EAI Endorsed Transactions
on Scalable Information Systems

Research Article EAI.EU

Determining Intrusion Attacks Against Online Applications Using Cloud-Based Data Security

Rekha M[1*], Shoba Rani P[2]

[1]Department of Information Technology, R.M.K. Engineering College (An Autonomous Institution) Kavaraipettai – 601206
[2]Department of Computer Science and Engineering, R.M.D. Engineering College, India

Abstract

Cloud technology makes it possible for users to access information from anywhere, all the time, on any device, and that is the major cause of the many different types of assaults. In principle, multiple dangers, including data leakage, information leakage, and unauthorized information accessibility, are active in cloud environment layering. Modern technological advancements are made accessible on a daily basis through cloud technology. In the cloud, access control and encryption solutions are more complicated. Because of this greater level, security flaws in online applications and systems are more likely to occur. Somewhere at the ends of the end nodes, a malignant insider can carry out protection assaults. Nevertheless, problems with user privacy and data protection on cloud-based social networking sites continue to exist. Such problems are not known to users. On that social networking site, they post a variety of images, videos, and private information that endures even after eradication. However, some of the data that has been made public was intended to be kept private; as a result, online social information has significantly increased the risk of personally identifiable information leaking. The context of cloud technology depends on the customer capabilities such as quick storing and retrieving offered through cloud computing environments. Dependable cloud providers use a number of methodologies to deliver various digital services, creating a variety of security risks. In this paper, the study of determining intrusive cyber-attacks over the online applications using the cloud data security. Restricting access to shared resources is essential to prevent hackers from stealing vulnerabilities in cloud computing to get unauthorised access to a user's activities as well as information. Gaining access to customer information and obstructing the use of cloud computing are the primary objectives of intrusions on cloud services.

Keywords: Cloud-Based Security, Personally Identifiable Information Leaking, Security Risks, Cyber-Attacks

Received on 16 November 2023, accepted on 26 January 2024, published on 05 February 2024

doi: 10.4108/eetsis.5028

Corresponding author. Email: mra.it@rmkec.ac.in

1.Introduction

Someone with access to the cloud can obtain files at every location worldwide. Access control, data manipulation, and information theft are major issues since they include sensitive and confidential information. Cloud safety precautions must be able to handle the demand for huge information processing as the public cloud deals with huge information storage and easy accessibility [1]. Remote users in a poorly constructed cloud computing system increase the danger of a security breach since a flaw in one user's app might give hackers access to the information of other users. The cloud infrastructure and how it functions have a significant impact on data loss or leakage. Nevertheless, there are a number of private information issues that prevent cloud services from being widely used. Cloud applications and the users who utilise them might be the focus of sophisticated adversaries that want to steal

information and do unwanted activities. Attacks can occur either by targeting a public application explicitly or implicitly by targeting individual users of a cloud application in order to obtain their online credentials. Implementation issues can lead to the misuse and manipulation of cloud services in terms of security concerns. Owing to the rapid development of online information, its cloud-based paradigm spreads processing duties over a vast set of servers as opposed to the original computing paradigm. This paradigm enables users to assign resources as needed and access disc storage devices as desired, delivering quick, effective, and affordable processing capabilities that meet users' storage service demands to the maximum extent possible. Data security is a major concern that cloud storage systems must quickly resolve. In recent days, hostile assaults on cloud-based services have increased, and information leaks from cloud services have also become increasingly common. Data integrity for users is a problem of cloud-based security. Intruders can use the cloud to get unapproved access to sensitive files kept there as more businesses adopt the technology [2]. Suppliers and service companies now face several security concerns as a result of the transition from conventional computing to the cloud. Cloud services have been used to transfer potentially hugely vital data.

Thus, cloud computing enables software, and software is flaw-prone, so attackers exploit it. Nevertheless, with cloud services, the provider as well as the public cloud parties are responsible for minimising the incidence brought on by these attack vectors, contrasting computer systems in a data centre facility. There are many facilities available to cloud users when using a cloud environment. The significance and responsiveness of such options vary from storing routine and open information to highly important and protected data, where attempting to access the latter type of information through someone other than the data user may result in disruptions [3]. When information is provided to a third party other than the owner, the data is compromised. In cloud technology, when data is controlled by a 3rd party and resource usage is encouraged between numerous users, it becomes even more crucial. The use of cloud technology has created attack vectors, such as session hijacking assaults. The two most important concerns that must be taken into consideration while developing a safe and secure computer system are privacy and confidentiality [4]. Cloud technology is exactly the same as all previous computer concepts. Users lose direct control over data administration because data and security are delegated to third-party providers, which may not be trustworthy. Because of this unique characteristic, cloud computing is vulnerable to a number of potential threats. The growing amount of information exchanged between businesses and cloud providers raises the possibility of intentionally and providing private information to untrustworthy third parties without consent. Most security incidents involving cloud storage were the result of criminal activity, malevolent insiders, ransomware, weak passwords, and user error.

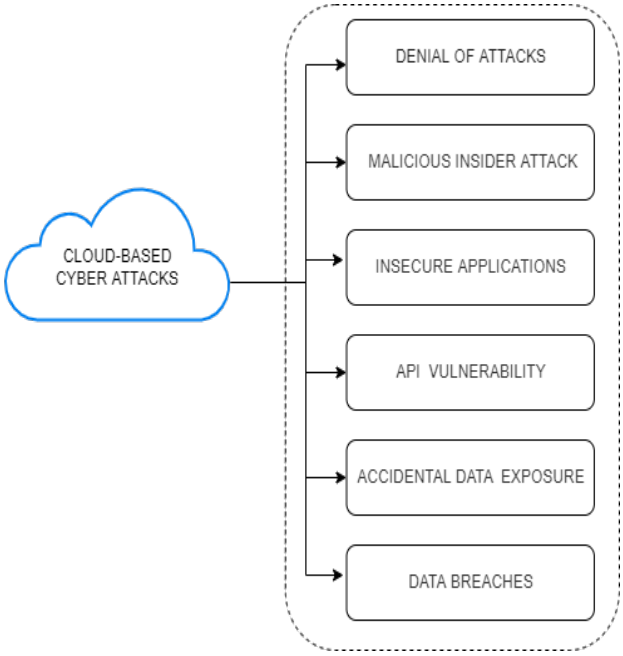

Figure 1. Cyber Attacks in Cloud Computing

In Figure 1, Malicious hackers, especially attackers, try to use known vulnerabilities within cloud computing to steal the private network data of a target company for financial gain or other illegal objectives. In general terms, the qualities that make internet services simple for users to enter through IT platforms simultaneously present a challenge for businesses to prevent illegal use. Public interfaces and verification present extra privacy threats to businesses adopting cloud storage. Advanced attackers target cloud infrastructures in an effort to gain access. Several diverse forms of data, including confidential data about customers or company operations, are stored in public cloud settings. Unfortunately, due to human error, software flaws, and unintended events, such information is prone to risk, invasion, or destruction. There are several ways for authorised cloud users to conduct operations or disclose information on cloud systems. As a result, criminals have the ability to seriously harm a large number of cloud users by taking advantage of flaws in each of these systems. Although cloud service systems are intended to be dispersed ecosystems of cloud storage, there is rarely security between these facilities. As a result, an attacker can utilise flaws in either particular cloud storage service to obtain information relating to real users without their permission.

2. Literature Review

Ajmal et al. [5] introduced the paper on several benefits for businesses using cloud service options. These include cost-effective CC schemes; effective IT administration; and accessibility from anywhere in the world with reliable connectivity. Further research is required to address related privacy risks on the internet. The investigators representing the research community, business, or regulatory domains were given a potential solution to this issue by the prior studies that had been publicized. This research offers a thorough analysis of the security threats related to several cloud service factors. The report also suggests a fresh categorization of this field's evolving security mechanisms. This study focuses on now and examines the specific safety issues that cloud enterprises, including cloud providers, data owners, and users, experience.

Zhe et al. [6] proposed the paper on the power of technology is one in which cloud technology is crucially significant. Using a significant number of cloud machines, cloud computing provides on-demand services via the Internet. This foundation of shared resources that cloud computing offers is virtualized. The biggest problem with cloud technology involves privacy. Cloud technology makes it possible for users to gain access to anything at any time through the internet, which is also the major cause of many different types of assaults. The above paper involves an examination of a proper theoretical research study on cloud technology that conveyed numerous potential threats as well as a taxonomic classification prototype in which a multitude of distinct attack vectors access every stack from using cloud services, in addition to the suggested processes as well as the alternatives previously available.

Umamageswaran et al. [7] illustrate how assaults on traffic get increasingly difficult to identify as internet traffic increases. Scientists have previously started to investigate machine learning approaches using cloud technology in order to categorize security attacks. Malignant attack vector sophistication has grown from traditional malignant attack technology solutions that include malicious user attack courses such as DoS, Probe, R2L, and U2R targeted hackers, particularly the zero-day strike in online applications. By identifying an invasion in cloud technology before it interferes with regular network operations, the paper describes the origin of the aforementioned problems. Some concepts of the newly developed spiked CNN architecture known as the NeuCube algorithms are adopted by the proposed integrated intrusion prevention cloud service.

In [8], the paper on deep learning has indeed been researched in a broad variety of sectors and delivered unmatched performance outcomes, especially with the development of methods in vast datasets and advanced computing capabilities. Data-based teaching methodologies will certainly raise user privacy problems as well as various governmental concerns regarding their application in the real world. Finally, we suggest SecureNet, the first private information and verified forecasting method, to safeguard consumer privacy and modelling validity in DNNs. During the prediction step, this can substantially withstand a variety of sensitive and confidential information. Our simulations of SecureNet using a real dataset demonstrate its improved results in identifying different integrity threats against Dnn's.

Choudhury et al. [9] introduced cost-effective CC schemes, effective IT administration, and accessibility anywhere in the world via reliable internet connectivity. Further research is required to address related privacy risks in the cloud. The earlier studies that had been reported gave investigators from the research community, business, and regulatory domains a potential solution to these challenges. This study provides a descriptive analysis of the issues, specifications, risks, and flaws related to cloud security. This paper's goal is to investigate the various components of CC as well as contemporary security issues. This research offers a thorough analysis of the security threats related to several cloud service factors. This report also suggests a fresh categorization of this field's evolving information security.

3. Methodology

Cyber-Attacks in Online Applications

Each web application has flaws, which are the most important places where hackers might exploit the system. Most of the majority of security flaws are caused by code errors that go unrecognised during the design phase. Privacy integration supports this by making it easier to identify unwanted access permissions. It is necessary to take precautions to prevent unauthorised access to any system components. Only after that could a system that ensures correct verification and accessibility restrictions be guaranteed. Since individuals are the weakest point in today's linked environment and account for the majority of security vulnerabilities, improving users' capacity to recognise, thwart, and fight cyberattacks is crucial. Phishing may become more persuasive and be made to fraudulently link victims to a legitimate company wherein victims could have an identity by collecting data about targets.

When victims submit sensitive data, like credit card info, users are sent to a fake website run by hackers. Drive-by download is indeed a type of malware software that spreads infection even without the perpetrator's awareness by taking advantage of flaws in webpages, plug-ins, or even other browser-related elements [11]. Users participating in a response phase may benefit from using a cyber-attack categorization and category to not only detect assaults but also propose countermeasures to avoid, reduce, and fix cybersecurity risks. When a user of a service or webpage is

refused access to it, it is described as a "denial of service." In this type of cyberattack, the perpetrator sends a huge number of requests to the target website's web application [12].

Due to it, the webpage uses all of its bandwidth utilisation and crashes or is unavailable for a while. Organizations could use a highly secured strategy to stop intrusions, safeguard technology, and enhance quality during an epidemic. In Table 1, Throughout the procedure, a suitable incident response plan defines the people in charge of various tasks.

Table 1: Cyber-Attacks in Cloud Computing

Cyber-Attacks	Description	How it Affects Cloud?
Data breach	Unauthorized access to or exposure of sensitive, privileged, or somehow safeguarded data.	Availability might expose the cloud to information known vulnerabilities.
Denial of service	An intrusion is a deliberate attempt to saturate a website with more traffic so as to interfere with its regular functions.	DDoS may drastically lower the efficiency of cloud applications by destroying their servers.
Malicious insider activity	An individual who deliberately and intentionally utilises login credentials to steal data, usually for personal or financial reasons.	A malicious insider could acquire the private information of a cloud service.
Insecure applications	Insecure APIs can be used by adversaries to expose or steal confidential and sensitive information.	To discover and use viable techniques for getting into and escaping a cloud used by an enterprise and stealing important data.
API vulnerability	Utilization of fraudulent credentials to obtain access to endpoints	It may result in cybersecurity threats and interfere with the accessibility of cloud infrastructure-based applications.
Misconfiguration	Attacks that take advantage of web and application infrastructure configuration flaws	When a user, administrator, or group disregards proper security measures in a cloud platform.
System vulnerabilities	A weak spot in a device or software that could be utilised by an intruder to cause harm or influence it in another manner.	Ineffective access restrictions and the abuse of employee credentials can lead to unauthorised users.
Accidental cloud data disclosure	Databases are simple objectives for malicious attackers since they may have weak passwords or don't necessitate any verification whatsoever.	Affects cloud data due to weak passwords or credentials of user.

Cloud Computing

With the advent of cloud computing, the traditional model of service delivery has changed. Utilizing the cloud has resulted in lower expenses, a profitable business model, and a high level of versatility. Transferring its services to the cloud has helped several businesses who have embraced cloud computing. Technologies for cloud computing have strong limitations on user information privacy because distant systems run by third-party service suppliers might acquire important user information in unsecured formats [15]. There are a number of methods for safeguarding user information against intruders. Advanced techniques and regulations are used in cloud technology to safeguard the architecture and applications, including information [16]. Cloud storage makes it possible for users to gain access from anywhere and at any time over the internet, which is a major cause of the numerous different types of assaults. However, safety remains a significant difficulty despite the fact that ongoing deployment and progress with respect to security risks and their remedies over cloud technology with the advancement of time.

4. Construction

Cloud Data Security

Cloud technology is comparable to cloud technology since it is built on a virtualized framework and offers operational systems, flexibility, and measurement capabilities [18]. The challenge of data security in cloud storage is becoming more difficult as data centralization and quantity rise. Data at rest refers to information that is stored online or that can be accessed through a network. This applies to both live and backup information. Data in transit often refers to information moving to and from the cloud. It's possible that this data will need to be used elsewhere, perhaps in the form of a cloud-stored database or document.

Cloud Data Integrity [19] - Prior to outsourcing, data is protected to guard against harmful internal or external assaults. Confidentiality is helpful in avoiding unauthorised individuals and external servers from accessing and disclosing your data. encrypted data in order to prevent unauthorised individuals from decrypting it. Confidentiality is the method used to prevent unauthorised users, external servers, or unlawful accessibility to and disclosure of information. Data is encrypted in order to prevent unauthorised users from decrypting it [20].

5. Experimental Results

Table 2. Review on Cloud Data Security Attacks with Countermeasures

Cyber-Attacks	Description	How it Affects Cloud?
Data breach	Unauthorized access to or exposure of sensitive, privileged, or somehow safe guarded data.	Availability might expose the cloud to information known vulnerabilities.
Denial of service	An intrusion is a deliberate attempt to saturate a website with more traffic so as to interfere with its regular functions.	DDoS may drastically lower the efficiency of cloud applications by destroying their servers.
Malicious insider activity	An individual who deliberately and intentionally utilises login credentials to steal data, usually for personal or financial reasons.	A malicious insider could acquire the private information of a cloud service.
Insecure applications	Insecure APIs can be used by adversaries to expose or steal confidential and sensitive information.	To discover and use viable techniques for getting into and escaping a cloud used by an enterprise

Cloud Data Availability - For cloud infrastructure services, availability refers to the percentage of the service's acquired time where the storage system is reachable or provides the intended IT function [21]. This method is used to make sure data is accessible to apps and end users when or as they require it. It is known as data availability. Availability is a crucial element since accessibility is related to information's persistence and accessibility.

Cloud Data Confidentiality - Data confidentiality is the capacity of a group of individuals to exchange private information whilst upholding the rights given to each user by the owner. Only the authorised and given permission devices are granted permission to view the information, which is guaranteed by confidentiality [15]. Confidentiality prevents unwanted data access both while it is being kept and while it is being transferred. Because these offer an extra layer of security against the revelation of personal details and shield organisations from potential financial consequences of revealing sensitive data to privacy violations, encryption methods are being utilised in several situations where data security is necessary. revelation of personal details and shield organisations from potential financial consequences of revealing sensitive data to privacy violations, encryption methods are being utilised in several situations where data security is necessary.

		and stealing important data.
API vulnerability	Utilization of fraudulent credentials to obtain access to endpoints [22].	It may result in cybersecurity threats and interfere with the accessibility of cloud infrastructure-based applications.
Misconfiguration	Attacks that take advantage of web and application infrastructure configuration flaws	When a user, administrator, or group disregards proper security measures in a cloud platform.
System vulnerabilities	A weak spot in a device or software that could be utilised by an intruder to cause harm or influence it in another manner.	Ineffective access restrictions and the abuse of employee credentials can lead to unauthorised users.
Accidental cloud data disclosure	Databases are simple objectives for malicious attackers since they may have weak passwords or don't necessitate any verification whatsoever.	Affects cloud data due to weak passwords or credentials of user.

6. Conclusion

Malicious Attackers in apps are dependable based on those individuals' having access to private resources. In Table 2**,** through using various tools, such as the router or intrusion detection system, individuals can carry out unauthorised actions to access corporate resources and cause damage, reputation damage, and financial difficulties by misrepresenting their actions as legitimate ones. Since cloud technology is complex and complicated, conventional safety is far from sufficient. Guarantees of cloud security compliance make sure the public cloud complies with established commercial and governmental standards. Maintaining compliance with any of these industry regulations is crucial. While cloud services assert that their technology is sufficiently protected and safe, assaults can occasionally occur on this system. Organizations may profit from security mechanisms that are required owing to the complexities of the public cloud. Nevertheless, certain user errors might still result in information disclosure. Whenever data is kept in the public domain, anybody with credentials to a cloud provider could improperly access data. A malicious app would be created by a hacker and introduced into SaaS, PaaS, or IaaS services. When viruses have been introduced into the cloud programme, this will reroute the user's request towards the hacker's modules, resulting in the execution of harmful software. Attackers insert malicious files into vulnerable website pages in order to obtain the victim's browser.

References

[1] Bella , H, K, Vasundra, S.: A study of Security Threats and Attacks in Cloud Computing, 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT),2022; pp. 658-666.

[2] Sansanwal, S, Jain, N.: Security Attacks in Cloud Computing: A Systematic Review, Third International Conference on Inventive Research in Computing Applications (ICIRCA), 2021; pp. 501-508.

[3] Balasubramaniam S, Joe V, Sivakumar TA: Optimization Enabled Deep Learning-Based DDoS Attack Detection in Cloud Computing. International Journal of Intelligent Systems. 2023; 2023:1-14

[4] Shantha R, Mahender K, Jenifer A: Security analysis of hybrid one time password generation algorithm for IoT data. AIP Conference Proceedings. 2022; 2418:1-10

[5] Ajmal, Ibrar, S, Amin, R.: Cloud computing platform: Performance analysis of prominent cryptographic algorithms, Concurrency Comput., Pract. Exper., 2022; vol. 34, no. 15: pp. e6938.

[6] Zhe, D, Qinghong, W, Naizheng S , Yuhan, Z.: Study on Data Security Policy Based on Cloud Storage,2017; pp. 145-149.

[7] Umamageswaran Jambulingam, Balasubadra, K, A Unique Multi-Agent-Based Approach for Enhanced QoS Resource Allocation in Multi Cloud Environment while Maintaining Minimized Energy and Maximize Revenue, International Journal of Computers Communications & Control, 2022; vol. 17: no. 2: pp. 4296.

[8] Praveena, A, Smys, S.: Ensuring data security in cloud based social networks, International conference of Electronics, Communication and Aerospace Technology (ICECA), pp. 289-295 ().

[9] Choudhury, T, Gupta, A, Pradhan, S, Kumar, P, Rathore, Y.S.: Privacy and Security of Cloud-Based Internet of Things (IoT), 3rd International Conference on Computational Intelligence and Networks (CINE),2017; pp. 40-45.

[10] Shaikh, A, A.: Attacks on cloud computing and its countermeasures, 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), 2016; pp. 748-752.

[11] Garkoti, G, Peddoju S, K, Balasubramanian, R.: Detection of Insider Attacks in Cloud Based e-Healthcare Environment, 2014 International Conference on Information Technology, 2014; pp. 195-200.

[12] Chen , D, Zhao, H.: Data Security and Privacy Protection Issues in Cloud Computing, International Conference on Computer Science and Electronics Engineering, 2012; pp. 647-651.

[13] Duncan, A , J, Creese , S, Goldsmith , M.: Insider Attacks in Cloud Computing, 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012; pp. 857-862 .

[14] Liu, Y, Ma, X, Y, Shu, L, Hancke, G.P, Abu-Mahfouz, A.M, From industry 4.0 to agriculture 4.0: Current status, enabling technologies, and research challenges, IEEE Trans. Ind. Inf.,2021; vol.17, no.6: pp.4322–4334.

[15] Friha, O, Ferrag, M.A, Shu, L, Nafa, M.: A robust security framework based on blockchain and SDN for fog computing enabled agricultural internet of things, in *Proc. Int. Conf. Internet Things and Intelligent Applications*, Zhenjiang, China, 2020; pp. 1–5.

[16] Tewari, A, Gupta, B, Security.: privacy and trust of different layers in internet-of-things (IoTs) framework, *Future Gener. Comput. Syst.*,2020; vol.108: pp.909–920.

[17] Xu, G, H. Li, H. Ren, Yang K, and Deng, R.K.: Data Security Issues in Deep Learning: Attacks, Countermeasures, and Opportunities, in IEEE Communications Magazine, vol. 57, no. 11, pp. 116-122 (2019).

[18] Le, D.C, Zincir-Heywood, A.N.: Machine learning based insider threat modelling and detection, in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manag. (IM)*, 2019; pp. 1–6, Apr.

[19] Morrow, T.: 12 Risks, Threats, & Vulnerabilities in Moving to the Cloud. Carnegie Mellon University's Software Engineering Institute Blog, http://insights.sei.cmu.edu/blog/12-risks-threats-vulnerabilities-in-moving-to-the-cloud/ Accessed August 8, 2022.

[20] Butt, U,A, Amin, R, Mehmood, M, Aldabbas, H, Alharbi, M.T, Albaqami, N.: Cloud security threats and solutions: A survey,'' Wireless Pers. Commun., 2023; vol. 128, no. 1: pp. 387–413.

[21] Touqeer, H, Zaman, S, Amin, R, Hussain, M, Al-Turjman, F, Bilal, M.: Smart home security: Challenges, issues and solutions at different IoT layers, J. Supercomput., 2021; vol. 77, no. 12: pp. 14053–14089.

[22] Yan H et al., Cost-efficient consolidating service for aliyun's cloud-scale computing.: IEEE Trans. Services Comput., 2019; vol. 12, no. 1: pp. 117–130.

[23] Okada, M, Suzuki, T, Nishio, N, Waidyasooriya, H, Hariyama, M.: FPGA-accelerated searchable encrypted database management systems for cloud services, IEEE Trans. Cloud Comput., early access,2020.

[24] Ajmal, Ibrar, S, Amin, R, Cloud computing platform.: Performance analysis of prominent cryptographic algorithms, Concurrency Comput., Pract. Exper.,2022; vol. 34, no. 15: p. e6938.

[25] Butt, U,A, Amin, R, Mehmood, M, Aldabbas, H, Alharbi, M.T, Albaqami, N.: Cloud security threats and solutions: A survey, Wireless Pers. Commun.,2023; vol. 128, no. 1: pp. 387–413.