World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Security challenges in cloud computing: A comprehensive analysis

Janet Julia Ang'udi *

Jaramogi Oginga Odinga University of Science & Technology, Kenya.

World Journal of Advanced Engineering Technology and Sciences, 2023, 10(02), 155–181

Publication history: Received on 06 November 2023; revised on 19 December 2023; accepted on 22 December 2023

Article DOI: https://doi.org/10.30574/wjaets.2023.10.2.0304

Abstract

The security issues surrounding cloud computing, a quickly developing technology that is now essential to both personal and business computing, are thoroughly examined in this study. Cloud computing presents serious security risks that require careful attention, despite its many advantages such as scalability, cost-effectiveness, and flexibility. In-depth discussions of a number of important security topics are covered in this paper, including network security, access control, data breaches, legal and regulatory framework compliance, and new threats and vulnerabilities. The paper illuminates the complexities of data and application security in the cloud environment by thoroughly examining these subjects. The study also looks at actual case studies to show how security breaches in cloud computing affect things and how to fix them. The study intends to offer insightful analyses of security challenges with practical implications by examining these cases and providing lessons learned from incidents that have happened in various cloud computing scenarios. Our comprehension of the complex nature of security threats and the tactics used to counter and mitigate them is improved by looking closely at these cases. This study looks into the potential benefits of cloud security enhancements from emerging technologies like artificial intelligence and machine learning, in addition to identifying existing challenges. The research investigates the potential benefits of these technologies in terms of automated security responses, adaptive access controls, and proactive threat detection. Cloud environments may be able to improve their security posture against new and sophisticated threats by utilizing the powers of AI and machine learning. Furthermore, by projecting future trends and challenges in cloud security, this paper offers a forward-looking view of the changing field. Comprehending these possible obstacles is crucial to creating proactive and flexible security approaches that can successfully tackle the ever-changing landscape of cloud computing. This paper's ultimate objective is to offer insightful information about practical approaches and industry best practices for safeguarding cloud environments. Organizations can navigate the complexity of the cloud landscape while protecting their data and applications from the ever-evolving threat landscape by striking a balance between the enormous potential of cloud computing and the necessity of maintaining strong security measures.

Keywords: Artificial Intelligence (AI); Emerging Technologies; Future Trends; Industry Best Practices; Cloud Environment; Cloud Computing; Cloud Security; Business Computing; Threats; Legal Compliance

1. Introduction

Cloud computing has revolutionized the way we store, process, and manage data, offering unprecedented levels of flexibility, scalability, and efficiency [1]-[6]. As businesses and individuals increasingly rely on cloud services for a wide range of applications, the security of cloud-based systems has emerged as a critical concern. In the context of an ever-evolving digital landscape, cloud computing represents a paradigm shift from traditional on-premises IT solutions to services provided over the internet. This shift, while advantageous in many respects, introduces a unique set of security issues. The distributed nature of cloud services, coupled with the sharing of resources, can lead to vulnerabilities that are distinct from those encountered in traditional IT environments [7], [8]. Figure 1 shows a typical cloud computing architecture. The importance of cloud security cannot be overstated, as the consequences of security breaches can be

* Corresponding author: Janet Julia Ang'udi

severe, including data loss, privacy violations, financial damages, and erosion of user trust [9], [10]. Furthermore, the dynamic and scalable nature of cloud services complicates the task of ensuring consistent security across different service models (Infrastructure as a Service, Platform as a Service, and Software as a Service) and deployment models (public, private, and hybrid clouds).

Cloud computing security is a multifaceted discipline aimed at protecting the vast array of resources and services hosted in cloud environments. One of the core challenges in cloud security lies in the shared responsibility model, where cloud service providers manage the security of the infrastructure, while customers are responsible for securing their data, applications, and user access [11]-[13]. Robust authentication and authorization mechanisms, coupled with stringent access controls, are crucial to preventing unauthorized access to sensitive information. Multi-factor authentication (MFA) adds an extra layer of protection by requiring users to provide multiple forms of verification before accessing cloud resources, reducing the risk of unauthorized access even in the event of compromised credentials [14], [15].

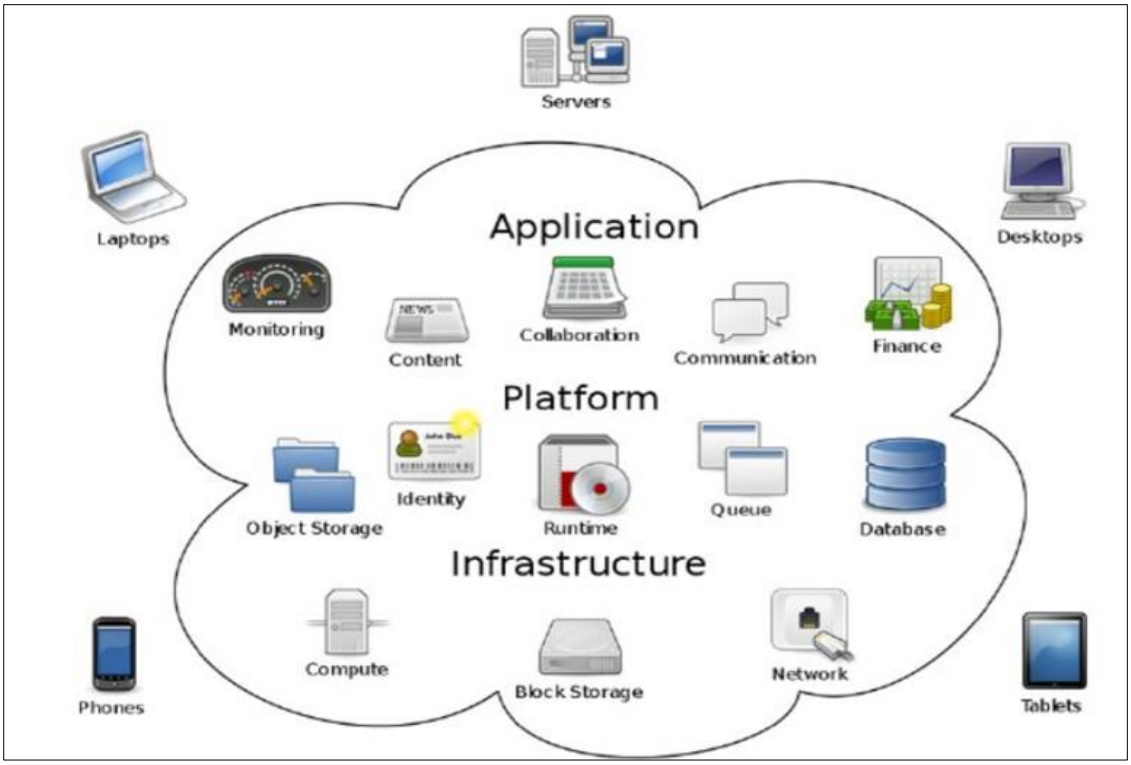

Figure 1 Cloud computing architecture

Encryption is a fundamental component of cloud security, safeguarding data both in transit and at rest. Secure communication channels, such as SSL/TLS, protect data during transmission, while advanced encryption algorithms like AES ensure that stored data remains confidential and tamper-resistant. Regular security audits, vulnerability assessments, and penetration testing are essential practices to identify and address potential weaknesses in the cloud infrastructure [16]-[19]. As cyber threats continue to evolve, cloud security measures must evolve in tandem, leveraging emerging technologies like artificial intelligence to detect and respond to new and sophisticated risks. The dynamic nature of cloud computing necessitates a proactive and collaborative approach between cloud providers and users to ensure a secure and resilient cloud environment [20]-[25].

This paper begins by outlining the basic architecture of cloud computing, followed by a detailed discussion of the key security issues. These include data security and privacy, access control, network security, compliance and legal issues, and emerging threats. The analysis is supported by case studies that shed light on real-world security incidents in cloud computing, providing valuable insights into the nature of these threats and the strategies used to mitigate them. In addressing these challenges, the paper also explores the role of emerging technologies in enhancing cloud security and anticipates future trends in the field. The goal is to furnish a thorough understanding of the current security landscape in cloud computing and to offer guidance on developing effective strategies to protect against these evolving threats.

2. Cloud Computing Deployment and Service Models

Cloud computing is defined as the delivery of various services through the Internet, including data storage, servers, databases, networking, and software [26], [27]. The emergence of cloud computing as a dominant force in the digital economy has ushered in a new era of information technology. To fully understand the security challenges it presents, it is essential to first grasp the basic architecture and underlying principles of cloud computing.

2.1. Service Models

Cloud computing service models encompass three primary categories: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) as shown in Figure 2. IaaS provides fundamental computing resources such as virtual machines, storage, and networks, allowing users to manage and control the underlying infrastructure.

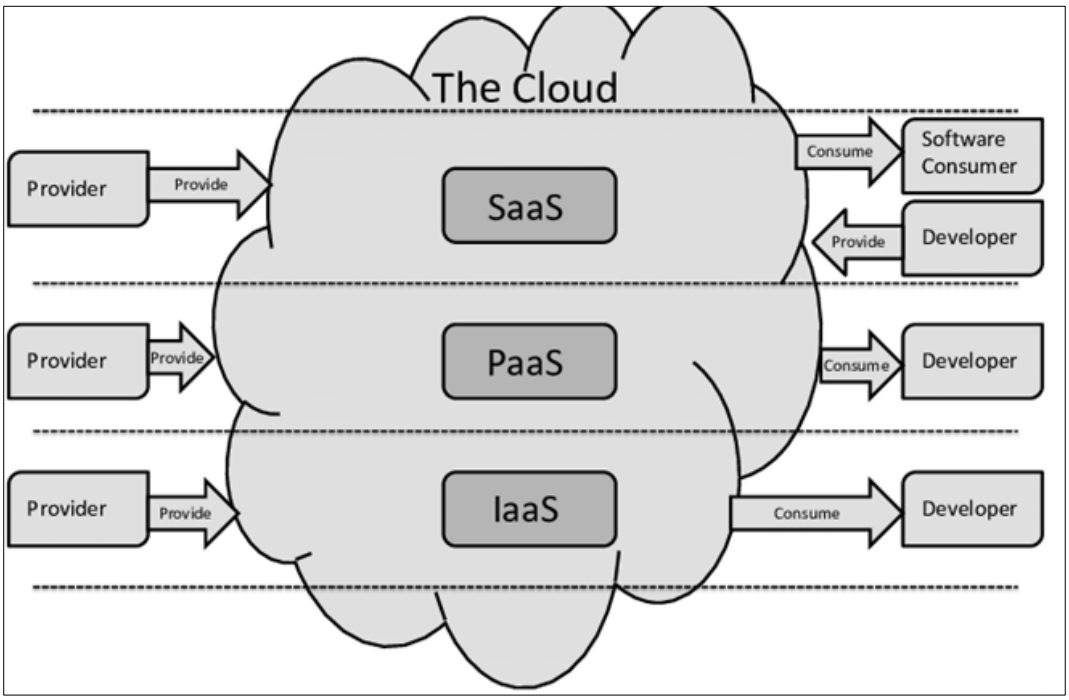

Figure 2 Cloud service models

PaaS offers a higher level of abstraction, providing a platform with development tools and services that enable users to build, deploy, and manage applications without concerning themselves with the intricacies of the underlying infrastructure. SaaS, on the other hand, delivers fully functional applications over the internet, eliminating the need for users to manage the underlying infrastructure, development, or maintenance, as these responsibilities are shouldered by the service provider. As shown in Figure 3, each service model offers a varying degree of control and responsibility, allowing organizations to choose the level of abstraction that best aligns with their specific needs and resources. A brief summary of these models is as follows:

- **Infrastructure as a Service (IaaS):** Provides virtualized computing resources over the internet [28].
- **Platform as a Service (PaaS):** Offers hardware and software tools, typically for application development [29]-[31].
- **Software as a Service (SaaS):** Delivers software applications over the internet, on a subscription basis [32].

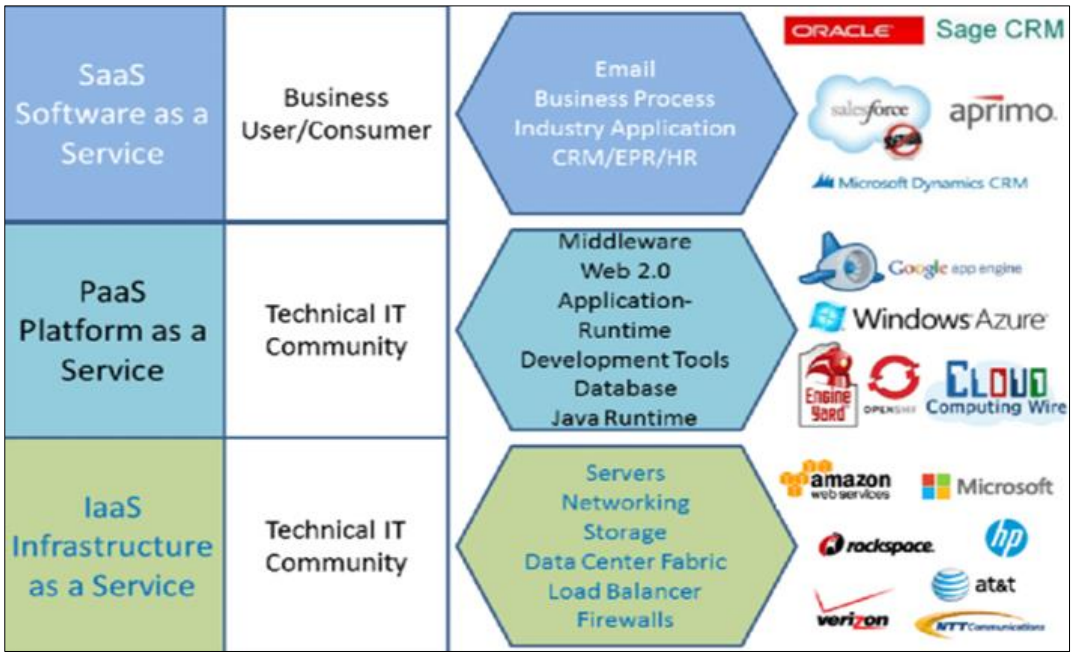

Figure 3 Cloud Computing Environment

2.2. Deployment Models

Cloud computing deployment models refer to the specific architecture and arrangement of cloud infrastructure, and they play a crucial role in determining the level of control, security, and customization a user or organization has over their cloud environment. As shown in Figure 4, the four main deployment models are public cloud, private cloud, hybrid cloud, and multi-cloud [33]-[37]. In a public cloud, services and resources are provided over the internet by third-party providers, offering a scalable and cost-effective solution for organizations without the need to manage their own infrastructure. Private clouds, on the other hand, are dedicated environments exclusively used by a single organization, providing greater control over security and customization but requiring more significant upfront investment and maintenance [38].

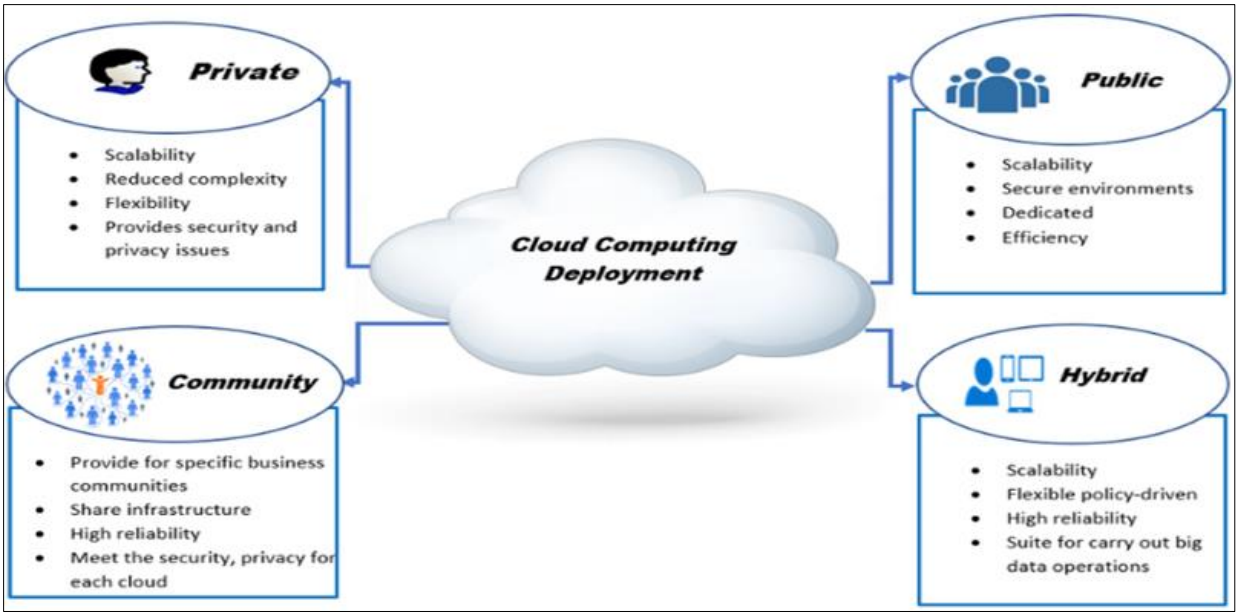

Figure 4 Cloud Deployment models

Hybrid clouds combine elements of both public and private clouds, allowing data and applications to be shared between them [39]. This model provides the flexibility to leverage the scalability of public clouds for non-sensitive operations

while keeping critical workloads in a more secure and controlled private cloud. Multicloud, often considered an extension of the hybrid model, involves using multiple cloud providers for different services or applications [40]. This approach mitigates vendor lock-in risks, provides redundancy, and allows organizations to choose the best-in-class services from various providers. The choice of a deployment model depends on factors such as security requirements, regulatory compliance, scalability needs, and the level of control desired by the organization.

3. Evolution of Cloud Computing

The evolution of cloud computing is marked by a transition from traditional on-premises data centres to remote, virtualized infrastructures. This evolution was driven by the need for greater scalability, cost-efficiency, and accessibility in computing resources. As the internet became more robust and widespread, it facilitated this shift, enabling organizations to access computing resources as needed without the high upfront costs of setting up and maintaining physical infrastructure [41]. Figure 5 depicts the evolution of cloud computing over the years. The evolution of cloud computing has been a transformative journey that has reshaped the way individuals and organizations manage and utilize computing resources. The concept of cloud computing can be traced back to the 1960s when mainframe computers were shared among multiple users, laying the foundation for the idea of resource sharing. However, the term "cloud computing" gained prominence in the mid-2000s when advancements in virtualization, broadband internet, and distributed computing technologies converged to enable scalable and on-demand access to computing resources.

The early 2000s saw the emergence of Infrastructure as a Service (IaaS) providers, offering virtualized computing resources over the internet. Amazon Web Services (AWS) played a pivotal role in popularizing the cloud computing model with the launch of Amazon Elastic Compute Cloud (EC2) in 2006. Following this, Platform as a Service (PaaS) and Software as a Service (SaaS) models evolved, providing more abstraction and simplifying the development and deployment of applications. Companies began to shift from traditional on-premises infrastructure to the cloud, leveraging its scalability, flexibility, and cost-efficiency. The evolution of cloud computing continued with the rise of containerization technologies, exemplified by Docker, and the orchestration tools like Kubernetes that facilitated the deployment and management of applications across diverse cloud environments. As cloud computing matured, emphasis grew on enhancing security, compliance, and governance measures to address concerns related to data protection and privacy.

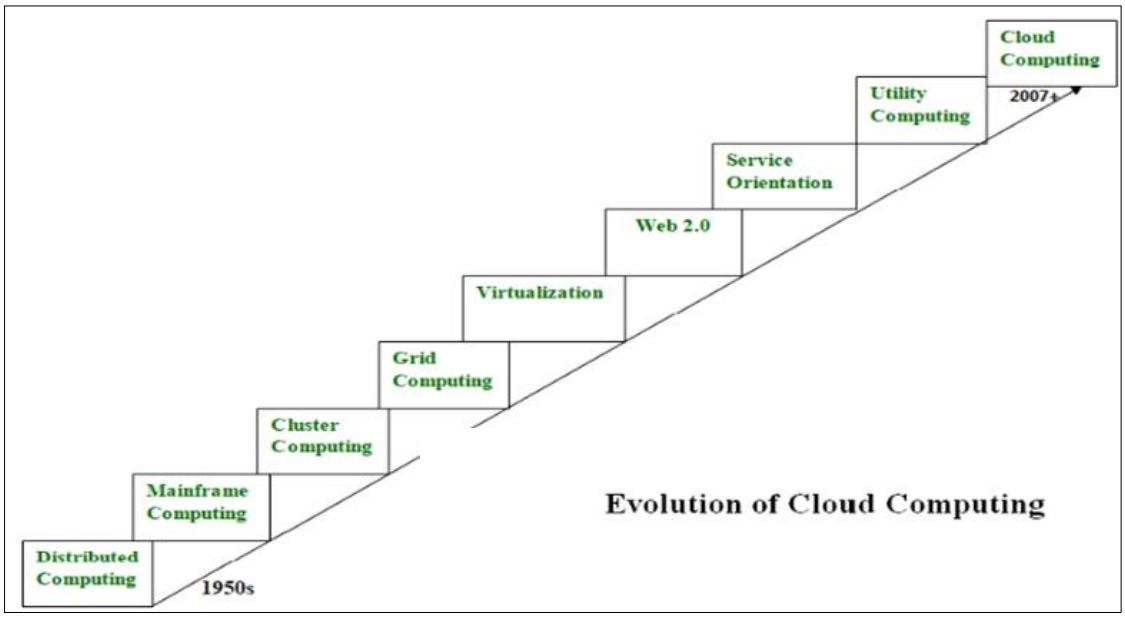

Figure 5 Evolution of cloud computing

The integration of artificial intelligence (AI) and machine learning (ML) into cloud services further augmented capabilities, enabling predictive analytics, automation, and improved decision-making. The ongoing evolution of cloud computing continues to be shaped by technological advancements, emerging use cases, and the evolving needs of a diverse range of industries.

4. Security in Traditional IT and Cloud Computing

Security in traditional IT systems primarily focuses on protecting physical assets and internal networks. In contrast, cloud computing security must account for data that travels over the public internet and resides on shared infrastructure owned and operated by third-party service providers [42]. This shift poses unique challenges, such as ensuring data privacy, securing data transfer and storage [43], and managing a shared responsibility model between cloud providers and users.

Security considerations in traditional IT environments and cloud computing differ in several key aspects, reflecting the distinct architectures and operational models of these two paradigms. In traditional IT setups, organizations typically invest heavily in on-premises infrastructure, where they have direct control and responsibility for securing servers, networks, and applications. This approach requires a robust perimeter defense strategy, often relying on firewalls, intrusion detection/prevention systems, and access controls to safeguard internal networks from external threats. Security measures are primarily hardware-centric, and organizations bear the responsibility for maintaining and updating all aspects of their infrastructure.In contrast, cloud computing introduces a shared responsibility model, where the cloud service provider (CSP) manages security of the cloud infrastructure, while the customer is responsible for securing their data, applications, and user access. Cloud security emphasizes a data-centric approach, incorporating encryption for data at rest and in transit, identity and access management (IAM) for controlling user permissions, and comprehensive logging and monitoring for real-time threat detection. Security in the cloud is dynamic and often employs automation and orchestration to respond rapidly to emerging threats. Additionally, the cloud's scalability allows for the implementation of advanced security services, such as distributed denial-of-service (DDoS) protection and threat intelligence, to be readily available on-demand.

Both traditional IT and cloud environments face common security challenges, such as the need to protect against malware, secure data storage, and ensure user authentication. However, cloud computing introduces new considerations, including shared resources in a multi-tenant environment, potential for misconfigurations, and reliance on the CSP's security measures. As organizations increasingly adopt hybrid and multicloud architectures, bridging the gap between traditional and cloud security becomes essential. This requires a comprehensive strategy that combines established security practices with cloud-native solutions, emphasizing the importance of continuous monitoring, regular audits, and adherence to industry compliance standards across the entire IT landscape.

5. Related Work

The evolution of cloud computing has revolutionized the way organizations manage and deploy their IT resources. However, with the increasing reliance on cloud services, there has been a parallel surge in security challenges. This literature review delves into various dimensions of security challenges in cloud computing, aiming to provide a comprehensive understanding of the current state of research in this field [46].

Researchers emphasize the need for strong IAM regulations to strike a balance between security and usability. Resilience and efficient incident response are crucial for reducing security issues, with proactive monitoring, quick detection, and clearly defined event response plans. International standards and regulatory compliance are also important aspects of cloud security, with the two most important parts being negotiating different regulatory frameworks and harmonizing international standards [47].

5.1. The Importance of Cloud Security

With the increasing adoption of cloud services for critical operations, the importance of robust security measures has become paramount [44]. Breaches can lead to significant financial losses, legal repercussions, and damage to reputation. Moreover, the evolving nature of threats in the cloud environment demands continuous vigilance and adaptation of security strategies.

The following sections of this paper delve into the specific security challenges posed by cloud computing, examining each in detail to provide a comprehensive understanding of the current security landscape and offering insights into effective mitigation strategies [45].

5.2. Data Security and Privacy

Data security and privacy are paramount concerns in cloud computing, given the nature of the cloud as a shared and remotely accessible infrastructure. Ensuring the confidentiality, integrity, and availability of data is crucial for both

service providers and users [48], [49]. Below are key challenges associated with data security and privacy in cloud computing.

5.3. Data Encryption

One major challenge is protecting data while it is being sent and stored, which calls for the use of strong encryption techniques. Although these algorithms are essential for protecting sensitive data, putting them into practice adds operational complexity and could affect system performance [50]-[55]. Adopting robust encryption solutions for data in transit and at rest is essential to properly addressing this situation. Furthermore, strengthening the entire data protection plan depends on guaranteeing the safe administration of encryption keys [56].

5.4. Access Control and Authentication

It is a constant challenge to manage the danger of unauthorized access to sensitive data. As shown in Figure 6, the assignment entails creating strong user authentication procedures and controlling access to cloud resources [57]-[61]. A diverse strategy is essential to effectively addressing these issues.

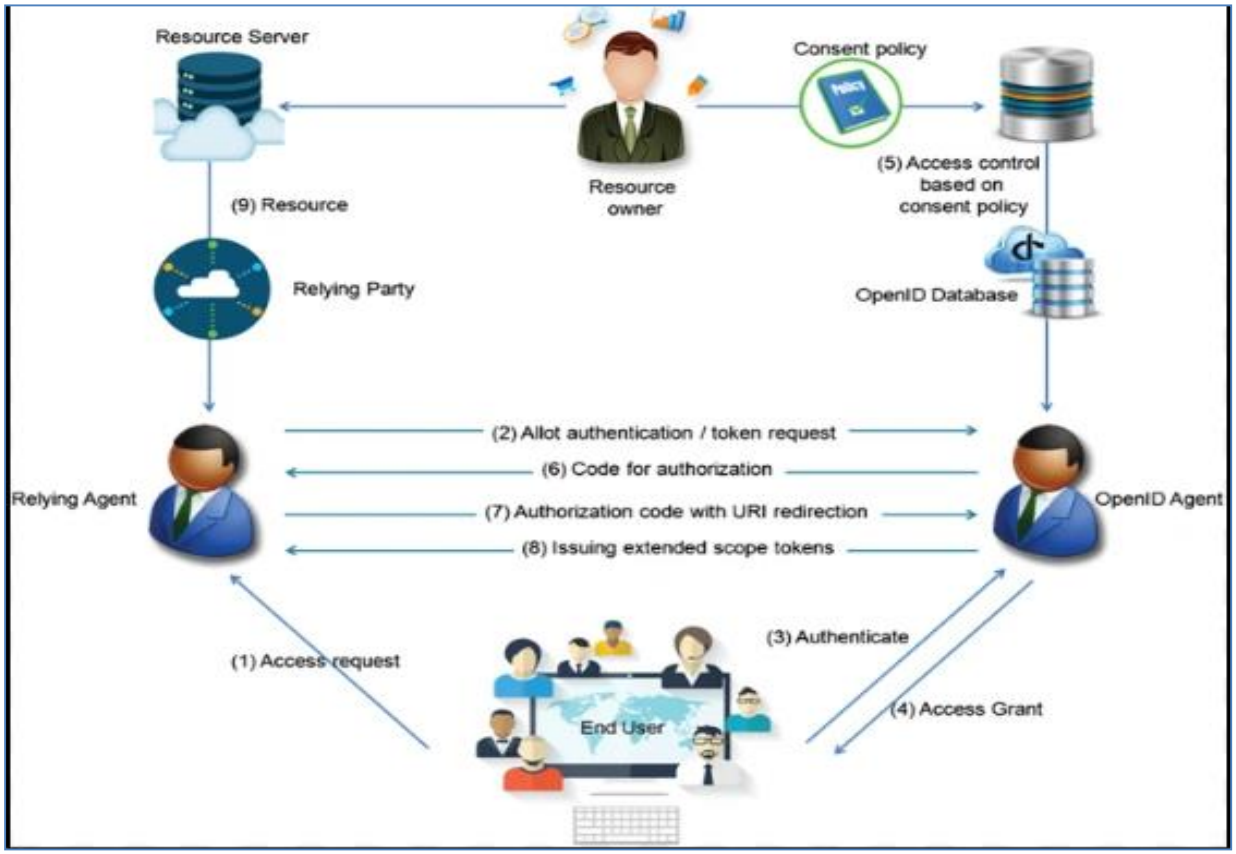

Figure 6 Access control and authentication in the cloud

This includes setting up role-based access control to customize permissions depending on user roles and implementing multi-factor authentication to add an additional layer of security. Regular access evaluations are also necessary to quickly detect and address any vulnerabilities and reduce the overall risk of unauthorized access [62].

5.5. Data Residency and Jurisdiction

Legal jurisdiction and data protection regulations compliance are raised by the difficulty of managing data residency in multiple geographic locations within the cloud context [63], [64]. It is crucial to carefully choose cloud service providers who comply with applicable data protection laws in order to address these concerns. Clearly stating data residency requirements in service level agreements with the selected providers is another essential component of the solution. This guarantees a proactive approach to compliance, reducing the possibility of legal issues and strengthening the observance of data protection laws.

5.6. Data Loss Prevention (DLP)

Data Loss Prevention (DLP) is a crucial strategy for protecting sensitive information from both intentional and unintentional disclosure. It involves using tools like activity monitoring and encryption to monitor and regulate the flow of sensitive data within the cloud environment [64]-[67]. Activity monitoring helps identify abnormal or unauthorized activities that could lead to data breaches, while encryption ensures data remains indecipherable even if accessed. By implementing comprehensive DLP solutions, businesses can strengthen their security posture and instil confidence in the protection of their valuable and confidential information [68].

5.7. Compliance and Regulations

Navigating the landscape of compliance and regulations poses a challenge for cloud users, who are obligated to adhere to diverse requirements like GDPR, HIPAA, and industry-specific standards [69]. Addressing this challenge requires a proactive approach, including staying abreast of pertinent regulations and collaborating with cloud providers that furnish compliant services. Moreover, the implementation of internal policies and procedures becomes imperative to ensure ongoing compliance, establishing a robust framework for meeting the multifaceted demands of regulatory environments [70].

5.8. Data Portability and Vendor Lock-in

Users who experience difficulty transferring data between cloud providers raise concerns regarding vendor lock-in and highlight the challenge of data portability. Selecting cloud services that actively promote data portability and conform to open standards is advised in order to solve this problem [71], [72]. Users can help to ensure more seamless data migration procedures by giving priority to these features. Furthermore, a clear exit strategy is necessary to reduce the risks associated with vendor lock-in and give users the flexibility and control they need to adjust to shifting business needs or preferences.

5.9. Incident Response and Forensics

The prompt and efficient [73] handling of security incidents assumes greater significance considering the difficulties in quickly detecting, responding to, and conducting forensic analysis in cloud environments. Figure 7 shows a typical automate incident response and forensics. In the event of a security incident, cloud-specific challenges may arise when gathering evidence.

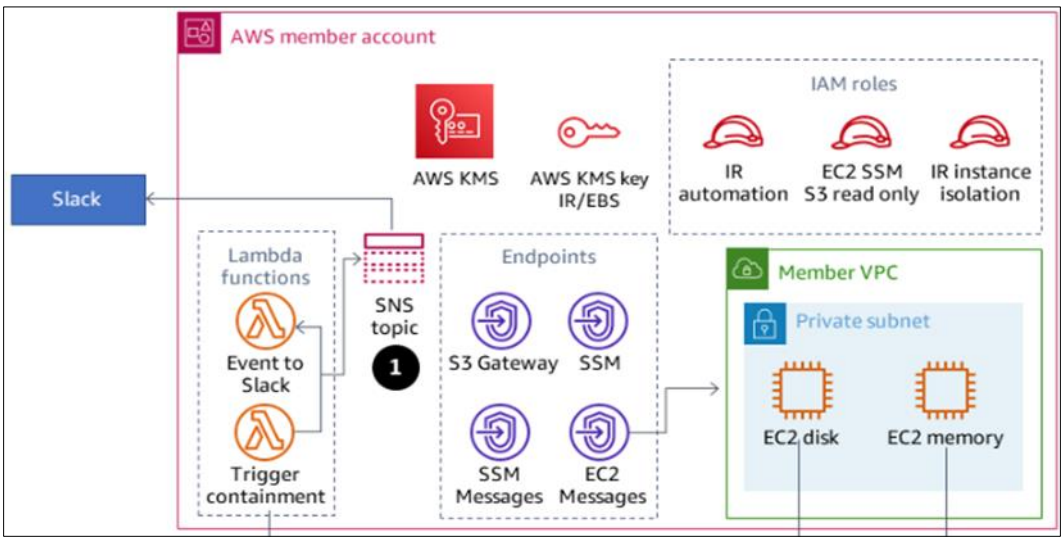

Figure 7 Cloud incident response and forensics

Creating and testing a customized incident response plan that is adapted to the specifics of cloud environments is crucial in order to address this [74], [75]. Close cooperation with the cloud provider is essential to a smooth incident investigation and resolution process, guaranteeing a planned and efficient method for managing security breaches and reducing possible harm [76], [77].

Therefore, a diversified strategy is needed to address the issues of data security and privacy in cloud computing. Strong encryption procedures, stringent access controls, adherence to compliance requirements, and constant monitoring and

reaction to security incidents are all requirements for organizations. As cloud computing develops, protecting the integrity and confidentiality of data [78] in the cloud will require applying best practices and staying aware of new threats.

6. Security Challenges in Cloud Computing

Cloud computing adoption has brought about many advantages, but it has also created a plethora of security challenges. The goal of this review of the literature is to group these difficulties into general categories, such as identity and access management, data security, network security, compliance and legal concerns, and emerging threats [79]-[83].

6.1. Data Security

Protecting confidential information in a shared environment is a complex task that requires a well-thought-out plan to guarantee the information's availability, confidentiality, and integrity. The challenges are in putting in place strong security measures that ensure data accuracy and dependability while also thwarting unwanted access [84]-[88]. It becomes essential to strike a balance between these crucial data security components in order to build a strong defense against potential threats and vulnerabilities in a shared environment [89].

6.2. Network Security

A number of issues in the field of network security require careful consideration. The protection of data while it is being transmitted is one of the most important issues, and strong encryption techniques are required to prevent illegal access or interception. Fortifying defences against a variety of network-based attacks, from sophisticated cyber threats to more common vulnerabilities, is another imperative [90]-[94]. Furthermore, maintaining strong network isolation is essential to preventing unauthorized parties from accessing confidential data. Comprehensive and flexible security measures must be put in place to address these issues and strengthen the confidentiality and integrity of data moving across the network [95].

6.3. Identity and Access Management

One of the main challenges in the field of Identity and Access Management (IAM) is managing user identities. This is managing and arranging user profiles and credentials in a system, which is a complex task. Proper authorization and authentication procedures must be guaranteed; this calls for strong protocols to confirm user identities and assign suitable access rights [96]-[100]. The problem also includes identity federation, which is the intricate process of organizing and simplifying user identities among various systems and domains. Maintaining the security and integrity of digital systems depends on successfully addressing these IAM challenges, which calls for the deployment of sophisticated authentication and authorization frameworks in addition to seamless identity federation solutions.

6.4. Compliance and Legal Issues

Organizations face a lot of difficulties when it comes to compliance and legal issues. One of the main issues is the necessity of making sure that a variety of laws controlling privacy and data security are followed. An important part of these challenges is managing data governance, which includes handling data in an ethical and responsible manner. Organizations that want to properly protect sensitive information must negotiate complex legal requirements. Completing industry-specific standards adds even more complexity, since various industries frequently have different requirements for compliance. Taking on these challenges requires a methodical approach that incorporates strong policies, procedures, and technologies in order to comply with regulatory requirements and maintain industry-specific standards for data governance [101].

7. Emerging Threats

Emerging threats constantly change the cybersecurity landscape, making it difficult for organizations to recognize and mitigate new risks in the ever-changing cloud environment. Malicious actors' strategies change along with technology, necessitating a proactive approach to cybersecurity [102]-[104]. To safeguard sensitive data and infrastructure, the difficulty is in keeping up with quickly changing threats, comprehending their subtleties, and putting in place efficient [105] countermeasures. In the constantly evolving digital landscape, organizations need to develop adaptable security strategies that use cutting-edge technologies and advanced threat intelligence to quickly identify and address emerging threats [106].

As a result, this literature review provides a thorough framework for comprehending the difficulties encountered by enterprises making the move to the cloud by methodically classifying the security issues related to cloud computing. The breadth of research presented in the literature review highlights the complexity of these issues and emphasizes the continued need for committed efforts to address them successfully. Because cloud computing is dynamic, it necessitates a constant commitment to addressing new threats and modifying security protocols [107]-[110]. Organizations must stay up to date on the most recent research findings as cloud technology advances in order to maintain a proactive security posture and robust defenses in cloud environments [111].

7.1. Data Security in Cloud Computing

A key component of cloud computing is data security, and different encryption techniques are essential for protecting sensitive data. Data is encrypted in order to render it unintelligible so that, in the event of unauthorized access, the data that has been intercepted cannot be decoded [112]-[116]. Because advanced encryption standards (AES) are reliable and effective at protecting data during processing, transmission, and storage, they are frequently used in cloud environments [117].

7.2. Maintaining data integrity

When it comes to cloud computing, one of the main worries is data integrity—keeping data reliable and unchangeable over the course of its existence. The significance of cryptographic hash functions in ensuring data integrity is emphasized by research in this field. By comparing the computed hash with the original, users can identify any unauthorized modifications to the data by using these functions to generate fixed-size hash values for the input data [118]-[122]. This method protects data integrity by thwarting nefarious changes made during transmission or storage [123].

7.3. Confidentiality

Another essential component of cloud data security is confidentiality. Maintaining the confidentiality of sensitive data is largely dependent on encryption, more especially end-to-end encryption [124], [125]. This technique lowers the possibility of unauthorized access during transmission and storage by guaranteeing that data is encrypted on the client side and stays encrypted until it reaches its intended recipient [126].

7.4. Authentication

Strong access controls and authentication procedures are just as important as encryption when it comes to cloud data storage security. User authentication procedures and access policies play a major role in limiting illegal access to data that is stored [127], [128]. The implementation of role-based access controls and multi-factor authentication is recommended in order to improve the security of stored data, according to research findings [129].

7.5. Secure transmission of data

In cloud computing, data transmission security is a major concern, particularly when data is moving across a network [130]-[134]. The protocols Transport Layer Security (TLS) and Secure Sockets Layer (SSL) are frequently used to create secure communication channels between cloud servers and clients. By ensuring that data is encrypted while in transit, these protocols reduce the possibility of illegal interception and eavesdropping [135].

7.6. Intrusion detection systems (IDS)

Systems for detecting intrusions (IDS) are crucial for protecting cloud environments from malicious activity. The development of advanced intrusion detection systems (IDS) specifically designed for cloud computing, which can recognize and react to unusual activity or possible security risks, has been the main focus of research. These systems help prevent security breaches from getting worse by identifying and resolving them before they have a chance to affect cloud infrastructures [135]-[138].

To sum up, cloud computing data security is a complex issue that calls for all-encompassing solutions. Security measures for data integrity, confidentiality, and encryption is essential for protecting data at every stage of its lifecycle. Advanced intrusion detection systems, access controls, authentication procedures, and encryption are also necessary for safe data processing, transmission, and storage. Ongoing investigations in these domains aid in the construction of strong security frameworks that guarantee the privacy, availability, and integrity of data in cloud computing settings [139].

7.7. Network Security in Cloud Computing

Ensuring the overall integrity and confidentiality of data in cloud computing requires securing the network architecture [140]. Several research works have examined this important factor, highlighting the necessity of strong security controls for cloud network environments. One area of particular emphasis is handling problems with data in transit, or the safe movement of data between various cloud infrastructure components [141]-[145].

7.8. Data protection in transit

Data protection in transit is a significant issue for cloud network security. Research emphasizes how crucial it is to use secure communication protocols in order to address this. The protocols known as Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are commonly used to create encrypted communication channels that protect data while it travels across the network. These protocols ensure the confidentiality of sensitive data by encrypting it during transmission, reducing the possibility of interception and eavesdropping [146]-[150].

7.9. Secure communication protocols

A key element of network security in cloud computing is the choice and application of suitable secure communication protocols. The results of research demonstrate how important it is to assess how well-suited, effective, and secure various protocols are to the particular needs of cloud environments [151]-[155]. This entails taking into account variables like the kind of data being transferred, how sensitive the information is, and how this will affect cloud network resource performance.

7.10. Network monitoring

Network monitoring becomes essential to preserving cloud environments' security. Real-time detection and reaction to possible security risks are facilitated by ongoing network activity monitoring and analysis [156], [157]. The creation of sophisticated network monitoring tools and methods specifically suited for cloud computing is the main area of research in this field. These applications are intended to help with timely responses to security incidents, identify anomalies, and offer insights into network traffic patterns [158].

7.11. Integrating intrusion detection and prevention systems

Furthermore, research emphasizes how crucial it is to incorporate intrusion detection and prevention systems into cloud network architectures. When it comes to spotting and stopping malicious activity that could jeopardize the security of the cloud infrastructure, these systems are essential. Intrusion detection systems improve the overall resilience [159] of the cloud network by proactively defending against potential threats through the use of complex algorithms and anomaly detection mechanisms.

In summary, the implementation of secure communication protocols addresses issues pertaining to data in transit as part of the process of securing the network architecture in cloud computing [160]-[162]. To guarantee the confidentiality and integrity of data in the cloud environment, meticulous protocol selection and ongoing network activity monitoring are crucial. Furthermore, the incorporation of intrusion detection and prevention systems strengthens the security posture as a whole, adding to the resilience of cloud computing's network security.

7.12. Identity and Access Management (IAM)

In the context of cloud computing, identity and access management (IAM) poses a number of issues that have been covered in-depth in the literature. The complexity brought about by the dynamic and scalable nature of cloud environments where users and resources are always changing is one of the main challenges. A major problem in such dynamic environments is the increased possibility of unauthorised access, therefore ensuring secure user authentication [163], [164]. Furthermore, efficient authorization systems are essential for controlling access to various cloud resources and services. The literature also emphasises how difficult it can be to safely manage identities in hybrid or multi-cloud environments when several platforms might have unique IAM frameworks. Strong answers are needed to address these issues.

Multi-factor authentication (MFA) and adaptive authentication schemes, which modify security measures in response to contextual circumstances, can be used to enable secure user authentication. By using policy-based methods and fine-grained access restrictions to effectively manage permissions, authorization issues can be lessened [165]. In order to provide centralised identity management and guarantee consistency across various cloud settings, efficient identity and access management (IAM) systems should also interface with Identity as a Service (IDaaS) platforms. In order to provide

a safe and well-managed cloud computing environment, the literature emphasises the necessity of comprehensive identification, authorization, and management (IAM) solutions [166].

7.13. Legal and Compliance Challenges

A great deal of research has been done on how the legal and regulatory environment is influencing cloud computing. The body of research highlights the various difficulties brought about by an intricate network of rules and legislation that affect the implementation and use of cloud services. Compliance concerns are especially prevalent, with foreign data transfer laws and data residency restrictions serving as important focal points [167]. The literature emphasises how difficult it may be to navigate the various and frequently incompatible data residency requirements, which require that particular data be kept within predetermined geographic limits. For cloud service providers hoping to deliver worldwide services while respecting regional legal systems, this presents a major obstacle.

Furthermore, the literature explores the complex world of international data transfer legislation, highlighting the necessity of adhering to different data protection standards, including the General Data Protection Regulation (GDPR) in the European Union. For example, the GDPR places strict limits on the international transmission of personal data. Because of this, cloud service providers must put strong safeguards in place to guarantee data security and privacy while transferring data across borders. The study delves into the possible obstacles linked to varying legal norms in different regions, necessitating cloud service providers to devise flexible approaches to fulfill diverse regulatory obligations [168].

It is evident that the literature highlights the difficulties with legality and compliance that cloud computing presents, especially when it comes to data residency and cross-border data transfers. Handling this complex environment requires a deep comprehension of local laws and the application of strong tactics to guarantee adherence while providing smooth and safe cloud services globally.

8. Emerging Threats and Technologies

The field of cloud computing security concerns has been the subject of significant recent literature that sheds light on the dynamic issues that have evolved in tandem with technology progress. Cloud computing security concerns are getting more complex, and researchers are finding new ways for bad actors to attack systems and launch attacks [169]. The body of research emphasizes how critical it is to deal with problems like denial-of-service assaults, unauthorized access, and data breaches, which are increasingly common and dangerous in cloud environments.

Concurrently, scholars have explored the assimilation of novel technologies as a preemptive measure to reinforce cloud security. In this context, research on artificial intelligence (AI) [170] and its applications to threat detection, anomaly identification, and predictive analysis is crucial. A subset of artificial intelligence called machine learning algorithms has great promise for improving cloud infrastructure resilience by enabling real-time security event detection and response.

The literature has also highlighted blockchain technology as a possible game-changer for cloud security. Blockchain's decentralized and immutable structure offers hope for safe and open cloud identity, access control, and data integrity management [171]-[175]. In order to build confidence and reduce the risks associated with centralized control, the research explores the viability and efficacy of incorporating blockchain into current cloud systems.

In summary, the literature examines the integration of cutting-edge technologies like blockchain and artificial intelligence (AI) to strengthen the resilience of cloud infrastructures while also providing a thorough picture of the changing security threats in cloud computing. The dynamic interaction of cutting-edge technology and new dangers highlights the necessity of ongoing study and development in the field of cloud security.

9. Synthesis of Findings

A review of the literature yields unique insights in the field of cloud computing security for a number of topic areas. The literature on Identity and Access Management (IAM) regularly highlights the difficulties brought about by cloud environments' dynamic nature, emphasising the significance of reliable authentication, authorization processes, and centralised identity management solutions. The difficulty of managing several, frequently incompatible regulations is a recurring theme in legal and compliance challenges, with an emphasis on foreign data transfer laws and data residency requirements in particular. There are two narratives that emerge when Emerging Threats and Technologies are integrated. On the one hand, research shows how sophisticated cloud security risks are becoming, including denial-of-service attacks and data breaches [176].

Conversely, there is a constant investigation of cutting-edge technologies as preventative steps to strengthen cloud security, such as blockchain and artificial intelligence. Overall, the synthesis identifies a recurring theme that highlights the necessity of creativity and adaptation to meet the changing security problems in cloud computing. The body of research continually emphasises how critical it is to keep up with new threats and use cutting-edge technologies to improve cloud infrastructure security and resilience.

10. Research Gaps and Future Directions

A comprehensive evaluation of the body of research on cloud computing security literature reveals some research gaps that point to areas that could be explored further. Identity and Access Management (IAM) difficulties are well covered in the literature; however, there is a noticeable knowledge gap regarding the efficaciousness and practical use of advanced IAM solutions, like multi-factor authentication [177] and adaptive authentication, in various cloud contexts. In addition, more research on the harmonisation of global regulatory frameworks and strategies for seamless compliance across jurisdictions would be beneficial for the Legal and Compliance Challenges thematic category, which while skilfully addressing the complexities of data residency and international data transfer regulations, could benefit from it [178], [179].

Regarding Emerging Threats and technology, the literature offers a thorough summary of how security threats are changing and how incorporating technology like blockchain and artificial intelligence [180] may benefit society. The evaluation of the resource implications and scalability of implementing these technologies in large-scale cloud infrastructures, however, is lacking in study. For practical adoption, it is essential to comprehend the obstacles and constraints associated with putting AI-driven threat detection and blockchain-based security measures into practice [181].

Future studies could use a mixed-methods approach, including qualitative and quantitative analyses, to fill up these research gaps. Comprehensive case studies of businesses deploying cutting-edge IAM solutions or handling challenging cloud-based legal compliance challenges are examples of qualitative research. Empirical evaluations of the performance impact and scalability of integrating developing technologies could be the main focus of quantitative research, offering insightful information about their viability in actual cloud systems.

Additionally, cooperative interdisciplinary research including legal professionals, computer scientists, and business professionals may help develop comprehensive answers. A dynamic picture of the topic could also be obtained through longitudinal studies that follow the development of security threats and related technical improvements over time. Finally, in order to close these gaps and create a more comprehensive and useful body of knowledge in this quickly developing field, future research in cloud computing security should focus on practical implementation challenges, harmonising regulatory landscapes, and conducting empirical assessments of emerging technologies [182].

11. Case studies

In this section, various case studies are investigated. The results highlight the diverse security challenges organizations face in cloud computing, ranging from misconfigurations and software vulnerabilities to supply chain attacks and DDoS incidents. The lessons learned from these cases emphasize the importance of proactive security measures, timely response, and effective communication with stakeholders to minimize the impact of security incidents in cloud environments [183]. Table 1: This table provides a concise overview of the security challenges, failures, and key findings from each case study.

Organizations navigating the landscape of cloud computing encounter a spectrum of security challenges that stem from the dynamic nature of the cloud environment. One significant challenge involves data breaches and unauthorized access, as the shared responsibility model requires robust identity and access management (IAM) practices to mitigate the risk of unauthorized users gaining access to sensitive information. Misconfigurations in cloud settings, often arising from human error, represent another prevalent challenge, as organizations grapple with the complexities of configuring and securing numerous cloud services. Additionally, the evolving threat landscape introduces concerns about the security of application programming interfaces (APIs), potential vulnerabilities in third-party integrations, and the need for constant vigilance against emerging cyber threats. Navigating these challenges requires a holistic approach that combines technological solutions, employee training, and adherence to stringent security protocols to ensure the confidentiality, integrity, and availability of data in the cloud.

Table 1 Analysis of the failures and findings

S. N	Case study	Security challenge	Failure	Key learnings
1	Capital One Data Breach	Misconfigured web application firewall (WAF) in AWS cloud environment	The misconfiguration allowed an attacker to gain unauthorised access to sensitive customer data	-Regularly review and audit cloud configuration to identify and remediate misconfigurations. -Implement automated security checks and compliance monitoring. -Follow the principle of least privilege (PoLP) for access control to minimize potential damage.
2	Dropbox Authentication Bug	-Software update introduced a bug, allowing any password to access any Dropbox account.	Inadequate testing of software updates resulted in a security vulnerability.	Thoroughly test software updates to identify and address potential vulnerabilities. -Have a well-defined incident response plan in place to respond to security incidents. -Maintain transparent communication with affected users during security incidents
3	Sony PlayStation network outage	Distributed denial of service (DDoS) attack and inadequate security measures.	Sony's security measures were insufficient to handle the scale of the DDoS attack, leading to a prolonged service outage	-Implement effective DDoS mitigation strategies, including traffic monitoring and resource scaling. -Communicate openly and transparently with users during service outages to maintain trust.
4	Adobe Systems Data Breach	Failure to promptly patch known vulnerabilities and secure internal systems.	Vulnerabilities in Adobe's infrastructure was exploited, resulting in a massive data breach.	Prioritize timely patch management and vulnerability assessments to protect cloud infrastructure. Develop and maintain a strong incident response plan. Implement encryption for sensitive data to mitigate risks
5	The GitHub Supply Chain Attack	Supply chain attack targeting the npm ecosystem	Malicious packages were published on npm, compromising developers' systems.	Organizations should employ strict software supply chain security practices, including code signing, package integrity verification, and monitoring for malicious activity in repositories.

12. Emerging technologies and future trends

Cloud computing is a dynamic and rapidly evolving field, and new security threats continually emerge as technology advances, these technologies and trends are likely to shape the landscape of cloud security in the coming years: Below is a comprehensive analysis of emerging threats based on existing literature [184]. Table 2 presents some of the emerging technologies for cloud security improvement.

Table 2 Emerging technologies and future trends

S.N	Technologies and trends.	Overview	Impact on Cloud Security
1	Zero Trust Security Model	This is an approach that assumes no trust within or outside an organization's network perimeter [185]. Every user, device, and application are treated as untrusted until proven otherwise.	Helps organizations secure access to cloud resources and protect data in multi-cloud environments.
2	Cloud-Native Security Tools	designed specifically for cloud environments and offer features like runtime protection, container security, and serverless security [186].	These tools provide enhanced security controls tailored to the dynamic nature of cloud platforms, helping organizations better protect their cloud-native applications and workloads.
3	AI-Driven Threat Detection and Response	Artificial intelligence and machine learning [187] are being used to detect and respond to security threats in real-time by analysing vast amounts of data for patterns and anomalies.	AI-driven threat detection and response enhance the ability to identify and mitigate cloud security threats rapidly
4	Cloud Security Posture Management (CSPM)	CSPM solutions offer continuous monitoring and assessment of cloud configurations to identify and remediate misconfigurations and security risks [188].	CSPM tools help organizations maintain a strong security posture in the cloud by proactively addressing configuration vulnerabilities.
5	Identity and Access Management (IAM) Enhancements	IAM solutions are evolving to provide more granular control over access, including continuous authentication and adaptive access policies [189].	Enhanced IAM capabilities improve access control and reduce the risk of unauthorized access to cloud resources
6	Homomorphic Encryption	Homomorphic encryption enables computation on 7encrypted data without decrypting it, preserving data privacy in cloud environments	Homomorphic encryption can enhance data security in cloud computing, allowing for secure processing of sensitive information [190].
7	Quantum-Safe Encryption	Quantum computing poses a threat to traditional encryption. Quantum-safe encryption algorithms are designed to withstand attacks from quantum computers [191].	As quantum computing matures, quantum-safe encryption will be essential to protect sensitive data stored in the cloud.
8	Cloud Security Automation and Orchestration	Automation and orchestration technologies are being used to streamline security processes, such as incident response and threat remediation [192].	Automation reduces response times and human error, improving overall cloud security posture.
9	Regulatory and Compliance Challenges.	Evolving data protection and privacy regulations, such as GDPR, CCPA, and emerging laws like the EU's Digital Markets Act, will continue to shape cloud security requirements [193].	Organizations must stay compliant with evolving regulations, requiring ongoing adjustments to cloud security strategies and practices.
10	Edge Computing Security	The growth of edge computing introduces new security challenges, such as securing edge devices, data transmission, and real-time threat detection	As edge computing becomes more prevalent, organizations must extend their security strategies to include edge environments and ensure data integrity and confidentiality [194].

11	Serverless Security	Serverless computing is gaining popularity, but it comes with unique security considerations, such as securing serverless functions and managing permissions [195].	Organizations must adopt security practices tailored to serverless architectures to protect cloud-native applications and functions.
12	Blockchain for Cloud Security	Blockchain technology is being explored for enhancing cloud security by providing immutable and tamper-resistant audit trails and securing digital identities [196].	Blockchain can enhance transparency and trust in cloud transactions and access control.

Emerging technologies and future trends are shaping the landscape of cloud security. Organizations need to stay informed about these developments and adapt their security strategies to address evolving challenges in cloud computing. Proactive measures, such as implementing zero trust security, leveraging cloud-native security tools, and embracing AI-driven threat detection, will be crucial to maintaining a strong security posture in the cloud. Additionally, compliance with regulatory requirements and a focus on emerging technologies like quantum-safe encryption and blockchain will be essential considerations in cloud security planning.

13. Solutions and best practices

These solutions and practices are designed to help organizations mitigate risks and enhance their overall security posture in the cloud [197]. Table 3 presents some of the recommended solutions and best practices.

Table 3 Summary of solutions and best practices

S.N	Solutions	Purpose	Best Practices
1	Implement a Zero Trust Security Model	Adopt a zero-trust approach that assumes no trust within or outside the network perimeter, verifying every user and device attempting to access resources.	Implement strong identity and access management (IAM) controls, employ continuous authentication, and enforce strict access policies based on the principle of least privilege (PoLP).
2	Multi-Factor Authentication (MFA)	Require multi-factor authentication for all users accessing cloud resources	Implement MFA for both user and administrative accounts to add an extra layer of security beyond passwords
3	Robust Access Control	Implement fine-grained access controls to limit user permissions and privileges.	Regularly review and update access policies, revoke unnecessary privileges, and follow the principle of least privilege (PoLP) to minimize potential damage from compromised accounts.
4	Regularly Audit and Monitor Configurations	Continuously audit and monitor cloud configurations to detect misconfigurations and security vulnerabilities.	Use cloud security posture management (CSPM) tools to assess and remediate misconfigurations, and implement automated compliance monitoring
5	Encrypt Data at Rest and in Transit	Implement encryption for data both at rest and in transit.	Use strong encryption algorithms and key management practices to protect sensitive data.
6	Cloud-Native Security Tools	Leverage cloud-native security tools and services provided by cloud service providers.	Utilize built-in security features such as AWS GuardDuty, Azure Security Center, and Google Cloud Security Command Center to enhance threat detection and response.
7	Continuous Security Testing	Implement continuous security testing, including vulnerability scanning and penetration testing.	Regularly scan cloud resources for vulnerabilities, conduct penetration tests, and promptly address identified security issues

8	Incident Response Plan	Develop and maintain an incident response plan tailored to cloud environments.	Ensure all team members are familiar with the incident response plan, conduct regular drills, and establish clear roles and responsibilities
9	Data Classification and Retention Policies	Implement data classification and retention policies to categorize data and define appropriate storage and access controls	Educate employees on data classification, enforce data retention policies, and regularly audit data storage and access
10	Cloud Security Education and Training	Provide ongoing security education and training to all employees and administrators.	Keep employees informed about security best practices, emerging threats, and the organization's security policies.
11	Supply Chain Security:	Assess and manage the security risks associated with third-party components and services.	Perform due diligence when selecting cloud providers and third-party services, conduct security assessments, and maintain vendor security agreements.
12	Backup and Disaster Recovery:	: Implement robust backup and disaster recovery strategies	Regularly back up critical data, test disaster recovery plans, and maintain offsite backups to ensure data availability in case of incidents
13	Compliance and Regulations	Stay informed about data protection and privacy regulations that apply to your organization.	Regularly assess your cloud environment for compliance, implement necessary controls, and maintain documentation to demonstrate compliance.
14	Security Awareness and Culture	Foster a security-aware culture within the organization.	Encourage employees to report security incidents, reward security-conscious behaviour, and conduct periodic security awareness training
15	Regular Security Updates	Keep cloud resources and applications up to date with security patches and updates.	Implement automated patch management processes and maintain an inventory of cloud assets to ensure timely updates.
16	Threat Intelligence	Stay informed about emerging threats and vulnerabilities.	Subscribe to threat intelligence feeds, participate in security information sharing communities, and use threat intelligence to inform security decisions
17	Cloud Governance and Compliance Frameworks	Implement cloud governance frameworks and compliance controls	Adopt industry-specific and cloud-specific compliance frameworks, such as CIS, NIST, or the Cloud Security Alliance's Cloud Controls Matrix (CCM), to guide security efforts.

Incorporating these solutions and best practices into your cloud security strategy can help address security challenges effectively and build a strong security foundation. The analysis of security challenges in cloud computing reveals several areas for future research. These include monitoring emerging threats and technologies, integrating machine learning and artificial intelligence in security, exploring blockchain technology for enhanced security, developing user-centric security solutions, ensuring regulatory compliance and international standards, quantifying the economic impact of security incidents, examining human factors contributing to security vulnerabilities, and examining ethical considerations in cloud security. Emerging threats and technologies, such as edge computing, quantum computing, and IoT, present both opportunities and challenges. The integration of machine learning and AI in security mechanisms presents both opportunities and challenges. Blockchain technology can be leveraged for secure data storage, decentralized identity management, and trust in multi-party transactions.

User-centric security solutions should prioritize the development of novel approaches to identity and access management, user authentication, and secure user interfaces. Regulatory compliance and international standards need further research to ensure compliance across diverse jurisdictions. Quantifying the economic impact of security

incidents is crucial for businesses and policymakers. Ethical considerations in cloud security practices, such as data privacy, responsible AI use, and ethical implications of security measures, are also important areas for future research.

14. Conclusion

The study highlights the complex landscape of cloud computing security challenges, emphasizing the need for a holistic and adaptive approach. The multi-faceted nature of security threats, from traditional data breaches to emerging threats like serverless architecture vulnerabilities, necessitates a comprehensive and adaptive security strategy. The shared responsibility model, a cornerstone of cloud security, emphasizes collaboration between service providers and customers to mitigate risks. Data encryption and privacy concerns are also highlighted, with robust encryption mechanisms for data at rest, in transit, and during processing. Identity and Access Management (IAM) is a key aspect of cloud security, balancing usability and security to prevent unauthorized access. Building resilience through redundancy, failover mechanisms, and robust incident response plans is crucial for minimizing security incidents. Continuous monitoring and compliance with industry standards and regulatory compliance are also essential for maintaining a secure posture. In conclusion, organizations must remain vigilant, adapt their security measures, and foster a culture of security awareness to effectively mitigate risks in the dynamic cloud computing landscape.

Compliance with ethical standard

Acknowledgement

All appreciation goes to my colleagues that supported me during the writing of this work.

Disclosure of conflict of interest

The author declares that she has no conflict of interest.

References

[1] Malallah HS, Qashi R, Abdulrahman LM, Omer MA, Yazdeen AA. Performance Analysis of Enterprise Cloud Computing: A Review. Journal of Applied Science and Technology Trends. 2023 Feb 5, 4(01):01-12.

[2] Gammelgaard B, Nowicka K. Next generation supply chain management: the impact of cloud computing. Journal of Enterprise Information Management. 2023 Mar 28.

[3] L'Esteve RC. New Horizons in Distributed Cloud Computing. InThe Cloud Leader's Handbook: Strategically Innovate, Transform, and Scale Organizations 2023 Jul 6 (pp. 123-134). Berkeley, CA: Apress.

[4] Ionescu SA, Diaconita V. Transforming Financial Decision-Making: The Interplay of AI, Cloud Computing and Advanced Data Management Technologies. International Journal of Computers Communications & Control. 2023 Oct 30, 18(6).

[5] Yang C, Huang Q, Li Z, Liu K, Hu F. Big Data and cloud computing: innovation opportunities and challenges. International Journal of Digital Earth. 2017 Jan 2, 10(1):13-53.

[6] Hussien ZA, Abdulmalik HA, Hussain MA, Nyangaresi VO, Ma J, Abduljabbar ZA, Abduljaleel IQ. Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. Applied Sciences. 2023 Jan, 13(2):691.

[7] Ahmad W, Rasool A, Javed AR, Baker T, Jalil Z. Cyber security in IoT-based cloud computing: A comprehensive survey. Electronics. 2021 Dec 22, 11(1):16.

[8] Dittakavi RS. Evaluating the Efficiency and Limitations of Configuration Strategies in Hybrid Cloud Environments. International Journal of Intelligent Automation and Computing. 2022 Nov 17, 5(2):29-45.

[9] Butt UA, Amin R, Mehmood M, Aldabbas H, Alharbi MT, Albaqami N. Cloud security threats and solutions: A survey. Wireless Personal Communications. 2023 Jan, 128(1):387-413.

[10] Chauhan M, Shiaeles S. An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. Network. 2023 Sep 12, 3(3):422-50.

[11] Ranaweera P, Jurcut AD, Liyanage M. Survey on multi-access edge computing security and privacy. IEEE Communications Surveys & Tutorials. 2021 Feb 26, 23(2):1078-124.

[12] Tiwari S, Bhatt C. A Comprehensive Study on Cloud Computing: Architecture, Load Balancing, Task Scheduling and Meta-Heuristic Optimization. InInternational Conference on Intelligent Cyber Physical Systems and Internet of Things 2022 Aug 11 (pp. 137-162). Cham: Springer International Publishing.

[13] Nyangaresi VO. Provably secure authentication protocol for traffic exchanges in unmanned aerial vehicles. High-Confidence Computing. 2023 Sep 15:100154.

[14] Mostafa AM, Ezz M, Elbashir MK, Alruily M, Hamouda E, Alsarhani M, Said W. Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud User Authentication. Applied Sciences. 2023 Sep 30, 13(19):10871.

[15] Ibrokhimov S, Hui KL, Al-Absi AA, Sain M. Multi-factor authentication in cyber physical system: A state of art survey. In2019 21st international conference on advanced communication technology (ICACT) 2019 Feb 17 (pp. 279-284). IEEE.

[16] Saranya N, Sakthivadivel M, Karthikeyan G, Rajkumar R. Securing the cloud: an empirical study on best practices for ensuring data privacy and protection. International Journal of Engineering and Management Research. 2023 Apr 10, 13(2):46-9.

[17] Sunday AE, Olufunminiyi OE. An Efficient Data Protection for Cloud Storage Through Encryption. International Journal of Advanced Networking and Applications. 2023 Mar 1, 14(5):5609-18.

[18] Pratyush K, Prasad VK, Mehta R, Bhavsar M. A Secure Mechanism for Safeguarding Cloud Infrastructure. InInternational Conference on Advancements in Smart Computing and Information Security 2022 Nov 25 (pp. 144-158). Cham: Springer Nature Switzerland.

[19] Umran SM, Lu S, Abduljabbar ZA, Nyangaresi VO. Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry. Internet of Things. 2023 Dec 1, 24:100969.

[20] Welsh T, Benkhelifa E. On resilience in cloud computing: A survey of techniques across the cloud domain. ACM Computing Surveys (CSUR). 2020 May 28, 53(3):1-36.

[21] Oladoyinbo TO, Adebiyi OO, Ugonnia JC, Olaniyi O, Okunleye OJ. Evaluating and establishing baseline security requirements in cloud computing: an enterprise risk management approach. Available at SSRN 4612909. 2023 Oct 25.

[22] Shamshirband S, Fathi M, Chronopoulos AT, Montieri A, Palumbo F, Pescapè A. Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues. Journal of Information Security and Applications. 2020 Dec 1, 55:102582.

[23] Lalitha P, Yamaganti R. Investigation Into Security Challenges and Approaches in Cloud Computing. Journal of Engineering Sciences. 2023, 14(08).

[24] Haghnegahdar L, Joshi SS, Dahotre NB. From IoT-based cloud manufacturing approach to intelligent additive manufacturing: Industrial Internet of Things—An overview. The International Journal of Advanced Manufacturing Technology. 2022 Mar 1:1-8.

[25] Nyangaresi VO. Extended Chebyshev Chaotic Map Based Message Verification Protocol for Wireless Surveillance Systems. InComputer Vision and Robotics: Proceedings of CVR 2022 2023 Apr 28 (pp. 503-516). Singapore: Springer Nature Singapore.

[26] Jawed MS, Sajid M. A comprehensive survey on cloud computing: architecture, tools, technologies, and open issues. International Journal of Cloud Applications and Computing (IJCAC). 2022 Jan 1, 12(1):1-33.

[27] Qi W, Sun M, Hosseini SR. Facilitating big-data management in modern business and organizations using cloud computing: a comprehensive study. Journal of Management & Organization. 2023 Jul, 29(4):697-723.

[28] Samha AK. Strategies for efficient resource management in federated cloud environments supporting Infrastructure as a Service (IaaS). Journal of Engineering Research. 2023 Oct 31.

[29] Di Orio G, Maló P. Providing the Key Ingredients of an Edge PaaS for Supporting and Facilitating the Development of Smart Energy Applications. InAPCA International Conference on Automatic Control and Soft Computing 2022 Jul 2 (pp. 142-154). Cham: Springer International Publishing.

[30] Rana ME, Mothi V. Cloud Computing as an Enabler in the Mobile Application Domain. In2022 International Conference on Data Analytics for Business and Industry (ICDABI) 2022 Oct 25 (pp. 184-189). IEEE.

[31] Nyangaresi VO, Abood EW, Abduljabbar ZA, Al Sibahe MA. Energy Efficient WSN Sink-Cloud Server Authentication Protocol. In2021 5th International Conference on Information Systems and Computer Networks (ISCON) 2021 Oct 22 (pp. 1-6).

[32] Seifert M, Kuehnel S, Sackmann S. Hybrid Clouds Arising from Software as a Service Adoption: Challenges, Solutions, and Future Research Directions. ACM Computing Surveys. 2023 Feb 9, 55(11):1-35.

[33] Zhao W, Yue S, Fei M, Chen R, Wei L. A new cloud computing deployment model: Proprietary cloud. InInternational Conference On Signal And Information Processing, Networking And Computers 2022 Sep 6 (pp. 130-137). Singapore: Springer Nature Singapore.

[34] Komar R, Patil A. Emerging Trends in Cloud Computing: A Comprehensive Analysis of Deployment Models and Service Models for Scalability, Flexibility, and Security Enhancements. Journal of Intelligent Systems and Applied Data Science. 2023 Jul 15, 1(1).

[35] Zheng Q, Gu D, Liang C, Fang Y. Impact of a firm's physical and knowledge capital intensities on its selection of a cloud computing deployment model. Information & Management. 2020 Nov 1, 57(7):103259.

[36] Stupar I, Huljenic D. Model-based cloud service deployment optimisation method for minimisation of application service operational cost. Journal of Cloud Computing. 2023 Dec, 12(1):1-32.

[37] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA. Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment. InApplied Cryptography in Computer and Communications: Second EAI International Conference, AC3 2022, Virtual Event, May 14-15, 2022, Proceedings 2022 Oct 6 (pp. 46-64). Cham: Springer Nature Switzerland.

[38] Gagged G, Murugaiyan J. Improved secure dynamic bit standard technique for a private cloud platform to address security challenges. Journal of Electronic Imaging. 2023 Jul 1, 32(4):042104-.

[39] Deb M, Choudhury A. Hybrid cloud: A new paradigm in cloud computing. Machine Learning Techniques and Analytics for Cloud Security. 2021 Dec 21:1-23.

[40] Heilig L, Lalla-Ruiz E, Voß S. Modeling and solving cloud service purchasing in multi-cloud environments. Expert systems with applications. 2020 Jun 1, 147:113165.

[41] Ghandour O, El Kafhali S, Hanini M. Computing Resources Scalability Performance Analysis in Cloud Computing Data Center. Journal of Grid Computing. 2023 Dec, 21(4):61.

[42] Singh UK, Sharma A, Singh SK, Tomar PS, Dixit K, Upreti K. Security and privacy aspect of cyber physical systems. InCyber Physical Systems 2023 Jan 11 (pp. 141-164). Chapman and Hall/CRC.

[43] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1, 142:103117.

[44] Abdel-Rahman M. Advanced Cybersecurity Measures in IT Service Operations and Their Crucial Role in Safeguarding Enterprise Data in a Connected World. Eigenpub Review of Science and Technology. 2023 Jul 15, 7(1):138-58.

[45] Suganya M, Prabha T. A Comprehensive Analysis of Data Breaches and Data Security Challenges in Cloud Environment. Available at SSRN 4111762. 2022 Apr 8.

[46] Rana NP, Slade EL, Sahu GP, Kizgin H, Singh N, Dey B, Gutierrez A, Dwivedi YK. Digital and social media marketing. Springer, 2020.

[47] Kim D, Kim KS. Privacy-preserving public auditing for shared cloud data with secure group management. IEEE Access. 2022 Apr 22, 10:44212-23.

[48] Kansal M, Singh P, Singh MK, Varshney S. A Systematic Study of Services and Security Model in Cloud Computing: A Brief Overview. Convergence of Cloud Computing, AI, and Agricultural Science. 2023:1-6.

[49] Al-Chaab W, Abduljabbar ZA, Abood EW, Nyangaresi VO, Mohammed HM, Ma J. Secure and Low-Complexity Medical Image Exchange Based on Compressive Sensing and LSB Audio Steganography. Informatica. 2023 May 31, 47(6).

[50] Gupta I, Singh AK. A holistic view on data protection for sharing, communicating, and computing environments: Taxonomy and future directions. arXiv preprint arXiv:2202.11965. 2022 Feb 24.

[51] Rasori M, La Manna M, Perazzo P, Dini G. A survey on attribute-based encryption schemes suitable for the internet of things. IEEE Internet of Things Journal. 2022 Feb 25, 9(11):8269-90.

[52] Gupta R, Gupta I, Singh AK, Saxena D, Lee CN. An iot-centric data protection method for preserving security and privacy in cloud. IEEE Systems Journal. 2022 Nov 23.

[53] Saleh M, Jhanjhi NZ, Abdullah A, Saher R. Proposing encryption selection model for IoT devices based on IoT device design. In2022 24th International Conference on Advanced Communication Technology (ICACT) 2022 Feb 13 (pp. 210-219). IEEE.

[54] Razzaq A. Blockchain-based secure data transmission for internet of underwater things. Cluster Computing. 2022 Dec, 25(6):4495-514.

[55] Nyangaresi VO. Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. InProceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 2023 Feb 23 (pp. 797-816). Singapore: Springer Nature Singapore.

[56] Banasode PS, Padmannavar S. Protecting and Securing Sensitive Data in a Big Data Using Encryption. EAI Endorsed Transactions on Smart Cities. 2020 Apr 17, 4(11):e5-.

[57] Khan AR, Alnwihel LK. A Brief Review on Cloud Computing Authentication Frameworks. Engineering, Technology & Applied Science Research. 2023 Feb 5, 13(1):9997-10004.

[58] Mohammad A. Distributed Authentication and Authorization Models in Cloud Computing Systems: A Literature Review. Journal of Cybersecurity and Privacy. 2022 Mar 4, 2(1):107-23.

[59] Ghori MR, Ahmed AA. Review of access control mechanisms in cloud computing. InJournal of Physics: Conference Series 2018 Jul 1 (Vol. 1049, No. 1, p. 012092). IOP Publishing.

[60] Qadir GA, Hussan BK. A An Authentication and Access Control Model for Healthcare based Cloud Services. Journal of Engineering. 2023 Mar 1, 29(3):15-26.

[61] Abduljaleel IQ, Abduljabbar ZA, Al Sibahee MA, Ghrabat MJ, Ma J, Nyangaresi VO. A Lightweight Hybrid Scheme for Hiding Text Messages in Colour Images Using LSB, Lah Transform and Chaotic Techniques. Journal of Sensor and Actuator Networks. 2022 Dec, 11(4):66.

[62] Saravanan N, Umamakeswari A. Lattice based access control for protecting user data in cloud environments with hybrid security. Computers & Security. 2021 Jan 1, 100:102074.

[63] Gharote M, Mondal S, Roy S, Sahu P, Ramamurthy A. Decision support framework for data residency compliance in cloud. CSI Transactions on ICT. 2022 Mar, 10(1):61-9.

[64] Turobova GO, Djangazova QA, Ganikhodjayeva DZ. Data Loss Prevention and Challenges Faced in Their Deployments. Oriental renaissance: Innovative, educational, natural and social sciences. 2021, 1(9):176-82.

[65] Stallings W. Data loss prevention as a privacy-enhancing technology. Journal of Data Protection & Privacy. 2020 Jun 1, 3(3):323-33.

[66] Alsuwaie MA, Habibnia B, Gladyshev P. Data Leakage Prevention Adoption Model & DLP Maturity Level Assessment. In2021 International Symposium on Computer Science and Intelligent Controls (ISCSIC) 2021 Nov 12 (pp. 396-405). IEEE.

[67] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1, 133:102763.

[68] Selvan MP, Sowmith RS, Dheeraj P, Jancy S. High Secured Data Access and Leakage Detection Using Attribute-Based Encryption. InAdvances in Electronics, Communication and Computing: Select Proceedings of ETAEERE 2020 2021 (pp. 433-445). Springer Singapore.

[69] Apeh AJ, Hassan AO, Oyewole OO, Fakeyede OG, Okeleke PA, Adaramodu OR. GRC Strategies in Modern Cloud Infrastructures: A Review of Compliance Challenges. Computer Science & IT Research Journal. 2023 Nov 25, 4(2):111-25.

[70] Mexmonov S. The role of the internal audit based international internal audit standards in Uzbekistan. Архив научных исследований. 2020 Sep 19, 33(1).

[71] Kumar P, Kumar P. Vendor Lock-In Situation and Threats in Cloud Computing. International Journal of Innovative Science and Research Technology. 2022, 7(9).

[72] Opara-Martins J. Taxonomy of cloud lock-in challenges. Mobile computing-technology and applications. 2018 May 30.

[73] Eid MM, Arunachalam R, Sorathiya V, Lavadiya S, Patel SK, Parmar J, Delwar TS, Ryu JY, Nyangaresi VO, Zaki Rashed AN. QAM receiver based on light amplifiers measured with effective role of optical coherent duobinary transmitter. Journal of Optical Communications. 2022 Jan 17(0).

[74] Manral B, Somani G, Choo KK, Conti M, Gaur MS. A systematic survey on cloud forensics challenges, solutions, and future directions. ACM Computing Surveys (CSUR). 2019 Nov 14, 52(6):1-38.

[75] Abiodun OI, Alawida M, Omolara AE, Alabdulatif A. Data provenance for cloud forensic investigations, security, challenges, solutions and future perspectives: A survey. Journal of King Saud University-Computer and Information Sciences. 2022 Oct 25.

[76] Rajendran S, Valarmathi A, Kumar MS. Threat Detection and Incident Response in Cloud Security. InPrivacy and Security Challenges in Cloud Computing 2022 Mar 14 (pp. 207-227). CRC Press.

[77] Yenugula M, Sahoo S, Goswami S. Cloud computing in supply chain management: Exploring the relationship. Management Science Letters. 2023, 13(3):193-210.

[78] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[79] Alenizi BA, Humayun M, Jhanjhi NZ. Security and privacy issues in cloud computing. InJournal of Physics: Conference Series 2021 Aug 1 (Vol. 1979, No. 1, p. 012038). IOP Publishing.

[80] Thabit F, Alhomdy SA, Alahdal A, Jagtap SB. Exploration of security challenges in cloud computing: Issues, threats, and attacks with their alleviating techniques. Journal of Information and Computational Science. 2020 Dec 2, 12(10).

[81] Osmani NM, Fatima S, Ansari A, Bari MA. Cloud Computing Security Challenges, Threats and Vulnerabilities. Mathematical Statistician and Engineering Applications. 2023 Jan 12, 72(1):1446-54.

[82] Akbar H, Zubair M, Malik MS. The Security Issues and challenges in Cloud Computing. International Journal for Electronic Crime Investigation. 2023 Mar 3, 7(1):13-32.

[83] Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA, Nyangaresi VO, Honi DG, Abdulsada AI, Jiao X. Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. IEEE Access. 2022 Feb 11, 10:26257-70.

[84] Javaid M, Haleem A, Singh RP, Suman R. Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. Cyber Security and Applications. 2023 Mar 11:100016.

[85] Arulprakash M, Jebakumar R. People-centric collective intelligence: decentralized and enhanced privacy mobile crowd sensing based on blockchain. The Journal of Supercomputing. 2021 Nov 1:1-27.

[86] Rajadevi R, Venkatachalam K, Masud M, AlZain MA, Abouhawwash M. Proof of Activity Protocol for IoMT Data Security. Computer Systems Science & Engineering. 2023 Jan 1, 44(1).

[87] Naim A, Alqahtani H, Muniasamy A, Bilfaqih SM, Mahveen R, Mahjabeen R. Applications of Information Systems and Data Security in Marketing Management. InFraud Prevention, Confidentiality, and Data Security for Modern Businesses 2023 (pp. 57-83). IGI Global.

[88] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[89] Talib AM. Ensuring security, confidentiality and fine-grained data access control of cloud data storage implementation environment. Journal of Information Security. 2015 Mar 12, 6(02):118.

[90] Steingartner W, Galinec D, Kozina A. Threat defense: Cyber deception approach and education for resilience in hybrid threats model. Symmetry. 2021 Apr 3, 13(4):597.

[91] James E, Rabbi F. Fortifying the IoT Landscape: Strategies to Counter Security Risks in Connected Systems. Tensorgate Journal of Sustainable Technology and Infrastructure for Developing Countries. 2023 Jan 9, 6(1):32-46.

[92] Tariq U, Ahmed I, Khan MA, Bashir AK. Fortifying IoT against crimpling cyber-attacks: a systematic review. Karbala International Journal of Modern Science. 2023, 9(4):9.

[93] Karyemsetty N, Narasimha PB, Tejaswi MP, Sivaji VN, Kamal CL, Samatha B. Cybersecurity Fortification in Edge Computing through the Synergy of Deep Learning. In2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) 2023 Oct 11 (pp. 1154-1160). IEEE.

[94] Abduljabbar ZA, Omollo Nyangaresi V, Al Sibahee MA, Ghrabat MJ, Ma J, Qays Abduljaleel I, Aldarwish AJ. Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks. Journal of Sensor and Actuator Networks. 2022 Sep 19, 11(3):55.

[95] Udipi S. The event data management problem: getting the most from network detection and response. Network Security. 2021 Jan, 2021(1):12-4.

[96] Mihailescu MI, Nita SL. A searchable encryption scheme with biometric authentication and authorization for cloud environments. Cryptography. 2022 Feb 14, 6(1):8.

[97] Esposito C, Ficco M, Gupta BB. Blockchain-based authentication and authorization for smart city applications. Information Processing & Management. 2021 Mar 1, 58(2):102468.

[98] Ghaffari F, Bertin E, Crespi N, Hatin J. Distributed ledger technologies for authentication and access control in networking applications: A comprehensive survey. Computer Science Review. 2023 Nov 1, 50:100590.

[99] Cha SC, Meng W, Li WW, Yeh KH. A blockchain-enabled IoT auditing management system complying with ISO/IEC 15408-2. Computers & Industrial Engineering. 2023 Apr 1, 178:109091.

[100] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[101] Milakovich ME. Digital governance: Applying advanced technologies to improve public service. Routledge, 2021 Sep 27.

[102] Dillon R, Lothian P, Grewal S, Pereira D, Kuah A. Cyber Security: Evolving Threats in an Ever Changing World. InDigital Transformation in a Post-Covid World: Sustainable Innovation, Disruption and Change 2021 Oct 3 (pp. 129-154). CRC Press.

[103] Akinrolabu O, Nurse JR, Martin A, New S. Cyber risk assessment in cloud provider environments: Current models and future needs. Computers & Security. 2019 Nov 1, 87:101600.

[104] Safitra MF, Lubis M, Fakhrurroja H. Counterattacking cyber threats: A framework for the future of cybersecurity. Sustainability. 2023 Sep 6, 15(18):13369.

[105] Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Spatial single mode laser source interaction with measured pulse based parabolic index multimode fiber. Journal of Optical Communications. 2022 Jun 21.

[106] Möller DP. Threats and Threat Intelligence. InGuide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices 2023 Apr 19 (pp. 71-129). Cham: Springer Nature Switzerland.

[107] Jarrott SE, Leedahl SN, Shovali TE, De Fries C, DelPo A, Estus E, Gangji C, Hasche L, Juris J, MacInnes R, Schilz M. Intergenerational programming during the pandemic: Transformation during (constantly) changing times. Journal of Social Issues. 2022 Dec, 78(4):1038-65.

[108] Mughal AA. Cybersecurity Hygiene in the Era of Internet of Things (IoT): Best Practices and Challenges. Applied Research in Artificial Intelligence and Cloud Computing. 2019 Jan 12, 2(1):1-31.

[109] Kokoris-Kogias E, Jovanovic P, Gasser L, Gailly N, Syta E, Ford B. Omniledger: A secure, scale-out, decentralized ledger via sharding. In2018 IEEE symposium on security and privacy (SP) 2018 May 20 (pp. 583-598). IEEE.

[110] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[111] Anusha T, Prathusha B, Chandra JV. Challenges and Defenses for Network and Cloud Security from Risks, Threats and Attacks in Cloud Computing. International Journal of Advanced Research in Computer Science. 2017 Nov 1, 8(9).

[112] Dakhare BS, Ragha LL. Securing Logistic Regression Model from Data Poisoning Attack using AES and RSA Encryption Techniques. In2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS) 2023 Aug 23 (pp. 1246-1253). IEEE.

[113] Ventre D, Guillot P. Electronic Communication Interception Technologies and Issues of Power. John Wiley & Sons, 2023 Sep 1.

[114] Yawalkar PM, Paithankar DN, Pabale AR, Kolhe RV, William P. Integrated identity and auditing management using blockchain mechanism. Measurement: Sensors. 2023 Jun 1, 27:100732.

[115] Prabha C, Sharma N, Singh J, Sharma A, Mittal A. A Review of Cyber Security in Cryptography: Services, Attacks, and Key Approach. In2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS) 2023 Feb 2 (pp. 1300-1306). IEEE.

[116] Nyangaresi VO, Abd-Elnaby M, Eid MM, Nabih Zaki Rashed A. Trusted authority based session key agreement and authentication algorithm for smart grid networks. Transactions on Emerging Telecommunications Technologies. 2022 Sep, 33(9):e4528.

[117] Durga R, Tamilselvi P. Detailed Review on Different Encryption Standards on Improved Cloud Data Security. Journal of Advanced Research in Dynamical & Control Systems. 2020 Mar, 12(4).

[118] Joy J, Devaraju S. Ensuring Data Integrity And Security In Diverse Cloud Environments To Prevent Duplicacy. Tuijin Jishu/Journal of Propulsion Technology. 2023 Nov 11, 44(4):4803-15.

[119] Mohammed SD, Rahma AM, Hasan TM. Maintaining the Integrity of Encrypted Data by Using the Improving Hash Function Based on GF (2 8). TEM Journal. 2020 Aug 1, 9(3).

[120] Fomichev V, Bobrovskiy D, Koreneva A, Nabiev T, Zadorozhny D. Data integrity algorithm based on additive generators and hash function. Journal of Computer Virology and Hacking Techniques. 2022 Mar, 18(1):31-41.

[121] Hanif F, Waheed U, Shams R, Shareef A. GAHBT: Genetic-Based Hashing Algorithm for Managing and Validating Health Data Integrity in Blockchain Technology. Blockchain in Healthcare Today. 2023, 6.

[122] Abood EW, Abdullah AM, Al Sibahe MA, Abduljabbar ZA, Nyangaresi VO, Kalafy SA, Ghrabta MJ. Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. Bulletin of Electrical Engineering and Informatics. 2022 Feb 1, 11(1):185-94.

[123] Thangavel M, Varalakshmi P. Enabling ternary hash tree based integrity verification for secure cloud data storage. IEEE Transactions on Knowledge and Data Engineering. 2019 Jun 12, 32(12):2351-62.

[124] Dechand S, Naiakshina A, Danilova A, Smith M. In encryption we don't trust: The effect of end-to-end encryption to the masses on user perception. In2019 IEEE European symposium on security and privacy (EuroS&P) 2019 Jun 17 (pp. 401-415). IEEE.

[125] Burkhalter L, Küchler N, Viand A, Shafagh H, Hithnawi A. Zeph: Cryptographic enforcement of end-to-end data privacy. In15th {USENIX} Symposium on Operating Systems Design and Implementation ({OSDI} 21) 2021 (pp. 387-404).

[126] Raja J, Ramakrishnan M. Confidentiality-preserving based on attribute encryption using auditable access during encrypted records in cloud location. The Journal of Supercomputing. 2020 Aug, 76:6026-39.

[127] Ayedh M AT, Wahab AW, Idris MY. Systematic Literature Review on Security Access Control Policies and Techniques Based on Privacy Requirements in a BYOD Environment: State of the Art and Future Directions. Applied Sciences. 2023 Jul 10, 13(14):8048.

[128] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1, 15:100210.

[129] Pathan A, Ingle MD. Security Provision for Data Stored in Cloud Using Decentralized Access Control with Anonymous Authentication. International Journal of Computer Applications. 2016, 146(12).

[130] Stergiou CL, Plageras AP, Psannis KE, Gupta BB. Secure machine learning scenario from big data in cloud computing via internet of things network. Handbook of Computer Networks and Cyber Security: Principles and Paradigms. 2020:525-54.

[131] Tabassum N, Reddyy CR. Review on QoS and security challenges associated with the internet of vehicles in cloud computing. Measurement: Sensors. 2023 Jun 1, 27:100562.

[132] Ometov A, Molua OL, Komarov M, Nurmi J. A survey of security in cloud, edge, and fog computing. Sensors. 2022 Jan 25, 22(3):927.

[133] Stergiou C, Psannis KE, Gupta BB, Ishibashi Y. Security, privacy & efficiency of sustainable cloud computing for big data & IoT. Sustainable Computing: Informatics and Systems. 2018 Sep 1, 19:174-84.

[134] Omollo VN, Musyoki S. Blue bugging Java Enabled Phones via Bluetooth Protocol Stack Flaws. International Journal of Computer and Communication System Engineering. 2015 Jun 9, 2 (4):608-613.

[135] Alhaj AA. Performance Evaluation of Secure Data Transmission Mechanism (SDTM) for Cloud Outsourced Data and Transmission Layer Security (TLS). International Journal of Cloud Applications and Computing (IJCAC). 2014 Jan 1, 4(1):45-9.

[136] Alghofaili Y, Albattah A, Alrajeh N, Rassam MA, Al-Rimy BA. Secure cloud infrastructure: A survey on issues, current solutions, and open challenges. Applied Sciences. 2021 Sep 27, 11(19):9005.

[137] Hassan W, Chou TS, Li X, Appiah-Kubi P, Tamer O. Latest trends, challenges and solutions in security in the era of cloud computing and software defined networks. Int J Inf & Commun Technol ISSN. 2019, 2252(8776):8776.

[138] Abduljabbar ZA, Nyangaresi VO, Jasim HM, Ma J, Hussain MA, Hussien ZA, Aldarwish AJ. Elliptic Curve Cryptography-Based Scheme for Secure Signaling and Data Exchanges in Precision Agriculture. Sustainability. 2023 Jun 28, 15(13):10264.

[139] Jouini M, Rabai LB. A security framework for secure cloud computing environments. InCloud security: Concepts, methodologies, tools, and applications 2019 (pp. 249-263). IGI Global.

[140] Guo J, Guo H. Real-Time Risk Detection Method and Protection Strategy for Intelligent Ship Network Security Based on Cloud Computing. Symmetry. 2023 Apr 27, 15(5):988.

[141] Robinson RJ. Insights on Cloud Security Management. Cloud Computing and Data Science. 2023 Jul 25:212-22.

[142] Can O, Thabit F, Aljahdali AO, Al-Homdy S, Alkhzaimi HA. A Comprehensive Literature of Genetics Cryptographic Algorithms for Data Security in Cloud Computing. Cybernetics and Systems. 2023 Jan 30:1-35.

[143] Zhang H, Kang K, Bai W. Hierarchical network security situation awareness data fusion method in cloud computing environment. Journal of Computational Methods in Sciences and Engineering. 2023 Jan 1, 23(1):237-51.

[144] Perilli ML, De Bonis M, Gallo C. Cloud Computing: A Security and Defense Proposal. InContemporary Challenges for Cyber Security and Data Privacy 2023 (pp. 1-16). IGI Global.

[145] Nyangaresi VO. Provably secure protocol for 5G HetNets. In2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) 2021 Nov 1 (pp. 17-22). IEEE.

[146] Illi E, Qaraqe M, Althunibat S, Alhasanat A, Alsafasfeh M, de Ree M, Mantas G, Rodriguez J, Aman W, Al-Kuwari S. Physical layer security for authentication, confidentiality, and malicious node detection: a paradigm shift in securing IoT networks. IEEE Communications Surveys & Tutorials. 2023 Oct 25.

[147] van Daalen OL. The right to encryption: Privacy as preventing unlawful access. Computer Law & Security Review. 2023 Jul 1, 49:105804.

[148] Jaime FJ, Muñoz A, Rodríguez-Gómez F, Jerez-Calero A. Strengthening Privacy and Data Security in Biomedical Microelectromechanical Systems by IoT Communication Security and Protection in Smart Healthcare. Sensors. 2023 Nov 3, 23(21):8944.

[149] Hadi HJ, Cao Y, Nisa KU, Jamil AM, Ni Q. A comprehensive survey on security, privacy issues and emerging defence technologies for UAVs. Journal of Network and Computer Applications. 2023 Apr 1, 213:103607.

[150] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones. 2022 Jun 22, 6(7):154.

[151] Parast FK, Sindhav C, Nikam S, Yekta HI, Kent KB, Hakak S. Cloud computing security: A survey of service-based models. Computers & Security. 2022 Mar 1, 114:102580.

[152] Hasan MK, Habib AA, Shukur Z, Ibrahim F, Islam S, Razzaque MA. Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. Journal of Network and Computer Applications. 2023 Jan 1, 209:103540.

[153] Teja PP, Praveen PN, Bhavya A, Aishwarya J, Gangashetty SK. Secure Cloud Communication–A Comparative Study of Cryptographic Protocols. International Journal of Modern Developments in Engineering and Science. 2023 Dec 3, 2(9):14-9.

[154] Karabulut MA, Shah AS, Ilhan H, Pathan AS, Atiquzzaman M. Inspecting VANET with Various Critical Aspects–A Systematic Review. Ad Hoc Networks. 2023 Aug 14:103281.

[155] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[156] George AS, Sagayarajan S, Baskar T, George AH. Extending Detection and Response: How MXDR Evolves Cybersecurity. Partners Universal International Innovation Journal. 2023 Aug 25, 1(4):268-85.

[157] Arogundade OT, Abayomi-Alli A, Misra S. An ontology-based security risk management model for information systems. Arabian Journal for Science and Engineering. 2020 Aug, 45:6183-98.

[158] Wright C. Essentials for selecting a network monitoring tool. Network Security. 2020 Apr 1, 2020(4):11-4.

[159] Zaki Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Signal propagation parameters estimation through designed multi layer fibre with higher dominant modes using OptiFibre simulation. Journal of Optical Communications. 2022 Jun 23(0).

[160] Jangjou M, Sohrabi MK. A comprehensive survey on security challenges in different network layers in cloud computing. Archives of Computational Methods in Engineering. 2022 Oct, 29(6):3587-608.

[161] Mrabet H, Belguith S, Alhomoud A, Jemai A. A survey of IoT security based on a layered architecture of sensing and data analysis. Sensors. 2020 Jun 28, 20(13):3625.

[162] Adil M, Khan MK. Emerging iot applications in sustainable smart cities for covid-19: Network security and data preservation challenges with future directions. Sustainable Cities and Society. 2021 Dec 1, 75:103311.

[163] Alhaidari F, Rahman A, Zagrouba R. Cloud of Things: architecture, applications and challenges. Journal of Ambient Intelligence and Humanized Computing. 2023 May, 14(5):5957-75.

[164] Nyangaresi VO, Ahmad M, Alkhayyat A, Feng W. Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems. 2022 Dec, 39(10):e13126.

[165] Pal S, Hitchens M, Varadharajan V, Rabehaja T. Policy-based access control for constrained healthcare resources. In2018 IEEE 19th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM) 2018 Jun 12 (pp. 588-599). IEEE.

[166] Singh C, Thakkar R, Warraich J. IAM Identity Access Management—Importance in Maintaining Security Systems within Organizations. European Journal of Engineering and Technology Research. 2023 Aug 31, 8(4):30-8.

[167] Voigt P, Von dem Bussche A. The eu general data protection regulation (gdpr). A Practical Guide, 1st Ed., Cham: Springer International Publishing. 2017 Aug 10, 10(3152676):10-5555.

[168] Sharma RP, Malik A, Singh S, Agarwal S, Kumar R. High Payload Lossless Steganography Using Image Interpolation. Security and Communication Networks. 2023 Nov 28, 2023.

[169] Tabrizchi H, Kuchaki Rafsanjani M. A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing. 2020 Dec, 76(12):9493-532.

[170] Yenurkar GK, Mal S, Nyangaresi VO, Hedau A, Hatwar P, Rajurkar S, Khobragade J. Multifactor data analysis to forecast an individual's severity over novel COVID-19 pandemic using extreme gradient boosting and random forest classifier algorithms. Engineering Reports. 2023:e12678.

[171] Li X, Wang Z, Leung VC, Ji H, Liu Y, Zhang H. Blockchain-empowered data-driven networks: A survey and outlook. ACM Computing Surveys (CSUR). 2021 Apr 17, 54(3):1-38.

[172] Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Blockchain for 5G and beyond networks: A state of the art survey. Journal of Network and Computer Applications. 2020 Sep 15, 166:102693.

[173] Habib G, Sharma S, Ibrahim S, Ahmad I, Qureshi S, Ishfaq M. Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing. Future Internet. 2022 Nov 21, 14(11):341.

[174] Gohar AN, Abdelmawgoud SA, Farhan MS. A patient-centric healthcare framework reference architecture for better semantic interoperability based on blockchain, cloud, and IoT. IEEE Access. 2022 Aug 29, 10:92137-57.

[175] Nyangaresi VO. ECC based authentication scheme for smart homes. In2021 International Symposium ELMAR 2021 Sep 13 (pp. 5-10). IEEE.

[176] Alouffi B, Hasnain M, Alharbi A, Alosaimi W, Alyami H, Ayaz M. A systematic literature review on cloud computing security: threats and mitigation strategies. IEEE Access. 2021 Apr 14, 9:57792-807.

[177] Ahmad MO, Tripathi G, Siddiqui F, Alam MA, Ahad MA, Akhtar MM, Casalino G. BAuth-ZKP—A Blockchain-Based Multi-Factor Authentication Mechanism for Securing Smart Cities. Sensors. 2023 Mar 2, 23(5):2757.

[178] da Silva EL, de Araújo Lima GC, da Veiga CR. Achievements and Challenges of the Regulatory Compliance Program in a Large Philanthropical Hospital Institution. International Journal of Professional Business Review: Int. J. Prof. Bus. Rev.. 2023, 8(1):26.

[179] Rakha NA. Navigating the Legal Landscape: Corporate Governance and Anti-Corruption Compliance in the Digital Age. International Journal of Management and Finance. 2023 Apr 2, 1(3).

[180] Honi DG, Ali AH, Abduljabbar ZA, Ma J, Nyangaresi VO, Mutlaq KA, Umran SM. Towards Fast Edge Detection Approach for Industrial Products. In2022 IEEE 21st International Conference on Ubiquitous Computing and Communications (IUCC/CIT/DSCI/SmartCNS) 2022 Dec 19 (pp. 239-244). IEEE.

[181] Wang D, Yu A. Supply Chain Resources and Economic Security Based on Artificial Intelligence and Blockchain Multi-Channel Technology. International Journal of Information Technologies and Systems Approach (IJITSA). 2023 Jan 4, 16(3):1-5.

[182] Dawood M, Tu S, Xiao C, Alasmary H, Waqas M, Rehman SU. Cyberattacks and security of cloud computing: a complete guideline. Symmetry. 2023 Oct 26, 15(11):1981.

[183] Ahmed AA, Hussan MT. Cloud computing: study of security issues and research challenges. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET). 2018 Apr, 7(4):13-23.

[184] Nag A, Hassan MM, Das A, Sinha A, Chand N, Kar A, Sharma V, Alkhayyat A. Exploring the applications and security threats of Internet of Thing in the cloud computing paradigm: A comprehensive study on the cloud of things. Transactions on Emerging Telecommunications Technologies.:e4897.

[185] Seaman J. Zero Trust Security Strategies and Guideline. InDigital Transformation in Policing: The Promise, Perils and Solutions 2023 Jan 3 (pp. 149-168). Cham: Springer International Publishing.

[186] Russo E, Longo G, Guerar M, Merlo A. Cloud-Native Application Security Training and Testing with Cyber Ranges. InInternational Conference on Ubiquitous Computing and Ambient Intelligence 2023 Nov 26 (pp. 205-216). Cham: Springer Nature Switzerland.

[187] Nyangaresi VO, El-Omari NK, Nyakina JN. Efficient Feature Selection and ML Algorithm for Accurate Diagnostics. Journal of Computer Science Research. 2022 Jan 25, 4(1):10-9.

[188] Mallikarjunaradhya V, Pothukuchi AS, Kota LV. An Overview of the Strategic Advantages of AI-Powered Threat Intelligence in the Cloud. Journal of Science & Technology. 2023 Aug 25, 4(4):1-2.

[189] Glöckler J, Sedlmeir J, Frank M, Fridgen G. A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity. Business & Information Systems Engineering. 2023 Sep 12:1-20.

[190] Kumar GS, Premalatha K, Maheshwari GU, Kanna PR. No more privacy Concern: A privacy-chain based homomorphic encryption scheme and statistical method for privacy preservation of user's private and sensitive data. Expert Systems with Applications. 2023 Dec 30, 234:121071.

[191] Stefan AD, Anghel IP, Simion E. Quantum-Safe Protocols and Application in Data Security of Medical Records. Cryptology ePrint Archive. 2023.

[192] El-Kassabi HT, Serhani MA, Masud MM, Shuaib K, Khalil K. Deep learning approach to security enforcement in cloud workflow orchestration. Journal of Cloud Computing. 2023 Jan 18, 12(1):10.

[193] Fiero AW, Beier E. New global developments in data protection and privacy regulations: Comparative analysis of European Union, United States, and Russian legislation. Stan. J. Int'l L.. 2022, 58:151.

[194] Tan H. An efficient IoT group association and data sharing mechanism in edge computing paradigm. Cyber Security and Applications. 2023 Dec 1, 1:100003.

[195] Ouyang R, Wang J, Xu H, Chen S, Xiong X, Tolba A, Zhang X. A Microservice and Serverless Architecture for Secure IoT System. Sensors. 2023 May 18, 23(10):4868.

[196] Malik JA, Zonain M, Akhter M. Empowering Cloud Security System With Blockchain Technology. International Journal of Advanced Sciences and Computing. 2023 Jun 30, 2(1):1-6.

[197] McCarthy C. Best practices can help manage complicated legal issues involving fraternities, sororities. Campus Security Report. 2023 Oct, 20(6):4-5.