate from your laptop or your mobile phone. The biggest threats in the area include malware, unstable and insecure Wi-Fi networks and hacking among others [1].The system works even when the security is under attack and all the operations are performed to the achievable limit. Resources and network play a big role in setting up an efficient cloud platform [2].

IV. CLOUD SECURITY THROUGH ENCRYPTION

Encryption is the technique we apply to protect our data from being misused by either some organization or by an untrusted user[1]. We achieve encryption by the *RSA algorithm.* It encrypts the information we are deploying to the cloud network. The concept undermining this algorithm is a digital login or signature. Once a particular message is transferred on the cloud we digitally check for a match in the credentials to allow user access. The user group at the receiving end is sure about the authenticity of the file if the digital signature matches. It improves the security in the cloud. It is a rare kind of algorithm which makes use of both public key and private key. The RSA algorithm works on the public key and digital login. In stage 1, digital signature makes sure the data is reduced to a small function which can be stored as a hash function and transferred over cloud quite easily. The hash function can be termed as the message signal. After that, the private key is used to encrypt and secure the message signal that is received. In the next stage, a digital signature is generated. The software applied for the RSA algorithm then decrypts as this is possibly the last stage. Decryption of message takes place by using the public as well as the private key. The digital signature is generated and encryption is successful. Digitally transmitting data can be a tough job with a number of problems like forgery, failed transactions but still, this is the correct way to secure data in the cloud environment. RSA finds use in e-commerce and it is highly beneficial in many other complex fields as well. It basically uses 3 steps - encryption and decryption being the two foremost ones and these two are achieved by the generation of keys (public and private) [3].

A. The Steps involved in RSA Algorithm are:

1) Data is present and needs to be generated to the cloud environment.
2) Data converted to a hash function which is a few lines.
3) Hash function generates a message signal to push the data further.
4) The message signal is encrypted by making use of a private key.

5) Finally, a digital signature is achieved using both public and private keys.

V. VARIOUS STANDARDS OF SECURITY IN CLOUD COMPUTING

A. Security Assertion Markup Language (SAML)

SAML is an XML-based format which provides a framework for exchanging security information between online business partners. This format is used for requesting security information. It was developed by the OASIS Security Services Technical Committee. It uses XML to contain user authentication and information. It defines three types of rules, user, identity provider, service provider. SAML has many kinds of components such as assertions, protocols, bindings, and profiles. SAML uses HTTP and SOAP as its communications protocol. This means that SAML protocol messages are transported between participants by these protocols [4][10].

B. OpenID

It is a faster and safe way to log in to websites. It is a decentralized, open protocol for user authentication control. The first OpenID authentication protocol was made by Brad Fitzpatrick in the year 2005. Users are allowed to log onto many services with the help of the same password. OpenID can be used instead of the common log-in process (giving username and a password), allowing users to log in only one time with your password which is only seen by your identity provider, no other website can see your password, and that provider confirms your identity to the websites you visit, so your identity is never compromised. An OpenID remains in the form of a URL. The OpenID does not depend on a central authority to authorize user's identity[4][13][14].

C. SSL/TLS

Transport Layer Security (TLS) and Secure Sockets Layer (SSL), commonly known as SSL are secure protocols designed to authenticate server and clients and then encrypt the messages to provide security for communications over TCP/IP. It was developed by Netscape Communications Corporation to protect the transactions over the WWW (World Wide Web) in 1994. Secure HTTP, or HTTPS, is a familiar application of SSL. SSL provides endpoint authorization and data privacy by using cryptography. SSL confine all communication between the server and client machine with the help of its four layers of protocols which are record layer, alert protocol, handshake protocol and change cipher spec protocol[4][12].

D. Open Authentication (OAuth)

OAuth can be defined as open authorization protocol that allows other services to use the user's account information, example Facebook, Google without revealing the user's password. It was started by Chris Messina and Blaine Cook. It can be said that it works like the client-server system, where the website that stores user's information act as a server and the website using its data act as the client. Basically, it helps in interacting and publishing the protected data. It is found that OAuth Core 1.0 does not provide many important features, like language support, a standard definition of resource access, signing algorithms, OpenID integration, etc. [4][11].

VI. CONCLUSION

Cloud computing has many benefits in comparison to the drawbacks. In this paper, we have started with introducing what work the cloud does, what areas it works on and what are the security issues faced in the field of cloud computing. Finally, we have thrown light upon some of the ways to achieve greater security. Security is lacking on a number of parameters like confidentiality, privacy, and integrity to name a few. We discussed the RSA algorithm, in brief, it works on encryption protocol to overcome these security issues. At last, we looked at the security standards that exist in this field. Cloud computing has the potential to lead the market in future and if these problems are tackled in the right way it surely will.

REFERENCES

[1] Hashizume, Keiko, et al. "An analysis of security issues for cloud computing." Journal of Internet Services and Applications 4.1 (2013): 5.
[2] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." Future Generation computer systems 28.3 (2012): 583-592.
[3] Kadam, Kalyani D., Sonia K. Gajre, and R. L. Paikrao. "Security issues in cloud computing." National Conference on Innovative Paradigms in Engineering and Technology (NCIPET-2012), Proceedings published by International Journal of Computer Applications (IJCA). 2012.
[4] Ertaul, Levent, Sarika Singhal, and Gökay Saldamli. "Security Challenges in Cloud Computing." Security and Management. 2010.
[5] What is cloud computing? - A beginner’s guide https://azure.microsoft.com/en-in/overview/what-is-cloud-computing
[6] Kaur, Supreet, and Amanpreet Singh. "Security issues in Cloud Computing." International Education and Research Journal 3.5 (2017).
[7] Goel, Abhishek, and Shikha Goel. "Security Issues in cloud computing." International Journal of Application or Innovation in Engineering & Management (IJAIEM) 1.4 (2012): 529-551.

[8] Hamlen, Kevin, et al. "Security issues for cloud computing." Optimizing Information Security and Advancing Privacy Assurance: New Technologies: New Technologies 150 (2012).

[9] Jain, R., S. Madan, and B. Garg. "Privacy sustainability scheme in cloud environment." CSI transactions on ICT 4.2-4 (2016): 123-128.

[10] Security Assertion Markup Language (SAML) V2.0 Technical Overview , 25 March 2008. Document ID saml-authn-context-2.0-os. See http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.htm

[11] OAuth - What does OAuth mean? https://www.techopedia.com/definition/26694/oauth

[12] SSL/TSL-What does it mean? https://technet.microsoft.com/en-us/library/cc784450(v=ws.10).aspx

[13] What does open Id mean? https://wordpress.org/plugins/openid

[14] OpenId definition? https://connect2id.com/learn/openid-connect