Cyber Security Threats in Cloud: Literature Review

Roaa Al Nafea
Computer Networks and communication Department
King Faisal University
Hofuf, Saudi Arabia
roaa.alnafea@gmail.com

Mohammed Amin Almaiah
Computer Networks and communication Department
King Faisal University
Hofuf, Saudi Arabia
malmaiah@kfu.edu.sa

2021 International Conference on Information Technology (ICIT) | 978-1-6654-2870-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICIT52682.2021.9491638

***Abstract*— In recent years, data has been expanding every second in terms of velocity, volume, and variety. This has resulted in enormous and complex big data, raising challenges in the storage, management, analysis of these big data and security thereof. Many organizations tend to use cloud systems in order to facilitate the operation in big data without being fully aware of the security and privacy challenges that the utilization of these systems pose and consequently ignoring the important practices and techniques that should be implemented when using cloud systems. These security threats therefore require more research in order to produce solutions to the cloud system environment. The goal of this paper is collection of most common cyber security threats in the cloud system environment and most common used mitigation techniques by reviewing the published papers in the period from 2019 to 2020 followed by cloud risk assessment case study in an organization in Saudi Arabia.**

Keywords—Security, threats, cloud, mitigation.

I. INTRODUCTION

The Cloud systems are on-demand, scalable services that help deal with and analyse big data. Recently it is widely used because of its cost saving due to the sharing of resources, its accessibility from a geographical perspective, round-the clock availability and the prevention of data loss due to the existence of multiple copies. The most prevalent disadvantages to cloud systems are the security and privacy issues which are both different to, and more numerous than traditional storing techniques [1]. This project is aimed at reviewing previous studies related to cyber security threats to cloud systems. In addition, it will identify and analyse the major threats in the cloud system environment.

In cloud system security is a big challenge as it is a mix of policies, technologies, controls and policies to protect the data, services, and infrastructure. Therefore, the vulnerabilities increase due to this combination [2]. Data in cloud outsourced to trusted or untrusted service provider which compromise the client privacy [3].

The objectives of this literature review is survey the previous studies conducted with regards to cloud system security techniques, and the mitigation techniques presented by these reviewed studies, followed by conducting a cloud risk in an organization in Saudi Arabia.

II. RESEARCH METHODOLOGY

In order to conduct this systematic review, four steps have been carried out by PRISMA [4]; the preferred reporting elements for systemic reviews and the meta-analysis process. In the first stage these research terms have been formulated as:

TI (security or cybersecurity) AND TI cloud AND TI (threats OR vulnerabilities OR challenges OR issues).

The search conducted in Saudi digital Library, and google scholar databases with the following inclusion criteria: Papers that represent threats in cloud system, and papers that published between January 2019 and February 2021

Where the exclusion criteria were as followed: Papers not written in English, papers not related directly to security in cloud computing and papers that are not accessible.

The source type specified as Academic journal or conference paper. In identification phase, 603 papers were founded from different data bases, after removing duplication 352 studies are remained. In the screening title and abstract phase, 277 papers have been excluded that not tightly matching the criteria. After full text assessing, In the Included phase, 31 studies chosen 16 of them were excluded to end up with 15 selected studies. This is shown in fig.1.

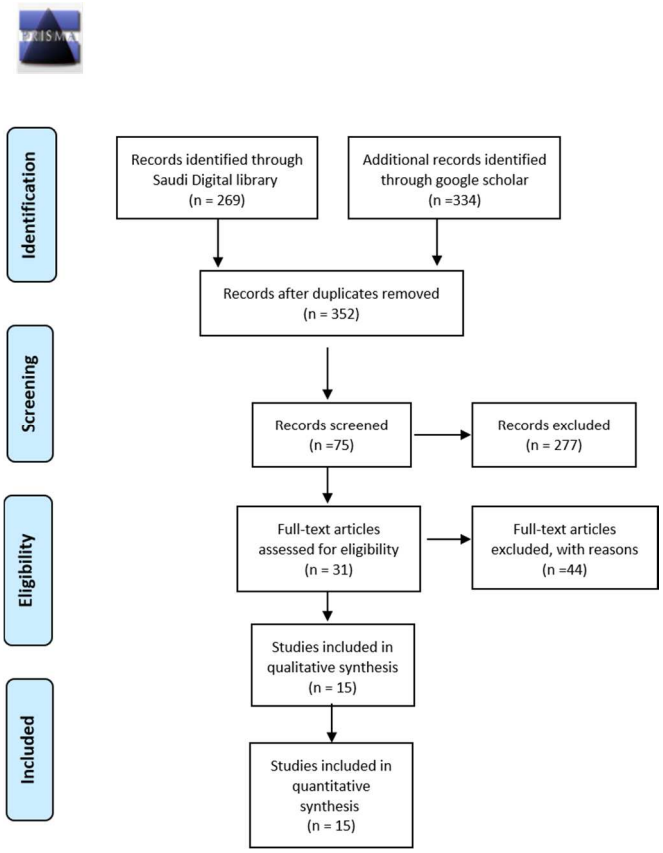

Fig .1 . Schematic diagram PRISMA Literature Review

III. EXISTING WORK

Several research studies have been reviewed and summarized in table. I by the publication year, the addressed threats by the researcher and the suggested mitigation techniques in each paper.

K Kushala and Shaylaja [5] performed a survey on recent trends on security issues in Multi-Cloud Computing. For both client and service provider, the transition from local computing to cloud computing has created several of the security issues. The objective of this paper is to explain the fundamental characteristics of CC, and Multi-Cloud Computing (MCC) along with their security problems, and potential solutions. The researcher address Addressed security risk, security mechanism used and type of cloud in each risk is occur.

Mondal et al. [6] review the cloud computing security issues and challenges. It highlights the major issues in securing cloud computing such as trust, authenticity, confidentiality, encryption, key management, multitenancy, data splitting, and virtual machine security, as well as possible solutions. The researchers address sharing resources issues of cloud as a major cause of vulnerabilities that should be conducted in future work.

Syed et el. [7] performed a review on cloud storage security risks, practices, and measures. The goal of this paper is to represent some of the security issues as well as existing state-of-the-art implementations to resolve them. With the rapid advancements in the cloud in this field, however, protection and privacy are at the top of the list of concerns and requirements. Poor data visibility, storage sinks without protected pointers, huge data overflows, and other issues can result in significant monetary and information loss for people. In order to mitigate these risks, the paper summarizes the security risk as lack of control, shared servers, data leakage, and API and storage sinks. The research identifies these essential practices in establishing cloud storage: Multi factor authentication, data classification, security encryption, and assessing cloud framework. Furthermore, the paper incorporates three more advanced practices while dealing with sensitive data: private encryption, in-Transit encryption, ransomware protection.

Balani and Varol [8] tried to capture Cloud computing security challenges and threats. In an online environment, data is accessible from anywhere in the globe. Furthermore, consumers are concerned about the security of their data in the cloud. The objective of this study is to suggest some strategies and techniques for protecting data in an online environment. These techniques are the most cost-effective, and they can be used by anyone as a simple way to protect themselves from threats. The findings indicate that a variety of methods and models have been suggested, but none has proven to be fruitful as there are no security standards for stable cloud computing, according to the researchers. Investigating cloud security standards is proposed by researcher as a future work.

Ghaffari et al. [9]survey the cloud security issues based on people, process and technology model. The survey tried to detailed identification of cyber security problems and answer these threats to categories of individuals, processes, and technologies in order to identify cost effective, reliable, and feasible security solutions based on this basis. The researchers go through some of the relevant cloud computing research. Then proposed the PPT model's concept for categorizing cloud security challenges and related solutions. After that, the proposed approach is used to categorize these challenges.

Gupta and kumar [10] performed a study in security threats in cloud computing. the aim of this study is to try to enhance the security problems related to cloud computing using different technique. It discusses cloud computing structure, models, current security threats and challenges. Gupta and Kumar proposed two-step authentication using fingerprint as a Solution for Account Hijacking.

Kumari et al. [11] conducted a mirror review in security issues and challenges in cloud computing that discussed that the potential for data breach in cloud computing system has been raised due to the evolution of new technology such as the Internet of Things (IoT) and Big Data and smart cities. In this paper, various privacy and security issues related to data security were discussed. It is also discussed what countermeasures are recommended to protect the data classified by technology. Future research should concentrate on finding a solution to the essentials security issues and creating a secure model, according to the paper.

Mandal and Khan [12] performed a study of security threats in cloud with the passive impact of COVID-19 pandemic. With the worldwide spread of Corona virus employees working from home and students taking classes remotely, hence companies make a significant shift to cloud computing. Related to the sudden usage of cloud services without proper protections, this paper addresses a number of security issues. The main objective of this paper is to identify the areas that are causing security breaches and to suggest general preventative measures. It discusses various cyber-attacks that expose cloud services and hosts to risk. The societal impact and safeguards have also been debated in light of recent attacks. The paper tried to raise public awareness about these attacks and to make recommendations for security policy changes. As a future work the researcher emphasize the need to an access control framework to prevent spoofing attack.

Bahajantri and Mujawar [13] conducted a survey of cloud computing security challenges, issues, and their countermeasures. The paper briefly reviews security concerns at the infrastructure, data, and cloud levels, as well as the definition of Identity and Access Control. Also addressed various countermeasures for avoiding security problems in cloud environments. This paper proposed a strong access control framework with Attribute based encrypted encryption and trust mechanism combined.

Narng and Gupta [14] review the different security issues and challenges in cloud computing. Many people believe that using cloud resources and services is risky. Cloud computing is risky since there is no guarantee that the information is monitored or preserved by the service provider. The paper has gone through a couple of the issues and challenges that come with cloud computing. It provides an overview of data security, privacy, and problems in the cloud. The paper also includes a literature analysis of cloud infrastructure problems and challenges, as well as a discussion of various security concerns. The researcher suggest that professional security standards should be developed as well as certification by third parties to ensure that standards are met properly and hence to win customer trust.

Nhlabatsi et al. [15] proposed a ThreatRiskEvaluator tool for assessing security risks that are specific and relevant to specific security risks in the cloud. Cloud providers usually perform general security mechanisms where practically different clients having different security requirement; therefore, the general mechanism is not always efficient. The ThreatRiskEvaluator tool applies a unique risk analysis approach that allows service providers to make perfect decisions about which protection mechanisms to use to address specific risks posed to clients based on their security requirements against specific risks. Performance evaluation of the tool shows that specifying the degree clients care about specific risk, help security team to provide efficient countermeasures. This proposed tool has this limitation: As the size of the topology grows larger, the current prototype will not be able to handle risk assessment well.

Patel et al. [16] Performed a detailed review of cloud security issues, threats and attacks. With more organizations embrace cloud computing, attackers take advantage of the cloud to gain unauthorized access to the valuable data stored there, these vulnerabilities are varying with the several technologies used by different service providers. The paper conclude that novel technologies used by cloud providers raising new vulnerabilities.

Santoso [17] conducted a study on opportunities for cybercriminals and security challenges in cloud technology. The main research question that this paper is try to answer is "which security demands will the transition to a cloud service implicate?" This research result in an assessment for security requirement that businesses and organizations can use as a starting point for initiating the transformation from local storage to the cloud technology to get its great benefits.

Siddique et al. [18] performed a study to avoid evasive threats to information security on cloud using blockchain technology. The goal of this paper is to provide step by step approach with the help of blockchain technology to solve Information system threats in the cloud. In addition, it discussed the challenges in the implementation of blockchain security. The combination of blockchain with cloud computing result in more security for the information system due to correlation and sequence for the information in each block.

Alatawi et al.[19] conducted a survey on cloud security issues and solution. The study reviews 4 papers that uses the blockchain system technology as a solution for cloud storage problems. Alatawi et al. aim at explaining the architecture of cloud system and major issues in it, providing readers with a better understanding of how block chain technology operates, and investigating the most powerful approaches and technologies for resolving cloud computing security issues using block chain techniques. Alatawi et al. research proposes a solution to the problem of cloud system protection. Three critical steps are used to create a block chin: open ledger, distributed open leger, and mining. This study result in that the best proposed system for cloud using block chain is the one presented by Shah et al.[20] in which AES is used for encryption and IPFS protocol is used for distribution and storing.

IV. Result

The result from the previous section for the most common threats in the selected papers can be summarized in fig. 2. This figure shows that most common threats in the cloud system are: account hijacking, data sanitization, data control and malicious insider. Where the data control is the most security control as data in the cloud usually controlled by the service provider and the clients do not have full control to their own data.

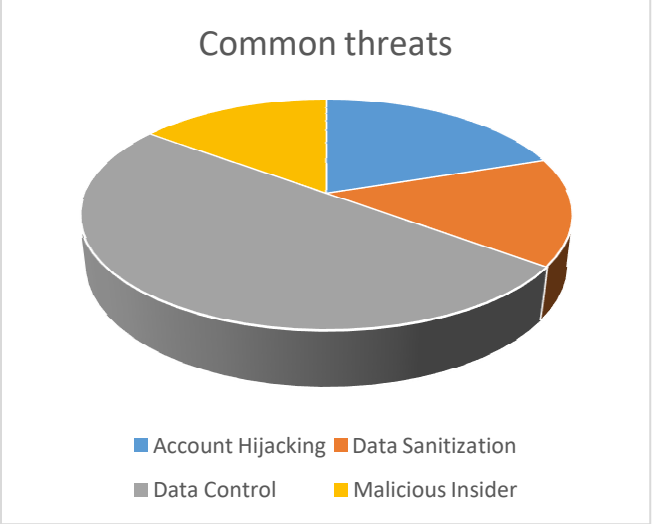

Fig .2 . Most common threats mentioned in cloud system.

The suggested mitigation techniques to address these threats are applying encryption, access control, using blockchain and service level agreement between client and provider.

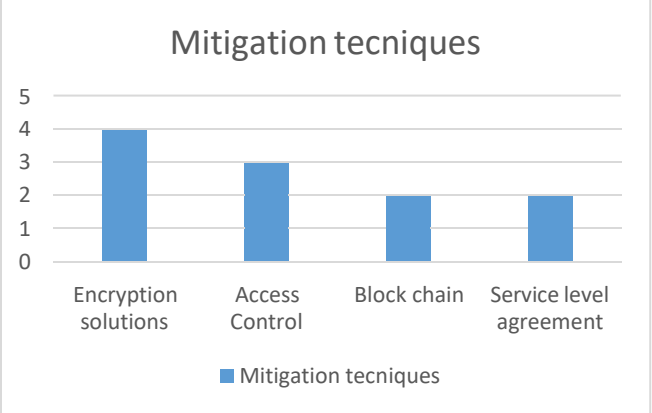

Fig .3 . Most common mitigations techniques mentioned in cloud system.

TABLE I. ADDRESSED THREATS AND MITIGATION TECNIQUES .

Author	Publication year	Addressed threats	Suggested mitigations
Kushala and Shaylaja [5]	2020	Control of stored data, Data sanitization, Service Availability, Authentication and Authorization, Confidential Computing and Virtualization.	RSA, Cloud Inter-operative Toolkit (CIT), Byzantine Protocol, Optimization Technique, Self-adaptive Technique, DepSky (Byzantine + secret Sharing + cryptography), RAID-like Technique + introduced RACS, ICstore (client centric distributed protocols), SPORC (fork), HAIL (Proofs + cryptography) and TCCP.
Mondal et al. [6]	2020	Trust Problem, Confidentiality Problem, Authenticity Problem, Encryption Problem, Key Management Problem, Data Splitting Problem, and Multitenancy problem.	end-to-end mechanism based encryption, fully Holomorphic encryption, P2P reputation system, Service Level Agreement, P2P reputation system, Secret Sharing algorithm and TMR Technique, Isolation, and two-level encryption solution.
Syed et el. [7]	2020	5 mainly type of threats: Account Control, Malicious Insiders, Data Control, Management Console Security and Multi-tenancy Issues.	Assessing cloud framework, Multi Factor authentication, Data Classification, Security Encryption, Private Encryption, In-Transit Encryption and Ransomware Protection.
Balani and Varol [8]	2020	Privileged user access, Regulatory compliance, Data location, Data segregation, Recovery, Investigation support and Long-term performance	Access control, Provide more security at minimum cost, and Event prevention and intervention.
Ghaffari et al. [9]	2019	Trust Issue, Human Resource, Compliance and Legal, Performance, Access Control, Data Security, Forensics, Multi-tenancy Issues, Virtualization, Software, Network and Service Related and monitoring.	Categorization of security challenges to allow managers to identify weak point and take most appropriate solution.
Gupta and kumar [10]	2019	Data Breach, Data Loss, Insider Threats, Data Location, Account Hijacking, Insecure Application Programming Interfaces and Multi Tenancy.	2 step authentication model with fingerprint to avoid hijacking.
Kumari et al. [11]	2019	Account Hijacking, User and service provider trust issues and Accessibility and data loss.	Service Level Agreements (SLA), Access Management and Encryption and Integrity Verification
Mandal and Khan [12]	2020	Issues with COVID-19 passive impact: Unskilled Usage, Psychological Effects on Cyber Security, Attacks Due to Using Dark Webm Attacks on Video tutorial softwarem Phishing Scams, Attacks on Hosts, Ransomware Attacks, and email scams.	Suggested group of practices for individuals and organizations including backup, awareness for the society etc.
Bahajantri and Mujawar [13]	2019	Infrastructure Security, Data Security and Identity and Access Management (IAM).	Proposed access control model.
Narng and Gupta [14]	2019	Data Sanitization, Data Location, Isolation of systems, sniffing of packets, scanning of the ports, IP Spoofing, Middle Attack, DDoS, Risk of Seizure, Data Integrity, Losing control over data, Failure in Provider's Security, Constant Feature Additions, and Incompatibility Issue.	Suggest employing some skilled security standardization, and third-party certification to ensure that standards are met.

Author	Publication year	Addressed threats	Suggested mitigations
Nhlabatsi et al. [15]	2019	General security mechanism by cloud provider is not effective for specific client security requirement.	Proposed ThreatRiskEvaluator tool.
Patel et al. [16]	2020	Data Breach/Loss, Abuse and Nefarious Use of Cloud services, Insecure Interfaces and APIs, Shared technology problem in multi-tenancy ecosystems, Risk Profiling, Inadequate Infrastructure Design and Planning, Loss of Operational & Security Logs, Malicious Insiders, Illegal Access to the Cloud, Supply Chain Failure, Isolation Failure, Network Management Failure, Authentication Attacks, Loss of Encryption Keys, Undertaking Malicious Probes or Scans, Loss/Modification of Backup Data, Compliance Risks, Identity theft, and Service/Account hijacking.	cloud's virtualization and multi-tenancy.
Santoso [17]	2019	Virtual Machines and Virtualization, Side Channel Attacks and Reverse Engineering, Subsystems, Hypervisor, Fate Sharing, Business Reputation, Distribution of Debt (Attribution of Blame), Mutual Auditability and botnet.	
Siddique et al. [18]	2020	Different information security threats in cloud.	Blockchain
Alatawi et al.[19]	2020	Several issues.	Blockchain

V. CLOUD RISK ASSESSMENT (CASE STUDY)

Risk Assessment process has been conducted in an organization in Saudi Arabia (we call it Alpha) using Delphi Approach to identify threats, vulnerabilities, and countermeasures in their cloud system. The Delphi approach allows all participants to iteratively update their perspectives and inputs rather than working together directly. Depending on the background and the expert views, the viewpoints of others may be influential, useful, informative, or useless. This anonymous collaboration allows members to express and revise their opinions in quantitative, iterative manner. This approach eliminates social pressure and other performance concerns that usually happens in group working [21]. Experts on those organizations have been asked to fill questionnaires through multiple stages with open ended questions, since close-ended questions can lead to a particular predicted response.

This Process Performed in four stages as follows: identifying threats to the cloud system in Alpha organizations and prioritize them, Second, identifying vulnerabilities. Third, determining the impact of these threats on the business operation. Fourth, selecting controls and evaluating the effectiveness of each selected controls.

A. Identifying threats.

Based on the expertise's answers to the questionnaire, the most common threats determined and prioritized based on their importance. These threats mapped to the STRIDE threat modeling elements [22] in table. II. STRIDE is stands for Spoofing, Tampering, Reputability, Information disclosure, Denial of Service and Elevation of privilege. The main founded threats are:

1) Denial of service.

Conducting Denial of Service (DoS) attacks on cloud service providers can result in users lacking access to their accounts. DoS attacks can be carried out by overwhelming the server with several requests to exhaust all available device resources, sending malicious data to the server that crashes an application procedure, repeatedly inserting incorrect passwords to lock the user account, and so on [23].

2) Unauthorized access and Account Hijacking.

Unauthorized access is more likely in cloud storage system with many customers since a flaw in one user's application cloud allows attackers to access other users' data. If an intruder is successful in stealing a customer's accounts (hijacking the account), they may be able to access their cloud resources, monitor their actions, exploit their records, and transfer users to unauthorized websites, potentially causing reputational harm and financial loss [24].

3) Data leakage.

Enterprises are susceptible to attack when data is not secure, whether it is in transit or at rest. However, if the data being upload or download, it will be exposed to higher risk.

4) Cloud provider malicious insider.

Malicious insider threats are a serious security concern especially in the cloud environment where the cloud system is shared with untrusted parties, accessible from the public internet, and organizations does not have full control on their system.

TABLE II. COMMON THREATS BASED ON EXPERTISE ANSWERS.

Threats	S	T	R	I	D	E
Unauthorized access and Account Hijacking	√	√	√	√		√
Data leakage				√		
Cloud provider malicious insider	√	√		√		
Denial of service attack					√	

B. Identifying vulnerabilities.

Vulnerability refers to "The probability that an asset will be unable to resist the actions of a threat agent. Vulnerability exists when there is a difference between the force being applied by the threat agent, and an object's ability to resist that force". [25] In this stage we identify the main vulnerabilities in the organizations based on expertise answers mapped to the CIA elements (Confidentiality, Integrity, and availability.) that this vulnerability violates in Table. III. These vulnerabilities are: poor access management, lack of data leakage prevention, and lack of strong security policies.

TABLE III. COMMON VULNERABILITIES IN ALPHA ORGANIZATION.

Vulnerabilities	CIA
Poor access management	Loss of Integrity, Loss of Confidentiality.
Lack of data leakage prevention	Loss of Integrity, Loss of Confidentiality.
Lack of strong security policies	Loss of Integrity, Loss of Confidentiality, Loss of Availability.
Poor input filtering and validation	Loss of Availability.

C. Identify risks and impact of these addressed risks.

During this stage we identify the risk in Alfa organization by mapping the threats to vulnerabilities and asking the expertise again individually to determine the probability on each risk based on historical data using qualitative method, also specifying the potential impact of every risk. The result of this shown in Table. IV.

TABLE IV. IDENTIFYING RISKS AND IMPACT OF IT.

Threats	Vulnerabilities	Probability	Impact	Risk level Probability * impact
Denial of service attack	Poor input filtering and validation	0.6	100	60
Unauthorized access and Account Hijacking	Poor access management	0.6	70	42
Data leakage	Lack of data leakage prevention	0.4	30	12
Cloud provider malicious insider	Lack of strong security policies	0.3	30	9

D. Suggested Controls and evaluating each control.

After deep reviews in the contracts and existing protection measures in Alfa organization three controls suggested by expertise to mitigate the risks addressed in the previous section.

1) Filter and monitor the traffic.

All requests should be filtered before they enter the target network in order to protect from denial-of-service attack using services like Amazon Shield and Cloudflare that defend against DoS and DDoS attacks by comparing incoming packet IPs against known attackers and only forwarding legitimate one.

2) Enforce multi-factor authentication (MFA).

Traditional password protection is insufficiently secure in the cloud storage against the most advanced forms of attack [26]. In this case multi-factor authentication should be used in which a user given access to a service only when presents two or more evidence.

3) Implement Data Loss Prevention (DLP).

Data loss prevention systems usually attempt to monitor sensitive data access and avoid leakage or unauthorized handling. Their primary goal is to monitor and manage the data while collect, move, and process of sensitive information in accordance with defined security policies [27].

At the end usefulness of these controls toward each threat is discussed with expertise and summarized in Table V.

TABLE V. USFULNESS OF THE CONTROLS.

Threats/Controls	Filter and monitor the traffic	Enforce MFA	Implement DLP
Denial of service attack	100	30	10
Unauthorized access and Account Hijacking	10	90	20
Data leakage	20	40	100
Cloud provider malicious insider	20	70	40

Results of this case study show that analyzing and assessing risks in the cloud necessitates a deep understanding of risk. The importance of risk assessment is to help company to find its vulnerabilities and prioritize the risks thus allow management to focus on most efficient controls to mitigate risks and achieve business continuity. We also can conclude that this case study contains important generic Information that would be useful in other similar organizations. Future studies should concentrate on alternate risk mitigation techniques as cloud rapidly growth resulting in new security issues that cannot be addressed with traditional techniques.

VI. CONCLUSION

This study review the studies on threats in the clous system environment in order to help organizations when they take the decision to move to the cloud to know the most common threats and be aware of using the suggested mitigation techniques.

Big companies use cloud technology extensively, but in recent years, many individual organizations and small enterprises have moved to cloud systems thus security issues need to be addressed when moving to the cloud. Although it is not possible to achieve security from end to end due to the complexity in cloud environment. However it is a shared responsibility between client and service provider to mitigate threats as much as possible at every possible stage.

REFERENCES

[1] Kumari K, Mrunalini M. A Survey on Big Data Security: Issues, Challenges and Techniques. International Journal of System & Software Engineering. 2018;6(2):23-36. Accessed February 13, 2021.

[2] M. Lori, “Data security in the world of cloud computing,” Co-published by the IEEE Computer And reliability Societies, pp. 61–64, 2009.

[3] Qadiree, Jahangeer, Neha Prasad, and Pratima Gautam. 2017. “Security and Privacy Approach of Cloud Computing Environment.” International Journal of Advanced Research in Computer Science 8 (7): 648–51. doi:10.26483/ijarcs.v8i7.4355.

[4] Moher, D., A. Liberati, J. Tetzlaff and D.G. Altman, 2009. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. Phys. Therapy, 89: 873-880. DOI: 10.1136/BMJ.B2535

[5] ushala, M. V., & Shylaja, B. S. (2020). Recent Trends on Security Issues in Multi-Cloud Computing: A Survey. In (pp. 777-781): IEEE

[6] Mondal, A., Paul, S., Goswami, R. T., & Nath, S. (2020). Cloud computing security issues & challenges: A Review. In (pp. 1-5): IEEE.

[7] Syed, A., Purushotham, K., & Shidaganti, G. (2020). Cloud Storage Security Risks, Practices and Measures: A Review. 2020 IEEE International Conference for Innovation in Technology (INOCON), Innovation in Technology (INOCON), 2020 IEEE International Conference For, 1–4. https://doi-org.sdl.idm.oclc.org/10.1109/INOCON50539.2020.9298281

[8] Balani, Z., & Varol, H. (2020). Cloud Computing Security Challenges and Threats. In (pp. 1-4): IEEE

[9] Ghaffari, F., Gharaee, H., & Arabsorkhi, A. (2019). Cloud Security Issues Based on People, Process and Technology Model: A Survey. In (pp. 196-202): IEEE

[10] Gupta, H., & Kumar, D. (2019). Security Threats in Cloud Computing. In (pp. 1158-1162): IEEE

[11] Kumari, C., Singh, G., Singh, G., & Singh Batth, R. (2019). Security Issues and Challenges in Cloud Computing: A Mirror Review. In (pp. 701-706): IEEE

[12] Mandal, S., & Khan, D. A. (2020). A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic. In (pp. 837-842): IEEE

[13] Bhajantri, L. B., & Mujawar, T. (2019). A Survey of Cloud Computing Security Challenges, Issues and their Countermeasures. In (pp. 376-380): IEEE.

[14] Narang, A., & Gupta, D. (2019, 2019 / 03 / 26 /). A review on different security issues and challenges in cloud computing.

[15] Nhlabatsi, A., Hussein, A., Fernandez, R., Fetais, N., Hong, J., Kim, D., & Khan, K. M. (2019). ThreatRiskEvaluator: A Tool for Assessing Threat-Specific Security Risks in the Cloud. In (pp. 1-6): IEEE

[16] Patel, A., Shah, N., Ramoliya, D., & Nayak, A. (2020). A detailed review of Cloud Security: Issues, Threats & Attacks. In (pp.758-764): IEEE.

[17] Santoso, L. W. (2019). Cloud Technology: Opportunities for Cybercriminals and Security Challenges. In (pp. 18-23): IEEE.

[18] Tabrez Siddiqui, S., Shuaib, M., Kumar Gupta, A., & Alam, S. (2020). Implementing Blockchain Technology: Way to Avoid Evasive Threats to Information Security on Cloud. In (pp. 1-5): IEEE

[19] Alatawi, S., Alhasani, A., Alfaidi, S., Albalawi, M., & Almutairi, S. M. (2020). A Survey on Cloud Security Issues and Solution. In (pp. 1-5): IEEE

[20] M. Shah, M. Shaikh, V. Mishra and G. Tuscano, (2020) Decentralized Cloud Storage Using Blockchain.

[21] Paul, C. L. A Modified Delphi Approach to a New Card Sorting Methodology J. Usability Studies Vol. 4, Issue 1, November 2008, pp. 7-30

[22] A. Mackman, Improving Web Application Security: Threats and Countermeasures, USA: Microsoft, 2003.

[23] Paxton, Napoleon C. "Cloud security: a review of current issues and proposed solut ions." 2016 IEEE 2nd Internat ional Conference on Collaborat ion and Internet Comput ing (CIC). IEEE, 2016.

[24] Qadri, Maroof Naieem, and S. M. K. Quadri. "Mapping cloud computing in university e-governance system." International Journal of Intelligent Computing and Cybernetics (2018).

[25] The Open Group, “Risk taxonomy”, 2009.

[26] R. K. Banyal, P. Jain and V. K. Jain, "Multi-factor Authentication Framework for Cloud Computing," 2013 Fifth International Conference on Computational Intelligence, Modelling and Simulation, Seoul, Korea (South), 2013, pp. 105-110, doi: 10.1109/CIMSim.2013.25.

[27] T. Wüchner and A. Pretschner, "Data Loss Prevention Based on Data-Driven Usage Control," 2012 IEEE 23rd International Symposium on Software Reliability Engineering, Dallas, TX, USA, 2012, pp. 151- 160, doi: 10.1109/ISSR

[28] Almaiah, M. A., & Alamri, M. M. (2018). Proposing a new technical uality requirements for mobile learning applications. Journal of Theoretical and Applied Information Technology, 96(19).

[29] Almaiah MA, Dawahdeh Z, Almomani O, Alsaaidah A, Al-khasawneh A, Khawatreh S. A new hybrid text encryption approach over mobile ad hoc network. International Journal of Electrical and Computer Engineering (IJECE). 2020 Dec;10(6):6461-71.

[30] Adil, M., Khan, R., Almaiah, M. A., Binsawad, M., Ali, J., Al Saaidah, A., & Ta, Q. T. H. (2020). An efficient load balancing scheme of energy gauge nodes to maximize the lifespan of constraint oriented networks. IEEE Access, 8, 148510-148527.

[31] Adil, M., Almaiah, M. A., Omar Alsayed, A., & Almomani, O. (2020). An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks. Sensors, 20(8), 2311.

[32] Khan, M. N., Rahman, H. U., Almaiah, M. A., Khan, M. Z., Khan, A., Raza, M., ... & Khan, R. (2020). Improving Energy Efficiency With Content Based Adaptive and Dynamic Scheduling in Wireless Sensor Networks. IEEE Access, 8, 176495-176520.

[33] Al Hwaitat, A. K., Almaiah, M. A., Almomani, O., Al-Zahrani, M., AlSayed, R. M., Asaifi, R. M., ... & Alsaaidah, A. (2020). Improved Security Particle Swarm Optimization (PSO) Algorithm to Detect

Radio Jamming Attacks in Mobile Networks. Quintana, 11(4), 614-624.

[34] Adil, M., Khan, R., Ali, J., Roh, B. H., Ta, Q. T. H., & Almaiah, M. A. (2020). An Energy Proficient Load Balancing Routing Scheme for Wireless Sensor Networks to Maximize Their Lifespan in an Operational Environment. IEEE Access, 8, 163209-163224.

[35] Adil, M., Khan, R., Almaiah, M. A., Al-Zahrani, M., Zakarya, M., Amjad, M. S., & Ahmed, R. (2020). MAC-AODV based mutual authentication scheme for constraint oriented networks. IEEE Access, 8, 44459-44469.

[36] Almaiah, M. A., & Al-Khasawneh, A. (2020). Investigating the main determinants of mobile cloud computing adoption in university campus. Education and Information Technologies, 25(4), 3087-3107