International Journal of Cybersecurity Engineering and Innovation

ARTICLE INFO

Article History: Received: 17-08-2025, Revised: 20-09-2025, Accepted: 22-09-2025, Published: 25-09-2025
Corresponding author Email: beautywings-1994@hotmail.com
DOI:

Vol. 2024 No.1

A systematic review of cyber security threats in Cloud Computing

Moza Alshabibi[1]

[1] *Fellowship Researcher, INTI International University, Nilai 71800, Malaysia*

Abstract

Cloud computing has become a fundamental technology for delivering scalable and cost-effective services; however, it faces significant challenges related to security and privacy. This study presents a systematic review of existing research on cloud computing threats and mitigation techniques using the PRISMA methodology. A total of 35 relevant articles were collected and analyzed to identify the major challenges affecting cloud environments and the solutions proposed in the literature. The review reveals that security and privacy issues represent the most critical challenges in cloud computing, with various types of cyberattacks targeting cloud infrastructures. Among these threats, Distributed Denial of Service (DDoS) attacks are the most frequently discussed and are considered the most severe due to their impact on service availability and performance. The findings highlight the urgent need for robust security mechanisms and effective countermeasures to mitigate DDoS attacks and enhance the overall security of cloud computing systems.

Keywords: Cyber security, Threats, Cloud Computing, and DDoS attacks, PRISMA methodology.

1. Introduction

One of the basic concepts that organizations should pay attention to is risk management, as it is very important and necessary for decision-making about the risk that may happen. Decisions must be accurate and made depending on the risk, and its level. In most parts of the world, it is used by IT managers [1]. This research is related to risk management and analysis, some define risk analysis as looking at the outcome of an event, but the origin is that risk analysis is a process that seeks to answer specific questions as to what might happen and what are the consequences and what is the probability [2], It was also defined as an analysis to identify and assess risks of systematic way [1]. This study analyzes information about cloud computing that are related and relevant to risk management, Cloud computing is the ability to jointly access computing resources and shared content over the Internet from anywhere as google drive. Computing has become popular due to the boom of mobile devices and the spread of Internet access. Some of the uses of cloud computing are that it allows sharing of storage, memory, and processing power as well as provides access to applications and services from any device from anywhere. [3] This project will talk about cloud computing and will contain analysis data of studies. It analyzes and document this study's analysis.

Cloud computing is one of the most important subjects in this vision, all people used it to can access their information anywhere and anytime they want [3] because they put their sensitive data and information in it. If any threats exist that will be a risk may affect in cloud provider's reputation, and profit. Some experts reported that due to the reliance on cloud

computing, some concerns have arisen, especially in matters of privacy and data, and that business operations that depend on computing services may be disrupted [3].

As mentioned in the background the cloud includes information in its storage and memory, this information must be secret because this is sensitive data to customers, and will be a big problem when this data is disclosed to the public. Vulnerability is the ability to expose systems to a specific risk [4], to that analysis, the vulnerability is important to make the cloud safe for customers and companies and its reputations. As we say in motivation, the problem in cloud computing is growing and making the risk available. To sustain trust in the company and business sustainability, it is important to take care of cloud computing. [5]. It is also rapidly evolving and the potential for threats is very high due to data sharing. On cloud computing the thread is being in several places, some in data, application, and infrastructure. [6] The top threat in Cloud Computing:

- DDOS attack: This attack is carried out by the malicious user to damage the services and resources used by the legitimate user of cloud computing [7].
- Masquerade: Many threats are associated with masquerading as the attacker's use of cloud-related resources [8].
- SQL: is launched by entering malicious characters into the input fields of web
- Applications resulting in a modified SQL query [9].

This research will cover case studies about cloud computing and its threat and challenges and will read them and analyze the knowledge to get many items from these studies. These items are the threat or challenge of the goal of articles, the problems that see it, and the methodology and result of each one.

2. Research methodology

The method that has been traced to select the papers was the PARSIMA method, to collect articles that related to the title. This review was carried out to determine the appropriate articles on the borders of four stages: identification, scanning, eligibility, and inclusion. The collection of the articles was initially based on the research term formulated as (Cloud or Cloud Computing) and (Cloud challenges or Cloud computing challenges or clouds threats) and (Attacks or Threats) and (Cloud Computing security) and (Cloud threat analysis or Cloud challenges analysis), the number of collected articles from doodle scholar and digital Saudi library are 69 that in 2018 – 2022. There are many reasons to remove articles from the list, some of them were not related to cyber security scope, related to the development of the cloud, analysis of the customer reviews, and some focus in implement the cloud. In identification there are 69 articles were selected from different databases, and the duplication was removed, the remainder is 64. In scanning the articles that have been read and removing what is not closely related, 10 articles are removed. And after eligibility 19 articles have been removed. In the last 30 articles that are taken. Divided into 4 of them quantities articles and 26 are qualitative.

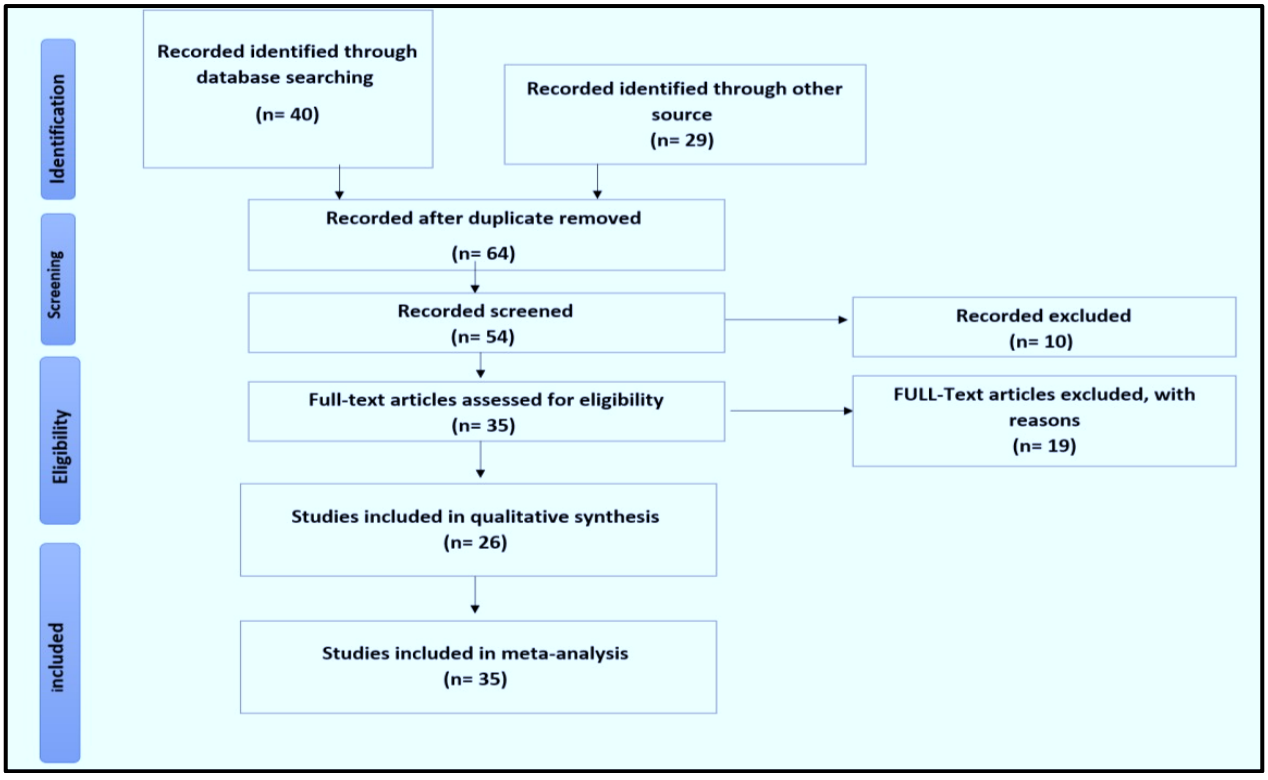

***Figure 1**, Diagram PRISMA Literature Review*

3. Related Works

To study and collect information about threats to cloud computing, relevant studies were collected and read to extract important information. Natalya Bromall, Sushma Mishra, Peter Draus, and John Stewart [10], aimed to known why have to determine the best cloud computing to their information. Companies resort to the cloud in order to solve some of the challenges facing information technology, one of the reasons for which the cloud is taken is that the cloud supply is more flexible and scalable, and also be low in costs, including maintenance. Turki ALQarni and Ahmed Barnawi [11], Aimed to analyse the factors of the cloud computing and present a framework, this research analyzed the previous literature to determine the factors that affect dependence on the cloud, and based on these factors, a cloud framework has been proposed that can be a guide for any organization to build a checklist or to identify the main challenges that affect in the cloud computing. Tong Kong,Liming Wang,Duohe Ma,Zhen Xu, Qian Yang and Kai Chen [12], Aimed to provide a strategies to protect the cloud against the attacks, The proposed strategy significantly reduces co-residence, has a minimal impact on workload and system performance, as well as scalability at scale.

Another study by Yoshita Sharma, Himanshu Gupta and Sunil Kumar Khatri [13], Aimed to explain the importance of the privacy in cloud computing, Companies are using cloud computing as a medium to save data, because of the fear of cloud computing from attacks, especially the DDoS attack, and the fear of data theft, so they proposed a model based on encryption. Haralambos Mouratidis, Shaun Shei and Aidan Delaney[14], Aimed to analyze the security requirements of the computing infrastructure, Due to the lack of developers in the field, the work sought to close gaps by providing its modeling language and set of techniques. S. Logesswari, S. Jayanthi, D. KalaiSelvi, S. Muthusundari and V. Aswin [15], Aimed to study the challenges that faces the cloud computing, the different security threats that get every year have been reviewed and solutions that are applied to some attacks have been limited. Ahmed Bakr. Abd El-Aziz, and Hesham A. Hefny[16], Aimed to mitigate the DDOS attack and the challenges that the cloud computing faces, It has provided a survey of DDOS attacks and techniques to mitigate them. Nailah Afshan[17], Aimed to discover the threats and vulnerability that are related to the cloud computing, It is a rapidly developing technology and is always adopted by companies, they must have a good understanding of the threats and weaknesses in order to be able to get rid of them and reduce the risk resulting from them.

Abdul Raoof Wani, Q.P. Rana, U. Saxena and Nitin Pandey [7], Aimed to detect and resolve the threats problems, Machine learning worked on a set of data and showed accurate results and very high performance, as it can detect the threat. Anupama Mishra and Neena Gupta [18], Aimed to checking the system against the vulnerability and DDOS attack, A large amount of security technologies have been discovered, but some technologies are serious, and some are ineffective in cloud computing. This paper presents a test of cloud computing security technologies. Omar Alia, Anup Shresthab, Akemi Chatfieldc and Peter Murray [19], aimed to discover and determined the factors that related to security and fixing them, in this paper, four main components of the cloud computing requirements framework are proposed: data security, risk assessment, legal requirements, and compliance. This research provides support for understanding these factors in measuring cloud computing security within organizations and government agencies, not only in the local governments. Rubens Matos, Jamilson Dantas, Eltton Araujo and Paulo Maciel [20], Aimed to detection the bottleneck in cloud computing, This paper proposed an approach to detect performance bottlenecks facing cloud computing and this approach uses hierarchical models to deal with the system, a method for sensitivity analysis of the system is developed.

In addition, Jing Zhan, Xudong, Jin Han, Yaqi Gao, Xiaoqing Xia and Qian Zhang [21]. Aimed to provide tools to protect the cloud computing from attacks, in this paper, a model is proposed that can detect attacks with low overheads, this model can make balnce between the network size, policy, and increased number of attacks. Martin Lněnička and Jan Čapek [22], Aimed to testing the security in cloud, The paper has reviewed previous relevant research papers, and the case study and its testing may provide important insight into the ways in which risks, and safety issues are assessed. Mohammed Farsia, Munwar Alib, Reehan Ali Shahc, Asif Ali Wagand and Radwan Kharabsheh [23], Aimed to ensure the data kept security in cloud computing, a comprehensive literature review was conducted on threats to cloud computing and security technologies. Yonggui Guo, Ibrahim Mohamed, Omar Abou-Sayed and Ahmed Abou-Sayed [24], Aimed to analyze the challenges of accessing data and the limitations of computing, the best way to take advantage of cloud computing technology is web-based applications, and it supports remote monitoring and can be applied to other field operations. Alin Zamfiroiu, Ionut Petre and Radu Boncea [25], Aimed to analysis the vulnerability of the cloud computing, the vulnerabilities of cloud computing solutions that give all three models of cloud computing have been analyzed. Rajat Saxena and Somnath Dey [26], Aimed to mitigate and prevent the DDOS attack, this paper, the approach to detecting and preventing DDoS attacks was presented, it was introduced by introducing special prevention standards, it helps to ensure security, the paper also dealt with the issue of IP spoofing.

Anupama Mishra, Neena Gupta and B.B Gupta [27], Aimed to mitigate the DDOS attack, in this paper the methodology used by expelling the attack rules and dropping of the requests from the attack. Neha Agrawal and Shashikala Tapaswi [28], Aimed to provide the defense against the DDOS attack, the methodology used in this research can detect and mitigate DDoS attacks in the cloud-based SDN environment very effectively, and the approach has been validated with the help of appropriate test-based experiments. Kriti Bhushan and B. Gupta [29], Aimed to detect the DDOS attacks, In DDoS attacks, the number of hits to the rule is very high compared to the number of times the flow without hybrids, so a method was proposed to calculate the distance of the information to be able to differentiate from offensive and non-offensive attacks. Hisham A. Kholidy [30], Aimed to detect the masquerade attack in the cloud, to link natural user behavior in cloud computing to distinguish between natural behavior and attack behavior, three correlation models were evaluated and compared with the results of their experience. Hisham A. Kholidy [31], Aimed to detecting the masquerade in cloud computing, because the detection of masquerade attacks is a difficult task in cloud computing, detection strategies must be linked from more than one source. Dharitri Tripathy, Rudrarajsinh Gohil, and Talal Halabi [32], aimed to be sure about the machine learning to detect the SQL injection, Machine learning has a high place and potential in cybersecurity, as most of the classifiers in it are characterized by very high accuracy in results. Gopal Singh Kushwah and Syed Taqi Ali [33], Aimed to detection the DDOS attack, a framework has been presented to detect these attacks, and this framework is characterized by very high accuracy, and has been tested on it. Hesham Abusaimeh [34], Aimed to detection and prevent the happened of DDOS attacks, the paper discussed the various types of DDoS attacks targeting resources in cloud computing, and suggested preventive measures against these malicious attacks by preventing, detecting or reducing the risks from them. Fursan Thabita, Prof.Sharaf Alhomdyc, Abdulrazzaq H. A. Al-Ahdalc and Prof. Dr. Sudhir Jagtap [35], Aimed to be sure from the component of the cloud computing to be safe for security issues, it has been attempted to present the various problems and challenges facing cloud computing and impeding its adoption, part of the reason to search for these is to understand the security flaws for cloud computing infrastructure, the proposed model discussed the classification of threats. Jin Xiao and john Rofrando [36], Aimed to managing the vulnerability that may be in cloud, the paper traced the weakness resulting in the cloud computing application. In addition, it proposed a model for tracking the availability of services. Sharad Dixit, Karuna P. Joshi and Seung Geol Choi [37], Aimed to protect the cloud computing in medical scope if safety, to address the flaws that occur in business related to the same field, a framework is proposed in this paper aimed at secure encryption and user authentication for privacy and security in cloud computing in a multi-authority environment.

Gopal Singh Kushwah and Virender Ranga [38], Aimed to defensing against attacks in the cloud, the improved version of Extreme Adaptive Evolutionary Machine Learning has been developed, considering it to be the best strategy for detecting DDOS attacks. Walid I. Khedr, Khalid M. Hosny, Marwa M. Khashaba and Fathy A. Amer[39], Aimed to Providing secure facilities for mobile phone users, to ensure secure facilities for cloud computing on mobile devices, an authentication protocol based on encryption has been proposed, which provides protection against common attacks. Steve Jones 1 & Zahir Irani & Uthayasankar Sivarajah & Peter E. D. Love [40], Aimed to implement the cloud in practical framework, Yunusa Simpa Abdulsalam and Mustapha Hedabou [41], Aimed to assessment the security and privacy without intrusion in security of cloud, it's models not focusing onthe continued privacy of the user may cause inflexibility and management control of the protocols and security that keep users safe for cloud computing. Pinki Sharma and Jyotsna Sengupta[42], Aimed to detection the attacks, Intrusions that could cause harm to the confidentiality, integrity and availability of services and products in cloud computing have been described. Intrusion detection system has been focused on to secure the computing environment. Ramzy Hamed Alhazmi & Uthman M. Ageeli[43], Aimet to learn about cloud in Saudi airlines, The paper indicated that cloud computing has helped a lot in saving data and helped provide advantages to its users, but nevertheless, it faces great challenges, the most important of which is the problem of internet outage, security and privacy protection, and this makes cloud computing less used in Saudi Airlines, and also may be the reason for the modernity of this Technical and the lack of trained personnel on this mechanism. Table 1 shows the literature analyzes of previous studies related to cloud computing.

Table 1. Literature analyses of previous studies related to cloud computing.

No	Title of project	Authors	Objective	Problem statement	Type of article	The methodology	Finding	Contributions
1	A CASE STUDY-BASED ANALYSIS OF INNOVATIVE CLOUD TECHNOLOGIES IMPLEMENTATION: CHALLENGES, TOOLS, AND BENEFITS OF AMAZON AWS	Natalya Bromall, Sushma Mishra, Peter Drau, and John Stewart [10].	Find out why you prefer AWS cloud provider over other cloud providers.	Organizations face many challenges when they decide to use a cloud computing provider, one of the most important of these challenges is that the ability to develop, flexibility and speed are less than required, in addition to the fact that the cost is high and other challenges.	Conferences	Turban's model	The most challenges are in responding to difficult situations, the lack of infrastructure for technology, and flexibility in increasing demand, and this also includes the lack of transparency and the inability to find solutions that lead to storing more data. Among the tools that made it so popular and reliable are EC2, and S3, as well as cloud organization	The study provided answers to the questions: - What are the business challenges/issues that make organizations seek cloud services such as AWS? - What are the common tools that are being deployed from AWS to meet business requirements? - What are the benefits of using AWS for businesses migrating to a cloud environment?

							tools and networking tools.	
2	A Cloud adoption framework: assessing the factors and determinants of adopting cloud computing technology	Turki ALQarni and Ahmed Barnawi [11].	Analyze the factors that affect the adoption of cloud computing and present a proposal for a framework.	The lack of a standard framework for the adoption of cloud computing, and the lack of knowledge about it.	Academic Journal	Use more than one method has been used, and previous research was reviewed to determine the factors that affect the cloud. To validate the form, TOE and DOI was used. The quantitative methodology was used as a validation tool for the framework.	A new framework has been proposed that can serve as a guideline for any organization, either to create a verification key or to identify the main challenges facing computing. The framework also clarifies the best factors for the technology and is evaluated before moving to the cloud platform.	Among the contributions made by this paper are virtualization and workload assessment, local data storage, and resilience.
3	A Secure Container Deployment Strategy by Genetic Algorithm to Defend against Co- Resident Attacks in Cloud Computing.	Tong Kong,Liming Wang,Duohe Ma,Zhen Xu, Qian Yang and Kai Chen [12].	Provide a secure strategy to defend against common attacks.	Lack of sharing means that the isolation is incomplete.	Conferences.	Secure Container Deployment Strategy (SecCDS).	The strategy significantly reduces the co- location of the cloud with very little impact on the workload and has been shown to be scalable over a wide range in addition to that, it is possible to modify the security requirements	The paper contributes to the formalization of the space formed, creating two scales to describe publication and co- residence, And the deployment strategy is developed by GA.
4	A Security Model for the Enhancement of Data Privacy in Cloud Computing	Yoshita Sharma, Himanshu Gupta and Sunil Kumar Khatri [13].	Explain the importance of data privacy	The data be more face to attackers and stealing data because almost of companies use cloud computing	Conferences.	Encryption technique.	The AES algorithm has been proven to be 6 times faster than the DES	A comparison of the encryption algorithm between DES and AES.

				to save data.			algorithm	
5	A security requirement modelling language for cloud computing environments.	Haralambos Mouratidis, Shaun Shei and Aidan Delaney[14].	Analysis of security requirements for cloud infrastructure..	Lack of support for developers to provide the security needs of the systems.	Academic journal.	Analysis techniques so that threats are analyzed so that the developer can determine the impact on computing, and then determine the costs of implementing security measures.	. A modeling language was defined to take the concepts of cloud computing, and through our work, it was also proven that the language is able to represent every abstraction and a very accurate perspective. The responsibilities towards the cloud have been determined in the framework of the requirements.	It introduces a new language for security modeling and a set of original analysis techniques, for security analysis of computing data
6	A study on cloud computing challenges and its mitigations	S. Logesswari, S. Jayanthi, D. KalaiSelvi, S. Muthusundari and V. Aswin [15].	Study the cloud computing challenges	Cloud computing is exposed to multiple attacks	Academic journal	SDN and CC	VM attacks are resolved, and the best procedures and possible solutions for mitigating attacks in a cloud computing environment are discussed.	Discussing and resolving some types of attacks, such as sharing resources and victims
7	A Survey on Mitigation Techniques against DdoS Attacks on Cloud Computing Architecture	Ahmed Bakr. Abd El-Aziz, and Hesham A. Hefny[16].	Identify challenges and techniques for mitigating DDOS in the cloud.	The danger of attacking information in cloud computing.	Review articles.	The survey, Scan information for mitigation and protection against attacks.	The basic form of DDOS attack in the cloud has been revealed and multi-tiered solutions designed specifically for cloud computing are enumerated.	This work provided a survey of DDOS attacks, and available mitigation techniques.
8	Analysis and Assessment of the Vulnerabilities in Cloud Computing	Nailah Afshan[17].	Discover threats and vulnerabilities related to cloud computing.	As against scalability, usability, and security in computing vulnerabilities and threats emerge.	Review articles.	Collect and analyze information	The following points are discussed and analyzed: core Cloud Technology Vulnerabilities, Essential Cloud Characteristic Vulnerabilities, Defects in Known Security Controls, and Prevalent Vulnerabilities in State-of-the-Art Cloud Offerings.	The paper will focus on gathering information about threats and vulnerabilities in cloud computing

9	Analysis and Detection of DdoS Attacks on Cloud Computing Environment using Machine Learning Techniques	Abdul Raoof Wani, Q.P. Rana, U. Saxena and Nitin Pandey [7].	Detect and resolve the attack problem.	Threats related to challenges of cloud computing and authentication and computing issuing.	Conferences.	Machine learning algorithms Support Vector Machine, Random Forest, and Naïve Bayes.	The best performing of the three models was SVM.	The work contributed to presenting the result of incorporating into various machine learning algorithms
10	Analysis of Cloud Computing Vulnerability against DDOS	Anupama Mishra and Neena Gupta [18].	Check for system vulnerabilitie s due to DDOS.	Cloud computing environment exposed to DDOS attacks.	Conferences.	Scan of previous articles and show the techniques used, an exhaustive review of existing defense mechanisms of DDoS.	Most attacks against cloud computing have been identified, and it is stated that it is difficult to develop a mechanism for all attacks.	Discuss the impact of DDOS attacks on cloud computing.
11	Assessing information security risks in the cloud: A case study of Australian local government authorities.	Omar Alia, Anup Shresthab, Akemi Chatfieldc and Peter Murray [19].	Identify and troubleshoot factors associated with security requirements.	Safety Concerns.	Academic journal.	Interviews.	This study helped in the planning and implementation of cloud services to achieve the strategic goals.	It contributed to explaining the extent to which commercial and technical requirements affected the hypothesis.
12	Bottleneck Detection in Cloud Computing Performance and Dependability: Sensitivity Rankings for Hierarchical Models.	Rubens Matos, Jamilson Dantas, Eltton Araujo and Paulo Maciel [20].	Bottleneck Detection in Cloud Computing .	Bottleneck attacks.	Academic journal.	The hierarchical heterogeneo us modeling approach	This approach made it possible to work with a high- level analysis in addition to practical details. This analysis indicated obstacles during the response and indicated two services, namely, the research service and the service of similar artists.	Contributed to the implementation of the approach to discover performance and availability bottlenecks in cloud computing systems.
13	CIADL: cloud insider attack detector and locator on multi-tenant network isolation: an OpenStack case study	Jing Zhan, Xudong, Jin Han, Yaqi Gao, Xiaoqing Xia and Qian Zhang [21].	Provide a tool to detect the attack.	Internal attack threats.	Academic journal.	Cloud insider attack detector and locator (CIADL) on multi-tenant network isolation for OpenStack platform.	Prove that the method can detect all violations and locate the attacks.	The first internal threat model and built a detection and method for the model-based attack, contributed to locating the threat with accurate details.

14	Classification and Evaluation of Cloud-Based Testing Tools: The Case Study of Web Applications' Security Testing.	Martin Lněnička and Jan Čapek [22].	Scanning the published results obtained, is also intended for security testing.	Challenges of cloud computing.	Academic journal.	Cloud-based testing methodology.	Cloud-based testing can produce different results, so it is not accurate, and this is due to its novelty.	Contributed to reviewing and discussing benefits and risks, providing a systematic evaluation and classification of strategies, and contributed to defining a methodology to help create a complex guide for cloud stakeholders, studying cloud testing tools
15	Cloud computing and data security threats taxonomy: A review	Mohammed Farsia, Munwar Alib, Reehan Ali Shahc , Asif Ali Wagand and Radwan Kharabsheh [23].	Ensure data security in the cloud.	The cloud faces a number of problems such as trust, efficiency, and risk management, and one of the main challenges is data security.	Review.	Review the security techniques in cloud such as encryption and other.	A comprehensive and critical literature review was conducted on security threats as well as cloud-related models and security-related technologies for the cloud.	The paper contributed to discovering current data security solutions.
16	Cloud computing and web application-based remote real-time monitoring and data analysis: slurry injection case study, Onshore USA.	Yonggui Guo, Ibrahim Mohamed, Omar Abou-Sayed and Ahmed Abou-Sayed [24].	Challenges is access to data and limitation that obtained to cloud computing data analysis	Monitoring the injections in web site, the web site provides data of injections stored in database of cloud.	Review articles.	Monitoring and analysis.	Through the injection monitoring web application, it is recognized that web-based applications are the ideal way to enhance field efficiency.	The paper points to a new application to access and analyze data for injection on a web-enabled device.
17	Cloud Computing Vulnerabilities Analysis	Alin Zamfiroiu, Ionut Petre and Radu Boncea [25].	Analysis the amount of vulnerability.	The presence of security vulnerabilities that affect the security of cloud computing technologies.	Review articles.	Analysis the models of cloud	The weaknesses of the solutions used were identified and analyzed so that there is no danger of the existence of these gaps, there are some solutions that do not have many weaknesses, and this does not mean that the solution is very secure.	Analysis of common weaknesses in computing solutions that cover all three models, Saas, PaaS, and IaaS

18	DdoS attack prevention using collaborative approach for cloud computing.	Rajat Saxena and Somnath Dey [26].	DDOS attack prevention and mitigation.	The difficulty for cloud users to identify the source of a DDOS attack	Academic journal	Third party auditor (TPA).	Easy DDOS prevention in computing environment is by cloud warrior. Helps to ensure security greatly. This approach shows a significant improvement in DDOS detection and prevention in the cloud.	A large number of DDOS attacks in the cloud were scanned and filtered based on the infrastructure, and the tools used in this attack were surveyed, with a study available to mitigate and prevent this attack
19	Defense mechanisms against DdoS attack based on entropy in SDN-cloud using POX controller.	Anupama Mishra, Neena Gupta and B.B Gupta[27].	Mitigation the DDOS attack.	With many models that mitigate the attack, there are different security threats.	Original paper.	Defense mechanisms	When explore the DDOS attack, the method will expel the attack and drop the subsequence from the DDOS attacks.	The paper contributed to the proposal of a method with a high detection rate, a low false rate, and the ability to mitigate the attack
20	Defense Mechanisms against DdoS Attacks in a Cloud Computing Environment: State-of-the- Art and Research Challenges.	Neha Agrawal and Shashikala Tapaswi [28].	Defense against DDOS attacks.	Low-rate DDOS attacks are hard to detect.	Review articles.	Survey	Strategies to reduce, prevent, and detect the attack are discussed.	Contributed to the consideration of all variants of DDOS attacks in a cloud environment. It also contributed to the discussion of many strategies for practicing defense for all types of DDOS attack, and also provides a comparative analysis of defense practices.
21	Detecting DdoS Attack using Software Defined Network (SDN) in Cloud Computing Environment	Kriti Bhushan and B. Gupta [29].	Detect the DDOS attacks.	Threats in cloud computing attacks has been growed.	Conferences.	SDN's flow table.	We have proposed a method for calculating the information distance to distinguish between offensive and non-offensive streams, once an attack is detected, the method removes it.	Contributed to the production of an approach to differentiate between attack and natural transmission

22	Detecting impersonation attacks in cloud computing environments using a centric user profiling approach.	Hisham A. Kholidy [30].	Detect masquerade attack.	Identity impersonation is one of the most dangerous attacks in cloud computing.	Academic journal.	Three approaches were used, the first one analyzes the style of system calls, the second analyzes the style of data, the third method combines the two methods using a neural network.	We extend DDSGA to define subsystems that detect masquerading as attacks through the chain of calls and data.	The paper contributed to clarifying the combination of call and data analysis, and the discovery of accurate results about the detection of attacks.
23	Correlation-based sequence alignment models for detecting masquerades in cloud computing.	Hisham A. Kholidy [31].	Detecting the masquerade.	Masquerade attacks are among the most dangerous attacks faced by cloud computing.	Research articles.	Correlating the user's behaviors in several virtual machines.	The output of the neural network model has the best accuracy depending on the data.	Contributed to addressing some problems in cloud computing and also in developing a dynamic approach to determine the characteristics of the user to be compared in virtual machines, developed a neural network model and contributed to the tuning and testing of the proposed approaches.
24	Detecting SQL Injection Attacks in Cloud SaaS using Machine Learning.	Dharitri Tripathy, Rudrarajsinh Gohil, and Talal Halabi.[32]	Validation of machine learning capabilities for SQL injection detection.	Security Challenges and SQL injection attack that is one of the most dangerous threats.	Conferences.	Classifiers trained on different malicious and benign payloads, the application of machine learning.	Most of the classifiers had an accuracy of 98%, and there is a classifier called the random forest outperforms all classifiers and achieves an accuracy rate of 99.8%, and one of the best features that were found is the length of the entry, the number of characters for numbering, as well as the number of bytes.	The paper compares different machine learning models for SQL attack detection.
25	Distributed denial of service attacks detection in cloud computing using extreme learning machine	Gopal Singh Kushwah and Syed Taqi Ali [33].	DDOS attacks detection.	Cloud computing suffers from various security risks, the most important of which is DDOS.	Academic journal	model based on extreme learning machine (ELM).	Experiments were conducted for 20 times for each of the binary classification and the multi-class classification, in the binary classification the	Contributed to the development of the DDOS-related attack detection model based on ELM. And experiments were conducted on the

							accuracy was 98.76%, while in the multi-class classification the accuracy was 98.73%.	developed model.
26	Distributed Denial of Service Attacks in Cloud Computing.	Hesham Abusaimeh [34].	Detect and prevent attacks for DDOS.	Because of the increase in expansion, the use of cloud computing has increased attacks, and one of these attacks is the DDOS attack.	Academic journal.	Comprehensive search on previous papers and surveys.	This paper discusses most types of DDOS attacks and presents the procedures that are followed to take the most used defense to prevent and detect an attack.	The paper provided information about the DDOS attack, and an attempt was made to distinguish between the types of this attack and explore its classifications.
27	Exploration of Security Challenges in Cloud Computing: Issues, Threats, and Attacks with their Alleviating Techniques.	Fursan Thabita, Prof.Sharaf Alhomdyc, Abdulrazzaq H. A. Al-Ahdalc and Prof. Dr. Sudhir Jagtap [35].	Check components for cloud computing as well as security issues.	Challenges of privacy and security.	Academic journal	Searching and analysis.	The paper reviewed computing security challenges and threats and reinforced countermeasures against them.	The paper contributed to the definition of different types of security threats, in addition to security concepts and techniques to mitigate attacks, and also contributed to giving recommendations for the future
28	Managing vulnerability in a cloud Native world with Bluefix.	Jin Xiao and john Rofrando [36].	Managing the vulnerability.	Challenges in cloud.	Research	Bluefix	Designing, discovering and creating the design process needed to address problems in the cloud world, and Bluefix was introduced as a vulnerability management solution in Devop's cloud environment.	The paper contributed to testing how security vulnerabilities are managed by the cloud and identifying control points.
29	Multi Authority Access Control in a Cloud I System with MA-ABE.	Sharad Dixit, Karuna P. Joshi and Seung Geol Choi[37].	Privacy of medical data in cloud.	Create a single point attack by creating a choke point or to share data.	Conferences.	Access framework with secure encrypted access control mechanism	A secure access control mechanism has been implemented to authenticate the user and the data encryption module to ensure protection, security, and privacy when transferring data.	The paper contributed to the proposal of a new framework that includes an encrypted and secure access control mechanism
30	Optimized extreme learning machine for detecting DdoS attacks in cloud computing.	Gopal Singh Kushwah and Virender Ranga[38].	Defending against these attacks.	DDOS attack is a security threat that is dangerous to cloud computing, that effect on the availability of services.	Academic journal	detection system based on an improved Self-adaptive evolutionary extreme learning machine (SaE-	The performance comparison of this developed technology with other based systems shows that this developed system works	An improved version of the machine learning has been developed called the Cross-Adaptive Extreme Self-Adaptive

						ELM).	better than other systems.	Learning Machine which is an adaptive model capable of adapting the best strategies, crossover rate, and crossover factor. It can also select the appropriate number of hidden neurons automatically. These features improve the ability to learn.
31	Prediction-based secured handover authentication for mobile cloud computing.	Walid I. Khedr, Khalid M. Hosny, Marwa M. Khashaba and Fathy A. Amer[39].	Providing secure facilities for mobile phone users.	Security and authentication are a big challenge.	Review articles.	Protocol that depends on the point of view of discovery and selection of the access network.	The protocol proposed in this paper has less burden than other protocols that rely on encryption and certificates. The proposed protocol provides advantages such as protecting against a number of common attacks such as man-in-the middle attack and replay attack, providing mutual authentication, key confidentiality, robust security, and efficiency and other of attacks. Using the schema for prediction solves the problem of creating a secure channel in authenticating untrusted networks. The proposed new protocol is a comprehensive solution for MCC delivery.	It contributed to the prediction of the delivery method to take care before the delivery occurs to reduce the risk to the quality of service and also contributed to the adoption of the authentication protocol used on symmetric encryption, and it also uses the prediction scheme to improve the quality of performance and accuracy of the proposed authentication protocol.
32	Risks and rewards of cloud computing in the UK public sector: A reflection on three Organisational case studies	Steve Jones 1 & Zahir Irani & Uthayasankar Sivarajah & Peter E. D. Love [40].	Implementation of cloud computing from a practical framework.	Potential risks when implementing technologies for the cloud	Academic journal	The methodology be in research design, data collection and data analysis.	It was widely disseminated at the level of users and employees.	Cloud computing deployment complements and improves approaches to IT implementation, brings out what's good for both the IT and research community, and allows for change through the enhancement of risk ratings

								for the cloud.
33	Security and Privacy in Cloud Computing: Technical Review	Yunusa Simpa Abdulsalam and Mustapha Hedabou [41].	Introduce security and privacy issues without interfering with cloud security.	Safety Concerns	Review.	STRIDE	The study showed that most businesses do not have a meeting on the design and implementation of cloud security schemes, and cloud models do not focus on user privacy, which confirms the lack of flexibility and control over security and privacy protocols.	Contributed to the different business present with a view to adapting and mitigating recurring future threats, while explaining why their models had not worked before and how they led to opposition to security in the cloud.
34	Survey of intrusion detection techniques and architectures in cloud computing.	Pinki Sharma and Jyotsna Sengupta[42].	Detection the attacks.	Because cloud computing is common, it is always vulnerable to various attacks	Survey	Intrusion detection systems (IDS).	Noted that it is important to integrate different detection mechanisms to achieve a higher level of security	Contributed to providing a comprehensive survey of intruder detection system structures assigned to cloud computing to deal with security.
35	The Reality of Cloud Computing at Saudi Airlines Information Center: A Case Study	Ramzy Hamed Alhazmi & Uthman M. Ageeli[43].	It aims to learn about cloud computing in Saudi Airlines	The most important problems are the user's fear of data privacy and the companions' need for network architecture.	Case study.	Descriptive analytical approach	The lack of cloud computing in the air plans is largely due to the lack of trainers and it is a very modern technology.	Contributed to understanding the extent of interest in the application of cloud computing and understanding the reasons that prompted the use of cloud computing, while realizing the advantages of cloud computing from the point of view of employees and realizing the obstacles facing the application of computing

4. Analysis and Results

Cloud computing is included in most companies and organizations. Cloud computing has a history full of achievements but also eventful [10]. The challenges that occur to cloud computing are mostly related to security and privacy problems, and as for the attacks, they have prompted many attacks, and the most important and most exposed to computing are DDOS and challenges on authentication, cost, safety, and other several things, as it is shown in Figure2.

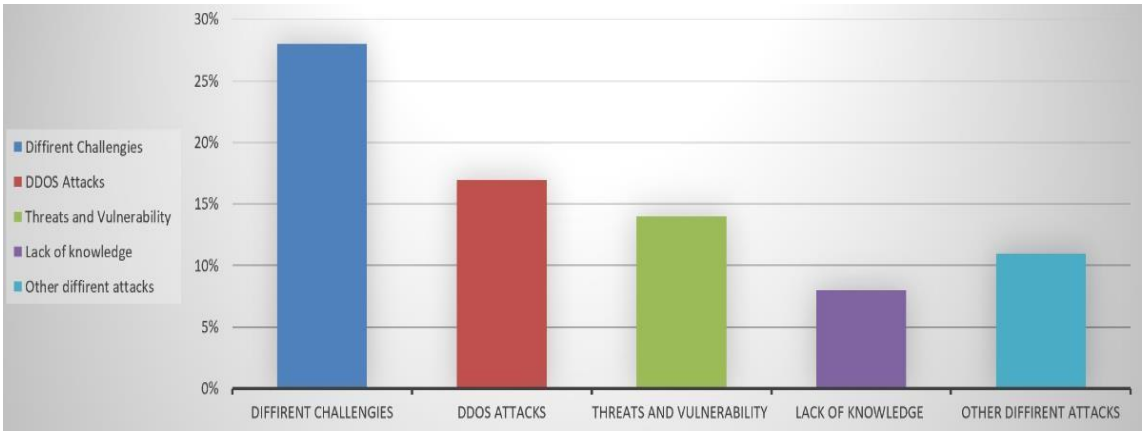

Figure 2. Problem statement analysis.

The findings indicated that many of the articles mentioned that DDoS attacks and included their types, while neglecting to include other attacks, the method of mitigation and prevention of the threat was by the model based on machine learning, comparing between articles, SDN's flow table, Third-party auditor (TPA), and other. For masquerade control it by correlating the user's behaviors in several virtual machines and analyzing the style of system calls, analyzing the style of data, and combining the analysis of data and system using a neural network. Many methods have been dealt with in these articles, including encryption, machine learning, the use of security and privacy protocols, and other effective methods that have brought the benefit of computing, the analysis of the method that outcomes from this research are shown in Figure 3.

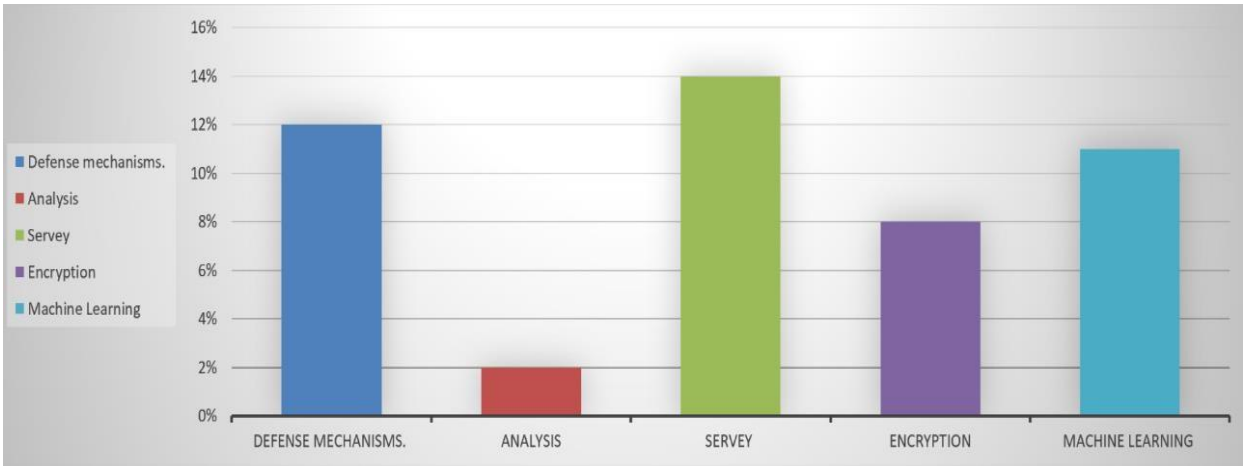

Figure 3. Method analysis.

5. Conclusion

By PRISMA methodology, the articles collected are 35 the collected papers contain information about cloud computing and the challenges that face it and the methods that take it to solve challenges or problems. The main problems that face cloud computing are privacy and security challenges, and the attacks of their different type. By reading the articles and highlighting the major information that wants, one of the more threats cover and talk about it was the DDOS attack and it's considered the most attack that clouds computing face.

References

[1] Amir samami, 2020, Risk management in information technology.
[2] Tom M.Logan, Terje Aven, seth guikema, roger flage, 2021, The Role of Time in Risk and Risk Analysis: Implications for Resilience, Sustainability, and Management.
[3] Skemp, Kerry, MA, Salem, 2022, Cloud Computing.
[4] Tyndall Centre for Climate Change Research, 2006, Vulnerability, risk and adaptation.
[5] Meredith Stein, Vincent Campitelli, and Steven Mezzio, 2020, Managing the Impact of Cloud Computing.
[6] Maniaha, Edi Abdurachman, Ford Lumban Gaol Benfano Soewito, 2019, Survey on Threats and Risks in the Cloud Computing Environment.
[7] Abdul Raoof Wani, Q.P. Rana, U. Saxena and Nitin Pandey, 2019, Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques.
[8] Hisham A. Kholidy, 2019, Correlation-based sequence alignment models for detecting masquerades in cloud computing.
[9] Mamdouh Alenezi, 2020, SQL injection attacks countermeasures assessments.
[10] Natalya Bromall, Sushma Mishra, Peter Draus and John Stewart, A CASE STUDY-BASED ANALYSIS OF INNOVATIVE CLOUD TECHNOLOGIES IMPLEMENTATION: CHALLENGES, TOOLS AND BENEFITS OF AMAZON AWS.
[11] Turki ALQarni and Ahmed Barnawi, 2019, A Cloud adoption framework: assessing the factors and determinants of adoption cloud computing technology.
[12] Tong Kong,Liming Wang,Duohe Ma,Zhen Xu, Qian Yang and Kai Chen, 2019, A Secure Container Deployment Strategy by Genetic Algorithm to Defend against Co-Resident Attacks in Cloud Computing.
[13] Yoshita Sharma, Himanshu Gupta and Sunil Kumar Khatri, 2019, A Security Model for the Enhancement of Data Privacy in Cloud Computing.
[14] Haralambos Mouratidis, Shaun Shei and Aidan Delaney,2020, A security requirement modelling language for cloud computing environments.
[15] S. Logesswari, S. Jayanthi, D. KalaiSelvi, S. Muthusundari and V. Aswin, 2020, A study on cloud computing challenges and its mitigations.
[16] Ahmed Bakr. Abd El-Aziz, and Hesham A. Hefny, 2019, A Survey on Mitigation Techniques against DDoS Attacks on Cloud Computing Architecture.
[17] Nailah Afshan, 2017, Analysis and Assessment of the Vulnerabilities in Cloud Computing.
[18] Anupama Mishra and Neena Gupta, 2019, Analysis of Cloud Computing Vulnerability against DDoS.
[19] Omar Alia, Anup Shresthab, Akemi Chatfieldc and Peter Murray, 2019, Assessing information security risks in the cloud: A case study of Australian local government authorities.
[20] Rubens Matos, Jamilson Dantas, Eltton Araujo and Paulo Maciel, 2019, Bottleneck Detection in Cloud Computing Performance and Dependability: Sensitivity Rankings for Hierarchical Models.
[21] Jing Zhan, Xudong, Jin Han, Yaqi Gao, Xiaoqing Xia and Qian Zhang, 2019, CIADL: cloud insider attack detector and locator on multi-tenant network isolation: an OpenStack case study.
[22] Martin Lněnička and Jan Čapek, 2018, Classification and Evaluation of Cloud- Based Testing Tools: The Case Study of Web Applications' Security Testing.
[23] Mohammed Farsia, Munwar Alib, Reehan Ali Shahc , Asif Ali Wagand and Radwan Kharabsheh, 2019, Cloud computing and data security threats taxonomy: A review.
[24] Yonggui Guo, Ibrahim Mohamed, Omar Abou-Sayed and Ahmed Abou-Sayed, 2019, Cloud computing and web application-based remote real-time monitoring and data analysis: slurry injection case study, Onshore USA.
[25] Alin Zamfiroiu, Ionut Petre and Radu Boncea, 2019, Cloud Computing Vulnerabilities Analysis.
[26] Rajat Saxena and Somnath Dey, 2019, DDoS attack prevention using collaborative approach for cloud computing.
[27] Anupama Mishra, Neena Gupta and B.B Gupta, 2021, Defense mechanisms against DDoS attack based on entropy in SDN-cloud using POX controller.
[28] Neha Agrawal and Shashikala Tapaswi, 2019, Defense Mechanisms against DDoS Attacks in a Cloud Computing Environment: State-of-the-Art and Research Challenges.
[29] Kriti Bhushan and B. Gupta, 2020, Detecting DDoS Attack using Software Defined Network (SDN) in Cloud Computing Environment.
[30] Hisham A. Kholidy, 2021, Detecting impersonation attacks in cloud computing environments using a centric user profiling approach.
[31] Hisham A. Kholidy, 2019, Correlation-based sequence alignment models for detecting masquerades in cloud computing.
[32] Dharitri Tripathy, Rudrarajsinh Gohil, and Talal Halabi, 2020, Detecting SQL Injection Attacks in Cloud SaaS using Machine Learning.
[33] Gopal Singh Kushwah and Syed Taqi Ali, 2019, Distributed denial of service attacks detection in cloud computing using extreme learning machine.
[34] Hesham Abusaimeh, 2020, Distributed Denial of Service Attacks in Cloud Computing.
[35] Fursan Thabita, Prof.Sharaf Alhomdyc, Abdulrazzaq H. A. Al-Ahdalc and Prof. Dr. Sudhir Jagtap, 2020, Exploration of Security Challenges in Cloud Computing: Issues, Threats, and Attacks with their Alleviating Techniques.
[36] Jin Xiao and john Rofrando, 2017, Managing vulnerability in a cloud Native world with Bluefix.
[37] Sharad Dixit, Karuna P. Joshi and Seung Geol Choi, 2019, Multi Authority Access Control in a Cloud EHR System with MA-ABE.

[38] Gopal Singh Kushwah and Virender Ranga, 2021, Optimized extreme learning machine for detecting DDoS attacks in cloud computing.
[39] Walid I. Khedr, Khalid M. Hosny, Marwa M. Khashaba and Fathy A. Amer, 2020, Prediction-based secured handover authentication for mobile cloud computing.
[40] Steve Jones 1 & Zahir Irani 2 & Uthayasankar Sivarajah3 & Peter E. D. Love, 2019, Risks and rewards of cloud computing in the UK public sector: A reflection on three Organisational case studies.
[41] Yunusa Simpa Abdulsalam and Mustapha Hedabou, 2020, Security and Privacy in Cloud Computing: Technical Review.
[42] Pinki Sharma and Jyotsna Sengupta, 2019, Survey of intrusion detection techniques and architectures in cloud computing.
[43] Ramzy Hamed Alhazmi & Uthman M. Ageeli, 2020, The Reality of Cloud Computing at Saudi Airlines Information Center: A Case Study.