# A STUDY OF IDENTIFYING AND DISCUSSING CLOUD COMPUTER THREATS AND ATTACKS WITH MITIGATION

**Ankur Biswas,**
Research Scholar, Dept. of Comp. Sc.& Engg.,
Adamas University, Kolkata, India
Email: ankur2u@gmail.com

**Abhishek Roy,**
Associate Professor, Dept. of Comp. Sc. & Engg.,
Adamas University, Kolkata, India
Email: dr.aroy@yahoo.com

**ABSTRACT:** Saving documents by the use of the cloud is identified as fast and expanding modern technology that helps in cooperating numerous internet activities to the customers. Additionally, it is incorporated in big companies such as Amazon, Apple, Google, Microsoft, and IBM. However, these companies have reported a great loss in their data due to malicious invaders, hackers, and many other unauthorized users as it al- lows third-party involvement. Therefore, the companies need to upgrade and maintain their positions in the fast computer-based environment and it's had to enhance services of large number of users. The fast-growing technology has raised needs that need to be addressed with security which hinders its work. Challenges in the security sectors such as threats and attacks have greater concerns that need to be addressed properly in avoiding security problems for better customer services. The paper identifies the use of internet storage, the obstacles, and insecurity plots with their immediate methods that can be used even in the future.

**KEYWORDS:** Cloud Computing, Security, Threats, Attacks.

## 1 INTRODUCTION

The use of cloud technology is flashbacked to the 1960s that were present on the systems only and with time evolving into the cloud. Therefore, the word cloud has come from the network symbols where the internet was mostly being referred to as a cloud. Therefore, technologies are virtual and clustering that include computing of grid which don't just offer low rates for their users, however, eliminating the cost of maintenance used in maintaining the data center [1]. The National Institute of Standards and Technology came up with the definition of cloud computing model used as a tool that enables network access in sharing a number of grouped resources like storage, network, services, and servers which might get easy provisioned including being given with a low managerial or the use of service providers. However, the use of the cloud has a good attribute on its security that is still new and it needs to be looked into in a broader manner. According to Subramanian et al. (2018), many researchers have placed them focus on insecurity issues, however, due to the technology concerning the core problem, cloud computing technology is still in its infancy [2]. This work provides a summary of basic insecurity threats that exists in the use of cloud technology but with a better explanation of a resolution of all the security threats.

## 2 CLOUD COMPUTING MODELS

The programs used in cloud computing have different models that are used in services deployment which include the hybrid cloud, private cloud, community, and public cloud computing as shown in Fig - 1

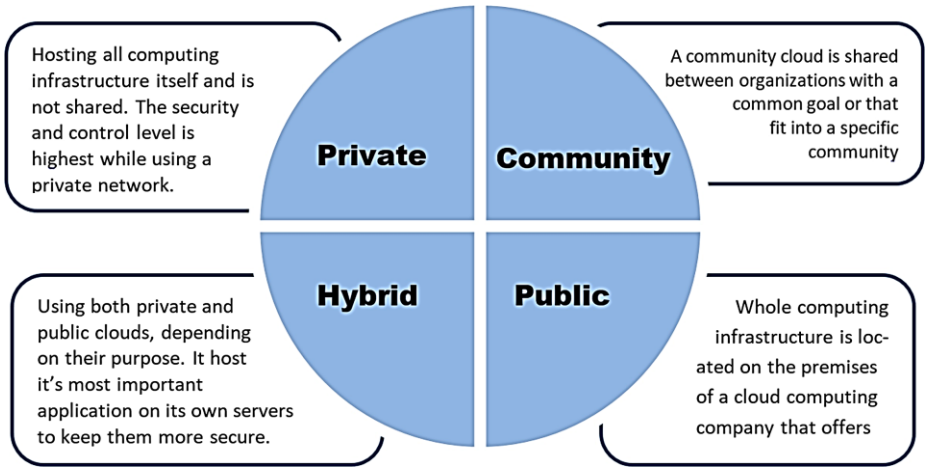


**Fig. 1.** FEATURES OF CLOUD COMPUTING STRATEGY.

## 2.1 PRIVATE CLOUD

Private cloud infrastructure is witnessed on networks that are private because it is controlled through an organization which is found inside the data center or by a provider of cloud services [3]. The infrastructure is more protected since an organization owns and has access to all systems including the control of service and packages delivery. The private cloud aims in addressing the dangers of insecurity which in return it offers control including coming up with methods and ways to reduce the operating and capital costs.

## 2.2 PUBLIC CLOUD

This type of cloud component has been created for an extensive group or public that is possessed including controlled by a storage provider. Besides, the service tends to be changeably issued on the demand as a pay for any usage approach [4]. Therefore, the resource tends to provide numerous benefits to the consumers such as scalability, location independence, including being flexible and without initial capital investments on the product.

## 2.3 HYBRID CLOUD

The service tends to be a union of the clouds which are connected to each other through a balanced technology in sharing information including the application despite of its possession and location [5]. The hybrid cloud provides more greater control and flexibility over the apps by combining the benefits while handlingthe constraints.

## 2.4 COMMUNITY CLOUD

Community cloud infrastructure has been designed and being used by numerous companies and organizations in a society having shared and common desires. All people within the community cloud have free access to the application's information and data. An extensive number of cloud deployment models tend to be developed due to the different consumers. Virtual Private Cloud for instance is a technique of using public cloud services in a private way including inter- connection of resources by a virtual private network [6].

# 3 THE IMPORTANT REQUIREMENTS OF SECURITY IN CLOUD COMPUTING

According to the International Standards Organization (ISO), data safety deals with the guidance regarding the cloud computing fundamental security needs for a very reliable and safe technology solution [7]. Therefore, it has identified numerous security concerns that overly affect cloud computing as shown in Fig- 2. Confidentiality is the first concern identified which implies the user's data and slowing the advantaged units to just have accessibility to data. Integrity is a concern which tends to ensure there exists no change or

alteration in the information as it is kept or being moved including being accessed by an authorized user to make changes, modifications, copying, and deleting the viable data [8]. Thirdly authentication concern assures identity for the user who gives accessibility to information and which may be performed by applying specific safety to their particulars. Availability deals with the assurance of data that have been demanded by the utilizers of the system or the operations a client requires are steadily available at any place and time. Lastly, the concept of authorization holds the meaning of ensuring the consumers have asked for specific data and possess a right to use the information.

| | | Cloud Delivery Models | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Public Cloud | | | Private Cloud | | | Hybrid Cloud | | |
| Data security requirements | Identification & Authentication | X | X | * | X | X | * | * | X | * |
| | Authorization | X | X | X | * | X | * | * | X | * |
| | Confidentiality | * | X | * | * | X | X | * | X | * |
| | Integrity | X | X | * | * | X | X | X | X | X |
| | Non-repudiation | * | X | * | * | X | * | * | * | * |
| | Availability | X | * | X | X | X | X | * | * | * |
| **Requirements** X = mandatory *= Optional | | IAAS | SAAS | PAAS | IAAS | SAAS | PAAS | IAAS | SAAS | PAAS |
| | | Cloud Deployment Models | | | | | | | | |

**Fig. 2.** CLOUD COMPUTING SECURITY REQUIREMENT

## 4 THREATS OF SECURITY IN CLOUD COMPUTING

Cloud computing has vast advantages in the storage systems of large firms and ensuring data is retrieved at any time access is granted. However, it encounters numerous security threats that mainly shift the customer's preference from embracing the advantages. Data loss is the first security threat identified to be occurring in numerous techniques excluding the famous malicious attacks [9]. The threat is identified in a manner that information may be altered due to modification, deletion, encryption key loss through means such as floods, fires, and earthquakes [10]. Therefore, in mitigating this threat, organizations and data management departments need to keep detailed data backup strategies of information in order to avoid data loss. Data breaches implies a continuous leakage of sensitive or highly profiled data to the intelligible and unauthorized system and application utilizers. Therefore, data intrusion may happen mainly due to having illegal authorization and authentication techniques, including controls of audit, the unpredictable utilization of encryption keys, the difficulties in disposal, as well as failures in the operating system [11]. There are numerous companies that previously reported this issue such as Apple's iCloud, Microsoft, Yahoo, Google, and many others [12]. Thus, data loss and data breaches are fundamental threats affecting cloud computing making many clients question their products, information, and big data safety. Similarly, account or service hijacking is a threat that occurs whenever an attacker gains access in longing in the credentials as the altered account turn into an initiation base and an attacker tends to eavesdrop the general customer businesses refund deceitful information, data manipulation and may mainly react to sessions including redirecting the consumers on prohibited websites and may launch numerous attacks [13]. The unsafe ap- plication programming interfaces (APIs) implies that overly standards area and protocols that many users incorporate in connecting with the cloud operations. Therefore, the safety of cloud computing services relies on the application programming interface to have protected certification values including appropriate access control as well as practice monitoring techniques and avoiding risks such as unknown accessibility, having reusable passwords or tokens, clear-text vali- dation, an inappropriate authorization, restricted supervision, as well as logging abilities. Besides, malicious insiders are the trustworthy individuals in any institution that tends to retrieve

organizational sensitive resources. These people may overly undertake unprivileged operations for infiltrating institutional resources including the damage of the brand, monetary and productivity losses through performing various operations such as the intrusion detection system (IDS) or firewall which pretends to be a legitimate operation. Another threat that occurs whenever an organization gets into the incorporation of the service provided by service providers lacking enough information for the cloud frameworks including its activities without comprehending which system tends to fit for them along-side the threats linked to them is insufficient due diligence. Shared tech concerns that happen in a multi-tenant system where on-demand operations are conveyed applying common infrastructure among several consumers have accessibility to similar cloud computing. Virtualized hypervisors susceptibilities ban the usage for isolation purposes allowing malicious users in having improper control as well as access to rightful consumers. The type of threat that tends to happen together with a notable advantage such as saving time via keeping infrastructure comprising offering ownership is Unknown Risk Profile. But the customers are never inclined to the inner safety processes, patching, including hardening, auditing, and logging process. They provide an increase in an unknown risk profile that causes adverse threats. Besides, there is identity theft that happens whenever an attacker imagines to be somebody through personification by using the actual user credentials in gaining resource access. Changing to the business framework is an adverse risk in which customer information can get reside over various boundaries that are run by several federal laws [14].

## 5 THE SECURITY ATTACKS IN CLOUD COMPUTING

The utilization of Cloud computing in storing and retrieving information, data, and files as it can get accessed at any place virtually can be applied in is used by extensive companies and organizations. Structured Query Language (SQL) Injection attacker involves standard SQL code where an attacker inserts a suspicious code to accessing the protected database in order to retrieve confidential information over the consumer. Therefore, the website tends to allow a data of the hacker to be accessed by SQL Server that considers it as data of the user leading to an attacker gaining knowledge concerning the way a site functions as well as the attacker's decision to change. It has been difficult to implement measures on this threat because the presented techniques for validating or filtering the user input are unreliable [15]. Some super techniques such as dynamic prevention tend to require less human interaction through incorporating extra metadata for imposing a limitation on consumer input that may alter the semantics of initial encryptions. Secondly, there are cross-site scripting attacks where an attacker introduces a suspicious code in the user's web and direct to the attacker's site, and retrieve confident information. These attacks may be used either utilizing the protected XSS that is lasting malicious code storage to an asset controlled by the web application, or the reflected XSS handling instantly reflecting suspicious code on the consumer and thus not kept permanently. The sanitization approach or content filtering allows incorporation of functions of filter that applications after a web application can read the consumer input and prior to incorporation in an activity. Therefore, after using content filtering, the elimination of improper content scripts is complex for software in which HTML mark-up in the consumer input is permitted. Phishing attacks are where the attacker utilizes cloud service. The attacker tends to manipulate a web link in directing the consumer to an incorrect link and through hijacking the account of the user thus accessing sensitive information. This type of attack might be mitigated by noticing pop-ups or spam emails that could be performed by the use of anti-spam applications. Additionally, man in the middle attacks (MITM) is identified when the hacker starts attempting to invade in an on-going communication aiming to inject false data for accessing sensitive information being shared. Therefore, to counter this threat secure socket layer is used which offers safety for the web-found apps. The SSL creates an open utilization of the TCP in providing important end-to-end safe operations through the use of basic protocols called handshake [16]. Cookie poisoning attacks deals with the constant of cookie that is changed in accessing the unapproved app on the web page. Tentatively, the cookie

has confident credentials concerning the user's information, and thus the attacker can access this information while performing these illegal activities [17]. Another threat is CAPTCHA Breaking Attacks. CAPTCHA is an acronym that represents completely Automated Public Turing tests. This is mainly used to inform if the consumer is a suspicious human or program. They are employed to identify whether suspicious applications such as Worms, Bot- nets Trojan are attempting to access a site. Therefore, an attacker can break CAPTCHA through the use of an audio system, text conversation software and can also break images basing on a video-based scheme [18]. Google hacking at- tacks are likewise identified as Google Dorking where the attacking technique uses Google search engines in finding safety configuration loopholes. Thus, with the assistance of search questions, the hacker may easily identify safety susceptibilities as they have the ability to gather data and information concerning the victim they desire to attack.

## 6 CONCLUSION

This work has provided a summary of the basic attacks and threats that exist in cloud operations attached to a viable explanation on the resolution for all the security threats. Cloud computing is a gradual growing technology which have delivered an attractive including viable measurable services allowing the organization to maximize their expenditure in organizations which increases their pro- duction level and profit while saving their cost. All basic safety risks and attacks exist in the cloud community with an appropriate explanation of a resolution for all security threats [19]. Cloud computing together with a rapidly developing tech conveys extraordinary and attractive assessable operations allowing organizations to maximize expenditure in their activities, increase productivity profit level as they save costs [20]. Cloud computing technology has remained a front runner in many companies as they assure the security of the stored data and information for a specified period of time and providing safe, fundamental, and economically practical resolutions. However, it has a dynamic and complicated nature that needs beyond traditional protection. Numerous past and current research have been conducted on cloud computing security engineers who have been not able to offer viable solutions as per the fast-increasing challenges faced in the locale. The security attacks and threats have affected the ideology of cloud computing for several years which calls for mitigation [21]. The mitigation such as the creation of techniques categorizing them regarding the cloud operations affecting and layers of net that offer the residence for the limitless execution of the prevention methods provided. Any later work relating to cloud computing attacks and threats with their prevention should enforce one of the approaches of evaluating the efficiency of available mitigation approaches as wells as mitigations on threats.

## REFERENCES

1. Putnam, A., Caulfield, A., Chung, E., Chiou, D., Constantinides, K., Demme, J., Esmaeilzadeh, H., Fowers, J., Gopal, G., Gray, J., Haselman, M., Hauck, S., Heil, S., Hormati, A., Kim, J., Lanka, S., Larus, J., Peterson, E., Pope, S., Smith, A., Thong, J., Xiao, P. and Burger, D., 2014. A reconfigurable fabric for accelerating large-scale datacenter services. 2014 ACM/IEEE 41st International Symposium on Computer Architecture (ISCA).
2. Islam, S., Mollah, M., Huq, M. and Ullah, M., 2012. Cloud computing for future generation of computing technology. 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER).
3. Biswas, A., Roy, A.: A study on Dynamic ID based user authentication system using smart card.: ajct [Internet]. (2019). [cited 26Feb.2020];5(2). http://www.asianssr.org/index.php/ajct/article/view/871.

4. Li, A., Yang, X., Kandula, S. and Zhang, M., 2011. Comparing Public-Cloud Providers. IEEE Internet Computing, 15(2), pp.50-53.https://10.1109/MIC.2011.36
5. Srinivasan, A., Quadir, M. and Vijayakumar, V., 2015. Era of Cloud Computing: A New Insight to Hybrid Cloud. Procedia Computer Science, 50, pp.42-51.https://doi.org/10.1016/j.procs.2015.04.059
6. Tapas, N., Merlino, G., Longo, F.: Blockchain-based IoT-cloud authorization and delegation. In: 2018 IEEE International Conference on Smart Computing (SMARTCOMP), Taormina, pp. 411–416 (2018)
7. Benhamouda, F., Halevi, S., Halevi, T.: Supporting private data on Hyperledger fabric with secure multiparty computation. In: IEEE International Conference on Cloud Engineering (IC2E), April (2018)
8. Ying, N., Yao, Z., Hua, Z.: The study of multi-level authentication-based single sign-on system. In: 2009 2nd IEEE International Conference on Broadband Network and Multimedia Technology, pp. 448–452 (2009)
9. Kansal, S., Kaur, N.: Multi-level Authentication for Internet of Things to establish secure healthcare network. Int. J. Adv. Res. Ideas Innov. Technol. (2016)
10. Peter, S., Gopal, R.K.: Multi-level authentication system for smart home-security analysis and implementation. In: 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore (2016)
11. Gupta, S., Gabrani, G.: A dynamic two-level priority-based authentication system for job scheduling in a heterogeneous grid environment. In: 2016 SAI Computing Conference (SAI), London, pp. 1100–1106 (2016)
12. Odelu V. (2020) IMBUA: Identity Management on Blockchain for Biometrics-Based User Authentication. In: Prieto J., Das A., Ferretti S., Pinto A., Corchado J. (eds) Blockchain and Applications. BLOCKCHAIN 2019. Advances in Intelligent Systems and Computing, vol 1010. Springer, Cham. https://doi.org/10.1007/978- 3-030-23813-1-1
13. Yu, Y., Zhao, Y., Li, Y., Du, X., Wang, L., Guizani, M.: Blockchain-Based Anonymous Authentication with Selective Revocation for Smart Industrial Ap- plications. IEEE Transactions on Industrial Informatics. 16, 3290-3300 (2020). https://doi.org/110.1109/TII.2019.2944678
14. Almadhoun, R., Kadadha, M., Alhemeiri, M., Alshehhi, M., Salah, K.: A User Authentication Scheme of IoT Devices using Blockchain-Enabled Fog Nodes. 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA). (2018). https://doi.org/10.1109/AICCSA.2018.8612856
15. Park, B., Lee, T., Kwak, J.: Blockchain-Based IoT Device Authentication Scheme. Journal of the Korea Institute of Information Security and Cryptology. 27, 343-351(2017). https://doi.org/10.13089/JKIISC.2017.27.2.343
16. Ghosh, A., Das, T., Majumder, S., Roy, A.: Authentication of User in Connected Governance Model. Data Science and Analytics. 110-122 (2020). https://doi.org/10.1007/978-981-15-5830-6 10
17. Khatun, R., Bandopadhyay, T., Roy, A.: Data modelling for e-voting system using smart card-based e-governance system. Int. J. Inf. Eng. Electron. Bus. 9, 45–52(2017). https://doi.org/10.5815/ijieeb.2017.02.06
18. Applebaum, B.: Key-Dependent Message Security: Generic Amplification and Completeness. Advances in Cryptology – EUROCRYPT 2011. 527-546 (2011). https://doi.org/10.1007/978-3-642-20465-4 29.

19. MAGUIRE, M.: A review of user-interface design guidelines for public information kiosk systems. International Journal of Human-Computer Studies. 50, 263-286 (1999). https://doi.org/10.1006/ijhc.1998.0243
20. Judmayer, A., Stifter, N., Schindler, P., Weippl, E.: Blockchain: Basics. Business Transformation through Blockchain. 339-355 (2018). https://doi.org/10.1007/978-3-319-99058-3 13
21. Judmayer, A., Stifter, N., Schindler, P., Weippl, E.: Blockchain: Basics. Business Transformation through Blockchain. 339-355 (2018). https://doi.org/10.1007/978- 3-319-99058-3 13