ISSN 2278-3091
Volume 9, No.3, May - June 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcs243932020.pdf
https://doi.org/10.30534/ijatcse/2020/243932020

Security Attacks in Cloud Computing and Corresponding Defending Mechanisms

Hesham Abusaimeh
Associate Professor in Computer Science, Middle East University, Amman, 11831 Jordan.
habusaimeh@meu.edu.jo

ABSTRACT

Cloud computing is considered as a rising model that becomes a necessity to accommodate the rapid growth in the use of technology. Cloud computing provides a wide diversity of facilities and services for the users without the need for having expensive computing devices and equipment. A cloud user can utilize remote software, processors, storage without owning them. However, remote access adds more difficulties and problems to cloud users, such as security. Authentication is one of the main security challenges where cloud servers and users need to identify and validate each other to complete the communication process and provide the service. In this study, we mention well-known authentication attacks and we include a number of studies that investigated each attack.

Key words: Authentication, Clouds, Communication system security, Security.

1. INTRODUCTION

Cloud computing is considered as a promising technology, which comes to accommodate the increasing development and growth in communication and computation technologies. When cloud computing is selected, computer resources and services are moved to special remote servers instead of being local [1], these services and resources include storage, computing power, software, hardware and many other computer capabilities. The use of remote resources means that users do not need to buy expensive computing devices and equipment. A cloud user utilizes cloud services remotely and gets complete benefits with a moderate cost paid for cloud provider.

In a cloud system, a cloud server provides a wide variety of services for cloud users, these services vary in their importance and sensitivity from storing normal and public information to highly critical and security sensitive information, in the latter type of information, accessing information by a person except the data owner can cause un-wanted events. For example, accessing and modifying customer's payment information included in vendor's data on a cloud can cause a high loss in business earnings.

So, authentication is one of the main security challenges where cloud servers and users need to identify each other before making any transaction or provisioning the service and it is necessary to provide powerful access control and authentication system. As the authentication system is stronger, the much users will accept cloud paradigm at all.

Many authentication schemes prevail for cloud computing to offer secure access for cloud data, it includes using passwords, which is the simplest, public keys [2], smart cards [3], biometric authentication [4] such as retina, fingerprint, iris. Etc. These schemes are used to authenticate cloud users either by using one scheme or by constructing complex authentication methods based on two or more schemes together.

2. BACKGROUND & METHODOLOGY

In this survey, we investigate a number of the most well-known authentication attacks and we mention a number of studies that have tried to solve these attacks.

A cloud system is prone to multiple authentication attacks. The effect of the attack depends on the level of data sensitivity and how much it is considered critical. Un-authenticated access for normal user documents can be negligible, accessing healthcare data for patients could be moderate risk, however, accessing financial data or highly private data can cause huge damage and terrible effect.

In this section, we will outline several authentication attacks with a brief description for each attack, in the next section, we will discuss two research works for each attack in which a solution has been suggested. From the wide variety of attacks, we have selected the following attacks:

A. Authentication Attacks

Brute force Attack

In this type, an attacker tries all possibilities for passwords or authentication codes to guess the correct one [5]. It takes a long time; the time increases as the length of a password becomes longer as shown in figure1.

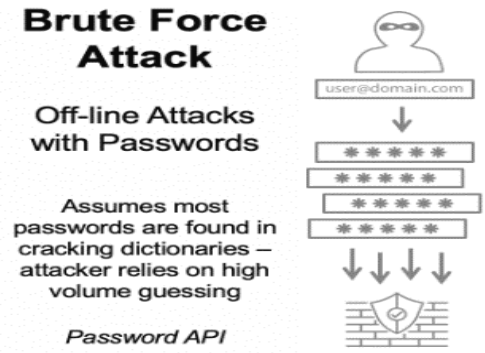

Figure 1: Brute Force Attack process

Dictionary Attack

The attacker tries all possibilities for passwords or authentication codes to guess the correct one [5]. It takes a long time, the time increases as the length of a password becomes longer.

Replay Attack

The attacker eavesdrops and intercept data transmitted through secure communication, then delays or resends it to misdirect the receiver into doing what the hacker wants as shown in figure 2.

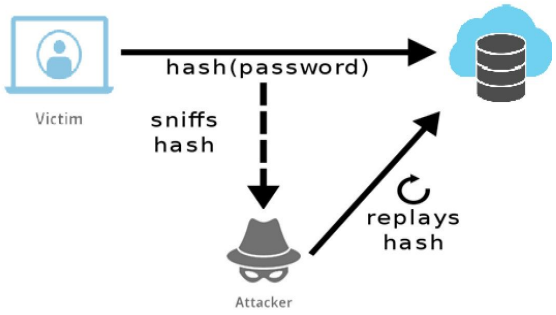

Figure 2: Replay Attack process

Phishing Attack

Figure 3 explain the attacker tries all possibilities for passwords or authentication codes to guess the correct one [5]. It takes a long time, the time increases as the length of a password becomes longer.

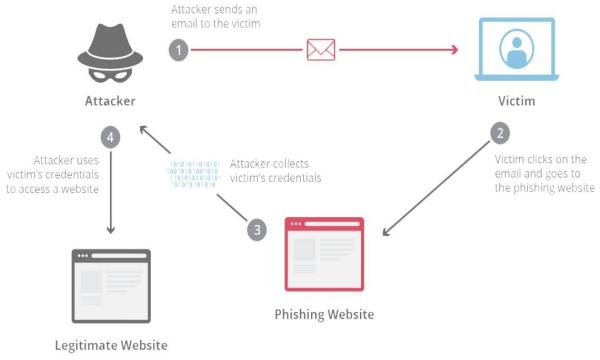

Figure 3: Phishing Attack process

B. Man-in-the-Middle Attack (MITM):

Wrapping Attack

The attacker initiates by user credentials get duplicated during the login period by SOAP messages exchanging when the communication set up between the browser and the server as shown in figure 4. The attacker uses XML signature to modify the message body to modified wrapping inserted in SOAP header, the inserted code to interrupt the functions of cloud servers [18]. Attacker tries all possibilities for passwords or authentication codes to guess the correct one [5]. It takes a long time; the time increases as the length of a password becomes longer as shown in figure 5.

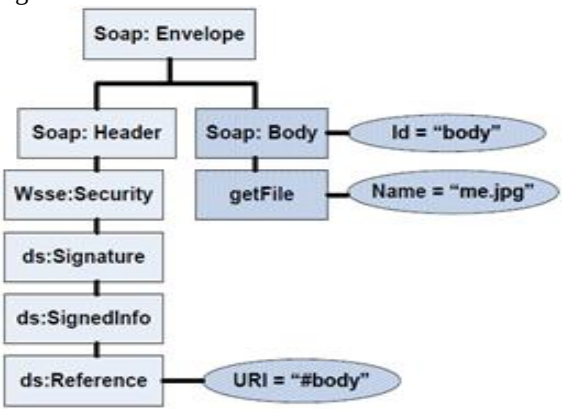

Figure 4: SOAP message body prior to wrapping attack [19]

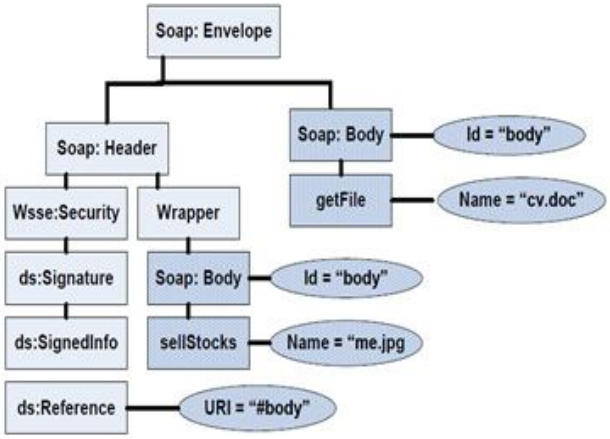

Figure 5: SOAP message body edited by wrapping attack [19]

Flooding Attack

The attacker floods the cloud servers with a lot of continues requests for service, the cloud server test the user credibility requesting before providing desired service, this process of checking consumes cloud resources like memory, CPU, etc. This process will result in stopping the services in a single server and moving the attack more by flooding to the rest of the system. This will yield into halting the service offering for legit users as in figure 6 [18].

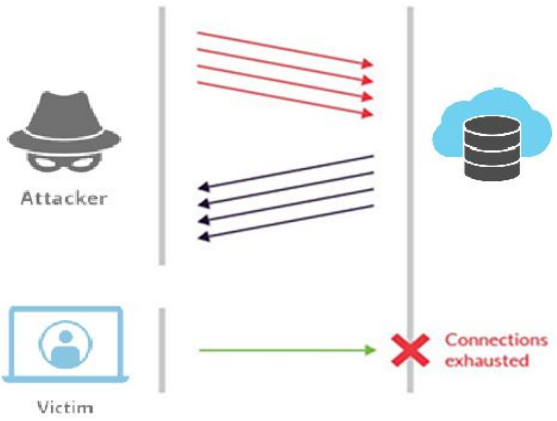

Figure 6: Flooding Attack process

Browser Attack

The attack that ends up with data theft that is carried out by disturb SOAP messages encryption & signature during message interpretation among browser and server, yield in the browser to think about the attacker to be authenticated user and proceed to answer attacker requests when interacting with the server as shown in figure 7 [20].

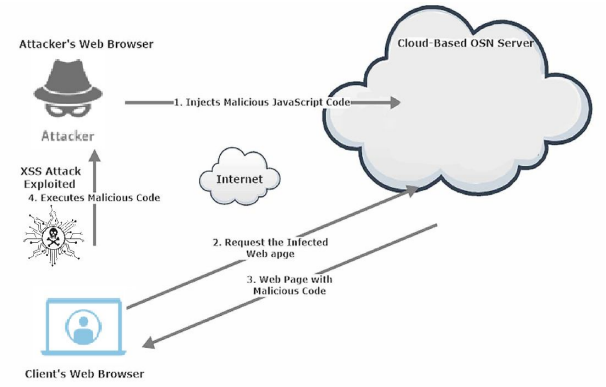

Figure 7: Browser Attack process

Impersonating Attack

The attacker masquerades as a legitimate user and expose the system to have the login information that employed to get the illegitimate reach to the services.

SSL Attacks

Secure Socket Layer (SSL) is a defense tool that used to encrypt the passed information between server and user, the type of attack is subcategorized as the following:

1. The attacker can exploit the limitation of SSL certificate by using SSL sniffing attack due to the fact that the Certifying Authority (CA) can't assure the website validity of and can't be placed in the web browser as in the figure 8.

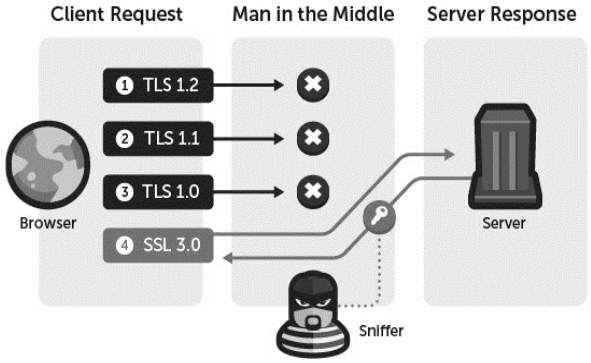

Figure 8: SSL Sniffing Attack process

2. Stripping Attack: The weakness of SSL is exploited by using "\0" (null character) in a website name, when the SSL from client side read the domain name fake certificate, the null will be treated as a valid certificate and then gives a full access to the attacker [22].

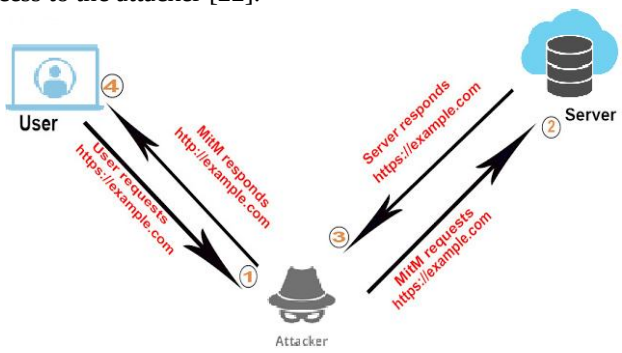

Figure 9: Stripping Attack process

C. Other Types of Attacks

Malware Injection Attack

The attacker manipulates user service information and uploads it to the cloud, then the attacker gain entry to user data by using this method, this will lead to leakage of user credential information and grant the attacker illegitimate login to cloud services. [23]

Cross VM Side-Channel Attack

As shown in figure 10, Virtualization is a primary permissive technology in cloud, the hacker's VM alter the services implementation in targeted VM and result in processor cash that mimic the actions of the legit user, attack chose to gather data containing energy consumption logs rather than tacking the virtualization layer, attackers use the energy consumption logs to acquire the chance to collect vital information about the cloud. The longer the time used in the attack accomplish by attacking the victim's computer, the bigger chance that the detection possibility of the attack. [25]

In [26] the authors checked the possibility of getting important information that is extracted coming out of the energy consumption logs that can pose a security threat to the user's privacy and security.

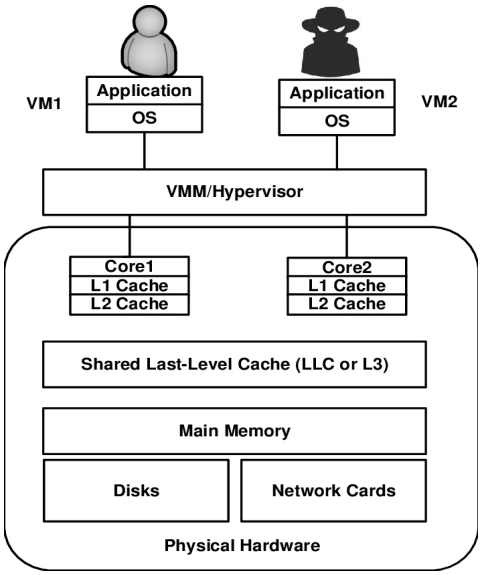

Figure 10: Cross VM Side-Channel Attack process

Botnet Attack

The attacker use group or cluster of infected computers/servers to attack called stepping stones, the attacker get the stepping stones through infecting them with botnet attack and setup what it's called Command and Control (C&C), attacker use C&C to eavesdrop on the user-cloud communication exchange, steal user/server information or gain illegal access to the cloud services as in figure 11.

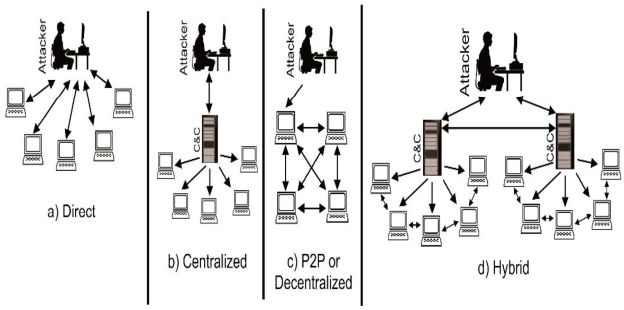

Figure 11: Botnet Attack categories

Reflection Attack

The attack starts by attacker sending fraudulent request to the targeted user, with tampered packets containing the user information and IP address as sender address, then each packet move across the internet until it arrives at the destined reflector server, the server tricked into thinking that the user sent the packets and send the response to the targeted user, with the other reflector servers responses the user will get overwhelmed with the servers responses, this will result in jamming the network. The attacker can use the same method to acquire user login info from the attacked server, and figure 12 shows that clearly [28].

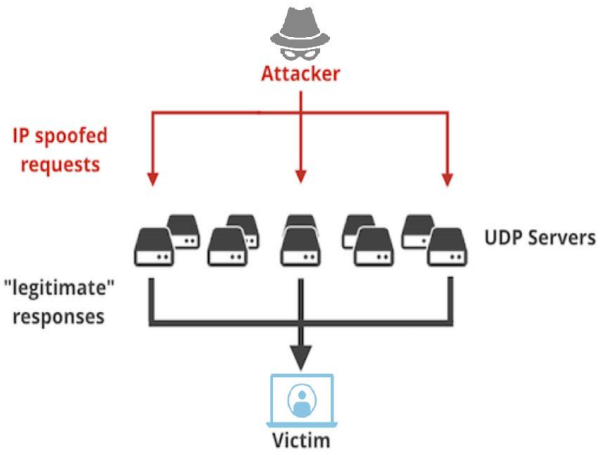

Figure 12: Reflection Attack process

Insider Attack

The attack occurs when an employee of an organization that operating cloud server, leaks user sensitive information or tamper with cloud server security measures for a financial gain or impose damage to the organization reputation [29].

3. PROTECTION MECHANISMS FOR EACH ATTACK

In this section, we discuss several research studies that have been devoted to propose a protection mechanism against the aforementioned attacks.

Brute force Attack

From the studies that investigated brute force attack, there are research papers [8] and [9]. In [8], multi-dimensional password is considered, where the authentication password is constructed from multiple elements including user detail, vendor details, service details, permissions details. These parameters are combined as textual and image to be input as login password. The use of multiple parameters password reduces significantly attacker ability to launch brute force attack. Both cloud provider and user must input parts of the password to a password generator to produce a multi-dimensional password. The authors of this paper concluded that the chance of brute force attack to break a password can be significantly limited with multidimensional password which is constructed from multiple factors such as signatures, images and textual data.

In [9], k-means algorithm is used to detect brute force attack in cloud computing systems. In brute force attack, the adversary can perform data analysis for data stored in a

database; this analysis can diminish the number of possibilities to break authentication system. The proposed scheme in [9] depends on adding fake records on the database. This starts by using multiple parameters for a user such as his name, address, income, age, phone number, and so on. Each parameter is considered as an attribute in authentication process, then, attributes are classified as vulnerable and non-vulnerable based of the attribute probability to be repeated. For example, employee national number cannot be repeated, while employee's age can be repeated for other employees, finally vulnerable attributes are divided into multiple clusters and fake records are added to hide any inspirations that can be appear with data analysis. The proposed framework has led to the conclusion that it can reduce the probability of breaking a password using bruit force attack; however, a tradeoff must be considered between accuracy and computational overhead when preserving privacy.

Dictionary Attack

From Research studies [10] and [11] have investigated dictionary attack, in [10], the proposed scheme depends on the use of multiple techniques to generate a strong password, these techniques include One Time Password (OTP) and multi-factor authentication, the authentication process passes through multiple stages and login activities from both user and cloud server , it include also a secret image from which a part is extracted each time to generate an (OTP). The proposed scheme is evaluated and proved to prevent dictionary attack as well as other attacks. The drawn conclusion implies that the proposed method was immune to multiple attacks as well as it can support important security features that previous schemes have failed to achieve.

In [11], cloud authentication system is protected against dictionary attack based on mutual authentication, where each of authentication parties is responsible for validating the other. The proposed scheme has achieved a high efficiency in the areas of computational cost, connection overhead and power consumption because of the use of ECC, Error Correction Code memory, which help to detect and prevent internal data corruption. Analytical evaluation is applied based on the formal language proof to show improvements provided by the proposed scheme, the final conclusion is that the proposed work is practical in the part of mobile cloud computing, especially with constraint devices in terms of energy and computing power, moreover, it has a comparative performance when compared to existing works.

Shoulder Surfing

Research studies [12] and [13] have been selected to present authentication mechanisms against shoulder surfing attack, [12] has considered the use of graphical instead of textual passwords, which have been found to has more vulnerabilities, especially for this attack, and need more enhanced authentication preserving mechanisms. The main points to consider include depending on variable size grid in logging step to be used for image selection as well as allowing users to input passwords in two ways instead of one. The proposed scheme is evaluated based on conducting shoulder surfing attack and getting user feedback. The conclusion stated that the introduced system is 100% immune to this attack when the login is keyboard-oriented. However, the system achieved 70% security with mouse login.

In [13], new scheme is proposed based on the use of an image as (OTP) beside passwords and other traditional authentication tools. This can make cloud system using this scheme more resistant to shoulder surfing attack, the (OTP) image is combined with one-way hash function and International Mobile Equipment Identity (IMEI). The final conclusion implies that the proposed scheme has shown a revolutionary authentication direction depend on use of a password and a secret image which empowers the process of authentication.

Replay Surfing

Research works [14] and [15] have selected as examples of protection mechanisms against replay attack, in [14] a new scheme is designed for banking systems, as authentication is very important requirement in this type of application. The authentication scheme depends on a multi-factor authentication where user ID, mobile number, secure question, e-mail, password, and a fingerprint is combined to authenticate a user. This scheme has shown a significant protection for sensitive information as well as user credentials from cloud attackers and concluded that the proposed approach can lead to a faster cloud-based banking system in addition to the added security and reachability.

In [15], a new framework is proposed based on two factor authentications. These two factors include PKI (Public Key Infrastructure) as well as Out-Of-Band (OOB) authentication. In (OOB) authentication, we depend on a separate channel to transfer secret data such as one-time passwords and secret keys. Each time a user log in to the cloud server, a onetime password is generated and transmitted through (OOB) channel, the proposed framework is analyzed and proved to be strong against replay attack, and concluded that the implementation of the two-factor authentication can increase the complexity of launching the unauthorized access attack within the cloud system.

Phishing Attack

In the last type of authentication attacks in this survey, research studies [16] and [17] have been selected. In [16], a new framework is proposed based on the use of collective authentication between cloud, users, identity management. Mutual authentication, which depends on the notion that a cloud server must authenticate the users and vice versa, can guarantee correct user identification each time, which leads to the conclusion that the use of two-factor authentication outperforms the one-factor authentication, moreover, the

authors concluded that the proposed framework is strong against phishing attack as well as man in the middle attack, replay attack, and denial of service attack.

In [17] a special case of authentication is considered, it the case when a user may need to login into distinct or unrelated application with one login process, that is without the need to own or input multiple usernames and passwords. In this study, authors suggest to combine openID, and single sign on (SSO) mechanisms, where the former is defined as allowing the user to login into different sites without the need to own distinct IDs and passwords, while the latter is defined by making one authentication process to access multiple services using one token. The concept of trusted computing, where the computer system must be trusted by doing what is expected, is adopting based on (SSO) and openID. The .NET environment is used to simulate the proposed solution and proved to be valid. The conclusion states that the combination of multiple factors such as trusted computing and OpenID can signifies authorization preserving and protect cloud system from identity theft.

Wrapping Attack

In [19] advise that to increase the security during the phase where the message moving from server to user portal with adding STAMP bit and the simple object access protocol header which will activate when message is hijacked by the attacker. Due to the fact that phishing attack includes editing the authentic message by adding hash to the sent message.

Flooding Attack

Flooding attack start with preparing the targeted servers providing service being cluster and the particular servers interacting between each other through message passing about the incoming requests. Hypervisor is often acclimated to organize the cluster execution, to inspect the request legitimacy and stop cluster coming out of getting overwhelmed with fraudulent requests. [19]

Browser Attack

WS-Security can be added to browsers, which let it to utilize the XML encryption that add throughout encryption in simple object access protocol messages that prevents messages eavesdropping. [20]

Impersonating Attack

By applying the two and multi point, authentication methods, which depend on personally identifiable information (PII) with the use of passwords, and privacy enhancing protocols, can be used to protect information and decline the storage of information. [21]

SSL Attack

Companies have to make portals that use WS-Security method rather than the throughout encryption provided by SSL/TLS, WS-Security can provide throughout encryption which does not need decryption, this process will block the attack which is incapable through acquiring SOAP messages. [22]

Malware Injection Attack

A solution to the attack "CloudAV" is provided in [24], CloudAV provide the following additions: Antivirus and N-version protection, these two additions will make the solution more efficient, and accurate as a malware detection system.

Cross VM Side-Channel Attack

Unfortunately, there is no efficient solutions to be provided yet to solve the energy consumption side and timing side channel attacks.

Botnet Attack

Identifying the cipher keys of the botnet transmission to arrange the botnet operations then it links to bot master, it includes the use of a replacement key recognition method and a method to track bot master around stepping stones in multiple clouds and servers, this solution mention the symmetric key cryptography but nothing about asymmetric cryptography. [27]

Reflection Attack

Limiting the communication between the server and single user to the minimum before authenticating the user identity to overcome the issue of masquerading by the attacker. [28]

Insider Attack

The best way to prevent an insider attack by monitoring massive data transmission outside the server, suspicious accounts management, repeated declined login attempts, and unauthorized software roles & access to files in the server.

The monitoring process can be done using special systems to assure the protection of the data in the cloud server from being leaked to unauthorized entity. [29]

4. RESULTS AND CONCLUSION

Authentication attacks is one of the most important issues to ensure that a high-quality cloud services are provided to cloud users, in this study, we have investigated research papers to study protection mechanisms for 15 selected authentication attacks. We conclude that the combination of multiple protection mechanisms and the use of image-based passwords instead or beside textual passwords are dominated in most research studies. The suitable future work for this study is to expand the sample of research papers to include a wider variety of protection mechanisms.

ACKNOWLEDGEMENT

The 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. Hayes, B. (2008). Cloud computing. Communications of the ACM, 51(7), 9-11. https://doi.org/10.1145/1364782.1364786
2. Li, H., Dai, Y., Tian, L., & Yang, H. (2009, December). Identity-based authentication for cloud computing. In IEEE International Conference on Cloud Computing (pp. 157-166). Springer, Berlin, Heidelberg.
3. Urien, P., Marie, E., & Kiennert, C. (2010, June). An innovative solution for cloud computing authentication: Grids of eap-tls smart cards. In 2010 Fifth International Conference on Digital Telecommunications (pp. 22-27). IEEE.
4. Vallabhu, H., & Satyanarayana, R. V. (2012). Biometric authentication as a service on cloud: Novel solution. International Journal of Soft Computing and Engineering, 2(4), 163.
5. Chouhan, P., & Singh, R. (2016). Security attacks on cloud computing with possible solution. International Journal of Advanced Research in Computer Science and Software Engineering, 6(1).
6. Ho, P. F., Kam, Y. H. S., Wee, M. C., Chong, Y. N., & Yee, L. (2014). Preventing shoulder-surfing attack with the concept of concealing the password objects' information. The Scientific World Journal, 2014. https://doi.org/10.1155/2014/838623
7. Hong, J. (2012). The current state of phishing attacks.
8. Dinesha, H. A., & Agrawal, V. K. (2012). Multi-dimensional password generation technique for accessing cloud services. Special Issue on:" Cloud Computing and Web Services", International Journal on Cloud Computing: Services and Architecture (IJCCSA), 2(3), 31-39.
9. Pawar, A., & Dani, A. (2014). Enhancing Privacy-Preserving Cloud Database Querying by Preventing Brute Force Attacks. International Journal of Computer, Information Science and Engineering, 8(1), 51-57.
10. Abdellaoui, A., Khamlichi, Y. I., & Chaoui, H. (2016). A novel strong password generator for improving cloud authentication. Procedia Computer Science, 85, 293-300. https://doi.org/10.1016/j.procs.2016.05.236
11. Mo, J., Hu, Z., Chen, H., & Shen, W. (2019). An Efficient and Provably Secure Anonymous User Authentication and Key Agreement for Mobile Cloud Computing. Wireless Communications and Mobile Computing, 2019.
12. Rodda, V., Kancherla, G. R., & Bobba, B. R. (2017). Shoulder-Surfing Resistant Graphical Password System for Cloud. International Journal of Applied Engineering Research, 12(16), 6091-6096.
13. Abdellaoui, A., Khamlichi, Y. I., & Chaoui, H. (2015). Out-of-band Authentication Using Image-Based One Time Password in the Cloud Environment. International Journal of Security and Its Applications (IJSIA), 9(12), 35-46.
14. Nagaraju, S., & Parthiban, L. (2015). A Secure Authentication and Authorization Scheme for Online Banking Systems in Cloud. International Journal of Applied Engineering Research, 10(76), 2015.
15. Lee, S., Ong, I., Lim, H. T., & Lee, H. J. (2010). Two factor authentication for cloud computing. Journal of information and communication convergence engineering, 8(4), 427-432.
16. Choudhury, A. J., Kumar, P., Sain, M., Lim, H., & Jae-Lee, H. (2011, December). A strong user authentication framework for cloud computing. In 2011 IEEE Asia-Pacific Services Computing Conference (pp. 110-115). IEEE.
17. Ghazizadeh, E., Zamani, M., Ab Manan, J. L., & Alizadeh, M. (2014). Trusted computing strengthens cloud authentication. The Scientific World Journal, 2014. https://doi.org/10.1155/2014/260187
18. B.Meena and K.A. Challa , "Cloud Computing Security Issues with possible solutions," Int, Journal of Computerr Science and Technology, vol.2, Issue: 1, Jan–March, 2012.
19. Vrbsky, Susan V.. "Security Attacks and Solutions in Clouds Kazi Zunnurhain", 2010.
20. Danish Jamil & Hassan zaki, "Security Measures in Cloud computing and Counter measures", International Journal of Engineering Science and Technology(IJEST), Vol.3 No.4 , 2011.
21. Y.Andree, "Implications of Salesforce Phishing Incident", 2007.
22. Larry Seltzer, "Spoofing Server-Server communication: How can you prevent it", 2009.
23. Gruschka, N.; Jensen, M. Attack surfaces: A taxonomy for attacks on cloud services. In Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing (CLOUD), Miami, FL, USA, 5–10 July 2010; pp. 276–279.
24. Oberheide, J.; Cooke, E.; Jahanian, F. CloudAV: N-version antivirus in the network cloud. In Proceedings of the 17th Conference on Security Symposium (SS '08); USENIX Association: Berkeley, CA, USA, 2008; pp. 91–106.
25. Aviram, A.; Hu, S.; Ford, B.; Gummadi, R. Determinating timing channels in compute clouds. In Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop (CCSW '10); ACM: New York, NY, USA, 2010; pp. 103–108. https://doi.org/10.1145/1866835.1866854
26. Hlavacs, H.; Treutner, T.; Gelas, J.; Lefevre, L.; Orgerie, A. Energy consumption side-channel attack at virtual machines in a cloud. In Proceedings of the 2011 IEEE Ninth International Conference on Dependable,

Autonomic and Secure Computing (DASC), Sydney, NSW, Australia, 12–14 December 2011; pp. 605–612.
27. Lin, W.; Lee, D. Traceback attacks in cloud—Pebbletrace botnet. In Proceedings of the 2012 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW), Macau, China, 18–21 June 2012; pp. 417–426. https://doi.org/10.1109/ICDCSW.2012.61
28. Lucas Kauffman, "About the recent DNS Amplification attack against Spamhaus: Countermeasures and mitigation", 2013.
29. D.Cappelli, A.Moore, and R.Trzeciak, The CERT Guide to Insider Threats: How to prevent, Detect and Respond to Information Technology Crimes (Theft, Sabotage , Fraud) ser. SEI series in Software Engineering. Addison-Wesley Professional, 2012.