Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Cloud Computing Security Challenges, Threats and Vulnerabilities

Nahdia Maryam Osmani*[1], Summaiya Fatima*[2], Afnan Ansari*[3], Dr. Mohammed Abdul Bari*[4]

*[1] *BE Student, Dept. of Computer Science Engineering, ISL Engineering College*

*[2] *BE Student, Dept. of Computer Science Engineering, ISL Engineering College*

*[3] *BE Student, Dept. of Computer Science Engineering, ISL Engineering College*

*[4] *Head Of The Department, Dept. of Computer Science Engineering, ISL Engineering College*

Article Info
Page Number: 1446-1454
Publication Issue:
Vol. 72 No. 1 (2023)

Article History
Article Received: 15 October 2022
Revised: 24 November 2022
Accepted: 18 December 2022

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.

1. 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. Microsoft SharePoint and Google applications are general examples of cloud computing services.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. [1]

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. [2]

The proposed solution to these recent attacks is based on criminal theories for the protection of the cloud. Security vulnerabilities and challenges arise from the usage of cloud computing

services. Currently, cloud computing models are the primary source of these challenges and vulnerabilities. [3]

The intruders exploit the weakness of cloud models in accessing the users' private data, by attacking the processing power of computer systems. The "Autonomous Cloud Intrusion Response System" (ACIRS) has been recently proposed to overcome the problem mentioned earlier. Before this work, the "Network Intrusion Detection and worked on the selection of the best countermeasures to mitigate the risks to cloud virtual networks. [4]

2. LITERATURE REVIEW

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. [5]

Through cloud computing, cyberattacks 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, 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. 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. [6]

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. [7]

In this data theft, accidently Epsilon exposed millions of name of the customer with their emails from the database. A similar case happened with Stratford where he was cyber-robbed with 860000 user names with passwords and 75000 credit card numbers. It is also possible that after 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. [8]

3. RELATED WORK

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. [9]

4. METHODOLOGIES

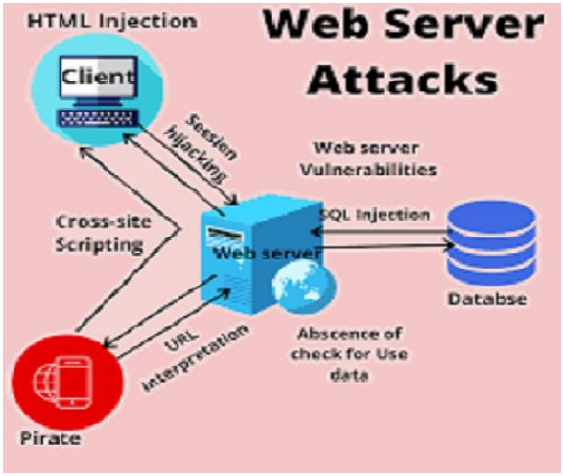

Fig 1. System Architecture

In this paper, we mainly focus on the integrity checking for data shared within a group. Suppose there is a scenario that a software engineer starts an open source project and calls on volunteers from the world to join the project. They work as a temporary team. All the codes of the project are stored on certain cloud server so that all the team members upload and modify the source code by Internet. The team may be very big, so it should be set up and managed efficiently. The volunteers may leave the team at any time, so the problem of user revocation from the

team should be considered. The most important thing is that there need some way to guarantee the integrity of source codes on cloud sever. Motivated by such requirement, we propose a new RDPC scheme for data shared in a group. Different from previous work, our scheme is based on the certifcateless signature technique to avoid the problems of certificate management and key escrow. In our scheme, the group creator generates the partial key for each group user on behalf of key generation center. Each user selects a secret value privately. The private key of each group user contains two parts: a partial key and a secret value. All the data blocks are signed by group user to get corresponding authentication tags. During the data verification, all the tags are aggregated to decrease the computation and communication cost. Based on CDH and DL assumptions, we prove the security of our scheme. Besides, our scheme supports public verification and efficient user revocation. We implement our scheme and perform some experiments. The experiment results indicate that our scheme has good efficiency.

5. PROPOSED ALGORITHM

SQL injection

SQL injection usually occurs when you ask a user for input, like their username/use rid, and instead of a name/id, the user gives you an SQL statement that you will unknowingly run on your database. Session simply means a particular interval of time.

Session Tracking

Session Tracking is a way to maintain state (data) of a user. It is also known as session management in servlet.

DATA MINING WITH PRIVACY

In this paper, we mainly focus on the integrity checking for data shared within a group. Suppose there is a scenario that a software engineer starts an open source project and calls on volunteers from the world to join the project. They work as a temporary team. All the codes of the project are stored on certain cloud server so that all the team members upload and modify the source code by Internet. The team may be very big, so it should be set up and managed efficiently. The volunteers may leave the team at any time, so the problem of user revocation from the team should be considered. The most important thing is that there need some way to guarantee the integrity of source codes on cloud sever. Motivated by such requirement, we propose a new RDPC scheme for data shared in a group. Different from previous work, our scheme is based on the certifcateless signature technique to avoid the problems of certificate management and key escrow. In our scheme, the group creator generates the partial key for each group user on behalf of key generation center. Each user selects a secret value privately. The private key of each group user contains two parts: a partial key and a secret value. All the data blocks are signed by group user to get corresponding authentication tags. During the data verification, all the tags are aggregated to decrease the computation and communication cost. Based on CDH and DL assumptions, we prove the security of our scheme. Besides, our scheme supports public verification and efficient user revocation. We implement our scheme and perform some experiments. The experiment results indicate that our scheme has good efficiency.

SNAP SHOTS

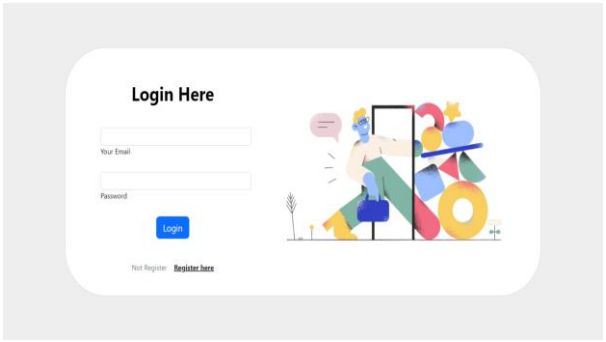

Fig 2. Login Page

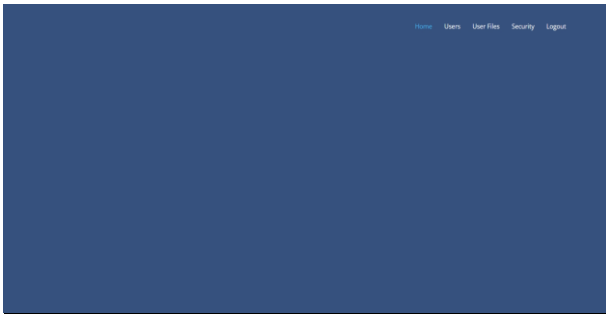

Fig 3. Admin login Page

Fig. 4: Admin login Page

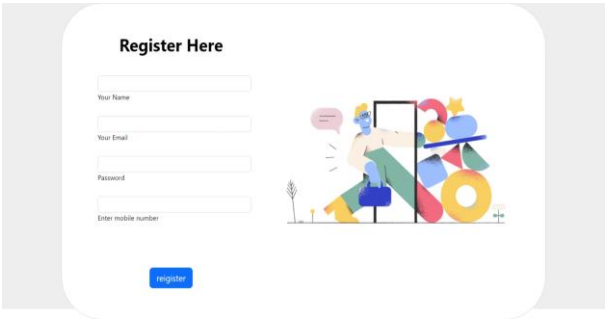

Fig 5. Registration Detail Page

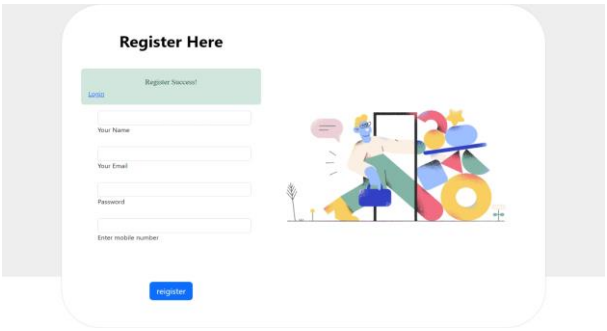

Fig 6. Registration Success Page

Fig 7. Data Owner Request Page

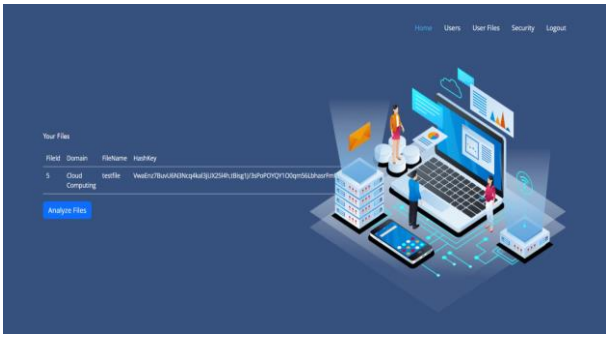

Fig 8. User Files Page

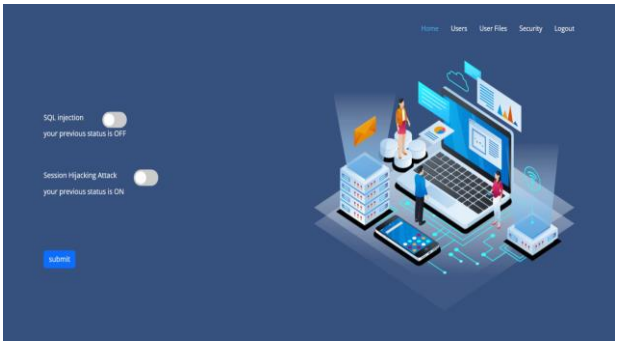

Fig 8. Security Page

.

6. CONCLUSION AND FUTURE ENHANCEMENT

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.GambhirAmruta, “ 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. Insider Threats Related to Cloud Computing, CERT, July 2012. http://www.cert.org/
10. Raghavendra, S., Dhabliya, D., Mondal, D., Omarov, B., Sankaran, K. S., Dhablia, A., . . Shabaz, M. (2022). Development of intrusion detection system using machine learning for the analytics of internet of things enabled enterprises. IET Communications, doi:10.1049/cmu2.12530
11. Rohokale, M. S., Dhabliya, D., Sathish, T., Vijayan, V., & Senthilkumar, N. (2021). A novel two-step co-precipitation approach of CuS/NiMn2O4 heterostructured nanocatalyst for enhanced visible light driven photocatalytic activity via efficient photo-induced charge

separation properties. Physica B: Condensed Matter, 610 doi:10.1016/j.physb.2021.412902

12. Sai Pandraju, T. K., Samal, S., Saravanakumar, R., Yaseen, S. M., Nandal, R., & Dhabliya, D. (2022). Advanced metering infrastructure for low voltage distribution system in smart grid based monitoring applications. Sustainable Computing: Informatics and Systems, 35 doi:10.1016/j.suscom.2022.100691
13. Sharma, R., & Dhabliya, D. (2019). A review of automatic irrigation system through IoT. International Journal of Control and Automation, 12(6 Special Issue), 24-29. Retrieved from www.scopus.com
14. "Security of Infrastructure as a Service Clouds: A Survey" by Rania Jammazi, Hanêne Ben-Abdallah, and Yacine Challal. Published in the Journal of Cloud Computing: Advances, Systems and Applications in 2016. (https://link.springer.com/article/10.1186/s13677-016-0052-4)
15. Hafsa Fatima, Shayesta Nazneen, Maryam Banu, Dr. Mohammed Abdul Bar," *Tensorflow-Based Automatic Personality Recognition Used in Asynchronous Video Interviews*", Journal of Engineering Science (JES), ISSN NO:0377-9254, Vol 13, Issue 05, MAY/2022
16. Mohammed Shoeb, Mohammed Akram Ali, Mohammed Shadeel, Dr. Mohammed Abdul Bari, "*Self-Driving Car: Using Opencv2 and Machine Learning*", The International journal of analytical and experimental modal analysis (IJAEMA), ISSN NO: 0886-9367, Volume XIV, Issue V, May/2022
17. Mr. Pathan Ahmed Khan, Dr. M.A Bari,: Impact Of Emergence With Robotics At Educational Institution And Emerging Challenges", International Journal of Multidisciplinary Engineering in Current Research(IJMEC), ISSN: 2456-4265, Volume 6, Issue 12, December 2021,Page 43-46
18. Mohammed Abdul Bari, Shahanawaj Ahamad, Mohammed Rahmat Ali," *Smartphone Security and Protection Practices*", International Journal of
19. Engineering and Applied Computer Science (IJEACS) ; ISBN: 9798799755577 Volume: 03, Issue: 01, December 2021
20. Shahanawaj Ahamad, Mohammed Abdul Bari, *Big Data Processing Model for Smart City Design: A Systematic Review* ", VOL 2021: ISSUE 08 IS SN : 0011-9342 ;Design Engineering (Toronto) Elsevier SCI Oct
21. Mohammed Abdul Bari, Shahanawaj Ahamad, Mohammed Rahmat Ali," *Smartphone Security and Protection Practices*", International Journal of Engineering and Applied Computer Science (IJEACS) ; ISBN: 9798799755577 Volume: 03, Issue: 01, December 2021 (International Journal,U K) Pages 1-6
22. Dr. M.A.Bari, "*EffectiveIDS To Mitigate The Packet Dropping Nodes From Manet* ", JACE, Vol -6,Issue -6,June 2019
23. M.A.Bari & Shahanawaj Ahamad," *Process of Reverse Engineering of Enterprise InformationSystem Architecture*" in International Journal of Computer Science Issues (IJCSI), Vol 8, Issue 5, ISSN: 1694-0814, pp:359-365,Mahebourg ,Republic of Mauritius , September 2011

24. M.A.Bari & Shahanawaj Ahamad, "*Code Cloning: The Analysis, Detection and Removal*", in International Journal of Computer Applications(IJCA),ISSN:0975-887, ISBN:978-93-80749-18-3,Vol:20,No:7,pp:34-38,NewYork,U.S.A.,April 2011
25. Ijteba Sultana, Mohd Abdul Bari and Sanjay," *Impact of Intermediate Bottleneck Nodes on the QoS Provision in Wireless Infrastructure less Networks*", Journal of Physics: Conference Series, Conf. Ser. 1998 012029 , CONSILIO Aug 2021