BioGecko

Vol 12 Issue 02 2023
ISSN NO: 2230-5807

Proposed on Attack Analysis Using Risk Assessment and Security Risk Assessment Using Attacks for Cloud Cyber Security

Umma Khatuna Jannat[1], Dr.M.Mohankumar[2], and Syed Arif Islam[3]

[1]Computer Science, Karpagam Academy of Higher Education,Coimbatore -641021, India,
(E-mail: ummakhatunajannat@gmail.com)
ORCID: 0000-0002-3531-2990

[2]Computer Science, Karpagam Academy of Higher Education, Coimbatore -641021, India
(E-mail: mohankumarcs@kahedu.edu.in)
ORCID: 0000-0002-7021-2725

[3]Computer Science, Karpagam Academy of Higher Education, Coimbatore -641021, India
(E-mail: syedarifislam@gmail.com)
ORCID: 0000-0002-2299-0733

Abstract

Clouds make it possible for people and corporations to use stable platforms to perform various tasks using their own data. A realistic network environment is created, business applications are implemented, specialised computer software is developed, and online storage space is provided by the cloud. In recent years, many people have begun utilising cloud services. Demands from users and the continued growth of cloud providers are hastening the rapidly changing landscape. Due to their ability to provide cloud administration and storage, cloud storage systems have become crucial in the current world. The active migration of data to the cloud by organisations, governments, and individual users in recent years have been led to a considerable increase in the amount of cloud data generated. Such big data sets have potential to be incredibly rich. However, this increases the chance of danger. In the meantime, hackers are increasingly attempting to take advantage of security holes in cloud architecture, which has led to an increase in data breaches at cloud services. This article focuses on actual cloud attacks as well as methods for using cloud computing infrastructure for security. In this article, this paper provides two cloud cyber security proposals. Firstly, attack analysis begins with assessing risk, followed by analysing exploits that are based on that risk.

Keywords: cloud computing, attacks, risk assessment, cloud security

1. Introduction

Big data, or more specifically, mega data, has become a crucial component of modern life. Every day, people deal with thousands of megabytes of data as a result of their personal or professional activities. A lot of storage space is required for all of this data, and it must be consistently available around the clock on all of the different devices that people frequently use and connect to. However, the physical storage space is constrained by the price and a few other elements, such as

the kind of device or the technology it uses to operate. To address the problems with data storage and accessibility for customers, many businesses have developed a fresh, quick, and affordable technology that is popularly known as cloud computing. The efficient operation of information technology is crucial because a lot of data is stored digitally, processed digitally, and transported through IT networks by corporations, government agencies, and individuals. Additionally, enterprises are switching to cloud environments today.

The scientific community has paid a lot of attention to cloud computing. Cloud computing is a strategy for providing simple, on-demand network access to a pool of configurable shared computing resources that can be quickly provided and released with little administrative effort. The cloud is a platform of the future that offers virtualization, high availability, and dynamic resource pools. Although embracing cloud computing has many advantages, also substantial impediments to adoption. Security is one of the biggest obstacles to adoption. Since cloud computing is still a relatively new paradigm in computing, security is the main concern from the standpoints of cloud customers and cloud service providers. The operations and assets of the firm will be impacted by any attack or risk assessment on the cloud, information technology assets in apps, and data. The usefulness of risk assessment is primarily based on this type of attack. The risks that are present in an organisation are an essential component of all business operations. Risk is defined as the likelihood of undesired or unfavorable occurrences. Risk associated with cloud computing and cyber technology is a process that involves detecting dangers based on their nature, likelihood, and potential effects. Once identified, these dangers can then be evaluated and mitigated. According to a different viewpoint, business risks, particularly those connected to use, ownership, operation, and involvement, are associated with cloud technology. For the long-term viability of information technology and to ensure partner trust, the attack on IT risk in the context of the cloud must be taken into account. For organisations moving outside of their data centres, migrating sensitive data and essential applications to a cloud environment is a major concern. The existing literature contains a large number of review papers that focus on cloud computing, but no high-quality research on cloud attack and risk assessment has been published yet to measure the attack and risk assessment.

The purpose of this study is to show how well the suggested system performs in security and analysis, respectively. First, attack analysis uses risk assessment, and second, risk-based exploits are used when an attacker executes a successful attack on the cloud. Therefore, we exclusively consider static attack situations in our suggested method to identify risk assessment in the cloud.

2.Related work

A layered design comprising several services and user control levels is used in cloud computing systems. There are security issues with the cloud system at every layer. Related risk issues and security assaults are taken into account for the SaaS, PaaS, and IaaS layers [1]. SaaS is offered with a specific license-based subscription, pay-as-you-go, in the cloud layer. Platform as a Service (PaaS) offers online services for multi-tenancy, network capacity, operating systems, and storage.

Utility computing, administrative task automation, dynamic scalability, desktop virtualization, policy-based services, and internet connectivity are all provided by infrastructure as a service (IaaS). IaaS offers customers virtual servers with specific IP addresses and storage pools. The idea of a hardware and infrastructure layer has been brought forward, and the hardware layer provides services based on hardware while the infrastructure layer offers system software services [2]. Because hardware and software are connected, it is possible to mix the infrastructure and hardware layers. The difficulties in setting up cloud computing give rise to exploration attacks on each layer. The risk and attacks were divided into the ensuing subsections.

2.1 Database attacks and risks

Data privacy is crucial since applications in cloud computing are deployed in shared resource environments. The three main obstacles to data privacy are availability (backup and replication), authorised access, and integrity. Data integrity guarantees that the data is not tampered with or corrupted while being transmitted. Authorized access guards against intrusion attacks on data, and backups and replicas enable quick access to data even in the event of a technical failure or disaster at a particular cloud site [3][4][5]. Data is exchanged and sent over the shared network backbone. In order to steal information such as login credentials and session details, hostile attackers or hackers can therefore set up covert proxy applications between the cloud provider and the customer. As a third party, a hacker may also use packet sniffing or IP spoofing to get access to and/or modify sensitive or prohibited data [6].

2.2 SaaS attack and risk assessment

SaaS attacks on APIs, publishers, web portals, and interfaces expose SaaS [7] [8]. Attacks on development tools and attacks on management tools are the two main categories under which SaaS attacks are divided [9]. Online services, web portals, and APIs are the most widely used SaaS services. By exploiting web portals and APIs, attackers try to obtain access to services and acquire control over them. Data privacy is impacted by these assaults. Through a variety of assaults and automated methods, hackers attempt to extract the sensitive data stored in publishers' API keys, private keys, and login credentials. The fact that a secure shell could be used to get important credentials could also be used as a way to attack this layer.

2.3 Attack using port scanning on PaaS

When self-service facilities' computing resources are coupled with cloud computing infrastructure, virtualization is a key component. With this capability, deploying and managing servers will take less time, effort, and money. The most harmful attack, port scanning, is thought to have little to no effect on virtual machines but allows the attacker to learn specifics about the state of the ports [10]. Using this knowledge, attackers can launch additional attacks like DDoS attacks, in which they exploit open port addresses to get details about the platform where the connection is made and launch the application process [4][11]. Since the real attack is carried out after the port scanning step, the attacker uses this knowledge along with the vulnerabilities to carry it out.

2.4 Interface attacks on the cloud and risk

A successful attack on the cloud interfaces can grant root-level access to a system without launching a direct attack on the cloud infrastructure [12]. The authentication system of clouds is subjected to two different sorts of assaults. Advanced cross-site scripting (XSS) methods and signature wrapping are both susceptible to the control interfaces [13]. A signature wrapping assault, often known as an XML signature wrapping attack, is the first category of attack [14]. Accounts using virtual machine activities or password resets. The second kind of attack takes advantage of the XSS flaw. Information regarding the login and password pair is stolen via the specific vulnerability attack.

3.Cyberattack on the Cloud

A cloud cyber-attack is a mechanism for abstractly expressing how a specific kind of observable attack is carried out. The paradigm is followed by a description of the scenario in which it is appropriate and then suggestions for minimising it. In order to get unauthorised access to data, an attack may take various different routes by employing scenarios that are described in the course of the attack by indicators and sequence. Analyzing observed occurrences is made easier and less time-consuming when there is an understanding of the impact's repercussions. Each assault scenario affects confidentiality, availability, or integrity in some way. Depending on the type of data, the risk agent's organization will determine the significance of each signal, sequence, and vulnerability.

The probability of an event occurring is referred to as the potential of it happening. The diagnosis of a successful attack is altered and made simpler by the risk score of the identified attack. The risk assessment's likelihood is changed concurrently by the sequence and attack indications.

The attack analysis uses the risk assessment to compute a score for each indication and sequence. Because of the Expectation- E of a security compromise, a threat event, and its Significance - S, we provide the following definition of Risk Assessment- RA:

$$RA = E * S\text{----------}1$$

The attack scenarios and sequence generated by all the probes in the cloud environment are compiled using the correlation we suggested. The risk assessment formula is shown in equation (2). While S can be given a value on a scale, the Expectation E is normally a fraction < 1. Each attack that is discovered will result in a proportionate increase in the value of E. We can determine the risk score for each attack by applying the method for risk evaluation of all suspicious actions:

$$R = \frac{1}{k}\sum S * E\text{----------}2$$

The organization and cloud provider will specify the impact S and probability expectation E of each sequence and attack in a risk assessment implemented across all clouds. The objectives are to entice a possible attacker away from a vital system and gauge the attacker's behaviour to evaluate a positive impact. The value of R for each attack will decide if it is successful or not based on how sensitive the target data is, which is set by the owner in the risk assessment.

4.A Cloud Cyber Risk Assessment

This section evaluates cloud-based risk assessment. The majority of dangers to the cloud cyber network come from all external packets, which also affect other aspects of the network. A couple of these characteristics serve as requirements for an exploit. These prerequisites prepare the cloud cyber network for further exploits when an attacker successfully carries them out. Figure 1 shows a cloud cyber attack scenario and cloud cyber security risk assessment.

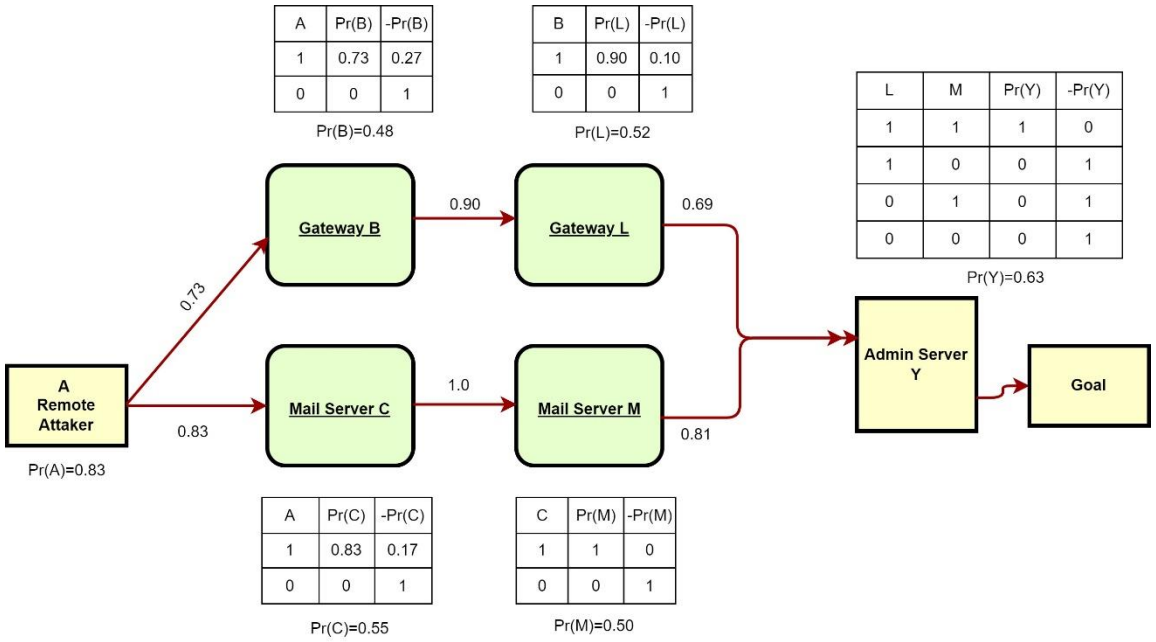

Figure 1: Illustration of an attack

The odds of those attacks packet succeeding will converge, causing estimates of the risk level to be reassessed. Forward propagation will be used to update the attackers of attack packet 0, 1. With backward propagation, the initial presumptions from static risk assessment will be corrected. The odds of success for a set of attacks packet A for which have a proof of an exploit is now 0, 1. As a result, ascertain the effectiveness of the attacks packet that A, the set of N P A, affects. We determine F (N|A).

$$\mathrm{F}j\ (N \mid A) = \frac{[\mathrm{F}j\ (\mathrm{A}|N)\times \mathrm{F}j\ (N)]}{\mathrm{F}j(\mathrm{A})} \quad \text{----------1}$$

$$\mathrm{F}j\ (L \mid Y) = \frac{[\mathrm{F}j\ (Y|L)\times \mathrm{F}j\ (L)]}{\mathrm{F}j\ (Y)}$$

Where,

$$\mathrm{F}j\ (Y \mid L) = \sum_{M\in T,F}\ [\mathrm{F}j(Y \mid L, M = T) \times \mathrm{F}j\ (M)]$$
$$= (1.00 \times 0.55)_T + (1.00 \times 0.52)_L \quad \text{-------2}$$
$$\mathrm{F}j\ (Y \mid L) = 1.07$$
$$\mathrm{F}j\ (L) = 0.52$$
$$\mathrm{F}j\ (Y) = 0.63$$

Therefore,

$$\mathrm{F}j\ (L \mid Y) = 0.83$$

where Fj(N) and Fj(A) are the corresponding packets' previous unconditional probabilities. Given their current conditions, A and N's conditional probability of happening together is calculated. If we have evidence that the result Y was compromised, we can calculate the effect on packet L.

In this case, the initial unconditional probability for the L was 0.52. L's posterior probability increased to 0.83 following the attack occurred at Y. This likelihood score can be used by a network administrator to pinpoint the packets that are most susceptible to assault.

5.Conclusion

Cloud computing is always being improved, so that clients can access various levels of on-demand services. Although there are many advantages to cloud computing, one major issue is security. Clouds still have a lot of vulnerabilities, and hackers are finding ways to use them. Security holes must be found, in order to offer cloud users a higher standard of service. This research paper brings forth an innovative technique for identifying issues in the system based on the assumption that users must be involved in data protection and attack deterrence. Here, advise employing a risk assessment to recognise and analyse assault operations. The proposed method defines an attack by classifying attacks based on the target and symptoms. The correlation process is visible to both the organisation and the user. Information will be protected by this classification, which also attempts to reduce attacks.

Future efforts will concentrate on applying this method with an image recognition system to detect attacks on cloud platforms.

References

[1] Haber, Morey J., Brian Chappell, and Christopher Hills. "Cloud computing." Cloud Attack Vectors. Apress, Berkeley, CA, 2022. 9-25.
[2] Li, Zhi, Ali VatankhahBarenji, and George Q. Huang. "Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform." Robotics and computer-integrated manufacturing 54 (2018): 133-144.
[3] Haber, Morey J., Brian Chappell, and Christopher Hills. "Cloud computing." Cloud Attack Vectors. Apress, Berkeley, CA, 2022. 9-25.
[4] Logesswari, S., et al. "A study on cloud computing challenges and its mitigations." Materials Today: Proceedings (2020).
[5] Sampson, Derrick, and Md Minhaz Chowdhury. "The growing security concerns of cloud computing." 2021 IEEE International Conference on Electro Information Technology (EIT). IEEE, 2021.
[6] Suciu, George, Muneeb Anwar, and Cristiana Istrate. "Mobile Application and Wi-Fi Network Security for e-Learning Platforms." eLearning & Software for Education 1 (2019).
[7] Rath, Annanda, et al. "Security Pattern for Cloud SaaS: From System and Data Security to Privacy Case Study in AWS and Azure." Computers 8.2 (2019): 34.
[8] Díaz de León Guillén, Miguel Ángel, Víctor Morales-Rocha, and Luis Felipe Fernández Martínez. "A systematic review of security threats and countermeasures in SaaS." Journal of Computer Security 28.6 (2020): 635-653.
[9] Mugunthan, S. R. "Soft computing based autonomous low rate DDOS attack detection and security for cloud computing." J. Soft Comput. Paradig.(JSCP) 1.02 (2019): 80-90.
[10] Alhenaki, Lubna, et al. "A survey on the security of cloud computing." 2019 2nd international conference on computer applications & information security (ICCAIS). IEEE, 2019.
[11] Thangavel, M., S. Nithya, and R. Sindhuja. "Denial of Service (DoS) Attacks Over Cloud Environment: A Literature Survey." Research Anthology on Combating Denial-of-Service Attacks (2021): 491-521.
[12] Hu, Tao, et al. "SEAPP: A secure application management framework based on REST API access control in SDN-enabled cloud environment." Journal of Parallel and Distributed Computing 147 (2021): 108-123.
[13] Kaur, Manjit, Manish Raj, and Heung-No Lee. "Cross Channel Scripting and Code Injection Attacks on Web and Cloud-Based Applications: A Comprehensive Review." Sensors 22.5 (2022): 1959.
[14] Krishnamoorthy, N., and S. Umarani. "An experimental study on cloud computing security issues and a framework for xml ddos attack prevention." Journal of Physics: Conference Series. Vol. 2007. No. 1. IOP Publishing, 2021.