REVIEWING OF CYBERSECURITY THREATS, ATTACKS, AND MITIGATION TECHNIQUES IN CLOUD COMPUTING ENVIRONMENT

KHOLOD SAEED ALQAHTANI[1], AZZAM MASHHEN ALBALAWI[2], MOUNIR FRIKHA[3]

[1, 2]Department of Computer Networks and Communications, College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia

E-mail: [1]222453715@student.kfu.edu.sa, [2]albluwiAzzam@gmail.com, mmfrikha@kfu.edu.sa

ABSTRACT

Cloud Computing (CC) is a great and promising technology due to its features, such as accessibility, scalability, and online storage, in that it provides a better cost reduction for organizations to run their businesses and financial activities over the cloud. Confidentiality, integrity, availability, and accessibility are crucial components of the cloud infrastructure. One of the key issues in providing uninterrupted services to cloud consumers is availability. Cloud security and privacy issues exist, and they have an impact on cloud utilities. With the increase in usages of cloud computing over the past few years, security issues and threats have increased simultaneously. In this paper, we review the most common attacks and countermeasures in the cloud computing environment by conducting a systematic literature review (SLR). Additionally, we propose an Automated Cloud Security Awareness Program (ACSAP) that aims to help organizations to increase awareness of individuals before using the cloud platform to reduce the risk of data breaches since mostly is caused by human error.

Keywords: *Five Cloud Computing, Threats, Attacks, Mitigation, Cybersecurity*

1. INTRODUCTION

In the network, an enormous number of computers are connected to several machines that are dispersed geographically. Network attacks and security risks are big challenges for computer networks. Online services or network security are two ways to get unauthorized access to the network. Additionally, attackers play a crucial role in security. The two related categories of attacks are passive attacks and active attacks. It is claimed that the network imposter captures data as it moves through the network. Some passive assaults include idle scans, wire patter, and port scanners. The command is given by the intruder to interfere with normal network operation. Attacks that are active are those. Active assaults include spoofing, denial-of-service attacks, man-in-the-middle attacks, and others. There are several different ways and policies in which this attack can be accepted. The primary component would be to block the victim's network system and render it inaccessible to other client computers. There are several methods to develop services that the intended users cannot use, instead of simply bombarding them with several IP packets. Various security flaws could also be used against the dupe by making it unstable, depending on the attack's specifics.

Cloud computing is the provision of on-demand resources such as storage, networks, hardware, and software from Cloud Service Providers (CSP) via the Internet to reach any computer or device as a fee-based service [2] [6]. The users only need an interface software, which could be simply a web browser, so the users will be able to request several types of services provided by the CSP [2]. Based on market needs and user demand, the CSP will allocate resources on a dynamic basis. The users pay only for what they use, which is known as a "pay-as-you-go" model [2]. This computing solution is becoming increasingly popular among small and medium-sized businesses. It provides a way to increase capacity and add new features without investing in new infrastructure, training new employees, or licensing software. Using this computing solution will contribute to increasing capacity and adding capability without the need to investigate new infrastructure, train new employees, or license software.

In this paper, a mini-literature review has been conducted to provide a structured and methodical approach for understanding aspects of research in cloud computing threats. The main objective is to provide an intellectual foundation for emerging scholars in the field of cloud computing, including attack and mitigation techniques.

1.1 Cloud Computing Characteristics

Cloud computing has a few essential characteristics, which are the following [2]:

- On-Demand Service.
- Broad Network Access:
- Multi-tenancy
- Elasticity and Scalability
- Resiliency
- Pay per Use

1.2 Cloud Computing Deployment Models

The deployment models are categorized based on organization structure and the provisioning location.

- Private Cloud
- Public Cloud
- Community Cloud
- Hybrid Cloud

Even though Cloud computing provides great advantages to the end users, there are several challenging issues that need to be addressed. The financial aspects while using cloud services based on Service Level Agreements (SLA), increase the need for attention to these issues. Given that there are currently over 2.6 billion smartphone users worldwide, cloud computing makes it possible for employees to access company data while on the go via smartphones and other mobile devices. A key security risk that prevents many people from using cloud services is the lack of trust between users and cloud service providers or cloud database service providers regarding the data.

The greatest weakness of cloud computing is the security and privacy part [3], and because of that we need to address the most common attacks. And too many incidents happened over the past few years such as the Facebook breach, In April of 2021 affecting millions of users' records, and it was publicly exposed on Amazon's cloud computing service. Understanding security dangers and identifying the proper security techniques used to minimize them in cloud computing are the key goals of this research. To be familiar with the security concerns and methods employed in the contemporary cloud computing environment. To determine the security issues that cloud computing will face in the future. To offer solutions for the issues that cloud computing may encounter in the future.

Although security threats and issues are ubiquitous in all types of cloud computing environments, cloud computing needs an appropriate form of mitigation techniques, security measurement, and assurance as there are no mitigation techniques up to the mark [7]. Despite the eagerness of businesses to establish security awareness initiatives, many of them are pleased with the procedure and the outcomes. Tiny and Medium-sized firms, which typically lack dedication and experience resources are exceedingly difficult to get by.

This paper’s scope is to provide a comprehensive literature review of previous studies in cloud computing security. Many papers will be read and analyzed to identify the common attacks, and mitigation techniques. In this paper we discussed automated cloud security awareness programs for reducing cyber security attacks. organizations, even those with devoted awareness teams, frequently struggle to a discernible change in user behavior brought about by security awareness training.

- Review the latest studies related to cloud computing security.
- Review what are the common types of Cybersecurity attacks in a Cloud Computing environment.
- Review what are the suitable Cybersecurity mitigation techniques for Cloud Computing attacks.
- Propose an automated cloud security awareness program and implementation details.

The remaining of this paper is organized as followed: In section 2, we review the latest

2. METHODOLOGY

To acknowledge the existing state of knowledge and address research questions 1,2,3 and 4, we evaluated earlier research in this study. Most earlier research projects used the conventional method of literature reviews, which has little value for science because it is not fair and non-rigorous. The systematic literature review has well-defined qualities and a more distinct scientific viewpoint.

Since surveys and interviews are considered secondary research methods, we have conducted a systematic literature review (SLR) as our primary research approach.

A Systematic Literature Review (SLR) is used to find the selected paper to provide a comprehensive analysis of the related papers. Our research was conducted using Google Scalar and Saudi Digital Library (SDL). The first phase of SLR is the identification phase where we found 18,600 papers. Then we narrow it down to 18 papers. The inclusion criteria are the following: 1) Paper that is related to cloud computing security where they present the threats. 2) Journal or conference papers. The exclusion criteria are the following: 1) Not related to cloud computing security. 2) Not written in English. 3) Electronically not accessible. We used the following search string to find the studies and papers:

The key (Cloud OR Cloud Computing) AND (Attacks OR Threats) AND (Mitigation OR Countermeasures)

2.1 Research Questions

- **Research Question 1:** what are the various security techniques being used by the leading Cloud Computing providers, to prevent active and passive attacks when the data is being transferred between the Cloud and a local network?
- **Research Question 2:** what are the various security techniques being used to prevent unauthorized access to data within the Cloud?
- **Research Question 3:** what are the major security challenges we expect in future Cloud Computing?
- **Research Question 4:** How can we handle security problems that are expected in future Cloud Computing?

3. RELATED WORK

This section summarizes and reviews all selected papers conducted by other researchers.

N. Amara, Huang Zhiqui, Awais Ali [1] conducted a survey of Cloud Computing Security Threats and Attacks with their Mitigation Techniques. This paper discussed the architectural principles of cloud computing, the fundamental security requirements for cloud computing, security threats and attacks against cloud computing, as well as future research issues.

D. Mozumder, M. Mahi, and M. Whaiduzzaman [4] conducted a survey of Cloud Computing Security Breaches and Threats Analysis. The number of people using cloud services has dramatically expanded over the past few years, and a lot of data has been stored in cloud computing environments. Consequences include an increase in cloud service data breaches. due to hackers, who continuously attempt to take advantage of the security flaws in the cloud architecture. In this paper, we go into and examine actual cloud assaults to show the methods hackers used to target cloud computing platforms and how to avoid such nefarious behavior.

P. Singh, S. Manickam, and S. Rehman [7] conducted a Survey of Mitigation Techniques Against Economic Denial of Sustainability (EDOS) Attack on Cloud Computing Architecture. This paper explained EDoS, or Economic Denial of Sustainability, is a brand-new class of economic and security risks to cloud computing. Instead of using the server's resources to shut down a specific service as is the case with classic Distributed Denial of Service (DDoS), EDoS makes use of the cloud service's elasticity. As a result of the EDoS assault, the resources must dynamically scale to meet the demand, which results in a high cost to the consumer. In this survey, we examine numerous EDoS mitigation strategies that have recently been presented.

A. Wani and Z. Lone [8] conducted a survey of cloud security and privacy issues and concerns related to cloud computing and provided possible solutions for each problem. This paper presented an overview of cloud characteristics, deployment models, and service models. This paper categorized the issues and attacks into two parts, external and internal issues, and attacks. Moreover, they also categorize which service model is affected by each issue and attack. For example, the data breaches affect the IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service), whereas the side channel attacks affect only IaaS. They provide detailed information about each issue, and attack.

M. Kumar and Kavita [9] performed a study on security issues and challenges in cloud computing. This paper aims to demonstrate security threats in cloud deployment such as public, private, community, and hybrid cloud, and cloud service models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), as well as the network threats within the cloud.

I. Aziz, I. Abdulqadder, and T. Jawad [10] Conducted a comprehensive review of state-of-art techniques to detect DDoS attacks on cloud computing environments. This paper aimed to describe several types of DDoS attacks such as web-based, peer-to-peer-based, and Internet relay chat-based. Moreover, it presents challenges against DDoS defense techniques. Finally, illustrates the limitations of various kinds of DDoS attack detection approaches.

A. Tahirkheli, M. Shiraz, B. Hayat, M. Idrees, A. Sajid, R. Ullah, N. Ayub, and K. Kim [11] conducted a survey of modern cloud computing security over smart city networks, they presented the threats and vulnerabilities, consequences, countermeasures for these issues, and the future and exiting challenges. The paper briefly reviews security challenges in the cloud computing environment and identifies which concept of the CIA (Confidentiality, Integrity, and Availability) triad is being compromised with each challenge such as information disclosure compromising confidentiality.

The paper by Ahmad and Colleagues [12] discusses cloud architectures, deployment models, and common attacks. Further, the paper outlines security issues in the cloud in four categories and discussed the associated issues in each. The authors provide various prevention measures in each of the outlined attacks.

Aldhyani and Alkahtani [13] conducted a study that aimed to produce an effective approach to mitigating EDoS (Economic Denial of Services) attacks in cloud computing by incorporating artificial intelligence. Various methods of detecting distributed attacks are proposed including hard-threshold, support vector machine (SVM), K-nearest neighbors (KNN), random forest (RF) tree algorithms, and deep learning. The proposed detection systems outperformed the existing EDoS attack detection systems.

In their paper, Aslan et al., [14], an intelligent behavior-based malware detection system that works in the cloud computing environment is presented. It focuses on two parts including cloud and client environment. The authors observe that the proposed system can effectively detect both known and unknown malware from the given data samples.

Butt et al., [15] review of machine learning algorithms for cloud computing security focuses on the security framework of cloud computing. The paper outlines various threats, attacks, and mitigation techniques. The paper outlines several types of machine learning algorithms that can be used for cloud security.

Kanimozhi and Jacob [16] conduct a study to identify the effectiveness of different classifiers as network intrusion detection systems. The study compares classifiers such as random forest, naïve Baye's, K-nearest neighbors, and AdaBoost with a decision tree, support vector machine, and artificial neural network classifier. Artificial intelligence outperforms all the other network intrusion detection systems.

Kholidy [17] presents and evaluates three approaches to detect impersonation and masquerade attacks in clouds. The paper shows that the proposed detection approaches are more accurate and outperform the SWAD-MMD, a masquerade detection framework that works in cloud computing systems.

Loganathan and Winster [18] conducted research to identify the effectiveness of using machine learning and big data for detecting DDoS attacks on cloud computing. The paper aims at providing businesses with a secure environment to provide their services effectively.

Pandey [19] conducted a research project on the major types of cybersecurity attacks. The research paper aims to outline the essential process, needs, and secure protocol that can be understood even by a common person interested in cloud computing. It outlines the concept of network vulnerabilities in the early stages and proposes several mitigation techniques.

Rout and Colleagues [20] conducted a study on VM side-channel timing attacks and proposes a new method to prevent VM side-channel timing attacks on cloud computing. The study also outlines previous studies on cloud computing cyber-attacks, thus providing valuable information.

Bhajantri and Mujawar [21] performed a survey on cloud computing security issues, challenges, and countermeasures. This paper briefly reviews the security challenges of access control concerns and various countermeasures. This paper proposed an access control model with the help of encryption and trust mechanisms to reduce the issues in the cloud computing environment.

Gupta and Kumar [22] conducted a study on cloud computing security threats. This study tries to reduce the security issues related to cloud computing using suggested techniques. It discusses the current security issues, threats, and challenges in the cloud computing environment. The authors proposed 2-Step Authentication using fingerprint as a solution for account hijacking.

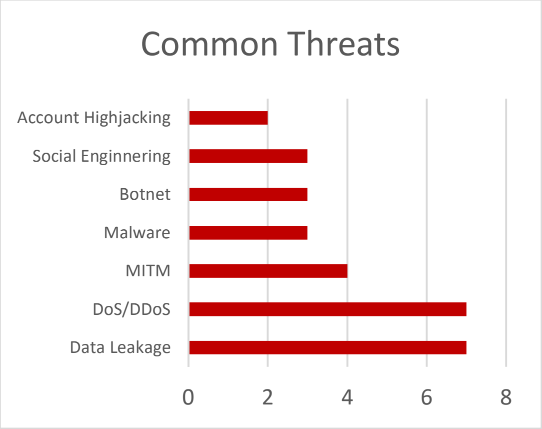

Figure 1: Findings of the most common types of cyber threats and attacks in cloud computing

3.1 Analysis and Result

In this section, we will try to answer the research questions. Based on our findings we found that the

selected papers used a qualitative method. To better comprehend ideas, opinions, or experiences, qualitative research entails gathering and evaluating non-numerical data. It might be utilized to discover intricate details about an issue or produce fresh research concepts.

3.1.1 Review what are the common types of Cybersecurity threats and attacks in a Cloud Computing environment

The most common threats and attacks in the cloud computing environment are shown in Figure 2, and they are Data Loss or Data Leakage, Denial of Service (DoS) Attack or Distributed Denial of Service (DDoS) Attack, Man-in-the-Middle Attack, Malware, Botnet Attack, Social Engineering, and Account Hijacking. Data Loss and DoS/DDoS are the most common that can cause serious issues in the CIA triad (Confidentiality, Integrity, and Availability). Data Loss will affect the confidentiality of the data, so we recommend not saving sensitive information in the cloud, and DoS/DDoS can affect the availability of services it will prevent you from login in to do your job or accessing your data.

Data saved in cloud-based systems can be shared easily. The ease of data sharing in the cloud, while a major asset and essential to collaboration, raises serious concerns regarding data loss or leakage. These environments are directly accessible from the public Internet and include the ability to share data easily with other parties via direct email invitations or by sharing a public link to the data. In fact, 69% of businesses cite this as their top concern regarding cloud security. Anybody with knowledge of the link can access data shared over public links or made publicly available in a cloud-based repository, and there are tools designed for looking for these unsecured cloud deployments online.

The capacity of many firms to conduct business depends on the cloud. Business-critical data is stored there, and they use the cloud to run crucial internal and client-facing applications. As a result, numerous companies are likely to be significantly impacted by a successful Denial of Service (DoS) attack against cloud infrastructure. DoS assaults that involve a ransom demand to end the attack thereby constitute a serious risk to an organization's cloud-based resources.

While we cannot totally stop the MITM (Main in The Middle) attack, we can endeavor to reduce the likelihood that it will happen on the network. Some of these security methods include host hardening, which entails upgrading operating systems on networked computers, network architecture from a security perspective, frequent updating of network devices and PCs on the network, and routine patch installation. By putting these solutions into practice, we can be sure that the MIM attacks will not affect us as much. However, MIM attacks will continue to be favored by both monitoring organizations and malicious actors.

Hijacking of cloud accounts is a significant issue for businesses in all industries. 86% of IT executives reported that this type of cybercrime cost them more than $500,000 in the previous year, according to a study. Account theft is also common. According to the same study, the average organization suffers from 64 cloud account hacks annually, with a third of them leading to the loss of confidential information.

3.1.2 Review what are the suitable cybersecurity mitigation techniques for Cloud Computing attacks

After analyzing the selected papers, we found the most suggested mitigation techniques are the following: 1) Intrusion Prevention System (IPS) and Intrusion Detection System (IDS), with Five papers recommending it. 2) Two-Factor Authentication with Three papers recommended it. 3) Firewall with three papers recommended it. 4) Machine Learning with three papers recommended it. 5) Data

Encryption with three papers recommended it. The most recommended technique is the IPS or IDS to mitigate the threats in cloud computing.

An intrusion prevention system (IPS) is a network security tool that continuously scans a network for harmful activity and responds to it when it does occur by reporting, blocking, or dropping it. It can be either hardware or software.

It is more sophisticated than an intrusion detection system (IDS), which can only alert an administrator and simply detect harmful activities. A next-generation firewall (NGFW) or unified threat management (UTM) solution may contain intrusion prevention technologies. They must be strong enough to scan a large volume of traffic without impairing network performance, like many network security systems.

Two-factor authentication (2FA) is a security procedure that requires users to provide two separate forms of identity, most frequently knowledge of an email address and evidence of mobile phone ownership.

Even if a perpetrator manages to get beyond the first authentication stage, the implementation of 2FA, which is added on top of the standard username/password verification, strengthens security (e.g., brute forces username and password).

To strengthen access controls to the most sensitive portions of a web service (such as admin panels or regions that store credit card information and/or personal data), 2FA is frequently used in online banking websites, social media platforms, and e-commerce sites today.

Cloud firewalls were developed because of security evolving as most organizations shifted to cloud-based applications. Cloud firewalls regulate the information flow between external domains and your internal system in a manner like classic firewalls. These systems, which are also sometimes called "Next-Generation Firewalls," combat today's sophisticated attacks and safeguard the data used in your operation.

Data is converted from plaintext (unencrypted) to ciphertext using data encryption (encrypted). With the aid of an encryption key and a decryption key, users can access encrypted data. There are numerous different encryption techniques, each created with specific security requirements in mind. Asymmetric encryption and symmetric encryption are the two primary methods of data encryption.

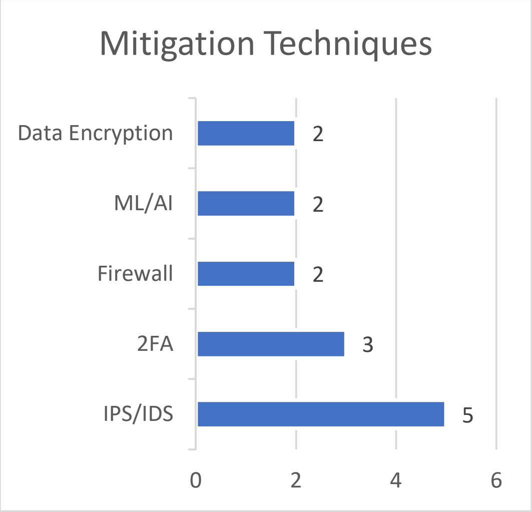

Figure 2: Most common mitigations techniques mentioned in Cloud Computing

The security of the cloud may be the responsibility of cloud service providers (CSPs), but the security of any data stored there is the client's responsibility. Sensitive information within an organization must be safeguarded while enabling authorized users to carry out their duties. This safeguard should include strong encryption key management, access control, and audit recording features in addition to data encryption.

4. AUTOMATED CLOUD SECURITY AWARENESS PROGRAM (ACSAP)

Most cybersecurity breaches are caused in large part by human error. In several cases, human error has allowed hackers to access an organization’s sensitive data. According to the IMB Cyber Security Intelligence Report: 95% of cyber security breaches are caused by human error. In addition, businesses lose millions of dollars to recover from these incidents. According to IBM’s Cost of a Data Breach Report 2020, human error-related cyber security breaches have an average cost of $3.33 million. However, traditional training programs designed to prevent these issues are only partially effective and typically fall short of inspiring and motivating the desired behavior.

While businesses are eager to deploy security awareness programs, few of them are satisfied with the implementation process and the outcomes. Small and medium-sized enterprises face special difficulties since they frequently lack the expertise and committed resources required. some of the addressed issues are:

- Lack of ideas on how to create educational goals.
- Training is time-consuming.
- Employees do not value awareness programs and do not develop their skills.

Security awareness training frequently fails to produce a noticeable change in user behavior, even in firms with dedicated awareness teams. Many businesses decide between one-time educational initiatives (such as "All about cybersecurity in 1 hour") and well-organized professional training programs, though they only utilize some of the basic features and tools. Because other programs aspects are too challenging to execute and manage, this typically consists of a few waves of simulated phishing attacks per year, along with a few overview courses. In either case, staff members fail to develop the solid abilities necessary to build a lasting sense of security for their company.

Introducing the core of the Security Awareness training offering, the Automated Security Awareness Platform. The Platform is an online platform that helps employees develop solid and useful cyber-hygiene skills all year long. The Platform may be launched and managed without the need for special setups or resources, and it offers the company built-in assistance along the entire path to a secure corporate cyber environment.

- Step 1:
    - ◦ Defining training goals and defending a program.
    - ◦ Establish objectives based on international benchmarking.
    - ◦ Strike a balance between each person's target level of security competency. The total amount of time needed to train a group of personnel to this extent.
- Step 2:
    - ◦ Ensuring that every employee receives the proper degree of training.
    - ◦ Utilize automated learning management to raise each employee's security skill level to that required by their risk profile.
    - ◦ Ensure that newly learned abilities be practiced preventing obliteration. Train individuals at their own speed to prevent over-training and rejection.
- Step 3:
    - ◦ Track data, trends, and forecasts in real-time and use actionable reports and analytics to keep track of progress.
    - ◦ Utilize real-time projections to meet the yearly training objectives. Deal with problems before they arise, for instance, by determining which organizational units require additional attention and influencing their performance. Your interim results should be compared to global lab data.
- Step 4:
    - ◦ Ensure training effectiveness and appreciation:
    - ◦ Provide learning situations applicable to participant's daily work life to engage them in the material and prevent information overload and training fatigue.

4.1 Implementation Details

- In just 10 minutes, begin your program:
    - ◦ Establish goals based on industry and global averages, begin training, and only pay for active users (those who are learning)
- Platform adapts to the unique learning styles and rates of each employee:
    - ◦ The platform automatically makes sure that users master the fundamentals before moving on to more advanced material. The time spent by management on manual adjustments and individual progress analysis is not necessary.
- Take advantage of learning routes that are tailored to each risk profile:
    - ◦ Use computerized rules to assign workers to specific groups according to their educational level that is desired. The danger the goal level depends on a specific function poses to the organization. The aim increases as the risk increases. Education should be for instance. Typically, IT or accountants represent a higher compared to most office worker's risk
    - ◦ Only the amount that each user group really analyses the material without taking up too much of your working day in training.
- Access timely reports at any moment:

  - Take advantage of dashboards that contain all the data required to assess progress.
  - Request advice on how to enhance outcomes.
  - Compare outcomes to global and sector benchmarks.

- Efficiency of training:
  - Ongoing micro-learning Level by level, from the simplest to the most complex, skills get better. Those who fail to finish a prior level receive extra learning from the platform automatically. This guarantees excellent skill retention and guards against obliteration. To prevent boring and tiresome long courses, the content is particularly arranged for micro-learning (2 to 10 minutes).
- Complete automation of training administration:
  - Use automated administration to raise each employee's security proficiency level to that required by their risk profile. Individually adjust the curriculum speed so that users can learn at their own rate without being overloaded. Strengthening of knowledge that aids in developing excellent skills. This comes in the following four levels: 1-Lesson, 2-Email Reinforcement (4 days after all lessons are finished), 3-Knowledge Test (7 days after all lessons are finished), 4- Simulated Attack (10 days after all lessons are finished)
- User-friendly dashboards & actionable reporting:
  - Get real-time forecasts, trends, and live data tracking. Address problems before they arise (e.g., you know which organizational units need more attention and can influence their results). To accomplish training objectives, use projections. Compare your outcomes against industry standards.

5 COMPARING OUR STUDY WITH THE OTHER PAPERS THAT ARE PRESENTED IN THE LITERATURE REVIEW.

By conducting a mini-literature review, we attempt to identify gaps in our paper. In many originations, we discovered a lack in employee awareness. Most of the issues addressed involved a lack of required expertise and resources. We contribute to developing an automated platform that will be used to minimize human error, by providing a full awareness program that helps employees develop solid and useful cyber-hygiene skills all year long.

6 STRENGTH AND WEAKNESS OF OUR STUDY.

Our study’s greatest strength is that it provides a literature review on selected research papers in the cloud environment and suggests a model to deal with and mitigate a vulnerability that was not discussed in the selected papers. Our research has limitations because the model we developed may not work for all businesses, especially those on a large scale, and could benefit from incorporating a broader range of conscious considerations.

7. CONCLUSION AND FUTURE WORK

In this paper, we reviewed the most common threats and countermeasures in the cloud using a systematic literature review (SLR), we found that data breaches are the most common threat in cloud computing. Data breaches are mostly caused by human error, and for that, we developed a platform we name it Automated Cloud Security Awareness Program (ACSAP), to help the organization train their employees before they start using the cloud. In this study, several research papers that focus on the threats and mitigation mechanisms that can be used in a cloud environment were reviewed and analyzed. After reviewing the papers, we concluded that awareness is not addressed anywhere in them. As a result of this, it has been suggested for future work to conduct more studies in the area in order to find a more effective solution to the problem.

6. FUNDING

This work was funded by King Faisal University, Saudi Arabia [Project No. GRANT2,802].

7. ACKNOWLEDGMENTS

This work was supported through the Annual Funding track by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Project No. GRANT2,802].

8. CONFLICTS OF INTEREST

All authors declare no conflict of interest.

REFERENCES

[1] N. Amara, Huang Zhiqui, Awais Ali, "Cloud Computing Security Threats and Attacks with their Mitigation Techniques", International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2017.

[2] P. Mell and T. Grance, "The NIST definition of cloud computing", Communications of the ACM, 2011. Available: http://csrc.nist.gov/publications/PubsSPs.html#800-145.

[3] R. Al Nafea and M. Almaiah, "Cyber Security Threats in Cloud: Literature Review", International Conference on Information Technology (ICIT), 2021.

[4] D. Mozumder, M. Mahi, and M. Whaiduzzaman, "Cloud Computing Security Breaches and Threats Analysis", International Journal of Scientific and Engineering Research, 2017.

[5] Top 5 cloud security breaches, CyberTalk, 2022. Available: https://www.cybertalk.org/2022/04/26/top-5-cloud-security-breaches-and-lessons.

[6] Q. Hassan, A. Raid, and A. Hassan, “Understanding Cloud Computing”, IGI Global, 2012.

[7] P. Singh, S. Manickam, and S. Rehman, “A Survey of Mitigation Techniques Against Economic Denial of Sustainability (EDOS) Attack on Cloud Computing Architecture”, Reliability, Infocom Technologies and Optimization (ICRITO), 2014.

[8] A. Wani and Z. Lone, "A Survey of Security Issues and Attacks in Cloud and their Possible Defenses", International Journal of Emerging Technologies in Engineering Research (IJETER), 2017.

[9] M. Kumar and Kavita, “Study on Security Challenges in Cloud Computing”, International Journal of Advanced Science and Technology, 2020.

[10] I. Aziz, I. Abdulqadder, and T. Jawad, "Distributed Denial of Service Attacks on Cloud Computing Environment: A Comprehensive Review", Cihan University-Erbil Scientific Journal (CUESJ), 2022.

[11] A. Tahirkheli, M. Shiraz, B. Hayat, M. Idrees, A. Sajid, R. Ullah, N. Ayub and K. Kim, "A Survey on Modern Cloud Computing Security over Smart City Networks: Threats, Vulnerabilities, Consequences, Countermeasures, and Challenges", Electronics, 2021.

[12] Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z, “Cyber security in IoT-based cloud computing: A comprehensive survey”. Electronics, 2021.

[13] Aldhyani, T. H., & Alkahtani, H., “Artificial Intelligence Algorithm-Based Economic Denial of Sustainability Attack Detection Systems: Cloud Computing Environments”, Sensors, 2022.

[14] Aslan, Ö., Ozkan-Okay, M., & Gupta, D., “Intelligent behavior-based malware detection system on the cloud computing environment”, IEEE Access, 2021.

[15] Butt, U. A., Mehmood, M., Shah, S. B. H., Amin, R., Shaukat, M. W., Raza, S. M., and Piran, M., “A review of machine learning algorithms for cloud computing security” Electronics, 2020.

[16] Kanimozhi, V., and Jacob, T. P., “Artificial Intelligence outflanks all other machine learning classifiers in Network Intrusion Detection System on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing”, ICT Express, 2021.

[17] Kholidy, H. A., “Detecting impersonation attacks in cloud computing environments using a centric user profiling approach”, Future Generation Computer Systems, 2021.

[18] Loganathan, V. and Winster, S.G., “A Novel Approach for Reduction of DDOS Attacks in Cloud Computing using Non-Parametric Hypothesis”, 8th International Conference on Smart Structures and Systems (ICSSS), IEEE, 2022.

[19] Pandey and Prabin, "Security attacks in cloud computing.", Turku University of Applied Sciences Thesis, 2021.

[20] Rout, C., Sethi, S., Badajena, J. C., & Sahoo, R. K., “Secure Virtual Machine Allocation for Prevention of Side-Channel Attacks in Cloud Computing”, International Conference on Intelligent Controller and Computing for Smart Power (ICICCSP) - IEEE, 2022.

[21] Bhajantri, L. B., and Mujawar, T, “A Survey of Cloud Computing Security Challenges, Issues and their Countermeasures”, IEEE, 2019.

[22] Gupta, H., & Kumar, D., “Security Threats in Cloud Computing”, IEEE, 2019.