ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Security in Cloud Computing For Contemporary Trends

Riyadh Abdulamer Abdlhusein
Assistant Lecturer
Department of Information Systems,
Ministry of Education, The Republic of Iraq.

ABSTRACT

Cloud computing can be distinguished as the Cyberspace Technology. The cyber security issues and privacy preserving challenges have been experienced by Cloud Computing. Cloud computing is providing three predominant services to the Cloud consumers. These are Software as a Service [SasS], Platform as a Service [PaaS] and Infrastructure as a Service [IaaS]. Cloud computing is providing huge amount of storage space, wide range of applications and different kinds of platforms and database services to the small and medium scale business organisations. Cloud computing is providing wide range of services at most economical pricing to the cloud consumers [1]. When the services and infrastructure is available at most economical pricing, most of the companies have waved towards the cloud.

The increasing demand in using the cloud computing has opened the threshold for the cyber criminals and cyber-terrorists to eavesdrop the information from cloud. This has led to network attacks, security challenges and privacy issues. The proposed research work is focusing on the security issues and privacy preservation challenges in cloud computing and showing the possible security measures for the frequently caused attacks with third party auditing and scanning techniques [2].

Keywords: ***Cloud Computing, Security Challenges, privacy preservation, admeasures, third party auditing.***

Introduction

Cloud computing has become as the fast growing paradigm for the small and medium sized entrepreneurs to have their service needs without investing much amount on the infrastructure and licences for software applications. The database services are more economical and stored securely in the cloud. This points have attracted the cloud consumers at huge amount of size.

The health care industry, the government organisations, financial institutions, Software Companies and Insurance companies have started to use the services of Cloud computing at high volume. Cloud computing has enabled the customers to user its resources from anywhere and anytime across the globe. The storage space can be used by the consumers at any quantity from anywhere at any amount of storage size. The services are plenty and charged per click and usage to the customers.

When the usage is at shorter quantity the charges are according to the usage. The attractive business models introduced in cloud computing has made it popular and become the golden threshold for the cyber criminals to hack the information from the predominant companies using the cloud services. The hackers and cyber criminals have attempted several times and eavesdrop the valuable and sensitive data from the cloud data centers. The cybercrimes have been stopped by configuring effective security system in the cloud could stop the external attacks and vulnerabilities. The internal attack and the loopholes in implicit mechanism have

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

opened the doors for the data leakage and vulnerabilities. The recent cyber-attacks have revealed the intensity of the vulnerabilities and caused great loss to the cloud consumers and their customers [4].

The threat preventive mechanism incorporated in Cloud computing has effectively encountered the vulnerabilities and attacks against the cloud computing. The privacy preserving models adopted in cloud computing are very good and protecting the database against any vulnerabilities. The recent attacks on cloud computing could not do much loss to the data store in the cloud servers. The most dangerous attacks like Ransomware attacks could not affect the cloud servers which not running with windows operating system. The servers with Linux and Unix operating systems could be safeguarded from Ransomware attacks.

The hardware and firmware threats are effectively stopped by cloud computing by implementing the admeasures and anti-firmware software and firewall system. So far the firmware is tactfully encountered by cloud computing by implementing the secured protection mechanism with virtualization. The malware delivery through the network attacks have been successfully encountered in cloud computing [5].

Hacktivists have started the new technique to enter into the cloud computing servers as a cloud consumers. They are registering the membership with face identification and entering the malware into the cloud servers from their account credentials. This could not be effectively stopped to intrude into the server mechanism. The cyber criminals who wants to hack the information from the cloud servers are sending the malware and infecting the data center partially and establishing the connection with the cloud servers to their destinated servers. They are steeling the information continuously. The stream is unstoppable and unidentified. This type of techniques are not detectable and even traceable. The present research work is focusing on the tactful malpractices of the cyber-criminals and Hacktivists [6].

The Hacking methodology

The Hacktivists are mostly instigating their techniques in public clouds only. Their tactics are not fruitful in the private cloud computing servers. These Hacktivists will observe the organisational potency for a long time and find the public cloud where their operations are conducted. They will enter and register fake address and credentials and start the operations. They will wait until the opportunity come. Once they find the opportunity they will instigate the virus malware into the cloud data centers and establish the connection with the other organisation database and connect the same with their targeted servers. This can be possible with most powerful malware available in the market [7].

The second loophole to expose the corporate information stored in the cloud computing is unsecured applications used by the enterprises. The corporate companies which are using cloud computing should use secureapplication to store the data. All corporate companies who are using cloud are not bothered about the security applicable at application layer. They are more concentrating on the economical pricing of the cloud services like SaaS, IaaS and PaaS. This point is paving the way for eavesdroppers to steel the information from the cloud data centers. Of course the recent development in technology has gifted DevOps and CloudOps. The predominant usage of these technologies to test the applications before placed and sold as a service in cloud. The complete test should be passed and allowed to keep in the cloud computing services.

Despite these security mechanisms the ethical behaviour need to be improved to stop the cyber-crimes in cloud computing. It is anyway not possible to change the attitudes of the criminals. The security breaches are the phenomenal activities of the cyber criminals. The severity of damage can be measured as soon as the security breach is done. Sometimes that may not be traced for long period of time until the cyber-criminal announce that the sensitive data has been hacked and demands for the money to safeguard the organisation credentials. This type of security breaches could be

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

instigated by the fake accounts created by the hackers of the data. The hackers or cyber criminals will insert the file inside the data center in their own account. The file will be opened and spread into the database root directory and capture the credentials of other corporate sensitive data. This file infection to the root directory can't be traced by any anti-virus software or any other malware protection mechanism. Slowly the virus will establish the connection with the outside servers when the virus patch or malware updations are happening.

This connection with the outside server may be traced by any ICT professional or it may not be known. This data leakage will damage the reputation of the organisations. This data breaches have been identified in the year 2017 more than 256 across the globe. These figures are announced by the ethical representatives of cloud computing. But unknown facts and hidden facts may be several [8].

Secure computing

Secure computing is possible by deploying a third party auditor to scan every file which is uploaded by the cloud consumer. Even if it is encrypted in any DES standards it should be scanned for the virus or malware traces [1].

It is always better to deploy a third party auditing mechanism for every upload. The cloud consumers should not feel that the confidentiality will be stolen by the third party auditor. But it is inevitable to safeguard the data centers from the vulnerabilities and data breaches. This policy will filter the original and genuine customers and then the fake customers will be automatically withdrawn from creating fake accounts. The third party auditor mechanism should verify each and every piece of upload and check for vulnerability. If the file contains vulnerabilities and suspicious code it should be rejected and kept hold the account until the ratification is approved.

It is the responsibility of the cloud consumer and cloud service provider to safe guard the privacy and data confidentiality of the preserving data in the cloud computing. This responsibility should be taken by both parties and incorporate in the Service Level Agreements as a mandatory item [6].

The service level agreement should also incorporate the CloudOps and DevOps to take the responsibility to test the application provided by the cloud computing service provider. The cloud services should pass the test conducted by automated testing mechanism by the DevOps and CloudOps. This ensures the services provided by the cloud service provider will be facilitating the only secure applications well tested in DevOps. According to the Microsoft's Security and Intelligence report nearly 300 per cent of the increase has been recorded in the cloud computing. The usage of DevOps and CloudOps are two things can ensure the application provided by the cloud computing service providers with safe and secure computing [9].

The data stored in the cloud computing should mandatorily converted into a distinct Advanced Encryption Standard code and preserve the data with encryption mode [11].

Conclusion

Cloud computing is one the fastest growing computer technology paradigm in the field of Cyber security. The proposed research work has discussed various security vulnerabilities and privacy preserving challenges to the data stored in the cloud computing. The new technology has given advantage to protect the cloud computing with reasonably good technology. The newest technologies like DevOps and CloudOps have taken the responsibility to check the applications strength and vulnerability protection capacity. The security breaches are happening with the unsecured applications provided by the cloud consumer without properly testing. When it is not done properly the vulnerabilities will always take advantage of the system and intrude inside the applications. The proposed research work is suggesting the cloud service providers and cloud consumers should appoint a third party auditor to check each and every piece of upload for the trace of vulnerabilities and malware intrusions. This

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

will definitelystop the uncontrollable virus intrusions and data breaches form the cloud computing.

Future scope of the work

The future scope of the work has to be done in the field of vulnerabilities and security breaches with Account hijacking, Insider threat and Ransomware attacks. These attacks have not been concluded with possible results in the field of security mechanism. The future scope of the work should also address different types of loopholes instigated by weak authentication and identity management. This is going to give complete security to the track the criminal evidence gathering [12].

References

[1] Alex Bennett (2017) 8 Public Cloud Security Threats to Enterprises in 2017 published in Comparethecloud.net

[2] McAfee Labs (2016) 2017 Threats Predictions published by McAfee labs in November 2016

[3] Dan Raywood (2017) Attacks on the Cloud Increase by 300% published by www.infosecurity-magazine.com

[4] Misha Govshteyn (2017)Virtualization Security published by INFOSECURITY MAGAZINE

[5] Chaoqun Yu, Lin Yang and Yuan Liu (2015) Research on data security issues of cloud computing published in IEEE Date Added to IEEE Xplore: 14 May 2015

[6] Rajarshi Roy Chowdhury (2014) Security in Cloud Computing published in International Journal of Computer Applications (0975 – 8887) Volume 96– No.15, June 2014

[7] Sultan Aldossary,William Allen (2016) Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions published in International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, 2016

[8] J., Wayne, T., Grance, Guidelines on Security and Privacy in Public Cloud Computing, U.S. Department of Commerce, January 2011.http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf [Accessed on: 23 October 2011]

[9] Rob Williams (2016) Top 4 Cybersecurity Threats to Watch in 2017 Posted by on Tue, Nov 01, 2016 @ 09:30 AM

[10] Z., Chen, J., Yoon, IT Auditing to Assure a Secure Cloud Computing, Services (SERVICES-1), 2010 6th World Congress on, pp. 253-259, September 2010.

[11] David Linthicum, InfoWorld | JUL 4, 2017The latest cyber-attacks show why the cloud is safer

[12] 2017 Cloud Security Trends by Kristen Corley Jan 4, 2017