International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET218346

Vulnerability Assessment and Penetration Testing Approach Towards Cloud-Based Application and Related Services

Anjani Tiwari, Dr. Priyanka Sharma
School of Information Technology, Artificial Intelligence and Cyber Security, Rashtriya Raksha University, Gandhinagar, Gujarat, India

Article Info
Volume 8, Issue 3
Page Number: 395-403

Publication Issue :
May-June-2021

Article History
Accepted : 01 June 2021
Published: 12 June 2021

ABSTRACT

Cloud solutions provide a powerful computing platform that enables individuals and Cloud users to perform a wide range of tasks, such as using an online storage system, implementing business applications, developing customized computer software, and establishing a realistic network environment. The number of people using cloud services has increased dramatically in recent years, and a massive amount of data has been stored in cloud computing environments. As a result, data breaches in cloud services are increasing year after year as a result of hackers who are constantly attempting to exploit cloud architecture's security vulnerabilities. In this paper, we investigate and analyse real-world cloud attacks in order to demonstrate the techniques used by hackers against cloud computing systems and how to prevent such malicious activities.

Index Terms - Data Breaches, Cloud Security, Cloud Vulnerability Assessment, Cloud Service Model Security Analysis.

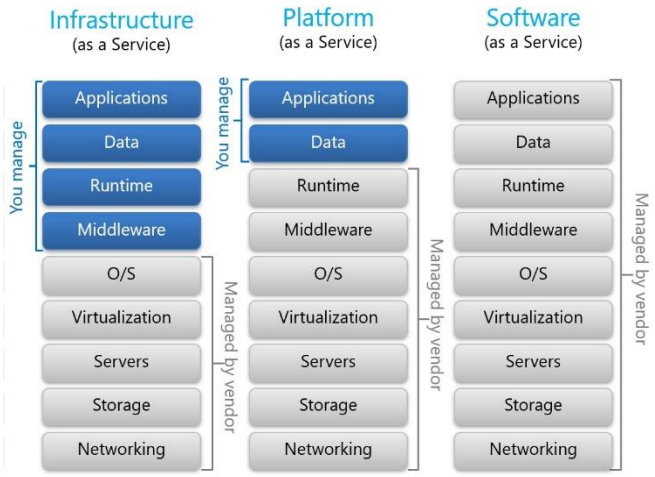
I. INTRODUCTION

CLOUD computing has become a part of everyone's life. It provides applications and storage space as services over the Internet at low to no cost. Most of us use cloud computing services on a daily basis for a variety of reasons. For example, we use web-based email systems to exchange messages with one another, social networking sites (such as Facebook, LinkedIn, and Twitter) to share information and stay in touch with friends, on-demand subscription services (such as Netflix and Vudu) to watch TV shows and movies, and cloud storage (such as Google Drive, Dropbox, OneDrive, and others) to store music, videos, photos, and documents. Cloud computing has also been used in business, such as e-commerce, where companies rent services from cloud computing service providers in order to reduce operational costs and develop money drift. Google has recently launched professional business mail services (e.g., G-suite), storage, data loss prevention, and many other features for G-suite users.

Without a doubt, the convenience and low cost of cloud computing services have altered our daily lives. For example, most mobile phone companies have attached a free cloud service for a limited time. However, the security issues associated with cloud

computing make us vulnerable to cybercrime, which occurs on a daily basis. Hackers use a variety of techniques to gain unauthorized access to clouds or disrupt cloud services in order to achieve specific goals. Hackers could trick a cloud into treating their illegal activity as a valid instance, granting them unauthorized access to the cloud's data. Once the precise location of data has been determined, hackers steal private and sensitive information for criminal purposes. According to Data- Loss DB's 2015 Data Breach Quick View report, external agents or activity outside the organization were responsible for 77.7 percent of reported incidents, with hacking accounting for 64.6 percent of incidents and 58.7 percent of exposed records. Incidents involving US entities accounted for 40.5 percent of reported incidents and 64.7 percent of exposed records. Epsilon and Stratford were both victims of data breaches. Epsilon's data leakage incident exposed millions of names and email addresses from customer databases. 75,000 credit card numbers and 860,000 user names and passwords were stolen from Stratford. Hackers could also use the massive computing power of clouds to launch attacks against users on the same or different networks. For example, hackers rented a server through Amazon's EC2 service and launched an attack against Sony's PlayStation Network. As a result, a thorough understanding of cloud security threats is required in order to provide cloud users with more secure services. A few of these techniques were highlighted in my paper to demonstrate how such attacks are very simple to deploy against any system via a security backdoor.

Cloud computing entails cloud computing service providers providing computing resources (e.g., servers, storage, and applications) as services to end users. Web browsers are used by end users to access on-demand cloud services. Cloud computing service providers provide specific cloud services while also ensuring the quality of the services. Cloud computing is composed of three layers: the system layer, the platform layer, and the application layer.



Cloud Service Model

The system layer is the lowest layer, and it contains computational resources such as server infrastructure, network devices, memory, and storage. It is referred to as Infrastructure-as-a-Service (IaaS). Users can access the computational resources as on-demand services. IaaS provides virtual machines through the use of virtualization technology, allowing clients to build complex network infrastructures. This approach not only lowers the cost of physical equipment for businesses, but it also reduces the burden of network administration because IT professionals are not required to continuously monitor the health of physical networks. Oracle Cloud, Microsoft Azure, Amazon EC2, and IBM-SmartCloud Enterprise are examples of IaaS cloud computing service providers. It offers a virtual computing environment with Web service interfaces, allowing users to deploy Linux, Solaris, or Windows-based virtual machines and run their own custom applications.

The centre layer is the platform layer and is referred to as a platform as a service (PaaS). It is designed to offer users a platform to develop their particular applications. The cloud-based services include application development tools and libraries that enable users to control application deployment and configuration settings. With PaaS, developers do not have to purchase tools for development of software

and thus reduce costs. Examples include Google Apps, a set of Google tools including Gmail, Google Calender, Google Docs, Google Talk, Google Sites, and Google Apps. Lastly, top layer is the software-as-a-service application layer (SaaS). Instead of being paid to purchase such applications, the user can rent applications running on clouds. SaaS is popular for companies deploying their businesses due to its ability to reduce costs. Groupon is a SaaS-used example.

II. LITERATURE REVIEW

Gokay Saldamli , Lo'ai, A. T. has researched Reconsidering significant data security and privacy in cloud and mobile cloud systems [1]. He has proposed a hybrid mobile-cloud model and conducted a simulation to prove the concept of using mobile cloud computing models in a real-life big data application. They have taken measured and compared the performance parameters delay and power consumption. The Cloud and mobile cloud computing platforms are appropriate to host and analyse big data. There are numerous developed and evolving security attacks that pose a threat to the Cloud and mobile cloud computing environments. Protecting big data in such environments needs new efficient countermeasures. Their research would investigate the real-time deployment of modern cryptographic methods such as homomorphic encryption and Format Preserving Encryption in real-world cloud environments to secure big data

In the research paper proposed by Patrick Mosca, Yanping Zhang, Zhifeng Xiao, Yun Wang, Cloud Security: Services, Risks, and a Case Study on Amazon Cloud Services [2]. They review the data storage scheme for Amazon's Cloud. Using Amazon Web Services as a case study, they can implore some of the basic terms and concepts of cloud computing and then discuss data security, API concerns, account hijacking, and other security concerns. These broad problems have been proved to be particularly relevant to cloud security. From a security standpoint, the fundamental contrasts between traditional services and cloud services are compared. Service and account hijacking are discussed, as well as potential defences. They proposed to investigate differences between security issues in cloud services and traditional services. From the practitioners' view, in brief overview the security in Cloud. They paper provides a guideline for research on cloud services and security issues. It gives some ideas on how to build a more secure cloud.

Thomas Länger, H.C., & Ghernaouti, S. has researched Selected Cloud Security Patterns to Improve End User Security and Privacy in Public Clouds [3], work on Cloud security patterns to improve end-user security and privacy in public Clouds. The authors developed several Cloud security patterns for everyday critical situations in the Cloud in the three fields of data storage in the Cloud, user privacy protection and data minimization, and authentication of stored and processed data. The authors focus mainly on protecting data in public Clouds; many security patterns, such as communication, secure architecture, and data governance, are not considered in this paper.

Security Issues and Trends in Cloud Computing, according to G.S.Raghavendra, D.R.N.S.Lakshmi, and S.Venkateswarlu's research paper [4]. This paper discussed about major security problems which stops the growth of cloud computing so far. Cloud computing security encompasses a wide range of topics and concerns. Many security techniques have been developed to safeguard cloud computing systems from various assaults. Researchers are always developing new solutions to increase cloud computing security. Several real-world examples of assaults on company clouds are described in this study. The following attacks are discussed: social engineering, XML signature wrapping, malware injection, account hijacking, and wireless local area network attack.

According to Jitendra singh Cyber-Attacks in Cloud Computing: A Case Study [5]. Given the privacy and regulatory laws, cloud computing security is a major concern. A number of organisations and working groups are collaborating to improve cloud computing security. Working groups are providing draughts of their reports on significant security concerns and offering various approaches to fight them. Despite the fact that numerous studies show that the hosted model is more secure than the on-premises cloud approach. Nonetheless, many assaults are aimed towards the hosted approach in order to exploit the weaknesses. The most common methods of cloud assault are DDoS and phishing. Finally, in light of the phishing and DDoS attacks that have been discovered in several of the cloud, it can be inferred that they are causing massive financial losses as well as damage to data privacy. Although a lot of solutions exist to combat various assaults, there is still a need to tighten security in both hosted and on-premises cloud environments in order to restore user confidence.

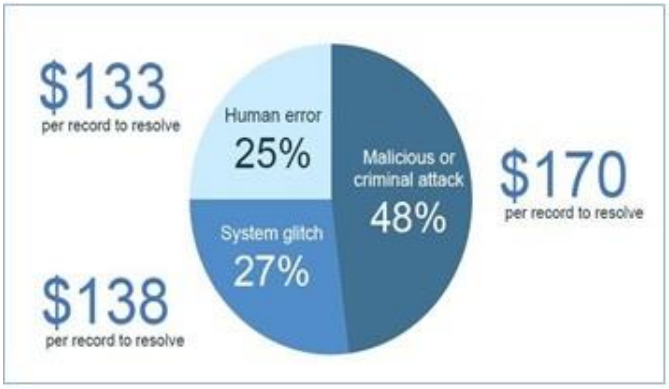
III. SENSITIVE DATA BREACHES STUDY AND COST ANALYSIS

Sensitive data breach occurs when an individual's identity, Home addresses, phone numbers, birth dates, medical record, financial record, or debit card, banking account numbers, credit card numbers, session tokens, Social Security numbers, and user account information including usernames and passwords information is potentially compromised, whether in electronic or paper format. In accordance with global data violations and our survey, three main causes of a data violation have been identified:

- Human error,
- System malfunction,
- A malicious or criminal attack.

The cost of a data breach varies depending on the cause and the security measures in effect at the time of the breach.

Nowadays, data breaches have become a major intellectual topic all over the world, and data breaches are inextricably linked to the global economy. WikiLeaks is a leading international non-profit organisation that publishes classified information, news leaks, and categorised media obtained from anonymous sources.



Cost of a data breach IBM 2016

To investigate this area, IBM is proud to sponsor the eleventh annual Cost of a Data Breach Study, the industry's gold-standard benchmark research, conducted independently by Ponemon Institute and published in 2016. The estimated cumulative cost of a data breach is $4 million, according to this year's report. The cost of each missing or stolen record containing sensitive and confidential information rose from $154 to $158, according to the report. Aside from cost information, the global study estimates that a material data breach involving 10,000 missing or stolen records will occur in the next 24 months at a rate of 26%.

The research also included gathering detailed information about the financial consequences of a data breach. For the purposes of this study, a data breach occurs when sensitive, protected, or confidential data is lost or stolen and put at risk. Over

a 10-month period, Ponemon Institute researchers interviewed IT, compliance, and information security practitioners from 383 organisations in 12 countries: The United States, the United Kingdom, Germany, Australia, France, Brazil, Japan, Italy, India, the Arabian region (a consolidation of organisations in the United Arab Emirates and Saudi Arabia), Canada, and, for the first time, South Africa.

According to our data mining, a large number of data breaches are occurring as a result of malicious attack or activity. As a result, nearly 25% of data breaches are linked to negligent employees or human intervention. A critical role is played by system failure or process gaps, which account for 27% of total data breaches.

IV. SECURITY ANALYSIS AND EXPLORATION ON CLOUD

Three cloud service models (SaaS, PaaS, and IaaS) not only provide different types of services to end users, but also reveal information security issues and risks associated with cloud computing systems. A few of the listed concerns can illustrate the most frightening aspect of cloud services –

- Data security
- Web application security
- Virtualization vulnerability
- Data Availability
- Data confidentiality
- Network security
- Data locality
- Data integrity
- Data access
- Data Backup process
- Identity management
- sign-on process.

IaaS Security Concerns: Specifically, hackers may use the powerful computing capability provided by clouds to conduct illegal activities. IaaS is located in the bottom layer and provides the most powerful functionality of the entire cloud. It maximises extensibility for users to customise a convincing environment that includes virtual machines running different operating systems. Hackers could rent the virtual machines, examine their configurations, identify vulnerabilities, and then attack other customers' virtual machines in the same cloud. IaaS also enables hackers to carry out attacks that require a large amount of computing power, such as brute-forcing cracking. Because IaaS supports multiple virtual machines, it provides an ideal platform for hackers to launch attacks (e.g., distributed denial of service (DDoS) attacks) that require a large number of attacking instances.

SaaS Security Concerns: As a result, data loss is a significant security risk of cloud models. In SaaS cloud models, companies use applications to process business data and store customer data in data centres. Developers in PaaS cloud models use data to test software integrity throughout the system development life cycle (SDLC). In IaaS cloud models, users create new drives on virtual machines and store data on those drives. However, data in all three cloud models can be accessed by unauthorised internal employees as well as external hackers. Internal employees can gain access to data either intentionally or unintentionally. External hackers use a variety of hacking methods, such as session hijacking and network channel snooping, to gain access to databases in cloud environments.

PaaS Security Concerns: In PaaS, the provider usually gives customers some power over the development of their own applications. However, there is still a security gap between application or host security and network security, which is entirely beyond the scope of the service provider to ensure platform security standards of access control and management for delivery or customer service. This scenario confirms

that PaaS is a more comprehensive platform than SaaS, and that providers must ensure that customers have access to more ready-to-use features. As a result, there would be enterprise service bus level process metrics in place to assess application or programme security, as well as adequate security metrics related to coding quality checking, vulnerability scoring, and patch security coverage. Service oriented architecture (SOA) applications at the application and machine levels are now scoring effectively on cloud platforms.

As a result, conventional network attack techniques can be used to harass cloud systems at three levels. Web browser attacks, for example, are used to manipulate cloud server authentication, authorization, and accounting flaws. Malicious software (viruses and Trojans, for example) may be uploaded to cloud systems and cause harm. Malicious operations (such as metadata spoofing attacks) can be encapsulated in a regular command, sent to the cloud, and executed as legitimate instances. In IaaS, a zero-day attack will compromise the hypervisor (e.g. VMware, vSphere, Hyper-V, and Xen) that handles administrative operations for virtual instances.

When it comes to SaaS protection, any malicious user may target any vulnerable system in order to gain access to or control data or systems. Underneath these things are fine to process in the same manner.

- Access control weaknesses
- Cross-site scripting[XSS]
- SQL injection flaws
- Cross-site request forgery[CSRF]
- Cookie manipulation
- Hidden Data field manipulation
- Insecure storage
- Insecure configuration.

In order to enforce better protection protocols to secure cloud computing environments, it is essential to recognise potential cloud threats. In the sections that followed, we looked at cloud security threats from three perspectives: unauthorised use of cloud computational resources, data breaches, and cloud security attacks. Recent real-world cloud attacks were also included to demonstrate the techniques used by hackers to exploit cloud system vulnerabilities.

V. MISUSE AND DATA BREACHES

In the past, hackers used multiple computers or a botnet to generate a large amount of computing power in order to conduct cyber-attacks on computer systems. This is a complicated process that can take months to complete. A powerful computing infrastructure, consisting of both software and hardware components, can now be easily created by completing a simple registration process with a cloud computing service provider. Hackers can launch attacks in a very short period of time by taking advantage of the prevalent computing power of cloud networks. For example, by leveraging the power of cloud computing, brute force and denial-of-service attacks can be launched.

According to IBM's "Cost of Data Breach Study" (2020), the United States is the most expensive country in terms of the average overall cost of a data breach, at $8.64 million. As Coram (2018) writes in his dissertation, the effects on organisations and consumers should not be misconstrued because they have predictable repercussions. He also looks at another independent study by the Ponemon Institute (an independent organisation that conducts research and provides consulting services to companies on developing data protection, privacy, and security applications) and Accenture (2017), which shows that cyberattacks cost companies in the United States about $21 million, which is 21.22 percent higher than the global average. Furthermore, the study claims that global costs have risen by 62 percent in the last five years.

VI. MISUSE OF CLOUD COMPUTING RESOURCES

A brute force attack is a method for cracking passwords. Since thousands of potential passwords must be submitted to a target user's account before it identifies the right one to access, the effectiveness of this assault is highly dependent on powerful computational capacity. The cloud hosting infrastructure offers the ideal environment for hackers to initiate such an attack. At the Black Hat Technical Security Conference, German researcher Thomas Roth showed a brute force attack. By renting a computer from Amazon's EC2, he was able to break a WPA-PSK secure network. Roth shot 400,000 passwords per second into the machine in around 20 minutes, and the cost of using EC2 service was just 28 cents per minute.

DoS attacks aim to interrupt a host or network resource, preventing legal users from accessing the computer service. They come in a range of shapes and sizes, and they tend to provide a variety of facilities. They are broadly classified into three types: the consumption of scarce, finite, or non-renewable resources, the destruction or modification of configuration material, and the physical destruction or alteration of network components. Among them, flooding is the most prevalent method by which hackers destabilise the victim's infrastructure by sending an excessive amount of fake requests; as a result, legitimate users' services are disrupted.

When a flooding attack is used against cloud services, two forms of denial of service (DoS) can occur in cloud computing systems: direct DoS and indirect DoS. When a cloud server receives a high number of flooded requests, it can allocate additional computing resources to deal with the malicious requests. Finally, the server's capacity is depleted, and all valid user requests are subjected to a direct Does. Furthermore, the flood attack could trigger indirect DoS to other servers in the same cloud if they share the workload of the victim server, resulting in a complete lack of availability on all services.

Cloud storage platforms may be used to send a large number of packets to a network of concern. For example, two security consultants, Bob and Alice, used Amazon's EC2 cloud infrastructure to conduct cloud-based DoS attacks against one of their clients in order to test its connectivity. They rented virtual servers on EC2 for a few dollars and used a homemade "Thunder Clap" programme to successfully flood their client's server and render the business unreachable on the Internet. According to his report, massive-scale DDoS attacks were launched against Bit-bucket, an Amazon-hosted Web-based hosting service, using two flooding techniques: a flood of UDP packets and a flood of TCP SYN link requests. Due to the extreme attacks, the organisation became inaccessible, and many developers lost access to projects hosted on Bit-bucket.

VII. SECURITY BREACH IN SONY

The Sony's security breach has informed the entire internet community. 100 million account records were compromised as a result of the attack. Instead of focusing on this strike, attackers launched another attack on Sony's online entertainment, exposing an additional 25 million users. An investigative team was formed by the corporation to determine the reasons. It was discovered that the attack occurred due to the presence of two servers behind the firewall. The web server and the application servers were the two servers. The attacker used application server vulnerabilities to target the web server.

DDOS ATTACK ON BITBUCHET

The Bitbuchet is a development company that hosts its infrastructure in the cloud. It has a subscription to Amazon EC2. This service abruptly ceased operations in 2009. As a result, the entire production was reduced. The problem persisted for several hours (19

hours approximately) before the services were restored. Only once the Amazon recognised the issue could it be addressed.

VII. RESEARCH GAP

There is a significant amount of security pattern study in software engineering. However, the study was more generic in nature and did not focus specifically on the Cloud. Furthermore, they limit themselves to very specific issues, such as authentication and authorization security or threat, and disregard some other security issues that they believe are unimportant, such as resource management. In our work, we concentrate on all areas of cloud security. We cover data and system security and privacy, which is often disregarded due to its complexity.

VIII. CONCLUSION AND FUTURE WORK

In this paper, we demonstrated experimentally how to build a cloud environments platform that includes user publishing via a global DNS service. Following that, we attempted to gather information about less secure Web services and revealed the specific connections that were responsible for data breaches. Furthermore, SQL injection was described as part of the pretesting process and demonstrated how to detect network traffic packets in conjunction with a Firewall ACL policy that confirmed and alerted if any anomaly packets passed or not. A few steps are discussed in relation to security reconciliation, together with cloud seal door architecture. For such environments or services, key-based access may be imposed or supplied. During access from particular or random devices, a real-time threat detection system or agent-based services tracking is recommended. We should implement a low-access rule, a daily check-maker, and impose security for all characteristics located in the onsite datacenter, cloud, and distant location, as well as an arrangement of sophisticated Security applications and appliances to lower the risk level.

IX. REFERENCES

[1]. Lo'ai, A. T., & Saldamli, G. (2019). Reconsidering big data security and privacy in cloud and mobile cloud systems. Journal of King Saud University-Computer and Information Sciences.

[2]. Mosca, P., Zhang, Y., Xiao, Z., & Wang, Y. (2014). Cloud security: Services, risks, and a case study on amazon cloud services. Int'l J. of Communications, Network and System Sciences, 7(12), 529.

[3]. Länger, T., Pöhls, H. C., & Ghernaouti, S. (2016, September). Selected cloud security patterns to improve end user security and privacy in public clouds. In Annual Privacy Forum (pp. 115-132). Springer, Cham.

[4]. Raghavendra, G. S., D. R. N. S. Lakshmi, and S. Venkateswarlu. "Security issues and trends in cloud computing." International Journal of Computer Science and Information Technologies (IJCSIT) 6.2 (2015): 1156-1159.

[5]. Singh, Jitendra. "Cyber-attacks in cloud computing: A case study." International Journal of Electronics and Information Engineering 1.2 (2014): 78-87.

[6]. "Sony Still Digging Its Way Out of Breach Investigation, Fallout" https://www.darkreading.com/attacks-breaches/sony-still-digging-its-way-out-of-breach-investigation-fallout/d/d-id/1135653?

[7]. "The NIST definition of cloud computing", Special Publication 800-145, National Institute of Standards and Technology, http://csrc.nist.gov/ publications/ PubsSPs.html#800145.

[8]. Xiao, Z. and Xiao, Y. (2013) Security and Privacy in Cloud Computing. IEEE

Communications Surveys & Tutorials, 15, 843-859.

[9]. Alruwaili, Fahad F., and T. Aaron Gulliver. "Secure migration to compliant cloud services: A case study." Journal of information security and applications 38 (2018): 50-64.

[10]. A. Hutchings, R. G. Smith, and L. James, “Criminals in the Cloud: Crime, Security Threats, and Prevention Measures,” in Cybercrime Risks and Responses, London: Palgrave Macmillan UK, 2015, pp. 146–162

[11]. OWASP Cloud Security Project. Available online: https://owasp.org/www-project-cloud-security/

[12]. Subramaniam, T. K., and B. Deepa. "Security attack issues and mitigation techniques in cloud computing environments." International Journal of UbiComp (IJU) 7.1 (2016).

[13]. Lo'ai, A. Tawalbeh, and Gokay Saldamli. "Reconsidering big data security and privacy in cloud and mobile cloud systems." Journal of King Saud University-Computer and Information Sciences (2019).

[14]. Li, Huan-Chung, et al. "Analysis on cloud-based security vulnerability assessment." 2010 IEEE 7th International Conference on E-Business Engineering. IEEE, 2010.

[15]. Nabeel, K, Al-Yasiri A (2018) Cloud security threats and techniques to strengthen cloud computing adoption framework. In: Cyber security and threats: concepts, methodologies, tools, and applications. IGI Global, pp 268–285

Cite this article as :

Anjani Tiwari, Dr. Priyanka Sharma, "Vulnerability Assessment and Penetration Testing Approach Towards Cloud-Based Application and Related Services", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 8 Issue 3, pp. 395-403, May-June 2021. Available at doi : https://doi.org/10.32628/IJSRSET218346
Journal URL : https://ijsrset.com/IJSRSET218346