ISSN 2278-3091
Volume 9, No.4, July – August 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse197942020.pdf
https://doi.org/10.30534/ijatcse/2020/197942020

Cloud Computing Authentication Attack and Mitigation Survey

Hesham Abusaimeh[1], and Rame Al-dwairi[2]
[1]Associate Professor in Computer Science, Middle East University, Amman, 11831 Jordan.
habusaimeh@meu.edu.jo | hesham@abusaimeh.com
[2]Network & Security Supervisor, Trust Holding Ltd, Amman, Jordan. rdwairi@hotmail.com

ABSTRACT

Securing the information and customer privacy are very important during the attacks are increased, and the biggest breach happened in the previous year's especially in cloud computing. In cloud computing, we need to use a secure authentication and authorization mechanism to access our data and other services, to ensure the CIA (confidentiality, integrity, and availability). During this survey, we will focus on the authentications attack and how we can have secure access to our environments by reducing the risk of the data breach and mitigate the authentication attacks.

Key words : Authentication Attack, Cloud Computing Attack, Cloud Computing Security, Security Awareness About four key words or phrases in alphabetical order, separated by commas.

1. INTRODUCTION

In the IT infrastructure, cloud computing is high availability, scalability, cost-effective, and easy deployment environments. When the new company needs to start its application and its requirement without any initial Capex cost during the shortest time and faster way, they chose cloud computing. These reasons make cloud computing very important and the attackers focus to breach cloud computing security, that means there are a lot of attacks in cloud computing and trying to breach the cloud computing.

Today cloud computing is a modernizing technology with all benefits encourage big company moved data center or new services to cloud computing. In the year 2019 Pentagon has assigned with Microsoft Azure 10 years contract and $10 billion for the Joint Enterprise Defense Infrastructure (JEDI) [1], this deal will support the cloud computing services to be spared more and increase the confidence of cloud computing.

Authentication is very important because it is easily a meathead to access cloud computing services and get the authority to access critical information. There is 3 main type of authentication mechanisms: something you know (PIN, password), something you have (token, smart card), something you are (fingerprint, iris) [2]. To get the high-security authentication mechanism we should use two or more types of authentication together.

On the other hand, cyber security is very important in the world. It is a technique of protecting compute, programs, networks, and data from attacks and unauthorized access. It is covered by network security, information security, application security, operation security, and business continuity [3] [4]. As a security overview, the people are the main assets in security, on the other hand, people are the weakness point in the IT security from this point the company must have security awareness training to reduce this risk. At least this training should include the below topics [5]:

1) Clean Desk Policy: the desk must be clean from any sensitive information.
2) Policy for Bring Your Own Device (BYOD): this policy must control and ensure the security of employee's devices like mobile personal laptops.
3) Data Management: to learn employees about the type of data.
4) Removable Media: to educate the employees about the removal media and the risk of using it
5) Safe Internet Habits: learn employees about phishing attacks, pop-up windows, etc...
6) Physical Security & Environmental Controls: that includes the paper on the printer, visitors, leaving passwords on the desk, etc.…
7) Social Networking Dangers: limit of used and explain the examples of the breach.
8) Email and malware: learn employees about using email and the malware types.

The important of cybersecurity comes from the data breaches happened in the world: Yahoo email service 3 billion account in 2013, 500 million account in 2014 by hacking, First American Financial Corp. 885 million account in 2019 by poor security, Facebook 540 million account in 2019 by poor security, Marriot International 500 million account in 2018 by

hacking, Friend Finder Network 412.2 million account in 2016 by hacking and poor security [6], and other data breaches that reported and a huge number of breaches are not reported.

The attacks are increased yearly, and they are using new technology to breach data, privacy, get important information, etc... By trying to get authorized access through the authentication attack.

2. METHODOLOGY

This paper consists of questions and research to answer these questions: what are the most authentication attack in the cloud computing? What is the best countermeasure to mitigate and reduce the risk of this attack? What are the important assets in the security view? Is the authentication to cloud computing secure?

The researchers were worked in many research surveys about the cloud computing attack and how to mitigate these attacks, and there are a few researchers worked in cloud computing authentication attacks. We didn't find any survey for cloud computing authentication attacks discussed the social engineering attack. During this survey, we will answer the questions and discuss the cloud computing attacks especially the important authentication attack and know how we can mitigate these attacks. In the conclusions part, we will focus on the main security issues that should be applied to get high security and ensure the CIA.

This survey is organized as the following: section III discusses some paper about cloud computing attack, authentication attack in cloud computing, and the possible way to mitigate it, during section IV will discuss our conclusions about the main steps to secure our data and environment in the cloud computing.

3. RELATED WORK

There are many surveys discuss security and attacks to the cloud computing. One of the most important attacks is authentication attack B. Sumitra et. al. [7], discussed 12 authentication attack in the cloud computing and how we can mitigate it, and noted the cloud computing offering for small to medium company, Sneha Naik et. al. [8] discussed 11 authentication attacks in the cloud computing. Regarding other cloud computing attacks, Subramaniam et. al. [9] discussed 7 attacks in cloud computing and the possible way to mitigate it. Muhammad et. al. [10] divided the threat of cloud computing into three types: Data Threats, Network Threats, and Cloud Computing Environment Specific threats then described the security techniques for protection. Eesa [11] divide the attacks into two types: internal attack (have access) like employees or 3rd party for support, and external attack (don't have access) then discussed the risk associated to cloud computing and how to mitigate it [21].

4. AUTHENTICATION ATTACKS IN CLOUD COMPUTING & COUNTER MEASURED

To access the cloud computing platform, storage, application, services, etc., we need authentication mechanism to get authorization and accountability, M. Hasan et. al. [12] classified authentications techniques to five parts depending to user input: text-based (like username and password), device-based (SMS, swiping card), image and biometric-based, third party authentication (Azure AD), and hybrid authentication (combination by two or more of above parts).

From the security perspective, the authentication mechanism must be very strong and secured with a minimum of two types of authentications.

In the below we will discuss the most and important authentication attacks in the cloud computing with counter measured to protect and reduce the risk of the data breach:

4.1 Man-in-the-Middle Attack (MITM)

This attack can be passive attack: just monitor the traffic or active attack: the attacker modifies the data transfers between the two endpoints [9], [13]. During the transmutation between the user and cloud computing the attacker interrupt the communication channel [12], or exploit the synchronization protocols then the authentication, there are 3 main types MITM attack for authentication [7]:

1. Wrapping attack: the customers used the web to access cloud computing services, so in the login phase the attacker can start to duplicate credential access by modifying simple object access protocol (SOAP) messages exchanged between the authentication server and the browser [9].
2. Browser Attack: during the translation of SOAP messages between the web server and browser the attacker destroys the encryption and signature of SOAP that make the browser think the attacker is authorized [7].
3. Flooding Attack: the main aim by attacking one server in the cloud computing and then flooding to other servers. When the attacker gets authorized access to one server, he can send a bogus request to this server, then the server will handle this request. This request will utilize the server resources (CPU, memory, etc..) and flooding its jobs to another server [7].

The main solution to mitigate these attacks by encrypted data with a different algorithm like DES, AES, 3DES, etc…, using two authentication methods [7], and awareness tanning for employees.

4.2 Man-in-the-Cloud computing Attacks

Storage applications like Google Drive and Dropbox are the target of this attack in 2015, the attackers exploit the user authentication token and synchronization protocol, by authenticated as an authorized user. The attackers used two ways to hack [14]:

1. Credential Swapping: the attackers change his authentication and synchronization with users, so the user will be used the attacker account and replicate his data with the attackers' account.
2. Account Sharing: the attackers share user account.

To mitigate this attack, the cloud computing provider implemented different mechanisms like encryption or using OAuthToken (the value name and authentication key were registered in the device) [14].

4.3 Denial of Service attack DoS

The main aim of this attack to prevent or interrupt the targets (application, services, servers, etc..) operations, by sending a huge service request to make the machine overloading and can't handle any requests [7], [8].

There are many types of DOS attacks: Semantic DoS attack is the type of DoS attack that the attacker flooded huge SYN requests to the target web with random IP addresses to hang or crash the target [14]. ICMP flood attack by sending huge ping packets without waiting replies [9]. Distributed Denial of Service (DDOS) attack is used multiple sources to send the huge number of requests [10] and it is growing 380% in Q1 2017 compared with Q1 2016 [15].

There are a lot of ways to mitigate the DoS attack as below:

1. A firewall can prevent the DoS packet in the signature filter base.
2. Intrusion Prevention System (IPS): can prevent the DoS packet in the signature filter base.
3. Azure cloud computing enabled basic DDOS protection solution by default without any additional cost, it is including traffic monitoring, automatic mitigation for L3/L4 attack, global deployed, and L7 protection with application gateway web application firewall (WAF) (figure 1) [15] .
4. Using the hup count filtering technique that can filter the spoofed packets [10].

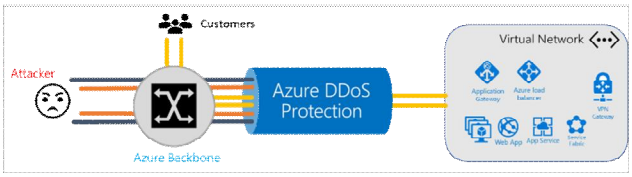

Figure 1: Azure DDoS

4.4 Password Discovery Attack

The attacker trying to discover and guesses the username and password of the authorized user. There are some strategies to get the password as below [7], [8]:

1. Brute force attack: The attacker trying all possible characters by using automated mechanisms with a high-performance computing server.

   To mitigate this attack by using SSL, TLS, using a Completely Automated Public Turing test (using a random image to ensure the user is a human), and limited of failed attempts [13].

2. Guessing attack: Today we are using the username and password for a lot of application and services so the users trying to use easier password to remember it like name, birthday, his mobile number, etc. that makes the attacker trying multiple time by using one of these words to get the credential to get authorized access [8].
3. Stolen Verifier Attack: After the attackers stole a password table or have access to it, they are using a script to compare the result message digest with the store in the table, until they get matched [8].
4. Video Recording Attack: The attacker using a camera, or video recorder to get the credential access [8].
5. Dictionary attack: Dictionary password is a list of most passwords used in the world. So, there is a dictionary password for most regional languages used by the attacker to guess the password like password, root, user123, etc... [13]

All these attacks can work in the offline application and can be mitigated by limited failed access, strong password, one-time password, and two-factor authentications [7], [8], [13], [20].

4.5 Cloud computing Malware Injection Attack

The main aim of this attack to create a virtual machine to be like a valid machine working in the cloud computing by the attacker when the machine created successfully, the attacker can redirect the requests from valid users to his server and get hash value of the original data [7], [16], [17], [20]. Another way of this attack, when the user requests a web server and log in by using his account the browser will communicate with web server so there is a small-time during this process of authentication and authorization, then the attacker can use this time to introduce harmful code to be like a service in the cloud computing then can be run as a single instance [9].

To mitigate this attack: cloud computing providers need to have Hypervisor with high security and high integrity of the instance.

4.6 Session Hijacking Attack

The attackers aimed to attack the session ID that is not secured by transfer it in clear text or using unsecured communication protocol to capture the login sequence then have access to user sessions by using packet sniffing tools [7].

To mitigate this attack, we should use encryption, secure communication protocol, Virtual privet network (VPN), and deployment IPS/IDS [10].

4.7 Eavesdropping Attack

Eavesdropping is a kind of reply attack [13], the attacker lessened to the data over the communication channel between customer and cloud computing then the attacker can use gathered information to get access and know the credential, At this point, the attacker has access to cloud computing services and stole important information [7].

The proper way to mitigate this by applying good authentication producer over HTTPS, encrypting transmitted data, and using the signature to ensure integrity [7], [13].

4.8 Phishing Attack

The attackers built a fake website like the original website, then send a phishing message include malicious attached or link to get the user credential, card information, or any sensitive data [13], [18].

This fake website maybe like a cloud computing provider, so the user thinks the attacker servers are the cloud computing provider web page. So, when the user accesses to the fake web site, the attacker can steal authentication credentials and have access to the cloud computing services. [7]

To mitigate this attack, we can use anti-virus, IDS/IPS, Firewall, digital certificate, using two authentication methods, and provide security awareness training for employees.

4.9 SQL Injection Attack

This attack exploiting access to the database of the web application. So, the attacker trying to get access to the SQL database, or break the verification security by injecting different commands or SQL statements [18].

To mitigate this attack, we should use a firewall, IDS/IPS, and WAF.

4.10 Secure Socket Layer (SSL) Attack

SSL is a mechanism using an asymmetric key to encrypt the information transferred between server and client, another use of SSL to identity the communication to cloud computing. There are two types of SSL attack [7]:

1. Stripping attack: exploit the SSL by adding a null character after a valid domain name directly. When reading the fake certificate will find a valid domain name that makes the fake certificate valid.

To mitigate this attack by using an Extended Validation SSL certificate that includes organization information.

2. SSL Sniffing: the attacker using the Certifying Authority (CA) to lunch this attack.

To mitigate this attack by using an Extended Validation SSL certificate that includes organization information.

4.11 Cookie Poisoning Attack

The cookie includes the identity of the authorized user so the attackers trying to modify it to have access.

To mitigate this attack, we can use IPS and WAF.

4.12 Social Engineering Attack

Social Engineering attack is the terms of tricky used to get access to sensitive information, access systems, or others. That includes direct calls or any electronic communications. It is depending to build a good relationship with people in the company by using human psychology with fear, compassion and imitation tools [3].

Social engineering attacks used a common four phases when attacking the target: 1) collecting information, 2) build relationships, 3) getting information and starting the attack, 4) leave without any traces. As figure 2 [19]

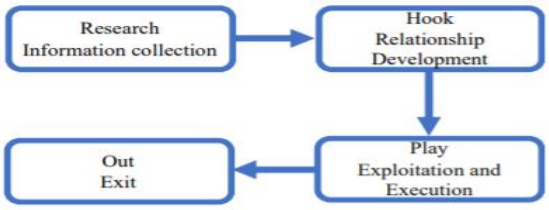

Figure 2: Social Engineering Attack phases

The social engineering can divide into two methods depending on the attacker way [3] [19]:

1. Human-Based: It is hard to detect because the attacker interacted with the target as a human-to-human and get information by using these popular methods a) Impersonation like a valid user, b) Poising as an important user like a manager, c) Third-party, d) Desktop support.

2. Computer-Based: the attacker used computer software to get sensitive information from the target by using these methods a) Phishing, b) Baiting by downloading move or USB flash with company logo, etc. c) On-Line Scams, d) Pop-up Windows, e) Email Attached, f) Email Scams, g) Chain Letters and Hoaxes, h)

Websites that offer free services.

There are three main steps to mitigate the social engineering attacks as below [3] [19]:

1. Education through training and awareness to make them aware of the attacks.

2. Polices are security controls to guide employees and puts roles for company security.

3. Audits used to ensure the employees are following the policy and procedures of the company.

There are some other techniques can help us to mitigate like IPS, Anti-Malware, Anti-Virus.

Finally, table 1 summarizes all authentications attacks in the cloud computing and how to mitigate it.

Table 1: List Of Attack And Mitigation

Attacks	***Description***	***Mitigations***
Mitm attack	The attacker interrupt communication channel. There are 3 main types: wrapping attack, browser attack, and flooding attack.	By using encryption, two authentication methods, and awareness training
Man-in-the-cloud Attack	The Storage application is the target of this attack by credential swapping or account sharing	By using Encryption or oauthtoken
Dos attack	Working to prevent or interrupt the targets operations. There are many types like semantic dos attack, icmp flood attack, and ddos attack	By using firewall, ips, azure ddos, waf, and hup count filtering technique
Password discovery attack	Trying to discover and guesses the username and password by using one of these strategies: brute force attack, guessing attack, stolen verifier attack, video recording attack, and dictionary attack.	By limiting failed access, strong password, one-time password, two factor authentications, and awareness training
Cloud malware injection attack	Trying to attack vm in the cloud computing then redirect the request to get the hash value of data	Having hypervisor with high security and high integrity of the instance
Session hijacking attack	Capture the login sequence from session id	By using encryption, secure communication protocol, (vpn), and ips/ids
Eavesdropping attack	The attacker knows the credential by lessened to the data over communication channel	By using encrypting and applying good authentication producer over https,
Phishing attack	The attackers built a fake website, then send a phishing message include malicious attached or link to get the user credential	By using anti-virus, ids/ips, firewall, digital certificate, two authentication methods, and security awareness training
Sql injection attack	Working to injecting different commands or sql statement in the sql database	By using firewall, ips, and waf.
Ssl attack	The attacker exploiting ssl, there are two type: stripping attack and ssl sniffing.	By using extended validation ssl certificate that include organization information.
Cookie poisoning attack	The attacker modifies the cookie poisoning	By using ips and waf
Social engineering attack:	Is a tricky used to get access to sensitive information, accesses systems, or others by using direct calls, or any electronics communications	Education, policy, audit, ips, anti-malware, and anti-virus

5. CONCLUSION

In this survey, we discussed the main authentication cloud attack with possible ways to mitigate and reduce the risk. Our main conclusions to invest in security awareness training and increase the security knowledge of employees. Now we will list our suggestion security issues must be implemented to be secure and protect our data with high availability in the cloud:

1. Policy, Standard, Baseline, Guideline, and procedure: the company must apply it to define the importance of security.
2. Ensure the cloud provider has a standers certificate like ITIL, ISO 27001, ISO 27002, etc.…
3. Awareness training: for all employees twice a year.
4. We should have auditing and monitoring software like Security Event Meager (SIEM) or get it in the cloud.
5. We should have anti-virus and anti-malware.
6. We should have a Firewall, IPS, WAF over cloud computing and in our Pc.
7. Using Vulnerability scan tools to define the weak point and trying to solve it. After that, we can run a penetration test to ensure the security applied, which will help us to early detect attacks [11], [14].
8. Keeping all systems up to date.
9. The company must have a Business Continuity plane (BC) and test it.
10. Encrypt data in transit and in the rest.
11. Using at least two authentication mechanisms.

In the cloud, the cloud provider has the biggest handling of security that depending on the cloud services we are used. A conclusion section is not required. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions.

ACKNOWLEDGMENT

The first author is grateful to the Middle East University, Amman, Jordan for the financial support granted to cover the publication fee of this research article.

REFERENCES

1. T. N. Y. Times, "New York Times," 9 December 2019. [Online].Available: **https://www.nytimes.com/2019/10/25/technology/dod-jedi-contract.html.** [Accessed 6 January 2019].
2. S. P. M. F. Nilesh A. Lal, "**A Review Of Authentication Methods**," *International Journal Of Scientific & Technology Research*, vol. 5, no. 11, pp. 246-249, 2016.
3. M. C. a. N. K. Anshul Kumar, "**Social Engineering Threats and Awareness: A Survey,**" *European Journal of Advances in Engineering and Technology*, vol. 2, no. 11, pp. 15-19, 2015.
4. Kaspersky, "Kaspersky.com," [Online]. Available: **https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security**. [Accessed 17 January 2020].
5. I. website, "Infosec website," 12 January 2020. [Online]. Available: **https://resources.infosecinstitute.com/top-10-security-awareness-training-topics-for-your-employees/#gref.** [Accessed 15 January 2020].
6. CNBC, "CNBC," 30 July 2019. [Online]. Available: **https://www.cnbc.com/2019/07/30/five-of-the-biggest-data-breaches-ever.html**. [Accessed 6 January 2020].
7. C. P. M. B.Sumitra, "**A Survey of Cloud Authentication Attacks and Solution Approaches,**" *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 2, no. 10, pp. 6245-6253, 2014.
8. S. Naik, "**Authentication Attacks in Cloud computing: A survey,**" *International Journal of Technology Research and Management*, vol. 2, no. 5, 2015.
9. T. K. D. B. Subramaniam, "**Security attack issues and mitigation techniques in cloud computing environments,**" *International Journal of UbiComp (IJU)*, vol. 7, no. 1, 2016.
10. S. Y. Z. Muhammad Kazim, "**A survey on top security threats in cloud computing,**" *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 6, no. 3, pp. 109-113, 2015.
11. E. Alsolami, "**Security threats and legal issues related to Cloud based solutions,**" *International Journal of Computer Science and Network Security*, vol. 18, no. 5, pp. 156-163, 2018.
12. M. M. H. R. M. A. R. Hasan, "**Authentication Techniques in Cloud and Mobile Cloud Computing,**" *IJCSNS*, vol. 17, no. 11, 2017.
13. A. a. N. S. Jesudoss, "**A survey on authentication attacks and countermeasures in a distributed environment,**" *Indian Journal of Computer Science and Engineering (IJCSE)*, vol. 5, no. 2, pp. 71-77, 2014.
14. S. I. R. K. L. A. A. O. A. S. Raja Mohamed Jabir, "**Analysis of cloud computing attacks and countermeasures,**" *International Conference on Advanced Communication Technology (ICACT)*, 2016.
15. Microsoft, "Microsoft Azure," 25 September 2017. [Online]. Available: **https://azure.microsoft.com/en-us/blog/azure-ddos-protection-service-preview/.** [Accessed 6 January 2020].
16. A. a. M. S. Singh, "**Overview of security issues in cloud computing,**" *International Journal of Advanced Computer Research*, vol. 2, no. 1, 2012.
17. A. a. D. M. S. Singh, "**Overview of attacks on cloud computing,**" *International Journal of Engineering and Innovative Technology (IJEIT)*, vol. 1, no. 4, 2012.
18. N. C. S. K. P. J. Vijaya Chandra, "**Authentication and Authorization Mechanism for Cloud Security,**" *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 8, no. 6, 2019.
19. N. K. Fatima Salahdine, "**Social Engineering Attacks: A Survey,**" *Future Internet*, vol. 11, no. 89, 2019.
20. H. Abusaimeh, "**Security attacks in cloud computing and corresponding defending mechanisms**", *International Journal of Advance Trend in Computer Science and Engineering (IJATCSE), Vol. 9, No. 3, 2020*. https://doi.org/10.30534/ijatcse/2020/243932020
21. H. Abusaimeh, H. Atta, and H. Shihadeh, "**Survey on cache-based side-channel attacks in cloud computing",** *International Journal of Emerging Trends in Engineering Research*, Vol.8, Issue 4, 2020. https://doi.org/10.30534/ijeter/2020/11842020