Prominent Security Vulnerabilities in Cloud Computing

Alanoud Alquwayzani, Rawabi Aldossri, Mounir Frikha
Dept. of Computer Networks and Communications (CCSIT), King Faisal University, Al Hassa 31982, Saudi Arabia

***Abstract*—This research study examines the significant security vulnerabilities and threats in cloud computing, analyzes their potential consequences for enterprises, and proposes effective solutions for mitigating these vulnerabilities. This paper discusses the increasing significance of cloud security in a time characterized by rapid data expansion and technological progress. The paper examines prevalent vulnerabilities in cloud computing, including cloud misconfigurations, data leakage, shared technology threats, and insider threats. It emphasizes the necessity of adopting a proactive and comprehensive approach to ensure cloud security. The report places significant emphasis on the shared responsibility paradigm, adherence to industry laws, and the dynamic nature of cybersecurity threats. The situation necessitates the cooperation of researchers, cybersecurity professionals, and enterprises to proactively address these difficulties. This partnership aims to provide a thorough manual for organizations aiming to bolster their cloud security measures and safeguard valuable data in an ever-evolving digital landscape.**

***Keywords*—Cloud computing; vulnerabilities; cloud security; cloud misconfigurations; data loss; threats**

I. Introduction

Cloud computing has revolutionized how companies manage data and information technology, offering flexible, on-demand resources that facilitate innovation and collaboration. Through services such as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS), businesses of all sizes can now optimize costs, improve agility, and enhance efficiency. Despite its numerous benefits, cloud computing is not without its challenges, particularly in the realm of security. misconfigurations, improper authentication, and phishing attempts are among the many vulnerabilities that have led to significant data breaches and financial losses for organizations [1]. The financial implications of these security vulnerabilities are stark, with the average cost of a data breach reaching $4.24 million in 2023, the highest in 17 years, according to the International Business Machines (IBM) Corporation. Moreover, breaches in cloud environments have proven to be more costly than traditional on-premises intrusions, underscoring the critical need for robust cloud security measures. This study aims to examine the impact of cloud computing vulnerabilities on organizations and review practical mitigation strategies to enhance cloud security. It seeks to explore the advantages and disadvantages of these solutions, considering security and usability trade-offs. The ultimate goal is to contribute to the cloud security literature and provide insights for practitioners and policymakers on safeguarding valuable data in an increasingly digital world.

The rest of the paper is organized as follows: Section II discusses the selection of papers through the PRISMA methodology, followed by a detailed literature review of related works in Section II. Section III presents cloud computing statistics, highlighting its growth and the paradigm shift in organizations. The methodology, including penetration testing and vulnerability scanning, is outlined in Section IV. The paper concludes with a discussion on future trends and a summary of the findings and recommendations in Section V.

II. Literature Review

A. Selection of Papers by PRISMA

This paper aims to conduct a rigorous Systematic Literature Review (SLR) of the existing literature on prominent security vulnerabilities in cloud computing, guided by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology. PRISMA's transparent, methodological approach ensures an unbiased selection and assessment of the papers, enabling a comprehensive and replicable review. In the first step, the search was conducted in the IEEE Xplore and Google Scholar databases using the querying combination of the following keywords: (Security Vulnerabilities OR Threats) AND Cloud Computing. The literature is restricted to studies published between 2012 and 2023 in English. Google Scholar revealed 8580 papers that discuss security vulnerabilities in cloud computing, specifically focusing on data breaches, unauthorized access, and other security threats. These 8,580 search papers were registered, with 2,000 duplicate papers removed before screening and 4,080 papers excluded for other reasons. Additionally, 29 papers were identified in the IEEE Xplore. Thirteen papers were excluded after screening the title and abstract due to unspecific goals. A total of 157 and 9 papers were assessed for eligibility from the Google Scholar and IEEE Xplore databases, respectively. Finally, after a thorough review and study of these papers, 44 papers were selected from the Google Scholar database and 7 from the IEEE Xplore, making a total of 51 papers selected. This selection process of papers, as conducted by PRISMA, is illustrated in Fig. 1.

B. Related Papers

Cloud computing has a significant role in modern business and individuals' lives. Numerous articles and studies are focused on different literary studies in this field. For instance, a review article written by Alouffi et al. [2] titled "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies" identified seven major security threats to cloud computing services, including data tampering and leakage, intrusion of data, and storage of data. Similarly, the paper identifies blockchain as a partnering technology to address some of the security concerns. Akello et al. in [3] summarized existing security surveys in the domains of cloud, fog, and edge computing. The paper underscores the need for

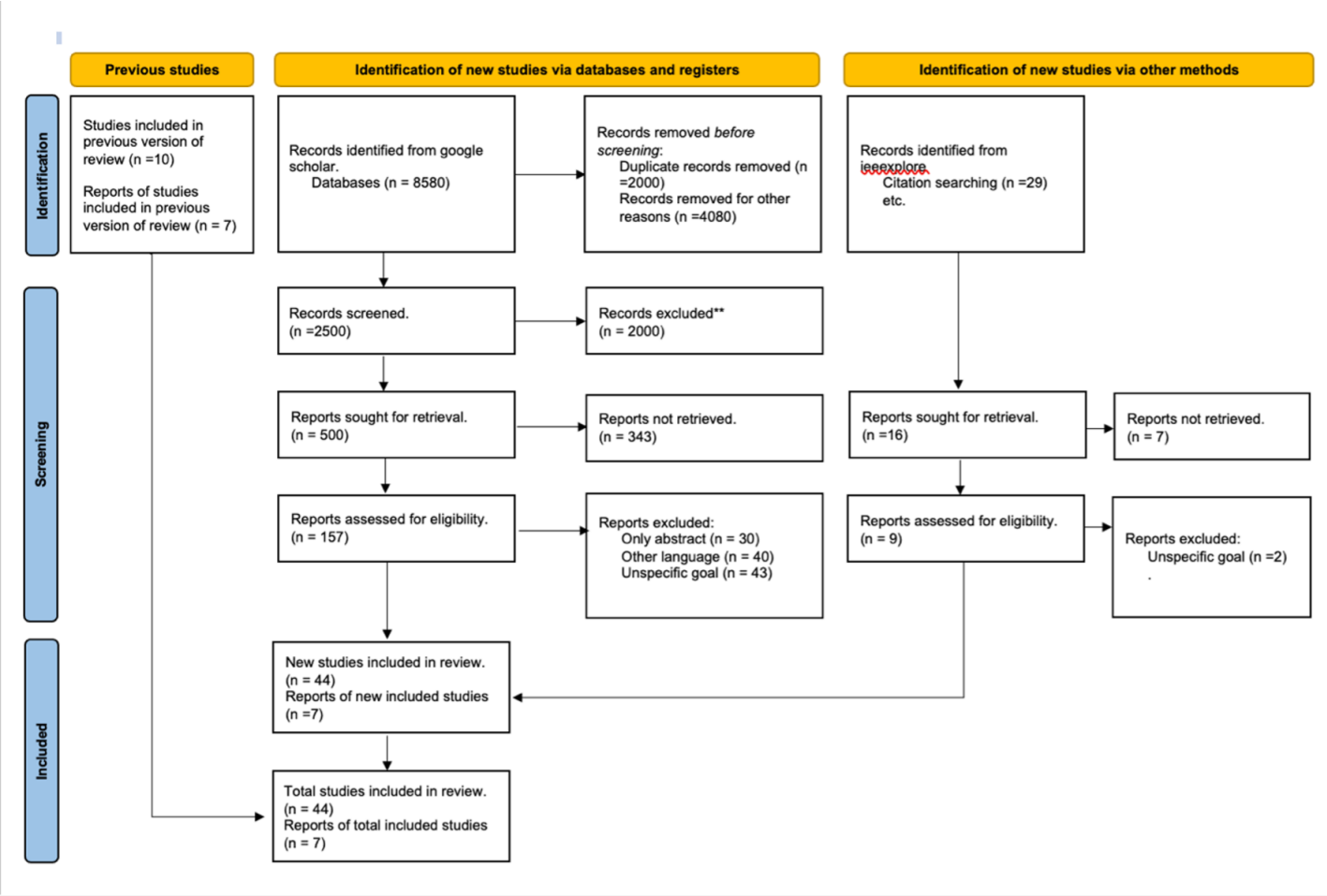

Fig. 1. Selection of papers for literature review using PRISMA.

addressing security problems related to these domains while carrying out a comprehensive examination of the different security problems associated with them.

Humayun et al. in [4] in their review paper titled "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study" included a list of existing studies relating to cyber security vulnerabilities and categorizes them considering the type of a commonly known security threat vulnerability, victim of a cyber threat, vulnerability degree, and method of data collection as well as verification. Another review paper in [5] titled "Security Issues in Cloud Computing: A Review on Security Problems in Cloud Computing—A Survey" also indicated security hurdles like data confidentiality, data integrity, and data privacy.

Numerous other articles exist [6], [5] that offer a comprehensive examination of the diverse security concerns within the realm of cloud computing. These scholarly articles delineate a number of security challenges, including but not limited to issues pertaining to data privacy, data confidentiality, and data integrity. It is imperative to acknowledge that although these articles offer a comprehensive examination of the diverse security concerns in cloud computing, they do not encompass all possible aspects. However, these resources provide a valuable foundation for individuals seeking to further their knowledge on this subject matter. The articles are summarized in the table below:

III. Cloud Computing Statistics

Scalability, flexibility, and cost-efficiency are among the benefits of cloud computing, which is continually growing. However, cloud computing presents severe security issues. Research shows that 90% of cloud data is unstructured and requires different processing and storage methods. This exponential increase is a major issue. Text, photos, audio, video, and other unstructured data have no standard or schema. Unstructured data is harder to manage and secure than structured data. Multi-cloud strategies are growing, with an estimated 87% of companies going multi-cloud by 2024. Multi-cloud setups do, however, also raise the complexity and risk of security breaches, which in 2022 accounted for 45% of all data breaches. The confidentiality, integrity, and availability of cloud data and infrastructure can be jeopardized by security breaches, which can lead to monetary losses, damages to one's reputation, legal ramifications, and regulatory fines. The average cost of these breaches globally was $4.35 million in 2022, and the healthcare industry faced costs as high as $10.10 million. The financial consequences are enormous. In addition, there was a 38% increase in cybersecurity threats between

TABLE I. SUMMARY OF LITERATURE REVIEW PAPERS

Author	Year	Description	Type of Paper
Prabadevi et al. [1]	2014	The paper reviews the list of existing studies relating to cybersecurity vulnerabilities and categorizes them considering the type of a commonly known security threat vulnerability, victim of a cyber threat, vulnerability degree, and method of data collection as well as verification. The authors suggested state-of-the-art techniques for recognizing human emotions from speech, facial expressions, and multimodal signals to address security issues.	Literature Review
Akello et al. [3]	2022	Provides a summary of security surveys in the cloud, fog, and edge computing domains.	Literature Review
Alouffi et al. [2]	2021	The research revealed seven primary security vulnerabilities that pose a risk to cloud computing services. These vulnerabilities include data manipulation and leakage, intrusion, and storage. The study also proposes the utilization of blockchain as a complementary solution to address security concerns.	Literature Review
Humayun et al. [4]	2020	identify available studies on cybersecurity vulnerabilities and categorize these solutions against commonly available security vulnerabilities, victims of cyber threats, vulnerability severity, and data collection and validation methods.	Mapping Study
Patel et al. [7]	2020	The paper overviews cloud security issues, threats, and related attacks.	Literature Review
Kumar et al. [6]	2017	Provide an overview of cloud computing security issues. The paper identifies several security challenges, such as data privacy, confidentiality, and integrity.	Survey
Tabrizchi et al. [8]	2020	Identify several security challenges such as data privacy, confidentiality, and integrity.	Survey
Shaikh et al. [5]	2012	Provides an overview of the various security issues in cloud computing. The paper identifies several security challenges, such as data privacy, confidentiality, and integrity.	Survey
Sharma et al. [9]	2021	The paper proposes a new topology for a single-phase inverter that can reduce the leakage current and increase the efficiency of photovoltaic systems.	Literature Review
Jabir et al. [10]	2016	Th paper presents a framework for conducting penetration testing on a private cloud computing infrastructure.	Research
Shetty et al. [11]	2012	Analyzes the security level of network applications on routers between cloud subscribers and cloud providers.	Research
Kumar et al. [12]	2019	A comprehensive survey focusing on cloud security requirements, threats, vulnerabilities, and countermeasures. It provides an in-depth analysis of cloud computing security challenges and offers a unified taxonomy for security in the cloud environment.	Survey
Sun et al. [13]	2020	This paper analyzes security and privacy protection in cloud computing. It reviews various privacy security issues, access control technologies, and attribute-based encryption (ABE) for cloud security. The paper also explores searchable encryption techniques and integrating various technologies for enhanced privacy and security in cloud computing.	Review
Stergiou et al. [14]	2018	This paper addresses security, privacy, and efficiency in sustainable cloud computing, particularly Big Data and IoT. It explores the integration of cloud computing with IoT technologies and the resulting security challenges while proposing a new system to improve cloud computing security through enhanced network architecture and encryption methods.	Review
Parikh et al. [15]	2019	The paper critically analyzes the unique security and privacy challenges in cloud, fog, and edge computing environments. It discusses the emerging security risks and privacy concerns in these distributed computing models, especially in relation to IoT integration and increasing data traffic. The study also proposes strategic approaches to mitigate these challenges, emphasizing the need for robust security mechanisms tailored to the complexities of interconnected computing systems.	Review
Ahmed et al. [16]	2016	This paper presents a detailed taxonomy for identifying security issues in cloud computing environments. It systematically categorizes various security threats and challenges in cloud computing, offering a structured framework for understanding and addressing these issues. The paper emphasizes the need for comprehensive security strategies to manage cloud security risks' evolving and complex nature.	Taxonomy Review
Guan et al. [17]	2018	The paper explores data security and privacy challenges in fog computing. It critically discusses the unique security and privacy issues that arise due to the nature of fog computing as an extension of cloud computing, especially with regard to IoT applications. The study highlights the need for innovative security approaches due to the limitations of existing cloud computing security solutions in the fog computing paradigm.	Review

2022 and 2023, underscoring the critical need for stronger security protocols to keep bad actors away from cloud data and infrastructure[1]. Phishing, ransomware, Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), malware, insider threats, and others are cybersecurity attacks. These attacks exploit cloud computing weaknesses such as misconfiguration, inadequate authentication, a lack of encryption, insufficient monitoring, and shared responsibility. Thus, organizations must take a holistic and proactive approach to cloud security that covers data protection, access control, encryption, identity management, threat detection, incident response, compliance management, and more. Some of the aspects under the problem statement are discussed in detail below:

A. Exponential Growth

The use of cloud services by numerous industries and sectors adds to the exponential expansion of cloud data. According to the International Data Corporation (IDC), global public cloud services and infrastructure investment expanded from $229 billion in 2019 to $500 billion in 2023, a 22.3% compound annual growth rate (CAGR). More companies are

[1]https://aag-it.com/the-latest-cyber-crime-statistics/

moving their data and apps to the cloud to maximize its scalability, flexibility, and cost-effectiveness [12]. However, more data is generated, processed, and stored in the cloud, presenting new data management and security challenges. Cloud data grows exponentially due to new technologies and trends that generate large amounts of data. The Internet of Things (IoT) is a network of internet-connected devices that collect and exchange data. Cisco predicted that global IoT connections would rise from 18.4 billion in 2018 to 43.9 billion in 2023, a 19% CAGR. It was also predicted that global IoT data traffic would expand from 14.4 exabytes per month in 2018 to 79.4 by 2023, a 41% CAGR. Since IoT devices have limited storage and processing, most data would be saved and analyzed in the cloud. Another reason driving exponential data expansion in cloud systems is the demand for data analytics and Artificial Intelligence (AI) applications. Organizations can improve customer experiences, processes, and insights with data analytics and AI [12]. The global business intelligence and analytics software market was estimated to expand from $23.1 billion in 2020 to $33.8 billion in 2025, a 7.9% CAGR, according to Gartner. The worldwide AI software market was to expand 33.2% from $22.6 billion in 2020 to $126.0 billion in 2025 [23]. Cloud storage and processing of enormous volumes of data are needed to train and execute these applications. According to IDC's prediction, there is an anticipated CAGR of 12.9% in spending on cloud infrastructure during the period of 2021–2026. This growth is expected to result in a total expenditure of $135.1 billion in 2026, representing 67.3% of the total expenditure on compute and storage infrastructure. The utilization of shared cloud infrastructure is projected to represent 72.3% of the overall cloud capacity, exhibiting a CAGR of 13.8%[2]. The expenditure on specialized cloud infrastructure is projected to see a CAGR of 10.7%, reaching a total of $37.4 billion. Expenditure on non-cloud infrastructure is projected to exhibit a CAGR of 2.3%, ultimately attaining a value of $65.6 billion by the year 2026. It is projected that expenditures made by service providers on compute and storage infrastructure would see a CAGR of 12.1%, ultimately reaching a total of $131.9 billion by the year 2026[3]https://infotechlead.com/cloud/cloud-spending-to-grow-17-to-88-9-bn-in-2022-vs-10-in-2021-idc-74765. This is shown in the graph below.

The global market for AI had a valuation of USD 454.12 billion in 2022 and is projected to reach approximately USD 2,575.16 billion by 2032, exhibiting a CAGR of 19% from 2023 to 2032, as shown below.

B. Paradigm Shift in Organizations

Cloud computing is a multifaceted phenomenon that encompasses both technological advancements and strategic considerations, exerting influence over various aspects of an organization, such as its structure, culture, and performance. Organizations that implement cloud computing can experience several advantages, including enhanced agility, innovation, and collaboration, with decreased operational expenses and complexity. Nevertheless, these organizations also have other obstacles, including the need to adapt to evolving roles and duties, effectively oversee numerous vendors and platforms, and guarantee the protection and confidentiality of data. The shared responsibility model is a fundamental component of cloud security, defining the allocation of security responsibilities between the cloud service provider and the consumer. The level of control and responsibility that customers have over the security of their data and applications varies depending on the specific type of cloud service they are utilizing, either IaaS, PaaS, or SaaS. In the context of IaaS, it is the customer's responsibility to ensure the security of the operating system, applications, data, and network traffic[4]. Conversely, the provider assumes the responsibility of securing the physical infrastructure, virtualization layer, and network. Within the realm of SaaS, the onus of ensuring data security and user access lies solely on the customer. At the same time, the provider bears the responsibility for all other aspects.

An additional crucial element of cloud security is adherence to industry-specific legislation and standards. Examples of these include the Health Insurance Portability and Accountability Act (HIPAA) for the healthcare sector, the Payment Card Industry Data Security Standard (PCI DSS) for the payment card business, and the General Data Protection Regulation (GDPR) for data protection inside Europe. The primary objective of these regulations is to safeguard the confidentiality, integrity, and availability of sensitive data and systems. Nevertheless, these regulations enforce stringent criteria and responsibilities for both the cloud service provider and the customer. As an illustration, it is mandated under the HIPAA that both entities involved must engage in the execution of a business associate agreement (BAA), which outlines their respective obligations and duties pertaining to safeguarding protected health information (PHI)[4]. The GDPR mandates that entities must conform to the fundamental principles of data minimization, purpose limitation, and consent. Hence, enterprises must undertake a comprehensive evaluation of risks and exercise due diligence prior to the selection of a cloud service provider. The user needs to ascertain that the service provider satisfies their security and compliance prerequisites while also offering transparency and accountability in their service provisions[5]. In addition, it is imperative for organizations to consistently engage in monitoring and auditing of their cloud infrastructure in order to identify and address any possible security risks or occurrences promptly. Therefore, cloud computing represents a significant shift in the prevailing paradigm, presenting numerous advantages and posing various obstacles for enterprises. Conducting research is necessary in order to comprehensively comprehend and efficiently tackle these difficulties[6]. Organizations may effectively use the capabilities of cloud computing while mitigating potential dangers by adhering to established best practices and standards in cloud security and compliance.

C. Security Vulnerabilities

In 2022, a significant proportion of data breaches were attributed to infiltrations into cloud-based systems. This emphasizes the pressing necessity of promptly addressing the

[2]https://solutionsreview.com/data-management/80-percent-of-your-data-will-be-unstructured-in-five-years/

[3]\unskip\protect\penalty\@M\vrulewidth\z@height\z@depth\dpff

[4]https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-vulnerabilities/

[5]https://www.cloudvulndb.org/

[6]https://www.cypressdatadefense.com/blog/cloud-computing-security-vulnerabilities/

distinct security risks that impact cloud environments. The vulnerabilities encompass a wide range of issues, including misconfigurations in cloud settings, inadequate user access controls, weaknesses in the architecture of cloud service providers, and advanced attack methodologies. Conducting research in this field is crucial for the identification of these vulnerabilities and the formulation of efficient strategies to protect sensitive data within businesses. Misconfigurations are identified as a primary contributing factor to data breaches occurring within cloud infrastructures[7]. Cloud services provide a wide range of choices, and enterprises frequently have difficulties configuring them in a secure manner. Misconfigurations have the potential to inadvertently expose data to unauthorized access, leakage, or alteration. Research can yield significant insights into prevalent misconfigurations and effective preventive measures. The infrastructure of cloud service providers represents an additional factor contributing to vulnerability. The security of data stored in cloud environments is frequently contingent upon the security measures implemented by the cloud service provider. Hence, it is vital to comprehend the prospective vulnerabilities within the provider's infrastructure and their potential impact on the data. Research also plays a crucial role in enabling enterprises to effectively monitor and stay updated on the most recent vulnerabilities. This allows them to ensure that cloud providers swiftly patch these issues. Furthermore, it is important to note that, with the continuous evolution of cyber threats, conducting research in this particular domain might provide valuable insights into emerging attack strategies and vulnerabilities that are unique to cloud computing. The acquisition of this knowledge is crucial for enterprises to adopt a proactive approach to safeguarding their data against developing dangers. Different scholars assert that it is important to enable firms to identify and address many types of attacks, including cryptojacking, denial-of-service, and server-side request forgery, within their cloud settings. It is imperative to note that the duty to ensure security in cloud computing is a collaborative effort between enterprises and cloud service providers. Gaining insight into the allocation of this responsibility and acquiring knowledge about successful collaboration are essential elements in the process of mitigating security vulnerabilities in cloud computing.

The exposed data included sensitive information such as authentication credentials, secret API data, and decryption keys. Moreover, documents contained in these servers revealed that the databases were storing data for Accenture's clients, including high-profile telecommunication companies and other Fortune 100 firms. The breach could expose Accenture and its clients to significant risks, including unauthorized data manipulation, fraud, and targeted phishing attacks. Fortunately, the exposed databases were discovered by a security researcher before any known malicious exploitation could occur. This incident underlines the critical need for stringent security practices in cloud storage configuration. The primary lesson here is the importance of regular security audits and implementing strict access controls. Companies must ensure their cloud services are correctly configured and regularly monitored for potential vulnerabilities.

The 2022 Thales Cloud Security Report by 451 Research, part of S&P Global Market Intelligence, found that 45% of businesses had a cloud-based data breach or failed audit in 2021, up 5% from 2020, raising increased concerns about cybercrime. Cloud adoption, especially multicloud usage, is rising globally. In 2021, enterprises worldwide used 110 SaaS apps, up from eight in 2015. 72% of enterprises now use multiple IaaS providers, up from 57% in 2021. One in five (20%) respondents use three or more providers, virtually doubling in 2021. Despite their growing popularity, businesses worry about the complexity of cloud services, with 51% of IT experts saying cloud privacy and data protection are harder. Complexity necessitates stronger cybersecurity. Most respondents (66%) reported that 21–60% of their sensitive data resides in the cloud. Only 25% indicated they could classify all the data. About 32% of respondents had to notify a government agency, client, partner, or employee of a breach. This should worry sensitive data-holding companies, especially in highly regulated industries. Cyberattacks continue to threaten cloud apps and data. Malware, ransomware, and phishing/whaling assaults increased for 26%, 25%, and 19% of respondents, respectively. IT professionals consider encryption essential for multicloud data protection. Most respondents use encryption (59%) and key management (52%) to secure cloud data. When asked how much of their cloud data is encrypted, just 11% replied 81–100%. Enterprises may also face key management platform sprawl. 10% utilize one to two platforms, 90% use three or more, and 17% use eight or more. Enterprises should prioritize cloud data encryption[8]. The practical usefulness of encryption platforms was shown when 40% of respondents said they avoided breach reporting because the stolen or leaked data was encrypted or tokenized. Positive signals of businesses investing in Zero Trust were also promising. About 29% of respondents are actually implementing a Zero Trust strategy, 27% are analyzing and developing one, and 23% are contemplating it. This is encouraging, but there is potential for improvement.

D. Financial Ramifications

The occurrence of data breaches inside cloud computing environments can result in major monetary losses for enterprises, impacting their immediate and sustained operational outcomes. Based on a report published by IBM, it has been determined that the worldwide mean expense associated with a data breach in the year 2023 amounted to USD 4.45 million, reflecting a 15% escalation over a span of three years[9]. Nevertheless, the financial implications of a data breach exhibit considerable disparity, contingent upon the geographical location and sector of the afflicted entity[10]. In addition to comprehending the possible financial implications associated with data breaches, it is imperative for enterprises to adopt proactive measures aimed at the prevention and mitigation of such incidents. According to a survey published by IBM, the utilization of security AI and automation has the potential to yield a reduction in the average cost of a data breach by USD 1.76 million in comparison to firms that do not employ these technologies. The implementation of security AI and

[7]https://www.upguard.com/blog/cloud-misconfiguration

[8]https://cpl.thalesgroup.com/about-us/newsroom/thales-cloud-data-breaches-2022-trends-challenges

[9]https://www.ibm.com/reports/data-breach

[10]https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs

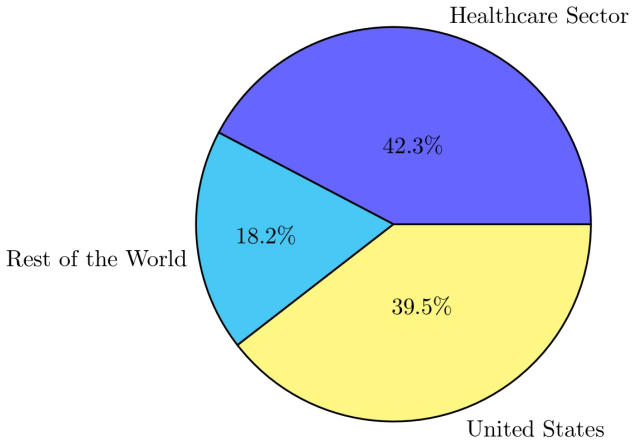

Fig. 2. The most affected sectors.

automation within businesses can contribute to the expedited identification and mitigation of potential threats, thereby reducing the adverse consequences of security breaches. In addition, it is advisable for firms to adopt comprehensive cybersecurity insurance policies, as they can provide coverage for the financial ramifications that may arise from security breaches. It is recommended that organizations allocate resources towards the implementation of cybersecurity training and awareness programs.

These initiatives aim to mitigate human errors and insider threats, which are prominent factors contributing to data breaches. By adhering to these suggestions, firms can enhance their readiness for the financial consequences associated with data breaches in cloud computing and mitigate their financial losses[11]. Data breaches can potentially lead to significant ramifications for the financial viability and long-term viability of companies as shown in Fig. 2 the healthcare sector has the lion's share of being attacked. However, these breaches can be averted and alleviated by implementing appropriate security measures and strategic investments. Conducting research in this domain can assist firms in making well-informed decisions pertaining to their cybersecurity strategy and policies.

E. Escalating Cybersecurity Attacks

The observed surge in cybersecurity attacks throughout the period spanning from 2022 to 2023 highlights the dynamic nature of the threat environment, as shown in Fig. 3. Conducting research in this domain is crucial in order to investigate the characteristics of these attacks and provide efficacious strategies to mitigate their impact. The complexity and variety of cyberattacks are increasing, incorporating a wide array of strategies like ransomware, zero-day flaws, social engineering, and supply chain attacks [18]. In recent years, there has been a notable increase in the occurrence and financial impact of ransomware attacks. Such attacks consist of an initial encryption of the victim's data before requesting a monetary ransom for the release of the hijacked information. In terms of ransomware expenditure, according to a survey by IBM in 2023, the global average expenditure was USD 5.66 million, a whopping hike of 21% from 2022. Zero-day exploits have increasingly seen their occurrence and impact. The menace this trend poses to critical infrastructure and the nation's security is substantial. These social engineering attacks are becoming more sophisticated and targeted, taking advantage of the growing use of social media and online environments. They are aimed at psychological tricks that would induce people to give out private data or engage in dangerous acts. Supply chain attacks that compromise software and hardware components from trustworthy vendors and partners pose serious challenges to firms. The assaults are capable of affecting different entities within several sectors. It is imperative for organizations to comprehend the dynamic strategies and underlying incentives driving these attacks. Research can provide valuable insights into the methods, techniques, and processes employed by cybercriminals, enabling firms to formulate proactive security plans. Research plays a crucial role in enabling companies to discern the indicators of compromise and the assault vectors employed by diverse threat actors, along with comprehending their goals and objectives.

Research can also aid firms in comprehending the behavioral and psychological elements that impact consumers' vulnerability to social engineering attacks, as well as in devising proficient awareness and education initiatives to alleviate such risks. Moreover, the proliferation of remote work and the use of cloud-based services have resulted in the expansion of the attack surface, hence heightening the susceptibility of enterprises to cyber threats. Research plays a crucial role in enabling firms to discern the precise issues presented by these transformations and formulate effective methods to safeguard remote and cloud-based operations. This encompasses the enhancement of identity and access management, the implementation of multi-factor authentication, and the improvement of threat detection and response capabilities. Research can additionally aid organizations in assessing the security stance and adherence to regulations of their cloud service providers, as well as establishing explicit roles and duties for the governance of cloud security [18]. The establishment of partnerships and cooperation among researchers, cybersecurity professionals, and other organizations is crucial to proactively addressing the increasing frequency and severity of cybersecurity threats. The dissemination of knowledge regarding emerging threats and vulnerabilities has the potential to facilitate the creation of enhanced security measures[12]. The investigation conducted in this field has the potential to make a valuable contribution to the collaborative endeavor of protecting data and systems in an ever more hostile digital environment.

F. Gap in Existing Literature

Cloud computing is a conceptual framework that presents a multitude of advantages, including scalability, elasticity, and cost-effectiveness. However, it also presents notable security obstacles. The presence of security vulnerabilities within cloud computing has the potential to jeopardize the confidentiality, integrity, and availability of both cloud services and data. This, in turn, can result in significant ramifications for both suppliers and users of cloud services. Hence, it is important to ascertain and evaluate the key security risks in cloud computing and put

[11]https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs

[12]https://onlinedegrees.sandiego.edu/top-cyber-security-threats/

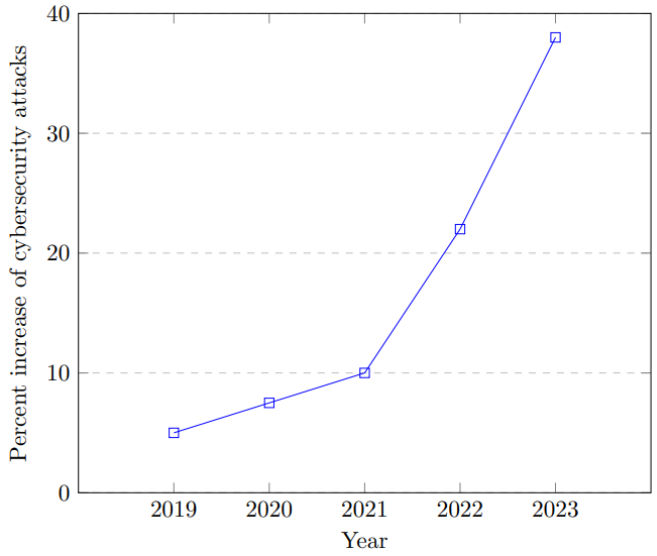

Fig. 3. Frequency increase of cybersecurity attacks between 2019 and 2023.

forth effective mitigation strategies. Nevertheless, the current body of scholarly work pertaining to cloud security is characterized by fragmentation and dispersion. It predominantly concentrates on specific aspects or domains of cloud security while lacking a comprehensive and methodical examination that encompasses the diverse security vulnerabilities, their ramifications, and the corresponding remedies within a unified and coherent analysis. The objective of this study is to address the aforementioned deficiency by undertaking a comprehensive examination of existing literature, known as a SLR, to identify and analyze the major security vulnerabilities present in cloud computing. A SLR is a methodological approach characterized by its rigorous and transparent nature that aims to locate, evaluate, and synthesize the available body of knowledge pertaining to a certain subject. This study aims to utilize the SLR approach to present a thorough and current examination of the existing research on vulnerabilities in cloud security. Additionally, it seeks to identify areas where further research is needed and suggest potential future directions in this field. This study aims to investigate the primary security issues associated with cloud computing, including questions: What are the ramifications of these security vulnerabilities for cloud service providers and their clientele? What are the productive mitigation solutions for these security vulnerabilities?

IV. Cloud Computing Security Assessment

A. Impact of Security Vulnerabilities in Cloud Computing

Cloud computing refers to providing various computing services, including storage, servers, databases, networking, software, analytics, and intelligence, through the Internet. Cloud computing has numerous advantages for both enterprises and individuals, encompassing scalability, cost-effectiveness, performance, reliability, and innovation. Nevertheless, the advent of cloud computing also presents novel security concerns and hazards that necessitate attention and resolution from both cloud service providers and their clientele[13]. Security vulnerabilities refer to inherent weaknesses or deficiencies inside a given system or application that can be potentially exploited by malicious actors with the intention of compromising the system's confidentiality, integrity, or availability, as well as the data it houses. Security vulnerabilities can result in significant consequences for both cloud providers and their clients[14]. These consequences include, but are not limited to, data breaches, financial losses, legal liability, reputational harm, and operational disruptions. The following are the impacts of security vulnerabilities in cloud computing:

1) Cloud misconfiguration: Cloud misconfiguration is a prevalent security vulnerability that occurs in cloud computing. Cloud misconfiguration refers to the situation in which a cloud resource or service is not appropriately configured in accordance with established security best practices or regulations. An instance may arise if a cloud storage bucket is inadvertently made accessible to the general public on the internet, hence enabling unauthorized individuals to get entry to confidential information[15].

Alternatively, a cloud user may possess an abundance of permissions or privileges that exceed the requirements of their designated position or function. Human error, a lack of knowledge base, or insufficient automation can all lead to cloud misconfiguration. Misconfigured clouds can have detrimental effects on both cloud service providers and users, including: Data breaches: Cloud misconfigurations may lead to data breaches wherein unauthorized individuals may access, steal, alter or delete confidential data stored in the cloud[16]. Data breaches can have adverse financial implications, legal obligations, government sanctions, and loss of the reputation of the customers and the cloud service providers themselves. Compliance violations: Cloud misconfiguration leads to non-compliance instances where cloud providers or clients cannot observe security standards or obligations enshrined in laws, rules, contracts, or industry frameworks. Non-compliance instances may attract fines, regulatory actions, legal proceedings or lack of confidence for cloud service providers and their customers.

Operational disruption: Cloud service/application availability and performance may be impacted by cloud misconfiguration. For example, a firewall that is not properly configured can block the lawful traffic network, and a load balancer that is not properly configured can cause the quality of service degradation. Operational disruption can cause customer dissatisfaction, reduced revenues, and diminished competitive advantage to cloud providers and their clients.

To prevent or mitigate cloud misconfiguration, cloud providers and customers should follow some best practices, such as:

a) Enforce the principle of least privilege: The principle of least privilege suggests that each user or service should possess only the essential level of access or permissions necessary to carry out their designated tasks. The use of this measure

[13]https://www.wiz.io/academy/common-cloud-vulnerabilities

[14]https://www.orientsoftware.com/blog/vulnerability-in-cloud-computing/

[15]https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/the-most-common-cloud-misconfigurations-that-could-lead-to-security-breaches

[16]https://www.techtarget.com/searchsecurity/definition/data-breach

can effectively decrease the attack surface and mitigate the potential extent of harm in the event of a security breach.

b) Use third-party tools: Third-party technologies can scan and identify instances of cloud misconfiguration, as well as offer advice or remedial measures. One illustration of how a cloud-native application protection platform (CNAPP) might enhance the visibility and security of cloud resources can be observed.

c) Review and audit regularly: Regular evaluation and auditing of cloud configurations by both cloud providers and clients is critical to ensuring adherence to security policies and best practices. In addition, it is essential for individuals to diligently oversee and record any modifications or actions pertaining to their cloud-based assets, with the purpose of identifying any irregularities or occurrences.

2) Data leakage: Data leakage is a prevalent security risk that is frequently seen in the realm of cloud computing. Data leakage is the unintended or purposeful transfer of data from a secure source to an unauthorized destination[17]. Unencrypted communication lines, unsecured APIs, employees with ill-intent within the organization, hacked passwords, third party dependencies may be potential data leakage avenues.

Data leakage is a serious threat for cloud service providers and their clients. These risks involve data breaches, which can lead to monetary losses, legal issues, fines, and damage to one's reputation. Also, it is worth mentioning that privacy breaches occur when the personal or confidential data is divulged without the due authority, therefore leading to identity theft, fraud, or harassment. Lastly, an unregulated data leakage is also capable of destroying a company's competitive advantage by revealing sensitive information such as secret knowledge, business strategies, or important assets to competitors. It is important to follow the current best practices in order to prevent or mitigate these risks. This involves putting up several security measures to make sure that the data is not accessed by individuals without authority to do so. These measures include encrypting data both when it is stored and when it is being transmitted, using secure application programming interfaces (APIs) that comply with recognized security standards, and deploying data loss prevention (DLP) solutions to identify, categorize, and safeguard sensitive data. Additionally, access and usage policies are enforced across both cloud-based and on-premise environments.

3) Shared technology vulnerabilities: The presence of shared technology vulnerabilities in cloud computing arises from the fundamental utilization of common infrastructure, platforms, and software for the provision of services to numerous consumers. Consequently, any flaw present in the shared technology possesses the capacity to pose a possible threat to all users. These vulnerabilities have the potential to result in data breaches, which can expose sensitive information and result in financial losses, legal consequences, and reputational damage for both service providers and customers.

Furthermore, these entities have the potential to interfere with many services, exemplified by their involvement in denial-of-service assaults, resulting in the deterioration or complete cessation of these services. Resource abuse is a significant worry in the realm of cybersecurity since malevolent actors exploit communal technology for illicit objectives, resulting in escalated expenses, diminished operational efficiency, and compromised availability [19]. In order to address these risks, it is imperative for both cloud providers and clients to adhere to established best practices. These include timely patching and update, resource isolation, segregation. Also, constant tracking and auditing should ensure prompt detection of irregularities or any breach in the security.

4) Insecure interfaces and APIs: Cloud computing security is a great problem due to insecure interfaces and APIs. The communication and interaction between the services are done through these interfaces and APIs, but if the interfaces or the APIs are poorly designed and also not secured, then they can be the biggest dangers that a system may have. They could arise through weaknesses in authentication, inappropriate encryption, ineffective input validation, and poor error handling [18]. The potential outcomes of these vulnerabilities might have significant ramifications, such as instances of data breaches where confidential data may be illicitly accessed, pilfered, altered, or erased. This can lead to financial detriments, legal implications, regulatory penalties, and reputational harm for both cloud service providers and their clientele[19]. Furthermore, service disruptions like DDoS attacks can have an impact on the availability and performance of cloud services and apps.

In summary, the exponential expansion of cloud computing has undeniably revolutionized the manner in which enterprises manage their data and information technology requirements, presenting a multitude of benefits in relation to adaptability, availability, and cooperation. Nevertheless, this paradigm shift has concurrently presented a plethora of security concerns and vulnerabilities that necessitate resolution in order to safeguard confidential information and uphold the authenticity of cloud infrastructure.

B. Cloud Security Assessment Techniques

1) Penetration testing: Penetration testing is a technique employed to assess the security of a cloud environment by emulating an attack originating from a malevolent entity. This process facilitates identifying familiar and unfamiliar vulnerabilities inside the cloud environment, encompassing misconfigurations, inadequate authentication mechanisms, insecure Application Programming Interfaces (APIs), data breaches, and more security weaknesses. It contains five stages, as shown in Fig. 4. By identifying vulnerabilities that malicious actors could exploit, penetration testing provides valuable insights and suggestions for improving the security posture and resilience of the cloud environment.

Penetration testing can be conducted at several levels inside the cloud environment, including the network, application, data, and user layers. Penetration testing can be undertaken from several perspectives, including black-box, white-box, or gray-box, depending on the test's scope and objectives. Black-box testing emulates the actions of an external adversary

[17]https://metomic.io/resource-centre/what-are-the-biggest-risks-of-data-leaks

[18]https://cloudsecurityalliance.org/blog/2022/07/30/top-threat-2-to-cloud-computing-insecure-interfaces-and-apis

[19]https://www.darkreading.com/application-security/insecure-apis-a-growing-risk-for-organizations

Fig. 4. Five stages of penetration testing process.

without prior knowledge of the cloud environment. White-box testing involves emulating an internal attacker who possesses comprehensive access to and understanding of the cloud infrastructure. Gray-box testing involves emulating a partially informed adversary with restricted access to or understanding of the cloud infrastructure.

An example of penetration testing within cloud computing is the AWS Penetration Testing service. This service enables customers to seek authorization to conduct permitted tests on their AWS resources. An additional illustration may be in the form of IBM X-Force Red Vulnerability Management Services. This service provides a comprehensive methodology for cloud penetration testing, encompassing many aspects such as infrastructure, apps, data, and users. In our research, penetration testing is critical for assessing cloud security vulnerabilities. This methodology is informed by the insights provided by Vasenius (2022) in his thesis "Best Practices in Cloud-Based Penetration Testing." Vasenius' comprehensive analysis of cloud-specific penetration testing approaches, tools, and best practices offers a valuable framework for our penetration testing strategy, particularly in the context of cloud environments and their unique security challenges[20].

In 2022, Khuong et al. in [20] studied a novel architectural approach called deep cascaded reinforcement learning agents (CRLA). This approach was developed to tackle the challenge of large discrete action spaces in an autonomous penetration testing simulator. In such simulators, the number of available actions grows exponentially as the complexity of the cybersecurity network being tested increases. Using an algebraic action decomposition strategy, the Comparative Reinforcement Learning Algorithm (CRLA) demonstrates superior efficiency and stability in determining the optimal attack policy in scenarios characterized by extensive action spaces. This outperforms the conventional deep Q-learning agent, frequently employed as an artificial intelligence approach for autonomous penetration testing.

In 2023, a research paper by Hu et al. in [21] introduced a precise grey box penetration testing methodology known as TAC. This strategy aims to identify instances of identity and access management (IAM) vulnerabilities and privilege escalation (PEs) in third-party services. Third-party cloud security services are frequently employed to identify potential PEs resulting from misconfigurations in IAM. In order to address the dual issues of labor-intensive anonymizations and potential exposures of sensitive information, TAC engages with consumers through a selective querying approach that focuses solely on the relevant information required. The primary finding of this article is that the IAM configuration contains a limited amount of pertinent information for the detection of IAM PE. This study introduces the concept of IAM modeling, which allows for detecting a wide range of IAM PEs by utilizing the limited information obtained from queries. In order to enhance the effectiveness and versatility of TAC, our objective is to reduce customer contacts by implementing Reinforcement Learning (RL) in conjunction with Graph Neural Networks (GNNs). This integration enables TAC to acquire the ability to minimize the number of queries made.

Our approach to penetration testing, especially in the context of mobile cloud computing, is informed by the findings and methodologies discussed by Bakar et al. in [22] provided a comprehensive overview of penetration testing techniques and best practices tailored for mobile cloud environments, which is particularly relevant for our research as it addresses the unique challenges and considerations in these settings. Our penetration testing methodology is significantly influenced by the groundbreaking work of Vuggumudi et al. in [23] outlined an innovative approach known as Compliance Based Penetration Testing (CBPT), specifically tailored for PaaS environments. This approach underscores the importance of a collective approach to security in cloud services, highlighting the necessity for ongoing monitoring and compliance-aligned testing. Such an approach is vital for our research, considering the ever-changing landscape of cloud environments and the continuous evolution of regulatory requirements.

2) Vulnerability scanning: Vulnerability scanning is a technique of systematically discovering, assessing, and reporting security vulnerabilities in a cloud environment and It goes through five stages as shown in Fig. 4. It helps enterprises uncover gaps in their cloud services, infrastructure, and applications that potentially threaten the confidentiality, integrity, or availability of their data and resources. Vulnerability scanning also helps firms comply with security standards and regulations, such as PCI DSS, HIPAA, GDPR, and more. Vulnerability scanning can be performed using numerous tools and approaches, such as automatic scanners, human audits, code reviews, or ethical hacking. Vulnerability scanning can be split into two types: active and passive. Active scanning involves sending probes or queries to the cloud environment to find vulnerabilities and measure their impact. Passive scanning involves monitoring the network traffic or records of the cloud environment to find vulnerabilities and irregularities.

An example of vulnerability scanning in cloud computing is AWS Amazon Inspector, which is an automated security evaluation tool that helps clients enhance the security and compliance of their AWS applications[21]. Another example is

[20]https://www.utupub.fi/handle/10024/173476

[21]https://docs.aws.amazon.com/inspector/latest/user/what-is-inspector.html

Digital Defense Frontline VM, which is a cloud-based vulnerability management tool that delivers continuous scanning and reporting of cloud assets. Our research methodology for vulnerability scanning incorporates insights and techniques from Mitchell and Zunnurhain's (2019) study, "Vulnerability Scanning with Google Cloud Platform," presented at the CSCI conference [24]. This paper presents a detailed examination of vulnerability scanning methods within the Google Cloud Platform, offering a specific lens on how these scans can be effectively utilized in cloud-based environments. Their work provides a valuable perspective on the practical applications and challenges of conducting vulnerability scans in such settings, directly relevant to our research focus.

We have heavily referenced the comprehensive analysis by Kritikos et al. [25] that meticulously evaluated the latest tools and databases pertinent to vulnerability assessment in the cloud. The survey's detailed insights into these tools' performance, range, and functionalities significantly influence our methodology, particularly in selecting and implementing the most effective techniques for extensive vulnerability scanning in cloud-based applications.

C. Future Trends in Cloud Computing Security

As cloud computing evolves, staying ahead of emerging security challenges is crucial. Cloud security landscape is expected to undergo significant changes in the coming years, influenced by technological advancements and shifts in cyber threats. Below are key trends that are likely to shape the future of cloud computing security:

1) Increased reliance on AI and Machine Learning (ML): AI and ML are set to play a pivotal role in cloud security. These technologies can analyze vast amounts of data to identify patterns indicative of cyber threats, enabling proactive threat detection and response. As cyberattacks become more sophisticated, AI-driven security systems will be critical in identifying and neutralizing threats before they can cause damage[26].

2) Greater emphasis on zero trust architectures: The traditional security model of 'trust but verify' is shifting towards a 'never trust, always verify' approach. Zero Trust Architecture (ZTA) will become more prevalent, where security protocols require verification from everyone attempting to access resources in the network, regardless of whether they are inside or outside the network perimeter. This approach minimizes the risk of internal threats and data breaches [27].

3) Expansion of edge computing: As the Internet of Things (IoT) expands, edge computing will become more common, processing data closer to where it is generated rather than in a centralized cloud-based data center. This shift will require new security strategies to protect data across more dispersed networks[22].

4) Enhanced regulatory compliance: With the growing concern over data privacy and security, regulatory compliance will become more stringent. Companies must adapt to these regulations, which will likely require more robust security measures to protect sensitive data, especially in industries like healthcare and finance [28].

5) Blockchain for improved security: Blockchain technology is expected to be increasingly adopted for cloud security because it offers decentralized security and reduces single points of failure. Its potential for ensuring data integrity and preventing tampering will make it a valuable tool in enhancing cloud data security[23].

6) Rise in cybersecurity mesh: Cybersecurity mesh is a flexible, modular approach that integrates various security services. This trend will allow organizations to deploy and integrate security where it's most needed and manage it in a more unified way, thus improving the overall security posture[24].

V. Conclusion

Cloud computing has rapidly changed how firms manage their data and IT demands, providing flexibility, accessibility, and cooperation. This change has also revealed many security risks that must be addressed to secure sensitive data and cloud settings. Mismanaging cloud resources or data frequently results in cloud misconfiguration and data leakage. These vulnerabilities can cause data breaches, compliance violations, and financial losses for cloud providers and clients. Additionally, cloud-based shared technological vulnerabilities are risky. Cloud computing allows numerous enterprises to share infrastructure and platforms, which can expose sensitive data to breaches, service outages, and resource misuse if not properly secured. Quick patching, resource isolation, and monitoring can mitigate these shared vulnerabilities. Furthermore, understanding the shared responsibility concept is crucial. This model defines cloud service providers and customer security duties. Organizations must know how to secure their cloud resources and data and use cloud providers' tools and services to improve security. Cloud services and emerging technologies like IoT and AI drive exponential data growth in cloud environments, creating unique problems. Securing varied cloud environments becomes more difficult as firms adopt multi-cloud strategies. Cloud data security and compliance need risk assessments, careful cloud service provider selection, and industry-specific requirements. Ransomware, zero-day exploits, social engineering, and supply chain assaults are becoming more sophisticated, requiring cybersecurity specialists, corporations, and researchers to share knowledge and information. To succeed in this changing world, enterprises must take a proactive, holistic approach to cloud security, covering technological and organizational factors. In an ever-changing digital world, organizations may protect their data, manage risks, and maintain their reputation and financial stability by remaining educated about new threats and vulnerabilities, applying best practices, and enhancing their cloud security maturity.

Acknowledgment

This work was made possible in part by a grant from the university, which allowed us to conduct the research and collect the necessary data. This work was supported

[22]https://techresearchonline.com/blog/edge-computing-an-extension-of-cloud-computing/

[23]https://www.computer.org/publications/tech-news/trends/blockchain-cloud-integration

[24]https://securityintelligence.com/articles/cloud-security-trends-cybersecurity-mesh/

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.GRANT5,690].

REFERENCES

[1] B. Prabadevi and N. Jeyanthi, "Distributed denial of service attacks and its effects on cloud environment- a survey," *The 2014 International Symposium on Networks, Computers and Communications*, 2014.

[2] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, "A systematic literature review on cloud computing security: threats and mitigation strategies," *IEEE Access*, vol. 9, pp. 57 792–57 807, 2021.

[3] P. Akello, N. L. Beebe, and K.-K. R. Choo, "A literature survey of security issues in cloud, fog, and edge it infrastructure," *Electronic Commerce Research*, pp. 1–35, 2022.

[4] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber security threats and vulnerabilities: a systematic mapping study," *Arabian Journal for Science and Engineering*, vol. 45, pp. 3171–3189, 2020.

[5] R. Shaikh and M. Sasikumar, "Security issues in cloud computing: A survey," *International Journal of Computer Applications*, vol. 44, no. 19, pp. 4–10, 2012.

[6] N. Kumar and J. K. Samriya, "Security issues in cloud computing: A survey."

[7] A. Patel, N. Shah, D. Ramoliya, and A. Nayak, "A detailed review of cloud security: issues, threats & attacks," in *2020 4th International conference on electronics, communication and aerospace technology (ICECA)*. IEEE, 2020, pp. 758–764.

[8] H. Tabrizchi and M. Kuchaki Rafsanjani, "A survey on security challenges in cloud computing: issues, threats, and solutions," *The journal of supercomputing*, vol. 76, no. 12, pp. 9493–9532, 2020.

[9] A. Sharma, U. K. Singh, K. Upreti, and D. S. Yadav, "An investigation of security risk & taxonomy of cloud computing environment," in *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*. IEEE, 2021, pp. 1056–1063.

[10] R. M. Jabir, S. I. R. Khanji, L. A. Ahmad, O. Alfandi, and H. Said, "Analysis of cloud computing attacks and countermeasures," in *2016 18th international conference on advanced communication technology (ICACT)*. IEEE, 2016, pp. 117–123.

[11] S. Shetty, N. Luna, and K. Xiong, "Assessing network path vulnerabilities for secure cloud computing," in *2012 IEEE International Conference on Communications (ICC)*. IEEE, 2012, pp. 5548–5552.

[12] R. Kumar and R. Goyal, "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey," *Computer Science Review*, vol. 33, pp. 1–48, 2019.

[13] P. Sun, "Security and privacy protection in cloud computing: Discussions and challenges," *Journal of Network and Computer Applications*, vol. 160, p. 102642, 2020.

[14] C. Stergiou, K. E. Psannis, B. B. Gupta, and Y. Ishibashi, "Security, privacy & efficiency of sustainable cloud computing for big data & iot," *Sustainable Computing: Informatics and Systems*, vol. 19, pp. 174–184, 2018.

[15] S. Parikh, D. Dave, R. Patel, and N. Doshi, "Security and privacy issues in cloud, fog and edge computing," *Procedia Computer Science*, vol. 160, pp. 734–739, 2019.

[16] M. Ahmed and A. T. Litchfield, "Taxonomy for identification of security issues in cloud computing environments," *Journal of Computer Information Systems*, vol. 58, no. 1, pp. 79–88, 2018.

[17] Y. Guan, J. Shao, G. Wei, and M. Xie, "Data security and privacy in fog computing," *IEEE Network*, vol. 32, no. 5, pp. 106–111, 2018.

[18] M. Alawida, A. E. Omolara, O. I. Abiodun, and M. Al-Rajab, "A deeper look into cybersecurity issues in the wake of covid-19: A survey," *Journal of King Saud University-Computer and Information Sciences*, 2022.

[19] Y. S. Abdulsalam and M. Hedabou, "Security and privacy in cloud computing: technical review," *Future Internet*, vol. 14, no. 1, p. 11, 2021.

[20] K. Tran, M. Standen, J. Kim, D. Bowman, T. Richer, A. Akella, and C.-T. Lin, "Cascaded reinforcement learning agents for large action spaces in autonomous penetration testing," *Applied Sciences*, vol. 12, no. 21, p. 11265, 2022.

[21] Y. Hu, W. Wang, and M. Tiwari, "Greybox penetration testing on cloud access control with iam modeling and deep reinforcement learning," *arXiv preprint arXiv:2304.14540*, 2023.

[22] A. B. Bakar, M. S. bin Che Mansor, M. S. A. bin Omar, and M. F. Bin, "Fundamental study of penetration testing on mobile cloud computing."

[23] S. Vuggumudi, K. Ragothaman, and Y. Wang, "Compliance based penetration testing as a service — aisel.aisnet.org," in *Proceedings of the Seventeenth Midwest Association for Information Systems Conference*, 2023.

[24] N. J. Mitchell and K. Zunnurhain, "Vulnerability scanning with google cloud platform," in *2019 International Conference on Computational Science and Computational Intelligence (CSCI)*. IEEE, 2019, pp. 1441–1447.

[25] K. Kritikos, K. Magoutis, M. Papoutsakis, and S. Ioannidis, "A survey on vulnerability assessment tools and databases for cloud-based web applications," *Array*, vol. 3, p. 100011, 2019.

[26] A. Li and W. Huang, "A comprehensive survey of artificial intelligence and cloud computing applications in the sports industry," *Wireless Networks*, 2023.

[27] L. Ferretti, F. Magnanini, M. Andreolini, and M. Colajanni, "Survivable zero trust for cloud computing environments," *Computers & Security*, vol. 110, p. 102419, 2021.

[28] S. E. Kafhali, I. E. Mir, and M. Hanini, "Security threats, defense mechanisms, challenges, and future directions in cloud computing," *Archives of Computational Methods in Engineering*, vol. 29, pp. 223 – 246, 2021. [Online]. Available: https://api.semanticscholar.org/CorpusID:255412617