A Detailed Survey Of The Security Issues And Defensive Tactic In Cloud Background

[1]A. Priya , [2]Dr. S. Saradha

[1]Research scholar, Department of computer science ,VISTAS, Chennai, India
[2]Research supervisor , Department of computer science ,VISTAS, Chennai, India

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 23 May 2021

ABSTRACT:
Cloud computing technology is a stretchy, price- efficient and provides a nice stand for the trade opportunities and the customer services via network. It is the main route to improve the capacity or else add the capability with dynamism without investing in new infrastructure. From the past few years cloud computing technology was the fastest growing segment in the IT filed. Extreme plenty of information has been stored in the cloud because of its convenience. In the face of of the public relations neighboring in the cloud the consumers are unwilling towards make a proposal for their business in the cloud. The growth of the cloud was deduced by the security issues in the cloud. The complications in the data privacy and the protection of the data will extending due to the clumpness in the market . The cloud architecture have several threatening issues the cloud service users need to be aware of the issues and the existing protective techniques. Hence in this paper a survey was held depends upon the different security issues belongs to the cloud and also its defensive methodology. There are several other existing methodologies are there which can improving the features in the cloud and also reduces the risk in the cloud. This survey was more specific to different safety problems also defensive mechanism in cloud computing.

Keywords: Cloud computing, cloud safety, safety issues

1.INTRODUCTION:

Inside this business world small and the medium business industries are increasingly depends upon the cloud by simply tapping over it and fast access of the business applications and can vigorously boost up their infrastructure resources at an affordable cost. NIST was the National Institute of Standards and Technology have a clear idea on the cloud computing which is a vital luggage compartment of the computing resources that can be opened and utilize from anywhere all the way through any devices with a least organizational effort. Cloud computing was bendy because it offers several useful services to the users. It can have several open arms like PDA, Laptop, desktop, and mobile phones. [1] There are lots of noteworthy technologies are there among them the enhanced technology is the cloud computing .It serves the ever-present, suitable, condemned network access to a communal group of convictable computing assets [2] which are quickly defend and unconfined with limited work effort with less interaction with the service provider . Cloud computing is the amalgamation of the several computing technological concepts which serves a many business opportunities for the professionals and can competing the requirements of the users by important data storage via online [3]. Also lots of remuneration are there in this technology which will move this technology to peak level [4]. But Unfortunately the cloud computing technology suffers a lot due to numerous tribulations like losing self control and safety burdens. The security issue is a huge eradicating issue in the cloud computing . Since Cloud Computing was absolutely a novel structure, hence some disbeliefs are there regarding this technology by some users related to security maintenance [5]. The security problem can affect the growth of the cloud computing. As a result, the vulnerability on the information violation be augmented gradually now a days. Extensive survey showed that there is a need to improve the protection for enhancing the characteristics of the cloud computing. The proposed paper is structured as represented below. The survey paper is to take a review in safety problems associated with the cloud computing in addition to that various existing techniques employed in the secured cloud computing with its methodology, advantage and the limitation.

The remaining portion of the paper be arranged in the form of : Part 2 depicts the outline on various existing secure cloud computing approaches. Various attacks on cloud and its countermeasures are discussed in part 3. Part 4 tabulates the existing approaches with its advantages and disadvantages. Finally, part 5 concludes the overall review of the paper.

2. OUTLINE ON EXISTING METHODOLOGIES DESCRIBES ABOUT SECURITY ISSUES AND SECURE CLOUD COMPUTING APPROACHES:

Here in this section the discussion was based on the some other present existing secure cloud computing approaches and the cloud computing issues. There are several attacks and coercion are present in a computing infrastructure. The most important confront here is the "Security". Different security issues are [6].

- Confidentiality – It refers to the eagerness status to depend of one party on another party to attain a intended goal [7]. In a cloud environment, confidentiality issue is mainly based on the preferred utilization model, as data, processes, and applications control are outsourced [8].
- Data reliability -Maintaining the reliability of cloud computing is considered as a major dispute to the cloud parties, as the coercion could be at the subscribers or providers level. To insure data integrity in the provider and subscriber level , a secure encryption algorithm could be used, but it could not get guaranteed that data wont changed through locating it in the cloud [9].
- Accessibility – [10] The accessibility refers to the ability of the subscriber to retrieve all the information at anytime.
- User authentication and authorization-Authentication refers to the procedure that will proves the users claimed exceptionality while they are trying to access any scheme [11].Authorization is the process of identifying the performance of the user. Loss of the authorization will leads of cloud breach.
- System vulnerabilities
- Multi-tenancy-Secure sharing of the resources among the clients.

To overcome the security issues in the cloud computing several protocols are available but claimbing of these protocols are very difficult. Hence in [12] an integrated model is used to ensure better Cloud security for Authentication and the multi-tenancy. Multi-tenancy means sharing of the resources and virtualization among the clients. Since multi-tenancy allows multiple users to access same possessions simultaneously, there is high probability of accessing confidential data without proper privileges. The model includes Kerberos authentication protocol to enhance the validation security. Here Elliptic Curve Cryptographic technique should be used. Cryptography ensures the confidentiality, authentication, availability, and integrity of the data. This can be done through the cryptographic algorithms like Data Encryption Standard , Advanced Encryption Standard and Blowfish. In [13] mobile computing was discussed. The problem of privacy of data with reducing the resources usage. For overcome the issues the three cryptographic algorithms was implemented. Blowfish, AES and DES provide more security based on the resources availability.

In [14] the most difficult issue was discussed in the development of the cloud computing and the trust management. Information privacy and security was a vital perception. On account of the dynamic nature of cloud condition trust management was to be tested .

In cloud computing different large number of the data are stored that can be pooled by the users . So the security is the utmost one. Hence in [15] the use of multiple encryption technique outlines the significance of the data security and privacy protection. The interruption of the issues results will leads to the corruption of the data. Hence the implementation of the AES algorithm will results in the multi-level encryption as an unauthorized user would need the encryption keys as well as the decryption keys in order to obtain data which would automatically become a difficult task to accomplish without a valid key. It is expected that using multilevel encryption with deliver more safety to data for cloud storage than by means of single level encryption.

In the [16] paper the author proposed a attractive novel secure model for developing the secure cloud environment by using the distributed hash table network, identity based timed –release encryption and attribute based encryption. Here at first the datas are encrypted by using the attributes and then the encrypted datas are converted in the form of the cipher text. Then, IDTRE algorithm has been used to encrypt the decryption key and combined the ciphertext. Then the ciphertext are distributed into the DHT network, and then it can be stored on the cloud servers.

3.ATTACK AND CORRECTIVE RECTIFICATION WITHIN A CLOUD

(a) SaaS layer attack:

In SaaS, the majority of the consumers are sore by means of the data dependent security issues like data backup, data accessing, data availability etc .

1. DoS attacks

DoS attacks called as the denial of service attack which was one of the outstanding attacks in the Cloud. The key plan of the hacker was to tire out the entire information about the user the through request packets via net.,[17, 18]

2.SQL injection attack:

The ultimate aim of the SQL attack was theft all the datas regarding user from the net like user name, passwords, credit card password etc by injecting malevolent cryptogram or else code into the network in the form of ordinary input. After that the hacker get illicit access to the user data [19].

3. Authentication attack

Authentication attacks was due to the weaker username and password of the users. Here this authentication attack somewhat crazy the hacker behave like a user and make fool on the system and get unauthorized access [20].

(B) PaaS layer attack:

This attack was also called as the side channel or cross site attack.

1. Port Scanning Attack

This was one of the familiar assault in which a attacker unauthorizely open the portal address and extract the information and destroy or misuse the information [21].

2.Metadata spoofing attack

Here in which the attacker access the file and make some modifications or else delete some of the important operations [22].

3. Man-in-the-browser attack

Here in which the attacker was stand between the sender and the receiver and can access the information [23].

4. Phishing / Spoofing attacks

Phishing or the spoofing attacks will have an effect on both the server and users. Here the user can redirected to the spoofed web link and the attacker can access and get the personal information about the user [24].

(c) **IaaS layer attack**

Resting on this layer, attacks will happen frequently since there is a lack of the defense opening in the virtualization administrator [30].

1**) Cross-virtual-machine attacks**

This attack is also called as the side channel attack . Here in which the user confidential information can be extracted and destroying the some second place able datas like power, volt, minutes etc. [25].

2) Virtual machine(VM) rollback attack:

Here the attacker can get the password of the virtual machines and can take a snapshot and run it without the awareness of the user. This attack occurs with the help of the brute-force attack. Also the assailant modify the users accessibility or the authorization code via rollback,which is a permission managing component [26].

3) VM escape attack:

In this type of attack, the attackers try to break the down guest operating systems or to access the memory information. Afterwards the attacker can control the entire guest operating system [27].

Depend upon the survey held on the severity of the issued in the cloud computing some on the rectification measures are identified they can be listed below in the table 1

Table:1 Types of attacks and its corrective rectification

Attack to be identified	**Attacked cloud services**	**Effects**	**Corrective rectification**
DoS	SaaS,PaaS and	Creation of the fake	Use of signature based approach

	IaaS	service	**[28]**
SQL injection attack	SaaS	Malicious service	Use of the proxy based architecture [29]
Authentication	SaaS	Privacy intrusion	Use of strong password authentication system [30]
Port scanning attack	SaaS,PaaS and IaaS	Service abnormality	Use of firewall [31]
Metadata spoofing attack	SaaS and PaaS	Privacy intrusion and Service abnormality	Strong authentication access [32]
Man-in-the-middle attack	SaaS,PaaS and IaaS	Loss of security and privacy	Socket layer machine learning algorithm [33]
Cross-virtual-machine attacks	IaaS	Attacker intrusion and VM control	Novel encryption and decryption needed [34]
Virtual machine (VM) rollback attack:	IaaS	Attacker intrusion and VM control	Use of auto recovery and self healing method [35]
VM escape attack:	IaaS	Attacker intrusion and VM control	Game theory approach [36],use of secure hypervisor

4. ADVANTAGESAND DISADVANTAGES OF THE EXISTING APPROACHES:

The advantages and the disadvantage of the existing method will makes the identification of the perfect methods against the cloud computing attack easily.

Table:2 Adavantages and disadvantages of the existing approaches

Existing paper	**Advantages**	**Disadvantage**
Vinnarasi et al.[28]	It can easily captures the action unique to the attack	New attack cannot gets detected
Simmos et al. [29]	Highly secure	Highly expensive
Mohammed et al. [30]	trouble-free to use and easy to install	Weak identity test
Neuvirth et al. [31]	Increase network	Unaware of Insider attacks

	security	
Busch et al.[32]	Increased login security	Sometime it turn against the users
Natarajan et al. [33]	High trust	Highly expensive and also some performance issues
Chabra et al. [34]	Protect the information and enhance the security	There is a chance of developing a false sense of security
Joseph et al. [35]	Cheap , fast	Chance of permanent loss of data
Prabhakar et al. [36]	Accurate behavior prediction	Arose of some uncertainty.

Thus, from the survey it was concluded that the existing techniques having both advantages and disadvantages. Therefore an effective method is required for improving the security in the area of cloud computing.

5. CONCLUSION:

Cloud safety was the critical factor in the field of business and also for the consumers. Each should needs their information should kept safe and secure .In this paper, the survey was focus on the existing work that address the security issues, threats and attacks in the cloud environment. So, appropriate countermeasures should be taken care to solve the security issues. Various existing solutions are there for the cloud attacks. But every existing method should possess a advantage and disadvantage. From this survey, it was concluded that still the cloud environment should have some open issues apart from the various solutions presented. Hence, this work catalyze the researcher to understand the issues and understand the urge of developing solutions for the issues.

6.REFERENCES:

[1] H. Karajeh, M. Maqableh, and R. Masa'deh, "Privacy and Security Issues of Cloud Computing Environment," in *Proceedings of the 23rd IBIMA Conference Vision*, 2020, pp. 1-15.

[2] C. Pettey, "Gartner identifies the top 10 strategic technologies for 2011," *Gartner http://www. gartner. com/it/page. jsp*, 2011.

[3] A. Marinos and G. Briscoe, "1st International Conference on Cloud Computing (CloudCom)," ed: Beijing, China, Heidelberg: Springer-Verlag Berlin) Community Cloud Computing, 2009.

[4] M. Chung and J. Hermans, "From hype to future: Kpmg's 2010 cloud computing survey," *KPMG Advisory NV, Amsterdam*, 2010.

[5] D. G. Rosado, R. Gómez, D. Mellado, and E. Fernández-Medina, "Security analysis in the migration to cloud environments," *Future Internet*, vol. 4, pp. 469-487, 2012.

[6] A. Sharma, B. Keshwani, and P. Dadheech, "Authentication Issues and Techniques in Cloud Computing Security: A Review," *Available at SSRN 3362164*, 2019.

[7] S. L. THARANI and M. A. RANI, "Improving Searchable Efficiency over Encrypted Cloud Data Using Multi-Keyword Ranked Search Schemes."

[8] C. Rong, S. T. Nguyen, and M. G. Jaatun, "Beyond lightning: A survey on security challenges in cloud computing," *Computers & Electrical Engineering*, vol. 39, pp. 47-54, 2013.

[9] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of network and computer applications*, vol. 34, pp. 1-11, 2011.

[10] N. Rjaibi, L. B. A. Rabai, and A. B. Aissa, "The mean failure cost cybersecurity model toward security measures and associated mechanisms," *International Journal of Cyber-Security and Digital Forensics,* vol. 2, pp. 23-36, 2013.

[11] E. Turban, J. Outland, D. King, J. K. Lee, T.-P. Liang, and D. C. Turban, *Electronic commerce 2018: a managerial and social networks perspective*: Springer, 2017.

[12] H. Dey, R. Islam, and H. Arif, "An Integrated Model To Make Cloud Authentication And Multi-Tenancy More Secure," in *2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, 2019, pp. 502-506.

[13] K. Kaviya, K. Shanthini, and M. Sujithra, "Evolving Cryptographic Approach for Enhancing Security of Resource Constrained Mobile Device Outsourced Data in Cloud Computing," 2019.

[14] Z. Yan, X. Li, M. Wang, and A. V. Vasilakos, "Flexible data access control based on trust and reputation in cloud computing," *IEEE transactions on cloud Computing,* vol. 5, pp. 485-498, 2015.

[15] Y. Sharma, H. Gupta, and S. K. Khatri, "A Security Model for the Enhancement of Data Privacy in Cloud Computing," in *2019 Amity International Conference on Artificial Intelligence (AICAI)*, 2019, pp. 898-902.

[16] S. Namasudra, "An improved attribute-based encryption technique towards the data security in cloud computing," *Concurrency and Computation: Practice and Experience,* vol. 31, p. e4364, 2019.

[17] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, "DDoS attacks in cloud computing: Issues, taxonomy, and future directions," *Computer Communications,* vol. 107, pp. 30-48, 2017.

[18] L. Alhenaki, A. Alwatban, B. Alamri, and N. Alarifi, "A Survey on the Security of Cloud Computing," in *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, 2019, pp. 1-7.

[19] P. Deshpande, S. Sharma, S. K. Peddoju, and A. Abraham, "Security and service assurance issues in Cloud environment," *International Journal of System Assurance Engineering and Management,* vol. 9, pp. 194-207, 2018.

[20] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," *Journal of Network and Computer Applications,* vol. 79, pp. 88-115, 2017.

[21] N. Almasalmeh, F. Saidi, and Z. Trabelsi, "A Dendritic Cell Algorithm Based Approach for Malicious TCP Port Scanning Detection," in *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, 2019, pp. 877-882.

[22] R. Anitha, P. Pradeepan, P. Yogesh, and S. Mukherjee, "Data storage security in cloud using metadata," in *2nd International Conference on Machine Learning and Computer Science (IMLCS'2013), Kuala Lumpur (Malaysia)*, 2013, pp. 26-30.

[23] A. Mallik, A. Ahsan, M. Shahadat, and J. Tsou, "Man-in-the-middle-attack: Understanding in simple words," *International Journal of Data and Network Science,* vol. 3, pp. 77-92, 2019.

[24] V. S. P. P. C. Kumar and S. P. Rao, "Phishing attack detection," ed: Google Patents, 2019.

[25] S. Anwar, Z. Inayat, M. F. Zolkipli, J. M. Zain, A. Gani, N. B. Anuar*, et al.*, "Cross-VM cache-based side channel attacks and proposed prevention mechanisms: A survey," *Journal of Network and Computer Applications,* vol. 93, pp. 259-279, 2017.

[26] P. Mishra, E. S. Pilli, V. Varadharajan, and U. Tupakula, "Intrusion detection techniques in cloud environment: A survey," *Journal of Network and Computer Applications,* vol. 77, pp. 18-47, 2017.

[27] Y. Xia, Y. Liu, H. Chen, and B. Zang, "Defending against vm rollback attack," in *IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN 2012)*, 2012, pp. 1-5.

[28] J. Vinnarasi and N. Sudha, "Security Solution for SDN Using Host-Based IDSs Over DDoS Attack," *Available at SSRN 3449613,* 2019.

[29] D. E. Simos, J. Zivanovic, and M. Leithner, "Automated combinatorial testing for detecting SQL vulnerabilities in web applications," in *Proceedings of the 14th International Workshop on Automation of Software Test*, 2019, pp. 55-61.

[30] F. Mohammed and D. Uliyan, "A New Password Authentication Scheme Resistant against Shoulder Surfing Attack," *技術學刊,* vol. 34, 2019.

[31] H. H. Neuvirth, R. H. Pliskin, T. Koren, J. Weizman, K. W. Reinsch, and E. Hudis, "Detecting attacks on web applications using server logs," ed: Google Patents, 2019.

[32] C. Busch, "Standards for Biometric Presentation Attack Detection," in *Handbook of Biometric Anti-Spoofing,* ed: Springer, 2019, pp. 503-514.

[33] J. Natarajan, "Cyber Secure Man-in-the-Middle Attack Intrusion Detection Using Machine Learning Algorithms," in *AI and Big Data's Potential for Disruptive Innovation*, ed: IGI Global, 2020, pp. 291-316.

[34] S. Chhabra and D. M. Durham, "Cross-domain security in cryptographically partitioned cloud," ed: Google Patents, 2019.

[35] L. Joseph and R. Mukesh, "Securing and Self recovery of Virtual Machines in cloud with an Autonomic Approach using Snapshots," *Mobile Networks and Applications*, pp. 1-9, 2019.

[36] K. Prabhakar, K. Dutta, R. Jain, M. Sharma, and S. K. Khatri, "Securing Virtual Machines on Cloud through Game Theory Approach," in *2019 Amity International Conference on Artificial Intelligence (AICAI)*, 2019, pp. 859-863.