Proceedings of the Sixth International Conference on Inventive Computation Technologies [ICICT 2021]
IEEE Xplore Part Number: CFP21F70-ART; ISBN: 978-1-7281-8501-9

Cloud Computing Security Challenges, Threats and Vulnerabilities

Manoj Kumar Sasubilli
GITAM Institute of Management
GITAM (Deemed to be University)
Gandhi Nagar, Rushikonda,
Visakhapatnam, India.

Venkateswarlu R
GITAM Institute of Management
GITAM (Deemed to be University)
Gandhi Nagar, Rushikonda,
Visakhapatnam, India.

***Abstract*—Cloud computing has grown to become an integral part of present as well as future information technologies. This technology has been designed to be used with internet by providing features such as information storage, remote access, etc. Cloud computing has been proved as an effective tool for all the provided services but it also comes with various types of threats. Over the years of its development, different fire attacks and data theft has been reported as a crucial factor since the data stored in the cloud by an organization or an individual user is basically confidential and sensitive. These data are illegally accessed by many hackers and further it will be used to fire attack the user. This paper mainly aims to highlight such attacks and provide suggestions for sorting the data breaching issues.**

Keywords—Cloud computing, security challenges, vulnerabilities in cloud computing, cyber attacks.

I. INTRODUCTION

Data storage has always been a place for useful information shortage. Even with large scale data storage devices, the space will not be adequate to store the existing huge amount of information. Cloud computing is basically considered as an internet-centric open standard model. This model is full of different types of services which include both hardware and software. The service providers do not require any high management efforts for provision and maintenance of these services. The term "cloud computing" aims to enhance the capabilities of high power computing systems. It also aims to reduce the price by hiking its efficiency as well as performance. Though the benefits and facilities provided are very much effective, the available technical barriers might stop cloud computing from being a ubiquitous service. One of the main constituents of the cloud computing is security and it also remains as the most significant concern of the system. It usually suffers from various types of security concerns and attacks like malicious codes. In addition, various new concerns like storage and moving of data through the cloud is a big problem for the user. The possibility of locating in a different place with different regulations adds a lot to this problem. It is also very much important for a cloud service provider to confirm the usability and availability of their services. There are various reasons that could affect the availability and the accessibility of the computing resources like service denial or natural/unnatural disasters. Data privacy is one of the prime concerns associated with the security of cloud computing as the data must be protected from any third party, which is frequently reported by the users. Since, cloud computing is used for sharing data, data theft is remaining as very common and big risk, which is available for both users and service providers.

Cloud computing uses different ways to meet the requirements of the consumer and one of these ways is virtualization. Though virtualization is brought in application to benefit the consumer but it has its own disadvantages like issues related to the isolation of the data and communication among the viral machines. Through cloud computing, cyber-attacks are more likely to happen. Lot of these cyber-crime belongs to the most common as well as potential encounters which has taken place in the wider internet like malicious insider, DDOS attack, nefarious use and abuse of cloud computing, programming interface of insecure application, etc. It is important for the service providers who deal in the field of cloud computing to enhance their cyber security and access control system to their resources in order to keep a record of who dealt with them. This paper presents the list of the problems related to challenges which falls over the security of the information. This paper also presents the three different categories which are threats, attacks and other challenges over the security.

Currently, the data shows the involvement of cloud computing in approximately everyone's life. It is because of the little or no cost services delivery for the storage spaces and the application. Most of the users uses these services on a regular basis. It can be easily explained with the example of email system which is used for exchanging information in forms of text, images videos, etc.; on demand subscription services; various social networking sites and collaboration tools for working along with the people in real time and over same document. The involvement of services of cloud computing does not end here as it is also brought in application within the various types of businesses and it also provides these services on rent to prevent a one-time investment of the companies. Undoubtedly, these services have changed our lives on a great extent but the issues of security which comes along with it makes the user vulnerable to many types of available cyber-crimes that can be heard and seen on daily basis. There are many techniques and methods used by the hackers for accessing cloud without being legally authorized and these criminals also create disruption the services associated with the cloud for attaining their targeted objectives. There is possibility that the services of cloud computing gets tricked by the hackers as they make their unauthorized entrance to the data as a valid entrance and thus gains control over access of the data stored in the cloud.

After gaining the access to enter illegally to the data, the hackers locate the place where the data is stored and then steal those data which might be very sensitive. As per the data which were provided by the Data Loss DB, 1047 data theft has been reported in just 1st 9 months of the year 2012. This number was 1041 in the year 2011. The 2 victims who suffered from this criminal activity were Stratfor and Eplison. In this data theft, accidently Eplison exposed millions of name of the customer with their emails from the database. A similar case happened with Stratfor where he was cyber-robbed with 860000 user names with passwords and 75000 credit card numbers. It is also possible that after

2021 6th International Conference on Inventive Computation Technologies (ICICT) | 978-1-7281-8501-9/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICICT50816.2021.9358709

hacking the data, the data could be misused for fire attacking against the same/different network user. In a recent incident, a server was bought on rent via EC2 service of Amazon and was used to fire attack the network of Sony Play Station. This is evident of the need of a proper understanding of the threats linked with the use of cloud security for providing additional security services to the user.

There are various advantages of the cloud such as cloud as well as online storage, remotely accessing the documents, etc. There are various models for providing services which are by the cloud computing. These models are mentioned below:

1. Software-As-Service: This model enables the user to remotely or directly accessing the software of the application and the database.

2. Platform-As-Service: In this computing model, the user is provided with different features in order to access the OS, web servers and the execution environment of the programming language.

3. Infrastructure-As-Service: This model is providing the user with virtual or physical machine.

It is evident because of many incidents that almost all the technologies have their loopholes which must be sorted for ensuring an error free communication with high efficiency. There are various types of security loopholes that are associated with the cloud computing in relation to cyber-attacks and storage of data. This paper presents few of the major problems which might hamper the cloud's services. Section III explains Security issues based on their categories. In the last section conclusion is presented. As businesses are moving on to the cloud, enormous amount of critical data are storing into the cloud data centers, as a result, many queries on security, privacy, reliability are coming up by cloud users and business organizations.

II. SECURITY ISSUES IN CLOUD COMPUTING

1. Software-as-a-service (SaaS)

Through this model, the service provider of cloud provides database and application software access. SaaS is a software with high demands. The problems which are faced with this application is with its security which are naturally centered revolving around the access and the stored information as almost all the models which are responsible for the data sharing security issues leave these 2 issues over the costumers of the SaaS. It is very much important and also the responsibility of every user to know the type of information they share with the cloud and who else is authorized to use that information. The users must know the level of protection they are provided with by the service provider.

Considering the provider of the SaaS's role is very significant in relation to the access of the information and the processes of the organization. Advancement like rising of golden eye ransom ware and Xcode ghost highlights that the attackers knows the cloud and software provider's value and consider them as a vector through which they can fire attack over the larger assets. This is resulting in increase of the focus of these attackers over this type of potential vulnerability. To protect the information, the user must be alert and scrutinize the security programs of the provider of cloud computation.

Top 10 security issues of applications of cloud which are faced with SaaS are mentioned below:

i. The applications of cloud do not provide a clear visible picture about what data is within it.

ii. Data theft from a cloud application through malicious actor

iii. The control in respect the accessibility of the sensitive data is incomplete

iv. Inability in reference of monitoring the data in transferring from/to cloud applications.

v. Cloud applications being provisioned outside of IT visibility (e.g., shadow IT)

vi. For managing the issues and development of security of the applications of cloud, the available staffs are not sufficient or skilled.

vii. Inability in reference of preventing malicious inside misuse of data or data theft.

viii. High tech fire attacks and threats against providers.

ix. Inability in reference of assessing the operation's security of the cloud application

x. Inability in reference of maintaining regulatory compliance.

2. Infrastructure-as-a-service(IaaS)

IaaS is a way of providing the user with virtual or physical machines like Hyper-V or virtual box which operate virtual machine. Protection is data is not an easy task in IaaS. As the responsibilities of the user increases to OS, network traffic as well as applications, more and more threats sums up. Organizations should not delay in considering the evolutions in attacks that has extended beyond the data which is the center of the risk associated with the IaaS. Lately, many malicious actors has conducted computing resources' hostile takeover for mining crypto currency. These resources are then further used as an virtual weapon to attack vector against other elements of the infrastructure of the enterprise and also against the third party.

When an infrastructure is built in the cloud, assessing your abilities is important in order for preventing the data theft and accessing of control. Hardening and securing orchestration tool, tracking the modification of the resources for identifying abnormal behaviors, addition of network analysing of both east – west and north to south traffic as a potential signal and to determine who is permitted to enter data into it are the ways which enhancing as standard measures to protect the infrastructure of cloud deployments at scale.

"Below are the Top 10 cloud security issues experienced with infrastructure-as-a-service (IaaS)

i. Cloud workloads and accounts being created outside of IT visibility (e.g., shadow IT)

ii. Incomplete control over who can access sensitive data

iii. Data theft hosted in cloud infrastructure by malicious actor

iv. Lack of staff with the skills to secure cloud infrastructure

v. Lack of visibility into what data is in the cloud

vi. Inability to prevent malicious insider theft or misuse of information

vii. Lack of consistent security controls over multi-cloud and on-premises environments

viii. Advanced threats and attacks against cloud infrastructure

ix. Inability to monitor cloud workload systems and applications for vulnerabilities

x. Lateral spread of an attack from one cloud workload to another"

3. Platform-as-a-service (PaaS)

The provider of this model avails the user with features for accessing the OS, web servers and execution environment of programming language. This model acts as bridge between IaaS and SaaS.

As per the NIST, the model of the cloud comprises of 4 core deployment models such as hybrid cloud, private cloud, community cloud and public cloud.

Fine-tuned control which is available with the environment of the private cloud is considered as important factor for the process of decision making for allocating resources to private vs public cloud. Additional level available for controlling and supplemental protection in private clouds can compensate for other foundation and it might make contributions to a practical transition.

With all these factors, the organizations should keep in consideration that the maintenance of fine-tuned control creates difficulty. Presently, much of the efforts are taken by the service providers upon themselves. Simplification of the management of security can be made by the users which can decrease the difficulty by abstracting the controls. This amalgamates private and public cloud platforms across and above hybrid, virtual as well as physical environment.

Below are the Top 5 cloud security issues experienced with private cloud:

i. Consistent spanning of control in relation to the security is lacking in the virtualized and traditional server private cloud infrastructure.

ii. Hike in the infrastructure's complexity results in more effort/time of maintenance and implementation.

iii. Skilled staff is available as per the requirement for managing the software defined data centre's security.

iv. Visibility is not complete over the software defined data centre's security.

v. Newly developed advance level attacks and threats.

III. SECURITY THREATS IN CLOUD COMPUTING

A force which act from outside through which the nodes which existed in one state gets transferred to another is termed as a threat. The data is stored in the node and this node provides the user with a platform for using the application in services form. Significant numbers of intrusions or attacks are available occurring within the applications of the cloud.

The 3 service models of the cloud provides various services to the user and also discloses data's issue of security as well as risks which are available within the systems of cloud.

1. SQL Injection Attack.

This is a virtual attack made to a computer and it mostly damages the SaaS. This attack damages SaaS the most because of the poor design of application. It also completes the execution of the commands of SQL (unauthorized) through taking benefits of insecure interface. These types are attacks are programmed for accessing unauthorized data which is under protection and not allowed to access publically.

2. Abuse And Nefarious Use of Cloud Computing

The hackers gain advantage of shortcomings in the process of authentic registrations of cloud. Further, they are provided with services of SaaS, PaaS, IaaS. It is possible for hackers to make their move with suspectible activities like Phishing and/or spamming. These threats are available in all the 3 layers.

3. Net Sniffers

It is also threat associated with SaaS. Through this type of threat, the hacker gains the access via applications. This enables them in capturing packets which flows within a network and also the data if they are transited through the captured packets unencrypted. If this happens, the data become available to everyone.

4. Session Hijacking

Over a protected network, it is an attack on the security of a user session. When a website is logged in by a user, a new session starts in that server. The new session comprises of all the data and the information of the user which the server uses so that password won't be needed every time the user enters a new page. With all the needed knowledge, the hackers can enter a running session and succeeds in gaining access of that session identifier via HTTP. Session identifier is used by the server in order to identify the user for that particular session. This session hijacking is used by the hacker for gaining the control over the session identifier which further enables them in gaining unauthorized control over the user's information. Cross site scripting, session fixation, session side-jacking and session prediction are the most commonly known session hijacking attacks.

5. Man In The Middle Attack

MITM attack is another kind of session hijacking in which a sniffer is used by the hackers to hack the communication among the devices through which data collection is done and hacker further transmits the data. An independent connection is established by the hackers with the user's device and the user is convinced that the connection is direct and private. But in reality, the hackers control the session completely. It is a big threat to the SaaS model.

6. Denial of Services

resources unavailable for the user virtually. This interruption may be both temporary and permanent.

7. Flooding Attacks

This is a type of "denial of service attack" which is used for increasing the conjunction of the network through flooding the network with various types of traffic in a large amount. This type of attack happens when the hackers overweight the services or the network with packets containing data. The server is attacked by it with connections which will remain incomplete and as a result it end with filling the buffer memory of the host with redundant and unused data. At the end when buffer is left with no space, the server won't be able to make any type of connections. This will result as the "denial of service". This attack occurs in IaaS and PaaS layers of the model of cloud.

8. Privacy Breach

Organization as well as users stores their data and information in the cloud. Therefore, any type of breach in the cloud will hack the information available of those users who are authorized. This will enable the unauthorized users in accessing the private information of the users which further might lead to unauthorized and unethical activities with the stored information. This will mostly affect the users of the SaaS model.

IV. COUNTER MEASURES

The infrastructure of the cloud computing comprises of a provider of the services which is responsible for providing resources for computing for the end user. For assuring the best possible services, it is important for the service providers to ensure the users regarding the security safety of the cloud. Through applying methods of advanced security as well as defining stringent security policies, this may be done.

1. DevSecOps processes — DevSecOps and DevOps are continuously been observed in order to decrease the options of vulnerability and exploitations, enhance the quality of the codes, deployment of features and hiking the application's speed. Including security procedures, advancement and QA in the units of the business/applications team rather than depending upon a single security verification team is important for the operations as per the demands of the today's businesses.

2. Automated application deployment and management tools —Hike in the speed and amount of security threats in combination with the insufficient skills in relations to the security leads to the fact that even the professional with highest experience of security cannot keep up. With the help of automation, ordinary tasks can be removed and it also supplement the human work benefits with that of machines which a basic element of advanced operations of IT.

3. Unified security with centralized management across all services and providers — It is not possible for a single vendor, service or product to deliver all the things but this can be delivered through multiple management tool which reduces the difficulty so that something can slip by. In combination with an open integration fabric, the system of

This is an attack in the layer of SaaS and through this attack; the hackers make the services and the network unified management decreases the difficulty to great extent by combining the parts and restructuring the flow of the work.

V. CONCLUSION AND FUTURE WORK

This paper aims to exhibit the challenges which are faced by the users of cloud computing over the securities issue and it also shows the most threatening factors which are a real matter of concern. There are various issues and challenges in relation to the security of the cloud computing. These issues have been recognized as high impacts over the confidentiality and trust of the users. All the security risks as well privacy risks with the advancing efficiency and impactful solutions are difficult tasks to understand. Availability, reliability, integrity and confidentiality are extensively are the factors which are extensively brought in applications for the security related issues. As the enhancement in the cloud computing is growing, future will be full of risk and threats over its security. The providers as well as users must be aware of the potential risks over the security and must prepare themselves with solutions to face these issues for protecting their information from any type of attack. Valuable suggestions and issues of main open research are also provided through this paper in order to understand the issues of cloud. This paper also aims over providing new direction to this field of study and help the researcher in finding out possible solutions for such threats and risks.

REFERENCES

[1] Jensen, M. Schwenk, J. Gruschka, N. Iacono, "On technical security issues in Cloud" IEEE International Conference on Cloud Computing, pp 109-16, 2009.

[2] Mather, T., Kumaraswamy, S., & Latif, S, Cloud Security and Privacy. New York: O'Reilly, 2009

[3] B. Reddy, R.Paturi, "Cloud Security Issues", IEEE International Conference on Services Computing, 2009

[4] J.Viega, "Cloud Computing and the Common Man", IEEE Computer Society, Vol 42, no.8, pp 106-108, 2009.

[5] A.Singh, M.Sharivastava, "Overview of Attacks on Cloud Computing",International Journal of Engineering and Innovative Technology (IJEIT), Vol 1, no.4, 2012

[6] G.Kulkarni, J.Gambhir Amruta, " Security in Cloud Computing" International journal of Computer Engineering & Technology (IJCET), Vol3, no.1, pp 258 – 265, 2012

[7] Habib, S. M., Hauke, S., Ries, S., & Mühlhäuser, M, "Trust as a facilitator in cloud computing: a survey", Journal of Cloud Computing, Vol 1, no.1, pp 1-18,2012.

[8] Zissis, D., & Lekkas, D,. "Addressing cloud computing security issues". Future Generation Computer Systems, Vol.28, no.3, pp 583-592, 2012.

[9] Cloud computing Environment against DDoS Attacks", IEEE, , pp. 1- Bansidhar Joshi, A. Santhana Vijayan, Bineet Kumar Joshi, "Securing 5,2011.

[10] Haoyong Lv and Yin Hu, "Analysis and Research about Cloud Computing Security Protect Policy", IEEE, pp. 214-216, 2011.

[11] M.Rajendra Prasad, R. Lakshman Naik, V.Bapuji," Cloud Computing :Research Issues and Implications ", International Journal of Cloud Computing and Services Science (IJ-CLOSER) Vol.2, no.2, pp. 134-140, 2013.

[12] Mladen A. Vouch, "Cloud Computing Issues, Research and Implementations", Journal of Computing and Information Technology, Vol. 4,pp 235–246, 2008.

[13] Devki Gaurav Pal, Ravi Krishna, Prashant Srivastava, Sushil Kumar, Monark Bag, Vrijendra Singh," A Novel Open Security Framework

for Cloud Computing ", International Journal of Cloud Computing and Services Science (IJ-CLOSER) Vol.1, no.2, pp. 45-52, 2012.

[14] Ashish Kumar," World of Cloud Computing & Security ", International Journal of Cloud Computing and Services Science (IJ-CLOSER) Vol.1, no.2, pp. 53~58 , 2012.

[15] Hemraj Saini, T. C. Panda, Minaketan Panda, "Prediction of Malicious Objects in Computer Network and Defense", International Journal of Network Security & Its Applications (IJNSA), Vol.3, no.6, pp.161-171, 2011.

[16] C. Modi, D. Patel, B. Borisaniya, A. Patel, M. Rajaajan, "A survey on security issues and solutions at different layers of Cloud computing", The journal of supercomputing, Vol. 63, no. 2, pp. 561-592, 2013.

[17] L.M. Vaquero, L. Rodero-Merino, D. Moran, "Locking the sky: survey on IaaS cloud security", Computing, Vol. 91, no. 1, pp. 93-118, 2011.

[18] Pankaj Patidar and Arpit Bhardwaj, "Network Security through SSL in Cloud Computing Environment", International Journal of Computer Science and Information Technologies, Vol. 2, no.6, 2011.

[19] Insider Threats Related to Cloud Computing, CERT, July 2012. http://www.cert.org/

[20] P. P. Ramgonda and R. R. Mudholkar, "Cloud Market Cogitation and Techniques to Averting SQL Injection for University Cloud," International Journal of Computer Technology and Applications, Vol. 3, .no. 3, pp. 1217-1224, 2012.

[21] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, 2011.

[22] Z. Wang, "Security and Privacy Issues within the Cloud Computing," in 2011 International Conference on Computational and InformationSciences,pp.175–178,2011.