INTERNATIONAL RESEARCH JOURNAL ON ADVANCED SCIENCE HUB
e-ISSN : 2582 - 4376
Open Access
RSP SCIENCE HUB
(The Hub of Research Ideas)
Available online at www.rspsciencehub.com

Special Issue of First International Conference on Social Work, Science & Technology (ICSST 2021)

A Scrutiny on Cloud Computing Security Issues

S. Jenifa Sabeena[1], Dr. S. Antelin Vijila[2]
[1]Research Scholar, Department of Computer Science and Engineering, Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu.
[2]Assistant Professor, Department of Computer Science and Engineering, Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu.
jenifasabeena1996@gmail.com[1], antelinvijila@gmail.com[2]

Abstract

Cloud computing is one of the widely used technology in the 20th century. Cloud has become an essential part in our day-to-day life, because the data are stored in the cloud in any one form such as Gmail, Google Drive etc. As the users store sensitive information in the cloud, the Cloud Service Providers need to provide proper data security for data stored in the cloud. There are many issues in Cloud Computing Security. This paper discussed about various issues in the Cloud Computing environment and the future work directions have identified for the Cloud Computing Security.

Keywords: Cloud Computing, Cloud Service Providers, Security, Hybrid and Portability.

1.Introduction

Cloud computing provide a shared pool of resources over the internet. It is the fastest growing part of network-based computing. Cloud computing provides many benefits to customers of all sizes: simple users, developers, enterprises and all types of organizations. Cloud computing has improved the efficiency of operation for the individual and also for the business people. Based on the user and business needs there are four types of clouds available, Public, Private, Hybrid, and Community. There are three types of cloud service model they are IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service). There are a lots of security concerns are in the implementation of the data accessing at cloud computing. Some of them are as follows: Data Transmission, Access to Servers and Applications - The Application server is the responsible ones for all the applications developed by individual servers in cloud. They also grant server accessing authority to the individual applications. Network Security, Virtualized Security – The virtualized security issues are related to the virtualized software based designed network in the field of information technology. These applications found their static and run time issues through the working of firewalls and routers. Data Privacy and Data Security, Data Location, Data Integrity, Data Segregation, Data Availability, Security Policy and Compliance – This system will effectively specify set of rules and formulations for the personnel specification and data accessing over the network [1]. These are considered as some of the basic security issues that are mainly concerned over the concept of cloud computing.

2.Literature Review

Yunchan et.,al., 2020, [7] "The aim of the work is to identify about different issues and corresponding solutions for the cloud based architecture. The review on different techniques on security is reported as the results of the paper. The effective analysis was done for the enhancement of trustworthy environment on the

cloud. The comparative research analysis was done for the effective primary data analysis on the data security and data privacy concepts and results were analysed on the basis of that" . Theebendra et.,al., 2020, [5], "This paper explains about the basic implementation of data security via cloud computing without affecting the network layers of the system. The protection of the data with proper authorization with server level protection is recommended. The implementation of data security is given as high priority. The data is highly secured on the network based on the user. This concept of cloud computing is highly preferred by several business and large as well as small industries". Rao et.,al., 2020, [6], "The paper provided several data later security challenges faced by the cloud environment and proper solutions for overcoming the issues. the effective result of encryption is suggested as one of the best solutions for the secured information transformation through cloud". Jathana et.,al., 2020,[4], "The giant software making industries including Microsoft are presently joining to develop the cloud services in better way with ensuring that data is secured and private. The customers are very much reluctant to deploy all their business details and data in the cloud despite of the hype about the cloud computing. The increase the complications over the data privacy and protection is affecting the cloud computing market. The cloud users need to understand about the basic risk and data breaches that are prevailing at the cloud environment". Suaib, 2018, [2], "This is considered as the new technique for service delivering over the internet networking. The security, trust and privacy are considered as the issues for the development of the organisations data storage through cloud computing. It is necessary to have proper knowledge about the issues before stepping into the world of cloud computing". Ahmed et.,al., 2019 ,[3], "Security privacy and trust or not robust and consistent at cloud computing. While at the same time the flexibility and lots of advantages are there for making the choice of cloud computing over the other with little credibility. There are lots of security issues and inference is there in association with the cloud computing and cloud infrastructure which have been analysed and effective solutions for made in this proposed paper".

3.Issues of Cloud Computing

In Cloud Computing Environment the Cloud Service Provider must confirm that the user does not face any data loss or security issues. Some of the cloud computing problems are listed below,

3.1 Data Related Issues

Data integrity - The exact accuracy and completeness along with the reliability of the information through the complete life cycle of data are considered as data integrity. it is one of the major concerns in cloud computing. The cloud-computing basically lacks the preservation of information integrity. Sometimes the data can be possibly lost and can be modified by unauthorised user. These are considered as that data integrity issue in cloud computing.

Data loss - The concept of data loss is an error condition which possibly occurs at the time of failure of data retrieval at the time of need by the user who authorised for the data at the cloud.

Data leakage - The concept of unauthorised data transmission by external source recipient are termed as data leakage at cloud computing.

Data location- The cloud usage implements vast area for locating the data. The location of data is exactly used for identifying and retrieval of data at the network by means of service provider. as the cloud Access vast to storage the possibilities for losing the location details and possible loss of data loss can be made at the cloud environment.

Unwanted access - The unwanted access is the access made by the third person without any proper authority over the store the data of other person at the cloud environment.

Data segregation - Data segregation is the concept of gathering the information from the clustered resource network by organising them under single categories of similar properties are homogenous network accessing which may possibly allowed the grouping of similar data at the cloud environment.

Vendor lock-in - The interlocking is one of the conditions which occurs at the cloud environment where the user is supposed to be forced continuation of using the product or service because there is no possibilities for switching into another vendor at the cloud. It is also known as proprietary lock.

Data deletion - As there is the vast storage of data modification which is provided at cloud

environment sometimes there are possibilities for mishandling of data and data deletion.

Data investigation - The concept of data investigation will involve art number of component enrolment for the formulation of problem which can be effectively that build with statistical manner by means of proper planning and collecting organising the validating data. This validation is excluded over cloud computing by means of mishandling data investigation process.

Secure data transfer - The lack of security in data transfer that can be accessed by an authorised user are still prevailing in cloud computing.

Customer data manipulation - The data manipulation by customer cannot be identified by cloud. These are some of the major data related issue at cloud.

3.2 Network Related Issues

Security provider - Security provider are the persons who are the authority for granting permission for accessing the data are giving security applications through means of internet networking. The misappropriations over the security provider are the network related issues in cloud computing.

Ownership - the ownership of defined as the actual owner or the person who is responsible for publishing a data and who is authorised the data modification editing and changing at the cloud. While there are possibilities of complexity in the network providers for data handling through ownership in cloud.

Multiplatform support - The multiplied phone support is another one of the important failure at cloud while it does not support multiple forms of platform-based oriented programs it is unidirectional and will not combined any other platform to support the activities which main issues network related issues.

Data recovery - The data recovery in case of data loss is not secured under cloud computing as there are possibilities to change in location over the cloud based storage.

Data portability and conversion - The data portability and conversion were also not supported by cloud computing as it is said as unidirectional and does not support multi-platform supporting activities this are considered as another one of the network related issues in cloud based computing as the source of the code will be modified in the cloud if there is no platform found. These are some of the major networks related issue at cloud.

3.3 Policy Issues

Unauthorized secondary usage - The secondary usage of the defined data by the unauthorized persons are termed as severe issue under cloud computing.

Data proliferation - The prodigious amount of data, speak maybe structure or not structure, generated in large volume by the business organisation or government which are accelerated to unprecedented rate and related with several usability problems in case of storing and managing the data are considered as data proliferation issue at cloud computing.

Dynamic provisioning - Concept of dynamic provisioning is the environment oriented concept which offers a simplified way for explaining the complex network which are operated over the server computing environment with computing instances and virtual machines under decentralized and centralised networking which be affected with supporting single area that network development by means of open shift container platform organisation and implementation at cloud computing. These are some of the major policies related issue at cloud.

3.4 Security Issues

Authentication and identity management - The Identity management is the process of ensuring the individual access over the utility resources and authentication is the process of proper authorization for accessing the individual data are application that is available at the cloud. issues regarding identity management and authentication where are considered as those serious issues of securities-based problems in cloud.

Backup - Sometimes the cloud failed to proper backup and backup retrieval process due to network loss and data leakage.

Lack of standardization - There is no standardization as it is a single path and does not allow any of the multi-dimensional operation and the process of data organization and utilization of data and data related applications where are also considered as lack of standardization.

Multi-tenancy - The multi tenancy is the concept of software architecture which have single instance for the application that is run on the server and create multiple service for the multiple tenants at the single time. This architecture is

considered as one of the failures of security issues at cloud computing environment.

Audit - The cloud environment lacks in proper auditing functions that is the review of the existing data and accounts and the applications were not properly verified at specific time. These are some of the major securities related issue at cloud.

3.5 Trust Issues

Weak trust relationships - The lack of trust in the relationship results in the vulnerability risk that will occur at the time of continuous data loss data leakage and network issues possible backup and retrieval functions failure at cloud.

Lack of customer trust - The failures and fluctuations in the cloud environment, makes the customers through go through the thought of lacking of trust over the cloud environment and cloud supporting applications while there is no confidential privacy and secured data transmission for sure. These are some of the major trusts related issue at cloud.

4.Attacks on the Cloud Environment

Cloud Malware Injection attack - The cloud malware injection is performed to take control over the user information that are present in the cloud. In the malware injection attack, the cyber attacker creates a malicious application and injects it into a SaaS or PaaS or IaaS solution. If the Injection is completed then the malicious module is executed, now the cyber attacker can make any sort of attack such as data manipulation, data theft or eavesdropping. Some of the common malware injection attacks are cross-site scripting attack (hackers inject malicious scripts such as flash, JavaScript etc), SQL injection attack (hacker targets the SQL servers with malicious database application). **Abuse of cloud services -** The cyber attackers use low-cost cloud services to place DoS and brute force attack on the targeted users, companies and other cloud providers also.

Denial of Service attacks (DoS) - Denial of service attack is a type of cyber-attack which is designed to overload a system and the services are made unavailable to the users. DDoS attack is more dangerous as the attacker use more zombie machines to attack large number of systems [8].

Side Channel attacks - The concept of side-channel attacks is one of the major threats at the computer security over cloud computing this attack is commonly based on the gaining of information from the cloud system by implementing the identification of weakness algorithm over the cloud and retrieving the data from the cloud system.

Wrapping attack - The wrapping attack is the process of attacking using fake the elements as a process message structure which will cover the clouds valid signature and modified data by projecting a fake the one which is processed by the logic of applications to retrieve the information by providing arbitrary web service required request for the authentication like a legitimate user.

Man-in-the-cloud attack (Mitc attack) **-** The man in the cloud attack is one of the malicious tactics that is used to for the accessing of victims in the cloud account and obtain the compromise user credentials beforehand.

Insider attack - The insider threat is one of the malicious threats that expose the security risk of the cloud environment by the target organisation itself. The hacker will be from the cloud environment itself.

Account or service hijacking - The process of service hijacking and account hijacking means the simple process of hacking The other person's account and services offered to them by the cloud and make the utilisation of the data and services from the cloud like accessing the personal data information of the account holders including the mail details, bank account details, social media details etc ….

Advanced Persistent Threats (APTs) - This kind of Stealthy threat, actors were consistent among the cloud environment for accessing the appreciation of other users for gaining that system under cover with unauthorised user access.

Spectre and Meltdown - Spectre are the vulnerable risk which allowed the unauthorised Access on arbitrary locations and allocated memory usage application data and related function over the cloud environment. And that Melton is the vulnerability risk that will allow the utilisation of can an authorised person to read all the memory space that are allocated for the other user in the given cloud system.

5.Security measures for cloud-based issues

Enhance security policies - The process of enhancement of security policies will be very much helpful for the improvise data security.

Use Strong Authentication - Strong authentication providing over the cloud will be

helpful for preventing data loss and other malicious attacks over the cloud environment.

Implement Access Management - The process of implementation of access management is necessary for the maintenance of privacy and data security and to prevent several attacks over the cloud.

Protect Data - Data protection with proper maintenance and monitoring of the system and verification of authentication over the data accessing will be helpful for providing secure the data transactions over the cloud.

Detect Intrusions - The process of detecting the instructions will be helpful for prevention of instructions over the cloud environment this can be effectively implemented by proper auditing and increasing standardization of the network over the cloud environment.

Secure APIs and access - The secured API and secured access over the data service and data accessing will be helpful for the accessing of data and data related applications by the authenticated user over the cloud based networking will prevent data leakage, data loss and can be helpful for avoiding un authentication access like possible avoidance of cloud based attacks and secure the data and data related details over the cloud.

Protect cloud services - the services offered by the cloud can be vulnerable to the risk of easy an authorised accessing over the cloud by means of false request to the cloud service provider by hacking the other users account and ID in appropriations. That secure data transmission over the cloud and their services offered by the cloud environment will be helpful for preventing the mitigate risk over vulnerability.

Encryption - The concept of data encryption is one of the best solutions for the problem of data handling over the cloud environment. There are a large set of encryption algorithm are available for proper data handling. [9] The best DES and AES algorithms will be helpful for the property encryption process other than this there are lots of available algorithms are there in the chapter of cryptography which will be effectively helpful for the prevention of cloud-based data services and applications.

Conclusion

Cloud Computing is an interesting and useful technology. Every technology has its pros and cons, where cloud offers many features to its users, it also has some issues based on its security and privacy. A generalized view of these issues has been presented here to enhance the importance of understanding the security flaws of the cloud computing framework and devising suitable countermeasures for them. In this paper the Issues of the cloud computing is discussed, hope this review will provide a better understanding of the security and privacy issues and pave the way for the future research.

References

Journals

[1].Amandeep verma and sakshi kausal, “Cloud Computing Security Issues and Challeges”, International Journal of Publications, Jan 2021.

[2].Mohammed Suaib, “Security Issues on Cloud Computing”, International Journal of Applied Computing, vol (2), no (6), Nov 2018.

[3].Monjur Ahmed and Mohammad Ashraf Hossain, “Cloud Computing and Security Issues in the Cloud”, International Journal of Network Security and its Applications, vol (6), no (1), Jan 2019.

[4].Rohan Jathana and Dhannama Sankar Jagli, “Cloud Computing and Security Issues”, International Journal of Engineering Research and Application 7(06): 30-40, June 2020.

[5].heebendra and Santhini, “Cloud Computing security – Data Storage and Data Transmission”, International Journal of Research in Computer Application and Robotics, Nov 2020.

[6].Velu Madhava Rao and Selvamani, “Data Security and Challenges and its Solutions in Cloud Computing”, Journal of Computer Science, Dec 2020.

[7].Yunchan Sun,Junsheng Zhang and Yongping Xiong, “Data Security and Privacy in Cloud Computing”, International Journal of Distributed Sensor Network , July 2020.

[8].Heshma Abusaimeh, “Security Attacks in Cloud Computing and Corresponding Defending Mechanism”, International Journal of Advance Trends in Computer Science and Engeneering, Vol. 9, No. 3, May – June 2020.

[9]. Abdullahi, Alhaji, Abdulhakeem and Asma’u, “The Study of Data Security in Cloud Computing”, EJECE European Journal of Electrical Engineering and Computer Science Vol. 4, No. 4, August 2020.

[10]. Hamed Tabrizchi, Marjan Kuchaki Rafsanjani "A survey on security challenges in cloud computing: issues, threats, and solutions", Journal of Super computing, Feb 2020.