Secure Data Management in Cloud Environments

Chris Gilbert[1], Mercy Abiola Gilbert[2], Maxwell Dorgbefu Jnr[3]

[1]Professor, Department of Computer Science and Engineering/College of Engineering and Technology/William V.S. Tubman University

[2]Instructor, Department of Guidance and Counseling/College of Education/William V.S. Tubman University

[3]Senior Lecturer, Department of Information Technology Education/Akenten Appiah-Menka University of Skills Training and Entrepreneurial Development (AAMUSTED), Ghana

DOI: https://doi.org/10.51584/IJRIAS.2025.10040003

Received: 19 March 2025; Accepted: 24 March 2025; Published: 26 April 2025

ABSTRACT

This article explores the challenges of secure data management in cloud environments and presents an innovative access control framework designed to address these issues. In the era of cloud computing, while the benefits of scalable storage and on-demand computational power are well recognized, persistent security concerns—such as unauthorized access, data leakage, and privacy breaches—remain significant barriers to adoption. To bridge this gap, we propose a novel framework that integrates a Rule-Based Keywords Role Management Model with traditional Role-Based Access Control (RBAC). This dual-layer approach enhances data confidentiality and ensures dynamic, fine-grained access control tailored to evolving organizational roles and security policies. The study employs a multi-phased methodology encompassing an extensive literature review, system development in a simulated cloud environment, and rigorous experimental evaluation. The prototype system incorporates an encryption module based on privacy homomorphism, an access control engine, and a robust backup and recovery mechanism. Comprehensive testing under various threat scenarios demonstrates that the proposed model not only reduces unauthorized access and false positives but also maintains high system performance and scalability. Case studies and real-world implementations further validate the framework's practical effectiveness, while our discussion of future trends highlights emerging technologies and open research challenges in metadata management, data sharing, and integrity assurance. Overall, our findings contribute to a more secure, efficient, and user-friendly approach to cloud data management, offering a significant step forward in the ongoing effort to safeguard sensitive information in dynamic cloud infrastructures.

Keywords: Cloud Security, Secure Data Management, Cloud Computing, Role-Based Access Control (RBAC), Rule-Based Keywords Role Management, Encryption, Privacy Homomorphism, Data Integrity, Access Control, Cybersecurity.

INTRODUCTION

In the contemporary digital landscape, public clouds offer robust storage and computational capabilities through cloud service providers (CSPs) that are geographically and operationally distinct from enterprise tenants (Calabrese, 2018; Sandu et al., 2022; Gilbert & Gilbert, 2024b). The security framework of these clouds relies on a blend of advanced policies, access control mechanisms, and encryption techniques (Srivastav, Das & Srivastava, 2024; Gilbert & Gilbert, 2024c; Namdev et al., 2024). These technologies facilitate the safe storage and processing of data, while simultaneously preventing unauthorized access by external entities and untrusted cloud services (Navale, von Kaeppler & McAuliffe, 2021; Holko et al., 2023; Gilbert & Gilbert, 2024d). Despite the evolution of stringent auditing measures and compliance standards within the public cloud ecosystem, there remains a persistent challenge in alleviating data security concerns for cloud users (Navale & Bourne, 2018; Mathur, 2024; Gilbert & Gilbert, 2024a). Consequently, ensuring the

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

protection of private and sensitive data, as well as maintaining compliance with diverse international regulations, poses a significant challenge for CSPs.

According to Ali et al.(2024), cloud computing represents a paradigm shift in data management and cost-effective computation, offering solutions to large-scale challenges that traditional methods, such as large-scale machine clusters, struggle to address in terms of time-to-market, management complexity, and operational expenses. However, despite the potential advantages, many organizations remain hesitant to fully embrace cloud-based data management due to enduring security and privacy issues (Gill et al., 2024; Gilbert & Gilbert, 2024e; Gill et al., 2022). Enterprises and institutions are particularly apprehensive about the exposure of their data and computational processes to both CSPs and external malicious actors (Gilbert & Gilbert, 2024f; Chakraborty et al., 2023; Ahmad et al., 2023). As a result, the migration or storage of critical data and the processing of complex computations in public clouds continue to be formidable hurdles that must be overcome (Sunyaev & Sunyaev, 2020; Angel et al., 2021; Gilbert & Gilbert, 2024g; Buyya et al., 2018).

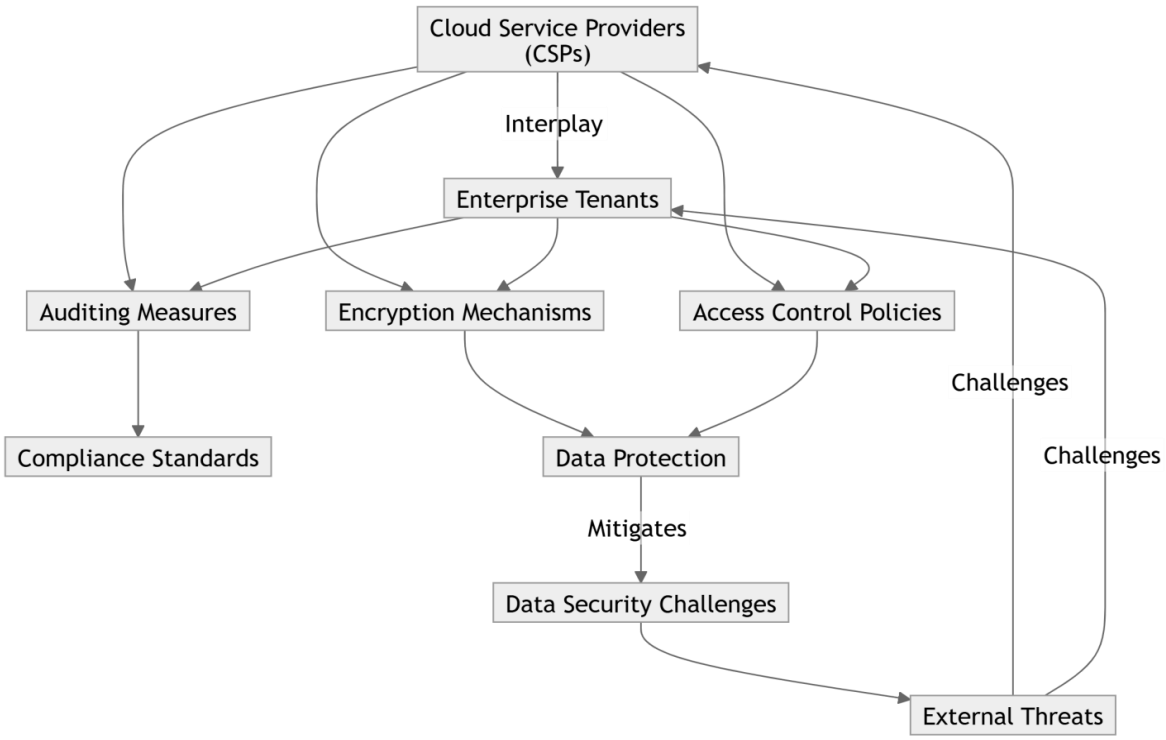

Figure 1: Cloud Service Providers (CSPs) and Enterprise Tenants.

Cloud Service Providers (CSPs) and Enterprise Tenants share responsibilities and must collaborate to protect data in the cloud. Auditing measures ensure compliance with industry standards, encryption secures the data itself, and robust access control governs who can view or modify information. Together, these safeguards address the main security challenges particularly external threats creating a stronger overall defense for cloud-hosted data.

BACKGROUND AND SIGNIFICANCE

In response to growing demands for scalability and efficiency, many enterprises are now developing private cloud infrastructures. This strategy involves hosting proprietary data and leveraging virtualization alongside advanced resource management techniques to achieve levels of scalability once exclusive to public cloud solutions (Rosa, Foschini & Corradi, 2024; Gilbert & Gilbert, 2024h; Sarwar, 2023; Tomarchio, Calcaterra & Modica, 2020). However, while such private cloud implementations facilitate the sharing of virtualized resources across robust physical hardware, they may inadvertently complicate systems management rather than simplifying it (Kait & Kumar, 2024; Soni & Dhurwe, 2024; Vankayalapati, 2025; Gilbert & Gilbert, 2025b). The rapid expansion of virtualized infrastructures is especially evident in cloud-centric applications within large-scale data centers.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

Cloud computing, by delivering scalable services and resources on demand, opens up unprecedented opportunities for companies to fine-tune their operational scales and cost structures in line with environmental demands (Shaik et al., 2024; Gilbert & Gilbert, 2024i). Nevertheless, the widespread adoption of cloud-based services remains contingent on the ability of cloud architectures to ensure robust privacy and data integrity. Currently, users must navigate a trade-off: although cloud storage provides enhanced flexibility and scalability, it often comes with a perceived reduction in control and security over their data when using commercial providers such as Amazon and Microsoft (Kommisetty & Nishanth, 2024; Gilbert & Gilbert, 2025a)

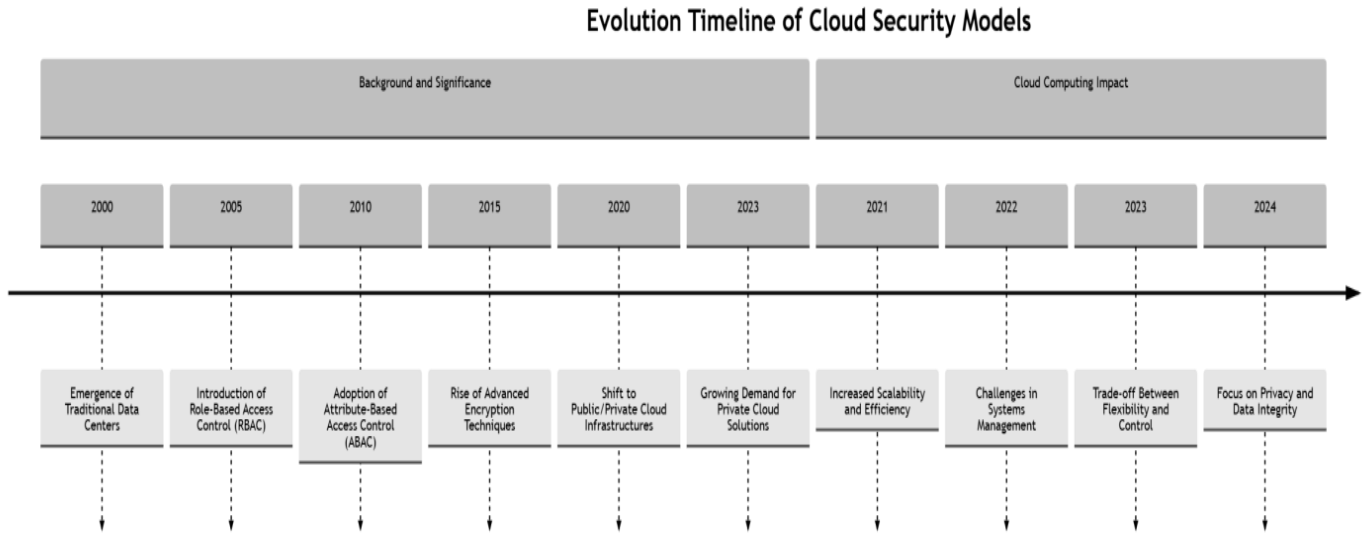

Figure 2: This timeline shows how data centers and access controls have evolved from 2000 to the mid-2020s.

Over the last two decades, data centers have moved from on-premises setups to more complex cloud platforms. Early 2000s saw traditional, in-house data centers; by 2005, role-based access control introduced a structured way to manage user permissions. Around 2010, attribute-based access control made security rules more flexible and context-aware. As data grew more sensitive, advanced encryption techniques rose in 2015. By 2020, organizations started mixing public and private clouds for added flexibility, with a notable shift toward private cloud solutions by 2023 for tighter control.

From 2021 onward, while cloud computing brought greater scalability and efficiency, it also posed new management challenges and forced a trade-off between convenience and oversight. By 2024, mounting privacy concerns and regulations have made data integrity and security top priorities in the cloud.

Research Objectives

This study aims to address the challenges of data security, sharing, and accessibility in cloud environments through the development of an innovative access control model. The objectives are two-fold. These are to:

i. Develop a Rule-Based Keywords Role Management Model.

ii. Integrate Role-Based Access Control (RBAC) with Keyword-Based Attributes.

Despite the significant advancements in security solutions for cloud-stored information, a persistent trade-off exists between maintaining robust security and ensuring legitimate accessibility and data sharing. RBAC is widely recognized as a promising strategy within cloud infrastructures; however, given the dynamic nature of organizational roles and the diverse requirements for access control, existing RBAC models often fall short. Therefore, the primary aim of this work is to create a specialized RBAC model that efficiently and effectively controls access to data by incorporating multiple attributes, ultimately striking a balance between security and accessibility.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

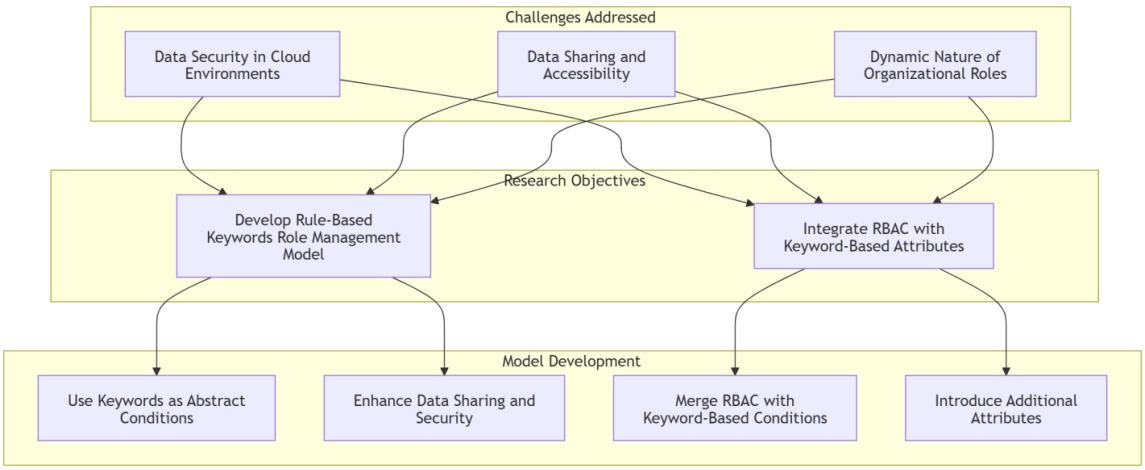

Figure 3: The challenges in cloud environments.

This approach addresses three key challenges in cloud environments: safeguarding data, enabling flexible sharing, and adapting to ever-changing organizational roles. It does so by proposing a rule-based keywords role management model and bolstering role-based access control (RBAC) with keyword-driven attributes. In practice, keywords act as triggers to grant or deny access, complementing existing role-based structures. The approach also involves incorporating additional contextual attributes like location or device type to refine access rules. Ultimately, it aims to create a more adaptable, secure, and efficient system for managing cloud data access.

METHODOLOGY

This study adopts a multi-phased, mixed-methods approach to design, implement, and evaluate a secure data management framework in cloud environments, focusing on the integration of a Rule-Based Keywords Role Management Model with traditional Role-Based Access Control (RBAC) mechanisms. The methodology is structured around three core phases: model development, system implementation, and experimental evaluation.

Model Development and Theoretical Framework

A rigorous theoretical framework underpins the design of the novel access control model. In the initial phase, the study conducted an extensive review of existing literature on cloud security, RBAC, and keyword-based access control methods (Chadwick et al., 2020; Gilbert & Gilbert, 2024b). This review informed the following key design decisions:

- **Rule-Based Keywords Role Management Model:** A set of abstract rules using keyword conditions is defined to encapsulate the diverse security requirements associated with data sharing and confidentiality in cloud environments (Kotha et al., 2022).

- **RBAC Integration:** Building upon standard RBAC practices, the proposed model incorporates keyword-based attributes as an additional layer of granularity. This dual approach facilitates dynamic adaptation to evolving security policies and user roles while mitigating the limitations of conventional access control systems (Yeboah & Abilimi, 2013; Sun, 2019; Gilbert & Gilbert, 2024j).

The conceptual model was iteratively refined through expert consultations and theoretical simulations, ensuring that it not only adhered to contemporary security standards but also addressed the unique challenges posed by cloud data storage and processing (Narayanan, Paul & Joseph, 2022; Gilbert & Gilbert, 2024k).

System Implementation

The second phase involves the concrete implementation of the proposed framework in a simulated cloud environment. The system architecture was designed with the following components:

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

- **Encryption Module:** Based on privacy homomorphism, this module encrypts data using symmetric keys and integrates binary decision trees to manage AND/OR operations for composite security policies. The encryption process was designed to minimize additional local computation or storage overhead during routine data interactions (Gilbert & Gilbert, 2024m; Iezzi, 2020; Opoku-Mensah, Abilimi & Boateng, 2013).

- **Access Control Engine:** This engine enforces the dual-layered access control policy. It processes user requests by first evaluating the RBAC parameters and then applying keyword-based conditions to determine the legitimacy of access requests. Detailed logs are maintained at the data processing level to ensure accountability and facilitate third-party auditing (Miao, 2023; Gilbert & Gilbert, 2024o).

- **Backup and Recovery Mechanism:** Recognizing the criticality of data backup in cloud settings, the system incorporates an on-demand data backup module. This module ensures that routine data updates do not compromise system performance, providing robust remote copy services and facilitating secure data recovery (Yeboah, Opoku-Mensah & Abilimi, 2013a; Gilbert & Gilbert, 2024p; Ahanger et al., 2024).

The implementation was executed in a controlled laboratory setting using a prototypical cloud environment that mirrors the operational conditions of public cloud service providers. Open-source components and established encryption libraries were employed to enhance the system's reliability and scalability.

Experimental Evaluation and Validation

To assess the efficacy of the proposed security framework, the study designed a comprehensive experimental evaluation comprising both simulation-based and real-world scenario analyses. The key elements of this phase include:

- **Testbed Configuration:** A simulated cloud environment was configured to replicate a multi-tenant architecture, including both public and private cloud instances. Diverse data sets representing sensitive and non-sensitive information were deployed to evaluate the system's performance across various access control scenarios (Tsai et al., 2017; Gilbert & Gilbert, 2024n; Galan et al., 2008).

- **Evaluation Metrics:** The experiments were designed to measure critical performance indicators such as access latency, encryption/decryption overhead, and system throughput. Additional metrics included the accuracy of access control decisions, robustness against unauthorized access attempts, and compliance with simulated audit trails (Abosata, Al-Rubaye & Inalhan, 2022; Fan et al., 2020).

- **Simulation of Threat Scenarios:** To validate the resilience of the model, the system was subjected to a series of simulated security threats including data leakage attempts, unauthorized access, and compromise of encryption keys. Each scenario was analyzed to gauge the model's ability to maintain data confidentiality and integrity under adverse conditions (Rekeraho et al., 2025; Steingartner, Galinec & Kozina, 2021; Zografopoulos, Ospina & Konstantinou, 2021).

- **User Workflow Replication:** The prototype was further tested by simulating typical user workflows involving data upload, secure sharing, and retrieval. Password-based key derivation and client-side decryption routines were evaluated to ensure that the user experience remained seamless without sacrificing security (Beltramelli, 2018; Kolthoff, Bartelt & Ponzetto, 2023; Moran et al., 2018; Gilbert & Gilbert, 2024q).

Quantitative results were analyzed using standard statistical methods to compare the performance of the integrated model against conventional RBAC systems. Qualitative assessments from domain experts provided additional validation of the system's practicality and scalability in real-world cloud computing environments.

In summary, the methodology of this study integrates a detailed theoretical framework with practical system implementation and rigorous experimental evaluation. This multifaceted approach ensures that the proposed

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

secure data management framework not only meets the complex requirements of modern cloud environments but also demonstrates improved performance, enhanced data confidentiality, and robust access control in both simulated and real-world scenarios.

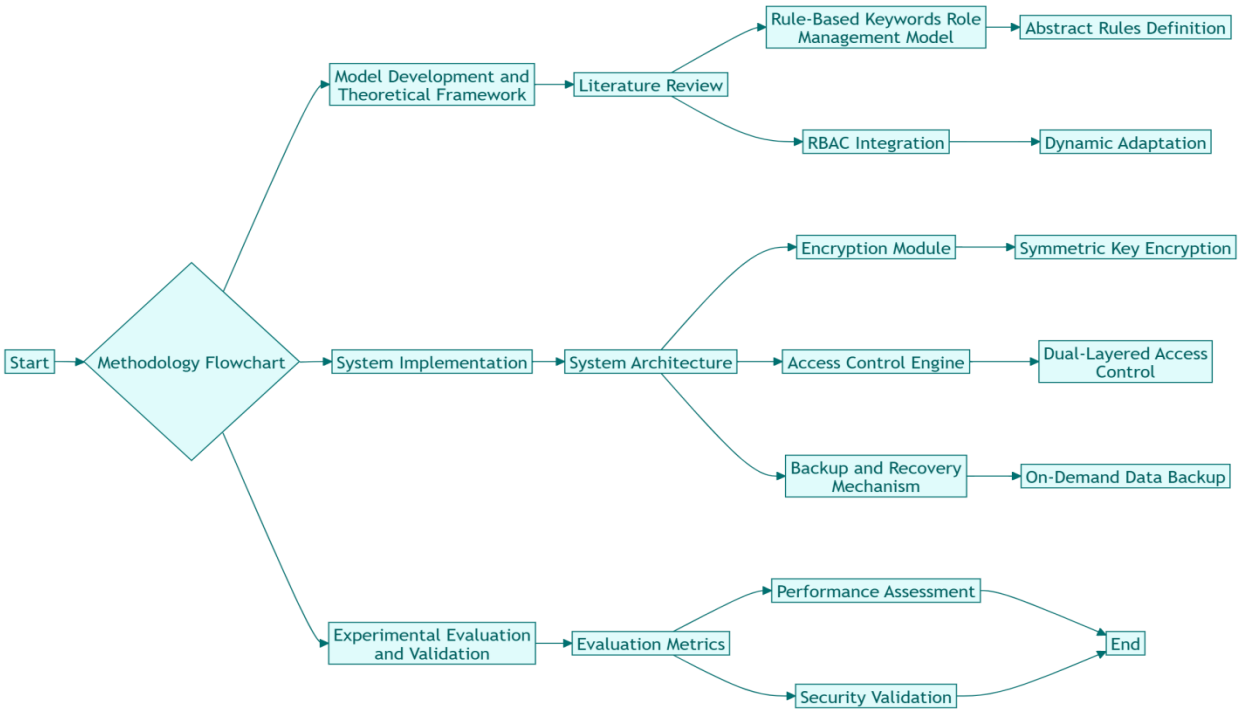

Figure 4: Three-phase methodology for developing and testing a secure, keyword-based role management system.

This flowchart describes a three-phase process for building and testing a secure, keyword-based role management system. First, **Model Development and Theoretical Framework** lays the groundwork by defining keyword triggers, integrating them with traditional role-based access control for adaptability, and adding symmetric encryption. Next, **System Implementation** covers the overall design, establishes a dual-layered access control engine combining keyword and role-based rules, and ensures on-demand data backup and recovery. Finally, in **Experimental Evaluation and Validation**, predefined metrics assess the system's performance, security, and reliability, confirming it meets its intended goals.

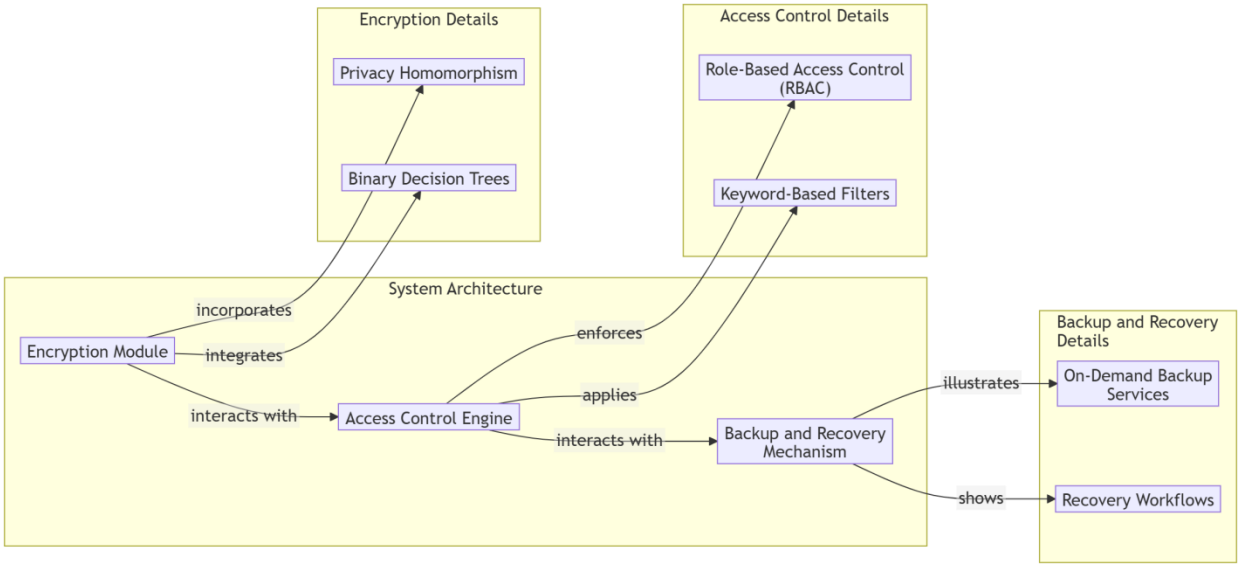

Figure 5: How three main components; encryption, access control, and backup/recovery,come together to form the system architecture.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

This system architecture merges three key components—encryption, access control, and backup/recovery—to secure and manage data in the cloud. The **Encryption Module** applies advanced techniques like privacy homomorphism and binary decision trees, enabling operations on encrypted data. Meanwhile, the **Access Control Engine** combines role-based access control with keyword-based filters, dynamically tailoring user privileges. Finally, the **Backup and Recovery Mechanism** ensures on-demand backups and clear recovery workflows. Together, these elements create a robust, secure framework that protects data, controls access, and provides reliable restoration when needed.

Fundamentals of Cloud Computing

Cloud computing is a concept that, while straightforward in its definition, poses significant challenges in its practical implementation (Sehgal, Bhatt & Acken, 2020). Fundamentally, cloud services are provisioned on demand, which means that resources—such as electricity, personnel, hardware, software, and physical infrastructure—are utilized only when necessary (Sehgal, Bhatt & Acken, 2020). This model enables users to access data from any location with an Internet connection, offering considerable flexibility.

For providers of data management services, cloud computing represents a valuable opportunity to offer and monetize their services while distributing costs and risks among multiple clients (Yang et al., 2017; Opoku-Mensah, Abilimi & Amoako, 2013). Extensive research has documented the transformative impact of cloud computing across various industries (Guo et al., 2021; Gilbert & Gilbert, 2024r). Key benefits identified include significant reductions in operational costs related to labor, infrastructure, energy, and equipment; the ability to concentrate on core business activities; improvements in efficiency, agility, and innovation; enhanced scalability of IT environments; and the acquisition of robust disaster recovery capabilities (Yang et al., 2019).

A modern IT infrastructure is indispensable for organizations seeking to manage and optimize their processes, operations, and decision-making (Abualoush, Bataineh & Alrowwad, 2018). Central to such infrastructure are the services and technologies that support data management (Niu et al., 2021). In recent years, cloud computing has emerged as a pivotal technology in this domain. It enables the shared processing of resources and digital storage over the Internet, encapsulating two primary features: on-demand availability of processing and storage services, and the ability to share and access a diverse array of computer resources, data, and related services hosted on remote servers (Biswas, Hossain & Comite, 2024; Gilbert & Gilbert, 2024s). This dual functionality underpins the growing reliance on cloud computing as a fundamental component in contemporary IT ecosystems for both private enterprises and public administrations (Wang et al., 2019; Floerecke, Lehner & Schweikl, 2021).

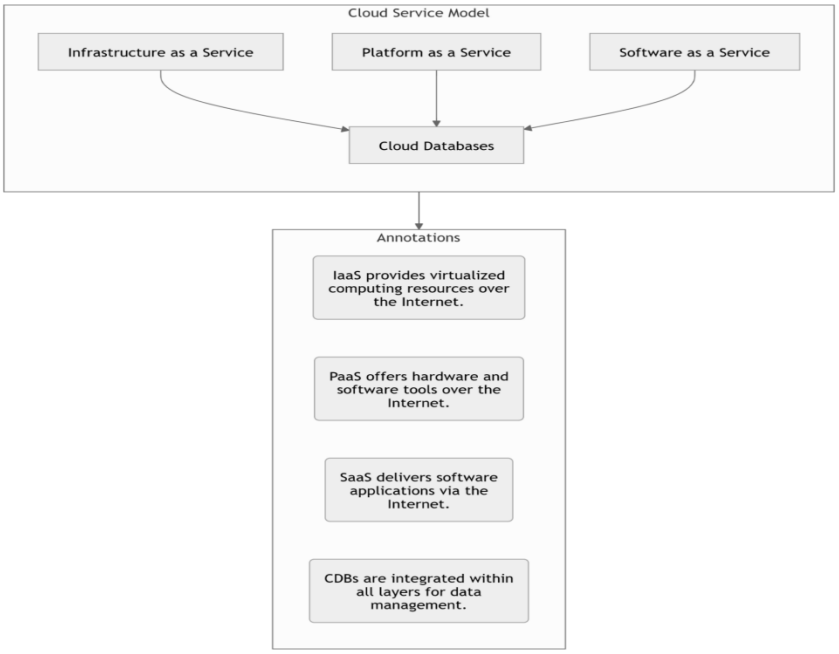

Figure 6: The three main cloud service models

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

In this diagram, the three major cloud service models Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)—all connect to cloud databases (CDBs). IaaS supplies virtual servers and storage over the internet, PaaS provides an online environment for building and deploying applications, SaaS delivers fully functional software accessible via a web interface. Meanwhile, cloud databases support data management across all these layers, ensuring seamless integration and accessibility.

Definition and Characteristics

In today's digital age, cloud databases have emerged as a distinct category within cloud computing. Here, "cloud databases" specifically refers to database systems deployed in cloud environments, which sets them apart from cloud computing database services (CDBS) offered under the Database as a Service (DBaaS) model (Ravi Kumar et al., 2019). Cloud computing itself is built on three primary service layers: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) (Peram, 2024). Essentially, a SaaS is built upon a PaaS, and a PaaS is supported by an IaaS, meaning that a cloud database engine is constructed and deployed over fundamental infrastructure such as storage and networking hardware.

From a practical standpoint, a cloud database (CDB) is simply a database engine operating in the cloud to provide cloud data services (CDS) (Gupta et al., 2022). These databases are managed within the virtualized data centers of third-party cloud service providers, offering distributed and scalable database solutions that meet modern cloud data management needs (Karunamurthy et al., 2023). Traditionally, the design and evaluation of cloud databases rest on two key pillars: a specialized cloud data management engine and an enhanced data model tailored for cloud environments (Buyya et al., 2018).

Table 1: Definition and Characteristics of cloud databases

Key Aspect	Description
Cloud Databases (CDB)	Database engines deployed in cloud environments to provide cloud data services (CDS). They are distinct from cloud computing database services (CDBS) offered under the Database as a Service (DBaaS) model.
Service Layers in Cloud Computing	Cloud computing is structured into three primary layers: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Each layer builds upon the one below it—SaaS is built upon a PaaS, and a PaaS is supported by IaaS.
Deployment Environment	Cloud databases are managed within the virtualized data centers of third-party cloud service providers. This ensures distributed, scalable, and efficient data management solutions that meet modern cloud data management needs.
Design Pillars	The design and evaluation of cloud databases are traditionally based on two key pillars: (1) a specialized cloud data management engine, and (2) an enhanced data model tailored for cloud environments.

This table highlights the core definitions, structural layers, deployment practices, and design principles underlying cloud databases.

Types of Cloud Services

In Infrastructure as a Service (IaaS) environments, the cloud tenant assumes responsibility for managing the operating system as well as the applications hosted on the virtual machines (Samha, 2024). The IaaS provider, on the other hand, maintains only the virtual infrastructure—namely, the virtual machines operating on the virtualization hosts (Laalaoui & Al-Omari, 2018; Gilbert & Gilbert, 2024s). This model is typically employed by businesses to eliminate single points of failure and enhance disaster recovery strategies. Additionally, there exists a robust market segment comprising large Internet Service Providers (ISPs), including entities such as

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

Google, Amazon, and Microsoft, which operate extensive data centers to offer these services to third parties (Stocker, Knieps & Dietzel, 2021; Gilbert & Gilbert, 2024t).

In contrast, within Platform as a Service (PaaS) frameworks, the provider not only supplies the virtual infrastructure but also delivers a partially managed application environment (Mimidis-Kentis et al., 2019). This integrated approach alleviates the need for cloud tenants to independently address concerns related to application provisioning, connectivity, security, and routine maintenance.

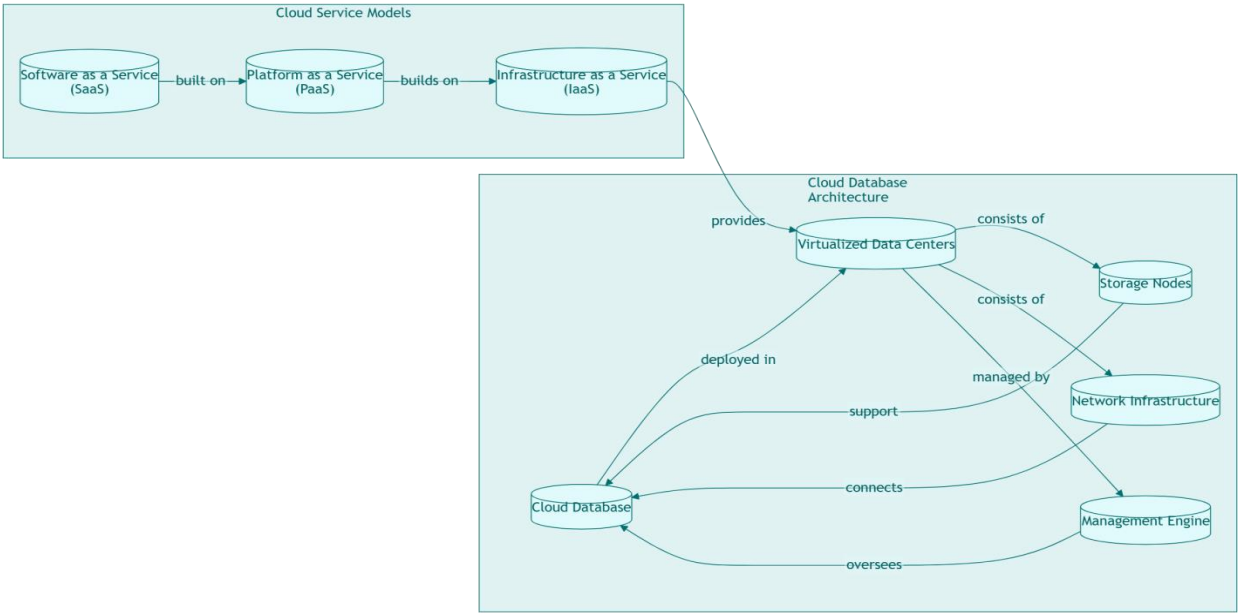

Figure 7: Cloud database architecture, in which virtualized data centers.

*This diagram highlights how **SaaS** (Software as a Service) builds on **PaaS** (Platform as a Service), which itself relies on **IaaS** (Infrastructure as a Service). Beneath these layers lies the **cloud database architecture**, powered by **virtualized data centers**. Within these data centers, **storage nodes** store information, a **network infrastructure** manages data flow, and a **management engine** oversees operations. The cloud database deploys across this virtual environment, ensuring that each service model runs smoothly on top of the underlying infrastructure.*

Data Security in Cloud Environments

Data security has long been recognized as a critical impediment to the widespread adoption of network-based storage solutions (Khalid et al., 2023; Musa et al., 2023). Within organizations, safeguarding data is paramount—not only for internal use but also when data is backed up to external network environments. When cloud services, managed by third-party providers, are employed, data becomes vulnerable to an array of security risks (Tabrizchi & Kuchaki Rafsanjani, 2020; Omer et al., 2022; Gilbert & Gilbert, 2024u). These risks stem from the relinquishment of physical control over data and the often insufficient security measures offered to cloud computing customers. Among the potential threats in cloud environments are data leakage, man-in-the-middle attacks, and unauthorized account termination, among others (Fereidouni, Fadeitcheva & Zalai, 2025; Rani, Sing & Singh, 2024; Abilimi & Adu-Manu, 2013). Furthermore, Aswathy & Tyagi (2022), stated additional challenges such as cyber terrorism and privacy breaches can lead to severe repercussions, including the exposure of personal information to malicious entities and the unauthorized disclosure of confidential corporate data.

Challenges and Threats

According to Ali et al.(2020), organizations, technical professionals, individuals, and governments must remain vigilant regarding the increasing threats associated with the growing reliance on Cloud Service Providers (CSPs) for data storage and management. Given that vast amounts of sensitive information are now

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

housed within these systems, ensuring confidentiality has become paramount. Although it is unrealistic and arguably undesirable to attempt to entirely restrict the advanced utilization of technology, the CSP industry continues to embody a commitment to intellectual freedom (Harris & Houlihan, 2016; Yeboah, Opoku-Mensah & Abilimi, 2013b; Gilbert & Gilbert, 2024v). This freedom must be safeguarded, provided that robust and secure control mechanisms are implemented.

It is incumbent upon computer professionals who leverage CSP services to enhance consumer awareness regarding potential vulnerabilities and threats (Tazi et al., 2024). By doing so, users can make more informed decisions about how their information is stored and managed. In an environment where significant resources are concentrated, consumers naturally expect service providers to safeguard their operations and data against breaches, data loss, and unauthorized access (Barona & Anita, 2017; Abilimi et al., 2013; Sampson & Chowdhury, 2021; Tabrizchi & Kuchaki Rafsanjani, 2020).

Sneider (2021), in his article indicated that, the primary challenge for CSPs, therefore, is to ensure both the confidentiality and integrity of data stored on their servers, as well as the privacy of consumer-generated information transmitted over the internet. To meet these expectations and attract customers who require comprehensive, integrated solutions, it is essential to prioritize rigorous security assessments (Landoll, 2021; Gilbert & Gilbert, 2024w). These evaluations should be conducted in collaboration with third-party organizations that can provide non-functional performance (NFP) evaluations, clearly outlining the safety capabilities of the solutions developed, as designated by Olmsted (2024).

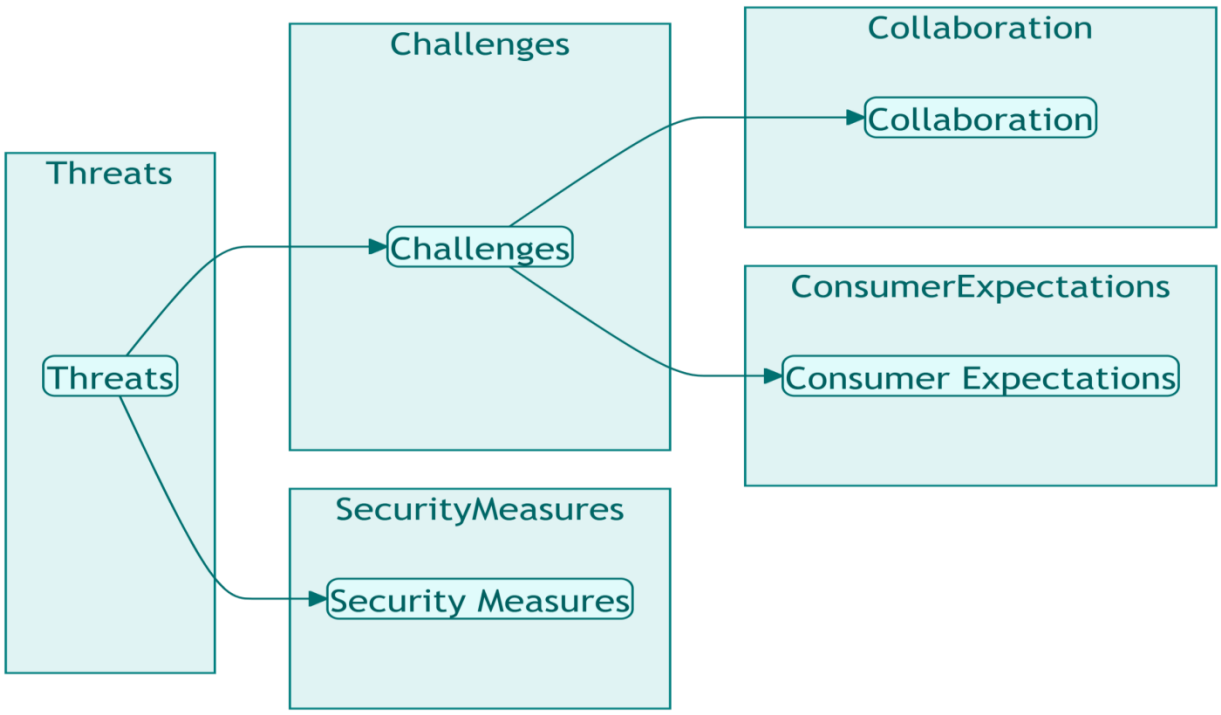

Figure 8: How threats in a system lead to challenges

This diagram shows how **threats** create **challenges**—particularly around collaboration and meeting consumer expectations. In response, organizations must introduce **security measures** to address these risks and maintain trust.

Importance of Data Security

Data security is a fundamental pillar of cloud computing, as trust in cloud services is critical for their widespread adoption. Users subscribing to cloud services expect that their computational and data resources will be managed and secured more effectively than if they were to manage them independently. Cloud service providers recognize this expectation and continuously strive to enhance security measures to meet customer demands (Nzanywayingoma & Yang, 2019; Gilbert & Gilbert, 2024v).

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

One of the key challenges in ensuring trust in cloud environments is addressing data security concerns, particularly encrypted search functionality (Abilimi & Yeboah, 2013; Sun, 2019). Early research in this domain was limited, with encrypted search often viewed as a niche problem due to the loss of plaintext search functionality associated with traditional encryption techniques (Katoch, Chauhan & Kumar, 2021; Gilbert & Gilbert, 2024x). However, as data volumes have exponentially increased, secure data processing especially in the context of encrypted search has emerged as a critical global concern. According to Arunkumar (2023), effectively addressing this issue is essential for managing the growing I/O traffic within cloud infrastructures. Consequently, security has evolved from being a secondary consideration to a central requirement in cloud environments. Given that security concerns remain one of the primary barriers to broader cloud adoption, the development of robust security solutions is imperative (Alghofaili et al., 2021; Christopher, 2013).

The significance of data management cannot be overstated, as it plays a crucial role in both business operations and information governance. The rapid expansion of digital data has underscored the necessity for organizations and individuals to implement effective data management strategies. In the paper by Roozbeh et al. (2018), with the proliferation of advanced IT infrastructures and the increasing availability of on-demand computational resources, the focus has shifted from hardware and software maintenance to high-level data management and security.

Emerging challenges in data management now demand significant computational effort across various sectors. Among these challenges, the **SCALE** (Scalability, Competent Access, Long-Term Archiving, and Ecological Safety) problem has gained increasing attention (Renzaho et al., 2022). Addressing SCALE requirements is particularly challenging due to the exponential growth of I/O traffic, which surpasses the capabilities of many existing high-performance computing systems. Additionally, as Wide Area Networks (WANs) increasingly integrate cloud storage services, there is a growing need for new, efficient data management frameworks that ensure both security and accessibility (Awaysheh et al., 2021; Gilbert & Gilbert, 2024y; Sakr et al., 2011; Al-Jumaili et al., 2023). Therefore, the development of innovative data security mechanisms must remain a top priority in the evolution of cloud-based services.

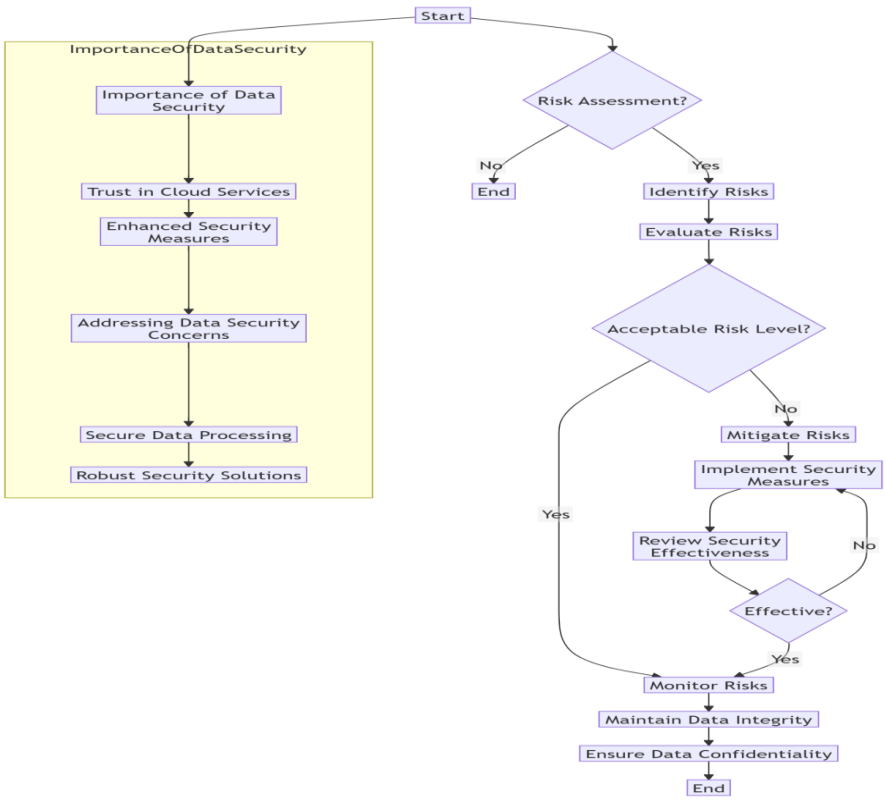

Figure 9: The importance of data security and risk-assessment process.

This diagram highlights two main streams. On the left, it explains the importance of data security showing how trust in cloud services drives enhanced protections, leading to secure data handling and robust security. On the

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

right, a risk-assessment process begins by identifying and evaluating possible threats. If risks are too high, security measures are put in place and then reviewed. Once deemed effective, ongoing monitoring ensures data integrity and confidentiality.

Techniques for Data Security

In cloud computing, ensuring the confidentiality and integrity of data is paramount. Two primary techniques are instrumental in achieving secure data management: encryption and access control (Vasconcelos Soares dos Santos, 2024; Gilbert & Gilbert, 2024f; Agrawal, Singhal & Sharma, 2024).

Secure Data Management through Encryption

Encryption is one of the most robust and widely implemented methods for safeguarding data against unauthorized access. By transforming data into a format that cannot be deciphered without the correct key, encryption effectively prevents misuse. This technique underpins many advanced data management strategies, where subsequent methods build upon encryption principles, particularly in the secure storage and handling of cryptographic keys (Seth et al., 2022).

Secure Data Management through Access Control

Access control serves as another critical pillar of data security. This approach entails rigorously managing who can request and obtain access to cloud-stored data. Organizations define and enforce access rules based on business requirements and security policies, ensuring that only authorized individuals or systems can interact with sensitive information (Wei et al., 2021; Gilbert, 2022; Uchibeke et al., 2018).

Overall, these techniques work in tandem to protect data from unauthorized use, including threats that may arise from internal actors. The subsequent sections will further elaborate on these methods, discussing their implementations, variations, and practical applications in the cloud environment.

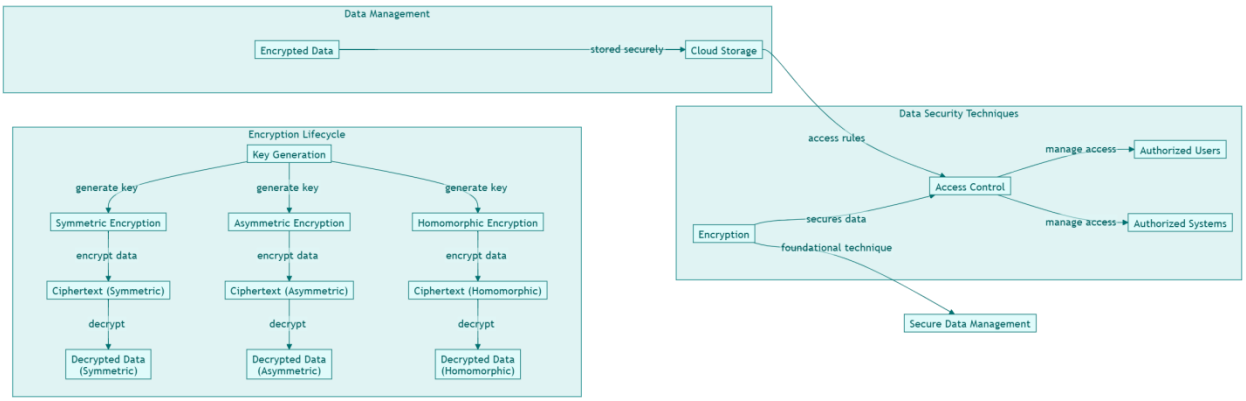

Figure 10: how encrypted data is securely stored in the cloud.

This diagram highlights two key elements of secure data management in the cloud: Encryption Lifecycle – Data is protected using symmetric, asymmetric, or homomorphic encryption. After generating a key, data is converted to ciphertext and later decrypted as needed, keeping it confidential throughout its lifecycle. Access Control – Determines which authorized users and systems can view or modify the encrypted data by enforcing specific access rules. By combining these two components—encryption as the protective shield and access control as the gatekeeper—organizations ensure data remains both secure and properly managed.

Encryption

A major challenge with the first method is its reliance on a cloud server instance to host the key server. This dependency poses a risk because any user with a cloud account can potentially disable the key server, which would cut off data access for all clients (Haddadi & Beghdad, 2018; Gilbert, 2021; Saravanan et al., 2019; Radain et al., 2021).

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

Our alternative method addresses this issue by employing privacy homomorphism to encrypt binary decision trees (Nocker et al., 2023; Sarpatwar et al., 2020; Cong et al., 2022; Gilbert, 2018). In this framework, each leaf node represents an attribute value, while each internal node is associated with an operator. For our study, we concentrate solely on the AND and OR operators. Specifically, an AND operator enables the combination of two encrypted decision trees, whereas an OR operator facilitates a combination of 2^n encrypted trees, where n indicates the number of trees involved.

Encryption is widely used as a core strategy for securing data management. In essence, it involves encoding data using symmetric keys so that only authorized users can access it (Mohamed, 2025; Hazra et al., 2024). The process begins by setting up a key server on a cloud platform. Clients then interact with the server in designated groups, eventually forming a subserver composed of several clients (Yan, Tong & Wang, 2023; Gilbert, 2012; Mehta & Shao, 2023). Through secure interactions among the client, server, and subserver, one client eventually acquires the key needed to communicate with the subserver, which is then used to encrypt and upload the data (Rajmohan et al., 2024). Notably, this approach does not introduce any additional local computation or storage overhead during the data usage phase.

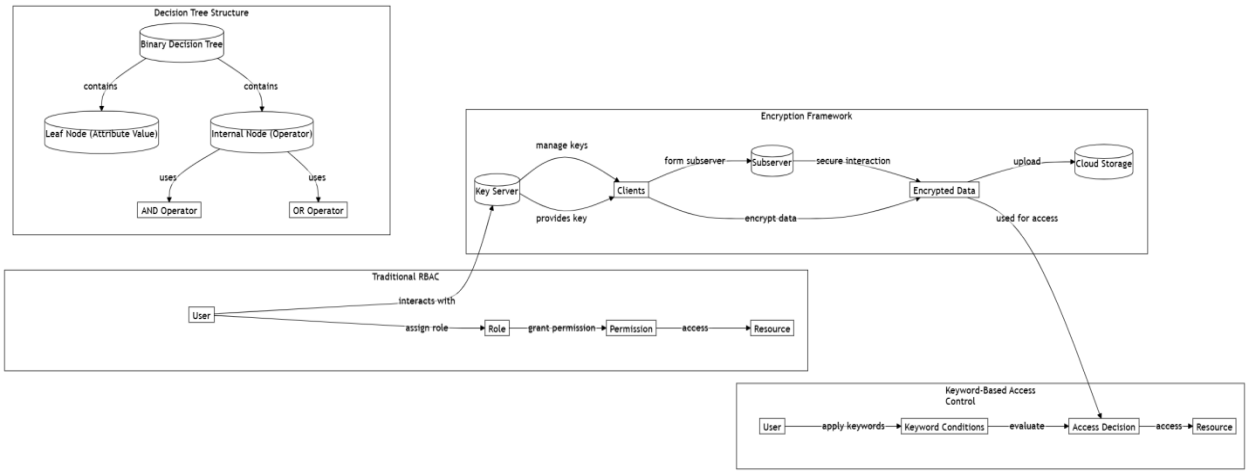

Figure 11: The four connected components of a proposed security approach

This diagram shows four interconnected parts of a security approach. First, the decision tree structure illustrates how binary trees use leaf nodes for attribute values and internal nodes for logical operators like AND and OR, enabling condition checking for access decisions. Next is the encryption framework, where a key server issues keys to clients, and a subserver uses these keys to encrypt data before it is stored in the cloud. The stored data is then decrypted only when authorized users present valid keys. Meanwhile, traditional role-based access control (RBAC) assigns users specific roles that come with defined permissions. In contrast, the keyword-based access control method evaluates keywords that users provide, applying rules to grant or deny access. Altogether, decision trees guide condition evaluation, encryption protects data, and the combination of RBAC and keyword-based access ensures both flexible and robust security.

Access Control

In cloud computing environments, while users have the ability to monitor access to their data, the management of external access is exclusively handled by an independent audit party (Tian et al., 2019). Every cloud operation that involves data must be meticulously logged at the level where the data is stored and processed (Hazela et al., 2022). This logging is crucial not only for maintaining security and privacy in cloud environments but also aligns with traditional data processing practices.

Access control in the cloud presents unique challenges that extend beyond the conventional issues of enforcing user permissions, privacy regulations, and data utilization policies (El Sibai et al., 2020; Cai et al., 2019). Cloud environments require additional measures to address complications arising from remote data storage and the transferability of control (Dong et al., 2024). The primary challenge lies in reconciling traditional access control models with emerging, less-tested management models (Dixit, 2024; Gu et al., 2023). This

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

reconciliation is necessary to ensure that dynamic data exchanges and processing activities in the cloud are rigorously protected.

Moreover, the cloud's inherent model, where data ownership is effectively transferred to service providers, amplifies the importance of privacy, compliance, and accountability (Murthy & Kar, 2024). To address these concerns, an independent auditor plays a critical role by conducting thorough security audits. These audits involve verifying adherence to security protocols at the operational level and triggering audit events when necessary, thereby reinforcing overall security and ensuring accountability.

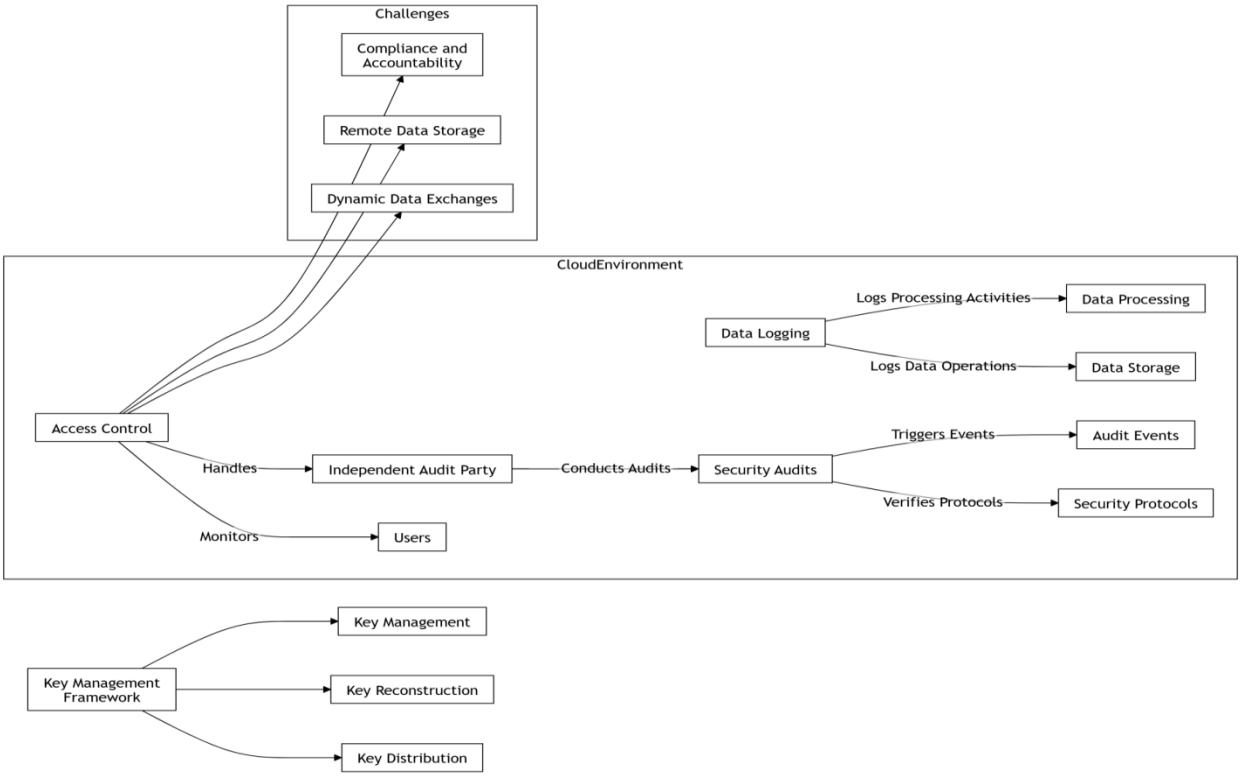

Figure 12: How access control and key management mechanisms address three major challenges in a cloud environment.

This diagram shows how access control and key management mechanisms address three key challenges in a cloud environment—compliance and accountability, remote data storage, and dynamic data exchanges. Access control oversees users' actions, working with an independent audit party to run security audits that produce events and verify protocols. Data logging captures both data processing and storage details, feeding into those audits to ensure transparency. Meanwhile, the key management framework covers key distribution, key reconstruction, and overall key management, forming the cryptographic backbone of secure data handling. By combining logging, auditing, and a robust key management system, organizations can meet regulatory requirements, protect stored data, and handle the demands of modern cloud operations.

Data Backup and Recovery

Syamsundararao et al.(2022), and Zhang, Xu & Shen (2020), specified in their articles that, while users have the ability to back up their data independently, relying on personal devices to manage temporary cloud-based storage can render the backup process both ineffective and overly complex. In scenarios where cloud storage is inaccessible or when users are engaged in computationally intensive tasks, data backup procedures may be inadvertently neglected. It is therefore essential for cloud storage providers to offer convenient on-demand data download and remote copy services that maintain users' existing access privileges, trust, and privacy (Akhtar et al., 2021; Spoorthy, Mamatha & Kumar, 2014). A robust, dynamic, and efficient data backup mechanism must be engineered to ensure that routine data updates during user interactions do not compromise the overall performance of cloud storage services.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

Ensuring data backup and recovery is critical in protecting information from accidental loss or malicious damage. In cloud environments, remote data backup typically requires the service provider to first download data from the user's cloud storage before performing any local backup operations; a process that can be considerably time-consuming (Prasetio et al., 2024). Moreover, because the initiation of data backup is user-driven, service providers may lack both the incentive and the resources to manage this process proactively. According to Ahanger et al.(2024), although historically many organizations have relied on third-party backup services, these solutions can be limited by complex security requirements, high development costs, and compatibility challenges. Within the open, multi-tenant framework of cloud computing, it remains particularly challenging to guarantee the security and availability of backup services provided by external parties.

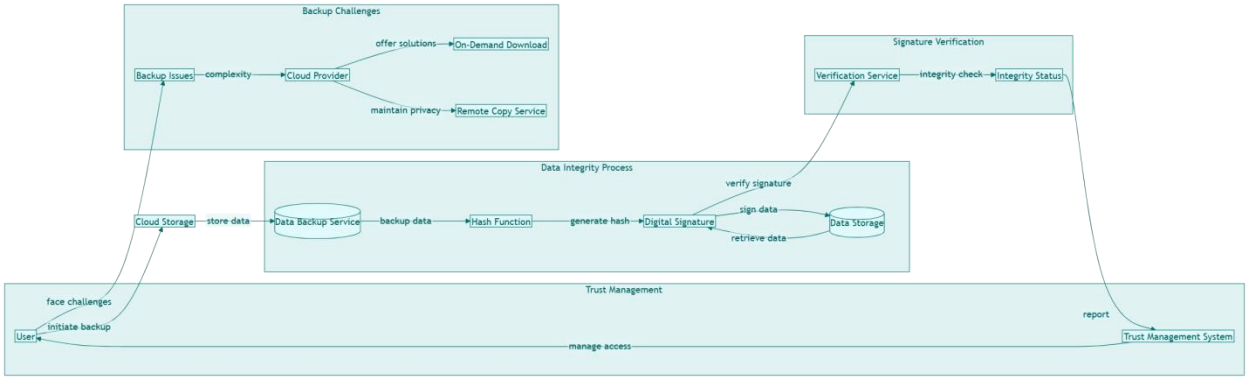

Figure 13: How users face various backup challenges.

This diagram illustrates how users encounter different backup challenges such as complexity and privacy, when storing data in the cloud. To overcome these, cloud providers can offer solutions like on-demand downloads and remote copy services. In the data integrity process, a backup service hashes and signs the data before sending it to cloud storage, ensuring that when the data is retrieved, a verification service can confirm its integrity by checking the signature. At the same time, a trust management system governs user access and keeps track of backup and integrity issues, giving users a reliable way to initiate backups and confirm data authenticity.

Case Studies and Best Practices

The growing impact of big data on industry, academia, and society underscores the necessity of projects that integrate statistical, mathematical, and technological expertise—an expertise that remains underdeveloped in many areas (Bibri, 2019; Bibri, 2021; Talebkhah et al., 2021). This underdevelopment carries inherent risks, such as reputational damage and the potential loss of funding when data protection measures are insufficient.

Case studies and best practices offer valuable insights by demonstrating the most effective approaches derived from the experiences of various companies and projects, as well as by aligning with established recommendation and certification standards (Williams, 2016). These use cases illustrate concrete scenarios and outcomes, highlighting best practices across selected organizations in addressing security challenges, implementing technical solutions, and optimizing organizational processes for secure big data, open data, and cloud computing practices (Mahmood et al., 2024).

Moreover, these case studies serve not only as validations of current methodologies but also as catalysts for future innovation (Toyao et al., 2019; Abraham et al., 2024). They emphasize the importance of real-world testing and validation, particularly in domains such as eHealth and social networks, where privacy-preserving big data technologies and methods, still in a relatively nascent stage, must be rigorously evaluated to meet essential functional requirements (Thapa, 2024; Marengo, 2024).

Real-World Examples

In both internal and external cloud environments, enterprises must rigorously assess whether a cloud provider's data protection mechanisms are effective and compliant with the legal and industry-specific

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

standards applicable to their operations (Singh, Chandna & Kongala, 2024). For organizations using a public cloud, however, the onus is largely on the customer to conduct thorough due diligence to ensure that their data is secure (Abdulsalam & Hedabou, 2021). Regardless of the deployment model, the ultimate responsibility for data protection resides with the customer.

From article by Rajesh, Kumar & Poojari (2024), similar to traditional IT infrastructures, enterprises hold a critical role in safeguarding data against unauthorized access whether that be from cloud provider employees, legal authorities through mechanisms such as subpoenas, or cybercriminals capable of infiltrating the cloud provider's systems. Additionally, in a public cloud setting, there is the added risk associated with the potential exposure stemming from other customers' virtual machines and data residing within the same environment (Omer et al., 2022).

Although there have been few documented instances of customer data being intentionally or inadvertently accessed by external parties and in those rare cases, the data were not publicly disclosed the implications of such breaches are particularly significant for sectors like healthcare, financial services, and government (Ronquillo et al., 2018; Yeo & Banfield, 2022; Chernyshev et al., 2019; Javaid et al., 2023). For example, the intense personal concern regarding the security of medical records is a key factor inhibiting the widespread adoption of electronic medical records. The unauthorized disclosure of sensitive information can trigger profound political, legal, social, and business consequences, along with raising ethical and safety issues (Chesney & Citron, 2019; Verstraete, Bambauer & Bambauer, 2022). This imperative to protect sensitive data including intellectual property, confidential customer and supplier details, and critical business forecasts is a universal challenge across all industries.

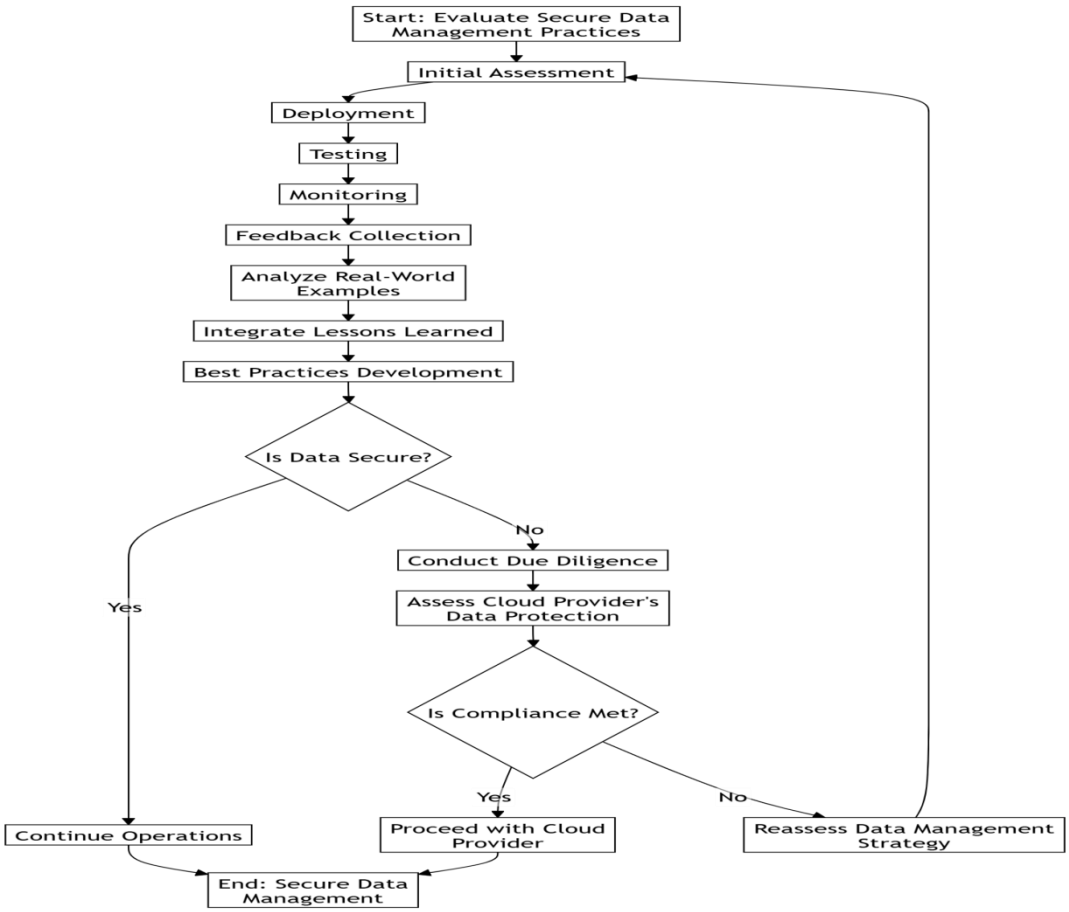

Figure 14: The process for establishing and maintaining secure data management practices.

This flowchart outlines a process to establish and maintain secure data management. It begins with an initial assessment of current practices, followed by deployment, testing, and monitoring to gather feedback. By analyzing real-world examples, teams can integrate lessons learned and develop best practices. Next, they must decide if the data is secure: if it is, operations continue; if not, they conduct due diligence and assess the cloud

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

provider's data protection. Finally, if compliance requirements are satisfied, the organization proceeds with the provider; otherwise, it must reassess its data management strategy to ensure robust security.

Lessons Learned

We defined, validated, and applied a series of fine-tuning parameters to develop a service-provider-managed solution for secure file synchronization via a proprietary cloud storage system. This approach partially addressed our challenges. Domain-specific data conflicts were resolved through reviewed access rights, while aggregated encryption helped lower security risks and simplified the solution's implementation. For additional data protection, custom encryption was necessary. Notably, the service integrates open-source components from the PrimeLife project for hardware-based encryption and signature verification over public web endpoints, ensuring that internal details remain undisclosed (Beebe, 2021; Akaichi & Kirrane, 2025; Di Cerbo et al., 2018).

The performance-enhancing methods were successfully deployed in a prototype synchronization application that supports both personal and permission-controlled delegated data sharing. From the perspective of the cloud storage owner, subscription-derived records were maintained even though many of the original data protection barriers were removed, as shared data continued to be protected. To replicate user workflows, secure decryption within the web browser was implemented using password-based key derivation and client-side binary encryption via a simple symmetric encryption NPM package (Lodder, 2023; Cherry, 2024). All test scenarios met the expected outcomes.

Our initial hypothesis was that current access control and encryption techniques would suffice for protecting data in cloud storage environments. This assumption held true to a degree, provided that the designed mechanisms were appropriately applied and that the complexity of conflicting access rights was kept minimal. When more intricate policies are necessary, a careful abstraction of access rights and tailored protection solutions are required (Radwan, Azer & Abdelbaki, 2017; Tadapaneni, 2020). These adjustments can range from modifying encryption types and operations to altering the sequence of access right manipulations, domain-specific aggregation, backwards-compatible encryption practices, and even combining Boolean logic with reference policies.

In summary, appropriately fine-tuning encryption methods and access management strategies can lead to highly optimized data protection for specific scenarios. This optimization improves performance and energy efficiency while keeping development efforts, performance degradation, and costs within reasonable limits—in essence, reducing unnecessary code and minimizing risk.

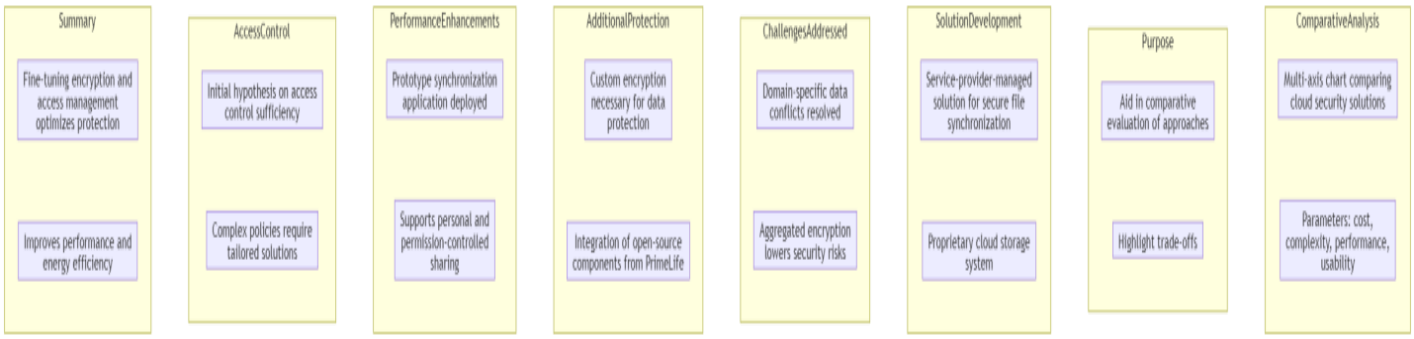

Figure 15: The proposed cloud security approach.

This diagram outlines multiple dimensions of a cloud security strategy, beginning with a summary that stresses how refining encryption and access management can enhance both protection and system performance. The access control section points to the complexity of security policies and the need for tailored solutions, while the performance enhancements component describes a prototype synchronization tool for personal and permission-based file sharing. Additional protection is provided through custom encryption, potentially leveraging open-source components like PrivEx, and the challenges addressed section shows how resolving domain-specific data conflicts can reduce risks via aggregated encryption. The solution development phase

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

involves a service provider's managed method for secure file synchronization with a proprietary cloud storage system, and its core purpose is to enable comparative evaluations of different security approaches, highlighting the associated trade-offs. Finally, the comparative analysis offers a multi-axis chart that weighs cost, complexity, performance, and usability, giving stakeholders a well-rounded perspective on selecting the most suitable cloud security solution.

Future Trends and Research Directions

This study outlines several research ideas designed to guide future work aimed at improving the security and privacy of cloud storage systems. It emphasizes that strengthening cloud storage security is not only essential for protecting data but also critical for boosting industry competitiveness on both national and international levels. By identifying the weaknesses in current state-of-the-art protocols, this report provides valuable insights for the scientific community, potentially paving the way for negotiations on implementation licenses with relevant patent holders. Such collaborations could enrich the collective knowledge in computer security and foster advancements in the global cloud infrastructure market, particularly in the context of Infrastructure-as-a-Service (IAAS) (KEPLER, 2024; Al-Qahtani, 2023; Ikwueze, 2024).

Furthermore, the paper reviews various security and privacy challenges inherent in cloud storage scenarios and delineates the necessary requirements for constructing systems where client data can be securely managed by an untrusted external storage provider. It introduces an efficient public protocol that facilitates file uploads, downloads, and modifications, while maintaining public verifiability all without depending on a trusted intermediary or necessitating ephemeral secret data. This solution is applicable to diverse data types and is effective in both short-term and long-term security contexts. In addition, the study offers a critical evaluation of Identity-Based Encryption (IBE), discussing its associated overheads and limitations, and compares it to symmetric encryption approaches to provide a comprehensive perspective on future security strategies.

Emerging Technologies

One effective approach to achieving robust anonymity is to preemptively encrypt data before uploading it to the cloud (Tyagi, 2023; Yeboah, Odabi & Abilimi Odabi, 2016). In this context, searching for data matches necessitates the decryption of the entire dataset, a process that distinguishes this method from conventional searchable encryption schemes. Although direct comparisons with classic searchable encryption and its derivatives are both pertinent and equitable, evaluating the system solely against an adversary intent on reducing its security to that of standard searchable encryption does not adequately capture the full spectrum of its security properties (Gui, Paterson & Patranabis, 2023).

An ideal secure storage system not only safeguards the confidentiality of the data but also empowers users with efficient access control mechanisms. However, practical implementations of file retrieval and search functionalities often compel the server to access and reveal segments of the data (Sikos, 2020). This complexity is compounded by the challenge of implementing real-time notifications, which require the server to possess file access in order to determine the appropriate files for notification dispatch (Marinakis et al., 2020).

Cloud storage has become indispensable across personal, corporate, and governmental applications (Tabrizchi & Kuchaki Rafsanjani, 2020; Omer et al., 2022). Platforms such as Dropbox, Google Drive, and Amazon S3 provide substantial storage capacities, enhanced flexibility, high availability, and cost-effectiveness (Mistry et al., 2024; Laxminarayana Korada, 2024; Murugesan, 2024). Additionally, the integration of mobile devices with cloud services facilitates seamless data and resource sharing (Segun-Falade et al., 2024; Gilbert, Oluwatosin & Gilbert, 2024). Given this widespread adoption, ensuring the security of cloud-stored data emerges as a critical necessity.

Traditional cryptographic methods, including standard encryption and digital signature schemes, are inherently limited in this environment (Wang & Tabassum, 2024; Abilimi et al., 2015). They often expose metadata such as filenames, file sizes, and client access patterns—even when the data itself is encrypted. Consequently, these techniques fall short of delivering the efficiency and stringent security assurances provided by block ciphers

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

and distributed systems (Gilbert, Auodo & Gilbert, 2024). Moreover, conventional client-side deduplication practices can inadvertently disclose content similarities to unauthorized third parties, thereby further compromising privacy.

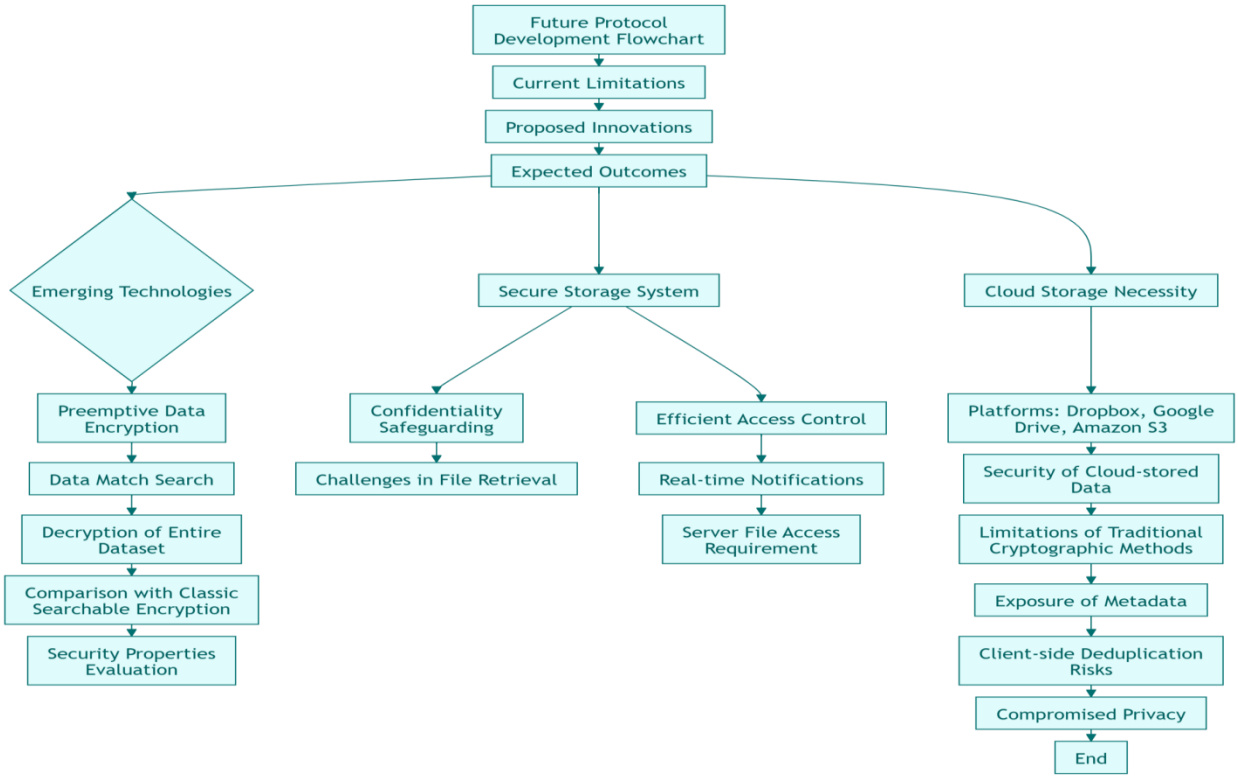

Figure 16: A Future Protocol Development process.

This flowchart shows how a proposed future protocol for secure data management takes shape by first identifying current data-security limitations, then outlining innovations that will lead to a secure storage system. One key branch examines emerging technologies such as preemptive data encryption, which enables data matching without fully decrypting the dataset, and compares this approach with classic searchable encryption to assess overall security.

Open Research Problems Overview of Open Research Problems.

Secure data management in cloud environments continues to present several research challenges. Key areas needing further investigation include metadata management, data sharing management, and data reconfiguration management (Agrawal, Das & El Abbadi, 2022; Mazumdar et al., 2019; Subaveerapandiyan, 2023). Additionally, inadequate integrity parameters may result in service provisions that do not meet customer expectations or Service Level Agreements (SLAs) (Ahmad et al., 2020; Rios et al., 2019).

Data Integrity Management

Recent data-centric approaches have successfully addressed many security issues, particularly those related to ensuring data integrity, confidentiality, and availability (Rios et al., 2019; Herath et al., 2024; Kumar et al., 2024; Bhatt et al., 2024; Mandal & Khan, 2021). However, as data and metadata reside in diverse conditions, ensuring their security demands solutions that offer isolated integrity redundancy as well as robust logical and physical protection mechanisms (Pan, Stakhanova & Ray, 2023; Bhaskaran, 2019; Harley & Cooper, 2021; Jia, Zhang & Lin, 2024). Data-driven methods may implement varied access and manipulation strategies to meet different security and privacy requirements (Bhaskaran, 2019; Pan, Stakhanova & Ray, 2023). Over the past twenty years, researchers have demonstrated that using standard quality-assurance criteria, along with freely available development tools (including open-source cloud database management systems), can effectively support these goals within a distributed cloud service delivery framework (Bernardo et al., 2024; Kwame, Martey & Chris, 2017; Patel, 2024).

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

Data Reconfiguration Management

The trend in cloud storage is shifting from simply transferring data into the cloud to reconfiguring and optimizing data once it is stored (Mazumdar et al., 2019; Mansouri, Toosi & Buyya, 2017). This includes not only migrating or replicating data for greater flexibility but also reconfiguring data semantically to better suit dynamic cloud environments (Mazumdar et al., 2019).

Data Sharing Management

Managing data sharing involves ensuring that multiple users with varying levels of authorization can securely access and manipulate shared data (Nguyen et al., 2023; Gupta et al., 2022). Future research can explore innovative mechanisms to establish multi-data sharing schemes with fine-grained access control (Li et al., 2024). For instance, data owners may need to track and record every operation performed on a shared data item to prevent unauthorized tampering. Potential solutions include using hidden files or directories to trace user activity and enhance overall system security, ensuring that all operations and logs remain untampered by malicious users (Vasilellis, Gkionis & Gritzalis, 2024; Azam et al., 2023).

Metadata Management

Metadata covering aspects such as relational operations, query execution plans, indexing, and a data distribution policy is critical for maintaining the efficient operation of SQL Server and similar systems (Ali et al., 2020; Sun et al., 2023). Currently, the lack of comprehensive metadata management solutions points to promising avenues for future research, including the development of cloud-enabled approaches that leverage emerging technologies like cloudlets (Yunlong & Jie, 2024; Sowjanya, 2024).

While current technologies and solutions provide robust methods for secure data management in the cloud, significant research challenges remain. Addressing these open problems in data integrity, reconfiguration, sharing, and metadata management will be crucial for evolving secure, efficient, and flexible cloud data management practices.

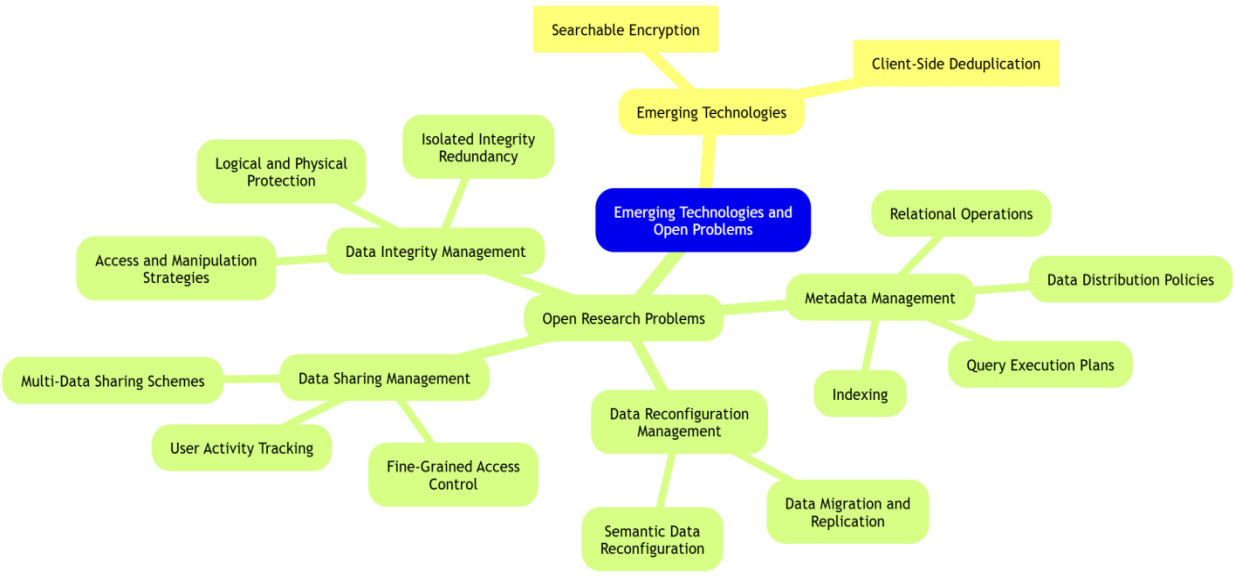

Figure 17: Emerging technologies and open research challenges in modern data management.

This diagram shows emerging security methods (searchable encryption and client-side de-duplication) alongside four open research areas in data management: Data Integrity Management covers logical/physical protections and strategies like isolated redundancy. Data Sharing Management involves multi-data sharing approaches, user activity tracking, and fine-grained access control. Metadata Management deals with organizing data through distribution policies, indexing, and query execution plans. Data Reconfiguration Management addresses how data is restructured, migrated, or replicated.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

CONCLUSION AND SUMMARY

In our work, we have demonstrated that enhancing cloud data security is achievable through more secure protocols at the protocol level. In future work, developing these advanced protocols could further increase the privacy of encrypted data stored in the cloud, especially given that data security is closely tied to how outsourced data is defined—specifically in terms of its dictionary and key dependencies.

Our approach represents a significant shift from traditional user access control methods. By delegating data protection to policy-based mechanisms, we provide an enhanced layer of security that applies to both encrypted and non-encrypted data. This shift enables the secure outsourcing of highly sensitive information, such as biometric data, and is particularly relevant in fields like health informatics and other security-critical applications.

More specifically, we have introduced a secure data management solution that emphasizes access policies based on the management of data rather than focusing solely on the identity of data entities. Although we examined four distinct types of outsourced data, our model is robust enough to handle encrypted data processing as well. Through simulations and experimental evaluations, we have shown that our approach to privacy-preserving data management in cloud computing is secure, feasible, and practical.

Overall, our main contribution is the creation of a cloud computing security scheme that empowers users to define which resources from the cloud provider they utilize for data storage, as well as to query their data securely.

Key Findings

This section outlines the primary research challenges associated with data security and privacy in cloud computing environments. These challenges form the basis for developing strategies to address the critical security concerns prevalent in modern cloud settings. In addition, survey-based reports are analyzed to highlight that security issues represent a significant barrier preventing many enterprises from adopting cloud technologies. The synthesized survey findings consistently indicate that, despite extensive interest in cloud computing, security remains the foremost concern. Moreover, the section provides a comprehensive overview of the major security threats, their subcategories, and the commonly implemented or proposed countermeasures, offering a detailed comparison within the cloud computing sector.

Implications and Recommendations

Our findings suggest a general set of requirements for addressing data management satisfaction and performance that goes beyond just security concerns. In addition to secure data handling, factors such as ease of use, system reliability, and the reputation of the vendor are crucial for building trust and gaining user acceptance. Therefore, our recommendations include:

- Organizational Buy-In: Ensure that the entire organization supports the cloud-based solution. It is critical that even key individuals who might be resistant to change are on board.
- System Configuration and Service Quality: Proper configuration of the system and consistently high-quality service are essential. The cloud solution should be user-friendly and genuinely meet the needs of its users.
- Simplicity in Security Measures: Avoid adding unnecessary complexity. Security measures should be practical and aligned with user needs.
- Focused Use of Cloud Solutions: The cloud solution should be applied only to those tasks that are vital to the business and require its specific capabilities.

Our research also highlights that ease of local access and the overall usability of the application significantly influence user satisfaction and perceived usefulness. Interestingly, while usability contributed to overall

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue IV April 2025

adoption, it did not differentiate between secure and non-secure use cases. Therefore, usability improvements should be a continuous effort across all groups.

Additionally, users reported higher satisfaction when the system was straightforward and unobtrusive. For those in secure environments, satisfaction was enhanced when their concerns were addressed in ways that aligned with both their organization's and their own business needs.

Although the secure group expressed slightly lower overall satisfaction, this did not affect their likelihood of continuing to use the service. This contrasts with broader trends in cloud applications, where secure data management is often seen as a drawback. In secure settings, users regarded the application as essential for their work, even if it did not necessarily encourage more data sharing. In other words, secure features affected usage and attitudes but did not directly lead to a more optimistic outlook on other factors.

Finally, our results indicate that in cloud environments dealing with data management, practitioners and researchers should consider evaluating a range of options. These include secure cloud services, alternative cloud providers, secure desktop systems, company-owned servers, dedicated secure servers, and secure tablets—each of which may offer unique benefits for managing specific types of data or applications. It is important to weigh these options against potential trade-offs in cost, complexity, usability, and impacts on system agility and functionality. Continuous advancements in security models, encryption, and digital rights management are necessary so that users have a variety of suitable options to choose from.

REFERENCES

1. Abdulsalam, Y. S., & Hedabou, M. (2021). Security and privacy in cloud computing: technical review. Future Internet, 14(1), 11.
2. Abilimi,C.A, Asante,M, Opoku-Mensah, E & Boateng, F.O. (2015). Testing for Randomness in Pseudo Random Number Generators Algorithms in a Cryptographic Application.Computer Engineering and Intelligent Systems, www.iiste.org, ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online) Vol.6, No.9, 2015
3. Abilimi, C. A., & Adu-Manu, K. S. (2013). Examining the impact of Information and Communication Technology capacity building in High School education in Ghana. International Journal of Engineering Research & Technology (IJERT),ISSN: 2278-0181,Vol. 2 Issue 9, September - 2013
4. Abilimi, C.A., Amoako, L., Ayembillah, J. N., Yeboah, T.(2013). Assessing the Availability of Information and Communication Technologies in Teaching and Learning in High School Education in Ghana. International Journal of Engineering Research and Technology, 2(11), 50 - 59.
5. Abilimi, C. A. & Yeboah, T. (2013). Assessing the challenges of Information and Communication Technology in educational development in High Schools in Ghana. International Journal of Engineering Research & Technology (IJERT).ISSN: 2278-0181, Vol. 2 Issue 11, November - 2013
6. Abosata, N., Al-Rubaye, S., & Inalhan, G. (2022). Lightweight payload encryption-based authentication scheme for advanced metering infrastructure sensor networks. Sensors, 22(2), 534.
7. Abraham, B. M., Jyothirmai, M. V., Sinha, P., Viñes, F., Singh, J. K., & Illas, F. (2024). Catalysis in the digital age: Unlocking the power of data with machine learning. Wiley Interdisciplinary Reviews: Computational Molecular Science, 14(5), e1730.
8. Abualoush, S., Bataineh, K., & Alrowwad, A. A. (2018). The role of knowledge management process and intellectual capital as intermediary variables between knowledge management infrastructure and organization performance. Interdisciplinary Journal of Information, Knowledge, and Management, 13, 279-309.
9. Agrawal, D., Das, S., & El Abbadi, A. (2022). Data Management in the Cloud. Springer Nature.
10. Agrawal, R., Singhal, S., & Sharma, A. (2024). Blockchain and fog computing model for secure data access control mechanisms for distributed data storage and authentication using hybrid encryption algorithm. Cluster Computing, 27(6), 8015-8030.
11. Ahanger, A. S., Masoodi, F. S., Khanam, A., & Ashraf, W. (2024). Managing and Securing Information Storage in the Internet of Things. In Internet of Things Vulnerabilities and Recovery Strategies (pp. 102-151). Auerbach Publications.

12. Ahmad, A. A., Arshah, R. A., Kamaludin, A., Ngah, L., Bakar, T. A., & Zakaria, M. R. (2020). Adopting of Service Level Agreement (SLA) in enhancing the quality of IT hardware service support. International Journal of Synergy in Engineering and Technology, 1(1).
13. Ahmad, S., Shakeel, I., Mehfuz, S., & Ahmad, J. (2023). Deep learning models for cloud, edge, fog, and IoT computing paradigms: Survey, recent advances, and future directions. Computer Science Review, 49, 100568.
14. Akhtar, N., Kerim, B., Perwej, Y., Tiwari, A., & Praveen, S. (2021). A comprehensive overview of privacy and data security for cloud storage. International Journal of Scientific Research in Science Engineering and Technology.
15. Akaichi, I., & Kirrane, S. (2025). A comprehensive review of usage control frameworks. Computer Science Review, 56, 100698.
16. Ali, G., Mijwil, M. M., Buruga, B. A., Abotaleb, M., & Adamopoulos, I. (2024). A survey on artificial intelligence in cybersecurity for smart agriculture: State-of-the-art, cyber threats, artificial intelligence applications, and ethical concerns. Mesopotamian Journal of Computer Science, 2024, 53-103.
17. Al-Jumaili, A. H. A., Muniyandi, R. C., Hasan, M. K., Paw, J. K. S., & Singh, M. J. (2023). Big data analytics using cloud computing based frameworks for power management systems: Status, constraints, and future recommendations. Sensors, 23(6), 2952.
18. Al-Qahtani, A. S. S. A. (2023). Towards Knowledge-Based economy: Assessing the ecosystem and value creation drivers through cybersecurity, intangible assets and blockchain technology in Qatar (Doctoral dissertation, Hamad Bin Khalifa University (Qatar)).
19. Alghofaili, Y., Albattah, A., Alrajeh, N., Rassam, M. A., & Al-Rimy, B. A. S. (2021). Secure cloud infrastructure: A survey on issues, current solutions, and open challenges. Applied Sciences, 11(19), 9005.
20. Ali, O., Shrestha, A., Chatfield, A., & Murray, P. (2020). Assessing information security risks in the cloud: A case study of Australian local government authorities. Government Information Quarterly, 37(1), 101419.
21. Ali, W., Saleem, M., Yao, B., Hogan, A., & Ngomo, A. C. N. (2020). Storage, indexing, query processing, and benchmarking in centralized and distributed RDF engines: a survey. Preprints.
22. Angel, N. A., Ravindran, D., Vincent, P. D. R., Srinivasan, K., & Hu, Y. C. (2021). Recent advances in evolving computing paradigms: Cloud, edge, and fog technologies. Sensors, 22(1), 196.
23. Arunkumar, J. R. (2023). Study Analysis of Cloud Security Chanllenges and Issues in Cloud Computing Technologies. Journal of Science, Computing and Engineering Research, 6(8), 6-10.
24. Aswathy, S. U., & Tyagi, A. K. (2022). Privacy Breaches through Cyber Vulnerabilities: Critical Issues, Open Challenges, and Possible Countermeasures for the Future. In Security and Privacy-Preserving Techniques in Wireless Robotics (pp. 163-210). CRC Press.
25. Awaysheh, F. M., Aladwan, M. N., Alazab, M., Alawadi, S., Cabaleiro, J. C., & Pena, T. F. (2021). Security by design for big data frameworks over cloud computing. IEEE Transactions on Engineering Management, 69(6), 3676-3693.
26. Azam, H., Dulloo, M. I., Majeed, M. H., Wan, J. P. H., Xin, L. T., & Sindiramutty, S. R. (2023). Cybercrime Unmasked: Investigating cases and digital evidence. International Journal of Emerging Multidisciplinaries Computer Science & Artificial Intelligence, 2(1).
27. Barona, R., & Anita, E. M. (2017, April). A survey on data breach challenges in cloud computing security: Issues and threats. In 2017 International conference on circuit, power and computing technologies (ICCPCT) (pp. 1-8). IEEE.
28. Beebe, N. H. (2021). A Complete Bibliography of Publications in Network Security.
29. Beltramelli, T. (2018, June). pix2code: Generating code from a graphical user interface screenshot. In Proceedings of the ACM SIGCHI symposium on engineering interactive computing systems (pp. 1-6).
30. Bernardo, S., Orviz, P., David, M., Gomes, J., Arce, D., Naranjo, D., ... & Pina, J. (2024). Software Quality Assurance as a Service: Encompassing the quality assessment of software and services. Future Generation Computer Systems, 156, 254-268.
31. Bhaskaran, S. V. (2019). Enterprise data architectures into a unified and secure platform: Strategies for redundancy mitigation and optimized access governance. International Journal of Advanced Cybersecurity Systems, Technologies, and Applications, 3(10), 1-15.

32. Bhatt, N., Bhatt, N., Prajapati, P., Sorathiya, V., Alshathri, S., & El-Shafai, W. (2024). A Data-Centric Approach to improve performance of deep learning models. Scientific Reports, 14(1), 22329.
33. Bibri, S. E. (2019). On the sustainability of smart and smarter cities in the era of big data: an interdisciplinary and transdisciplinary literature review. Journal of Big Data, 6(1), 25.
34. Bibri, S. E. (2021). Data-driven smart sustainable cities of the future: An evidence synthesis approach to a comprehensive state-of-the-art literature review. Sustainable Futures, 3, 100047.
35. Biswas, T. R., Hossain, M. Z., & Comite, U. (2024). Role of Management Information Systems in Enhancing Decision-Making in Large-Scale Organizations. Pacific Journal of Business Innovation and Strategy, 1(1), 5-18.
36. Buyya, R., Srirama, S. N., Casale, G., Calheiros, R., Simmhan, Y., Varghese, B., ... & Shen, H. (2018). A manifesto for future generation cloud computing: Research directions for the next decade. ACM computing surveys (CSUR), 51(5), 1-38.
37. Cai, F., Zhu, N., He, J., Mu, P., Li, W., & Yu, Y. (2019). Survey of access control models and technologies for cloud computing. Cluster Computing, 22, 6111-6122.
38. Calabrese, B. (2018). Cloud-based bioinformatics platforms. Encyclopedia of Bioinformatics and Computational Biology: ABC of Bioinformatics, 257.
39. Chadwick, D. W., Fan, W., Costantino, G., De Lemos, R., Di Cerbo, F., Herwono, I., ... & Wang, X. S. (2020). A cloud-edge based data security architecture for sharing and analysing cyber threat information. Future generation computer systems, 102, 710-722.
40. Chakraborty, A., Kumar, M., Chaurasia, N., & Gill, S. S. (2023). Journey from cloud of things to fog of things: Survey, new trends, and research directions. Software: Practice and Experience, 53(2), 496-551.
41. Cherry, A. (2024). A secure password manager governance framework for web user authentication (Doctoral dissertation, University of York).
42. Chesney, B., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. Calif. L. Rev., 107, 1753.
43. Chernyshev, M., Zeadally, S., & Baig, Z. (2019). Healthcare data breaches: Implications for digital forensic readiness. Journal of medical systems, 43, 1-12.
44. Christopher, A. A.(2013). Effective Information Security Management in Enterprise Software Application with the Revest-Shamir-Adleman (RSA) Cryptographic Algorithm.International Journal of Engineering Research & Technology (IJERT),ISSN: 2278-0181,Vol. 2 Issue 8, August - 2013.
45. Cong, K., Das, D., Park, J., & Pereira, H. V. (2022, November). Sortinghat: Efficient private decision tree evaluation via homomorphic encryption and transciphering. In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (pp. 563-577).
46. Di Cerbo, F., Martinelli, F., Matteucci, I., & Mori, P. (2018). Towards a Declarative Approach to Stateful and Stateless Usage Control for Data Protection. In WEBIST (pp. 308-315).
47. Dixit, A. (2024). Improving the Identity and Access Management Capabilities of Industrial Internet of Things (Doctoral dissertation, City, University of London).
48. Dong, H., Zhang, C., Li, G., & Zhang, H. (2024). Cloud-native databases: A survey. IEEE Transactions on Knowledge and Data Engineering.
49. El Sibai, R., Gemayel, N., Bou Abdo, J., & Demerjian, J. (2020). A survey on access control mechanisms for cloud computing. Transactions on Emerging Telecommunications Technologies, 31(2), e3720.
50. Fan, C., Ghaemi, S., Khazaei, H., & Musilek, P. (2020). Performance evaluation of blockchain systems: A systematic survey. IEEE Access, 8, 126927-126950.
51. Fereidouni, H., Fadeitcheva, O., & Zalai, M. (2025). IoT and man-in-the-middle attacks. Security and Privacy, 8(2), e70016.
52. Floerecke, S., Lehner, F., & Schweikl, S. (2021). Cloud computing ecosystem model: evaluation and role clusters. Electronic Markets, 31(4), 923-943.
53. Galan, F., de Vergara, J. E. L., Fernandez, D., & Munoz, R. (2008, April). A model-driven configuration management methodology for testbed infrastructures. In NOMS 2008-2008 IEEE Network Operations and Management Symposium (pp. 747-750). IEEE.
54. Gilbert, C.(2012). The Quest of Father and Son: Illuminating Character Identity, Motivation, and Conflict in Cormac McCarthy's The Road. English Journal, Volume 102, Issue Characters and Character, p. 40 - 47. https://doi.org/10.58680/ej201220821.

55. Gilbert, C. (2018). Creating Educational Destruction: A Critical Exploration of Central Neoliberal Concepts and Their Transformative Effects on Public Education. The Educational Forum, 83(1), 60–74. https://doi.org/10.1080/00131725.2018.1505017.
56. Gilbert, C. (2021). Walking the popular education spiral - an account and analysis of participatory action research with teacher activists. Educational Action Research, 30(5), 881–901. https://doi.org/10.1080/09650792.2021.1875856
57. Gilbert, C. (2022). Making the Invisible Visible: Professional Development to Support Teacher Activism. Kappa Delta Pi Record, 58(1), 14–19. https://doi.org/10.1080/00228958.2022.2005426
58. Gilbert, C. & Gilbert, M.A.(2024a). Unraveling Blockchain Technology: A Comprehensive Conceptual Review. International Journal of Emerging Technologies and Innovative Research (www.jetir.org | UGC and ISSN Approved), ISSN:2349-5162, Vol.11, Issue 9, page no. ppa575-a584, September-2024, Available at : http://www.jetir.org/papers/JETIR2409066.pdf
59. Gilbert, C. & Gilbert, M.A.(2024b). Strategic Framework for Human-Centric AI Governance: Navigating Ethical, Educational, and Societal Challenges. International Journal of Latest Technology in Engineering Management & Applied Science, 13(8), 132-141. https://doi.org/10.51583/IJLTEMAS.2024.130816
60. Gilbert, C. & Gilbert, M.A.(2024c). The Impact of AI on Cybersecurity Defense Mechanisms: Future Trends and Challenges.Global Scientific Journals.ISSN 2320-9186,12(9),427-441. https://www.globalscientificjournal.com/researchpaper/The_Impact_of_AI_on_Cybersecurity_Defense_Mechanisms_Future_Trends_and_Challenges_.pdf.
61. Gilbert, C. & Gilbert, M.A. (2024d). The Convergence of Artificial Intelligence and Privacy: Navigating Innovation with Ethical Considerations. International Journal of Scientific Research and Modern Technology, 3(9), 9-9.
62. Gilbert, C. & Gilbert, M.A.(2024e). Transforming Blockchain: Innovative Consensus Algorithms for Improved Scalability and Security. International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.11, Issue 10, page no.b299-b313, October-2024, Available :http://www.jetir.org/papers/JETIR2410134.pdf
63. Gilbert, C. & Gilbert, M.A. (2024f). Future Privacy Challenges: Predicting the Agenda of Webmasters Regarding Cookie Management and Its Implications for User Privacy. International Journal of Advanced Engineering Research and Science, ISSN (Online): 2455-9024,Volume 9, Issue 4, pp. 95-106.
64. Gilbert, C., & Gilbert, M. A. (2024g). Navigating the Dual Nature of Deepfakes: Ethical, Legal, and Technological Perspectives on Generative Artificial Intelligence (AI) Technology. International Journal of Scientific Research and Modern Technology, 3(10). https://doi.org/10.38124/ijsrmt.v3i10.54
65. Gilbert, C., & Gilbert, M. A. (2024h). Revolutionizing Computer Science Education: Integrating Blockchain for Enhanced Learning and Future Readiness. International Journal of Latest Technology in Engineering, Management & Applied Science, ISSN 2278-2540, Volume 13, Issue 9, pp.161-173.
66. Gilbert, C. & Gilbert, M.A. (2024i). Unlocking Privacy in Blockchain: Exploring Zero-Knowledge Proofs and Secure Multi-Party Computation Techniques. Global Scientific Journal (ISSN 2320-9186) 12 (10), 1368-1392.
67. Gilbert, C. & Gilbert, M.A. (2024j). The Role of Artificial Intelligence (AI) in Combatting Deepfakes and Digital Misinformation.International Research Journal of Advanced Engineering and Science (ISSN: 2455-9024), Volume 9, Issue 4, pp. 170-181.
68. Gilbert, C. & Gilbert, M.A.(2024k). AI-Driven Threat Detection in the Internet of Things (IoT), Exploring Opportunities and Vulnerabilities. International Journal of Research Publication and Reviews, Vol 5, no 11, pp 219-236.
69. Gilbert, C., & Gilbert, M. A. (2024l). The security implications of artificial intelligence (AI)-powered autonomous weapons: Policy recommendations for international regulation. International Research Journal of Advanced Engineering and Science, 9(4), 205–219.
70. Gilbert, C., & Gilbert, M. A. (2024m). The role of quantum cryptography in enhancing cybersecurity. International Journal of Research Publication and Reviews, 5(11), 889–907. https://www.ijrpr.com
71. Gilbert, C., & Gilbert, M. A. (2024n). Bridging the gap: Evaluating Liberia's cybercrime legislation against international standards. International Journal of Research and Innovation in Applied Science (IJRIAS), 9(10), 131–137. https://doi.org/10.51584/IJRIAS.2024.910013

72. Gilbert, C., & Gilbert, M. A. (2024o). The Effectiveness of Homomorphic Encryption in Protecting Data Privacy. International Journal of Research Publication and Reviews, 5(11), 3235-3256. https://www.ijrpr.com.
73. Gilbert, C., & Gilbert, M. A. (2024p). CRYPTOGRAPHIC FOUNDATIONS AND CYBERSECURITY IMPLICATIONS OF BLOCKCHAIN TECHNOLOGY.Global Scientific Journals,ISSN 2320-9186,12(11),464-487. https://www.globalscientificjournal.com
74. Gilbert, C., & Gilbert, M. A. (2024q). Advancing privacy standards through education: The role of academic initiatives in enhancing privacy within Cardano's blockchain ecosystem. International Research Journal of Advanced Engineering and Science, 9(4), 238–251.
75. Gilbert, C., & Gilbert, M. A. (2024r). Leveraging artificial intelligence (AI) by a strategic defense against deepfakes and digital misinformation. International Journal of Scientific Research and Modern Technology, 3(11). https://doi.org/10.38124/ijsrmt.v3i11.76
76. Gilbert, C., & Gilbert, M. A. (2024s). Evaluation of the efficiency of advanced number generators in cryptographic systems using a comparative approach. International Journal of Scientific Research and Modern Technology, 3(11). https://doi.org/10.38124/ijsrmt.v3i11.77
77. Gilbert, C., & Gilbert, M. A. (2024t). Cybersecurity risk management frameworks for critical infrastructure protection. International Journal of Research Publication and Reviews, 5(12), 507–533. https://www.ijrpr.com/
78. Gilbert, C., & Gilbert, M. A. (2024u). Organizational and leadership aspects of cybersecurity governance. International Journal of Research Publication and Reviews, 5(12), 1174–1191. Retrieved from www.ijrpr.com
79. Gilbert, C., & Gilbert, M. A. (2024v). The development and evolution of cryptographic algorithms in response to cyber threats. International Journal of Research Publication and Reviews, 5(12), 1149–1173. Retrieved from www.ijrpr.com
80. Gilbert, C., & Gilbert, M. A. (2024w). Privacy-preserving data mining and analytics in big data environments. Global Scientific Journal, 12(12). Retrieved from www.globalscientificjournal.com
81. Gilbert, C., & Gilbert, M. A. (2024x). Investigating the challenges and solutions in cybersecurity using quantum computing and cryptography. International Research Journal of Advanced Engineering and Science, 9(4), 291–315.
82. Gilbert, C., & Gilbert, M. A. (2024y). The integration of blockchain technology into database management systems for enhanced security and transparency. International Research Journal of Advanced Engineering and Science, 9(4), 316–334.
83. Gilbert, C., & Gilbert, M. A. (2025a). Artificial intelligence (AI) and machine learning (ML) for predictive cyber threat intelligence (CTI). International Journal of Research Publication and Reviews, 6(3), 584–617. http://www.ijrpr.com
84. Gilbert, C., & Gilbert, M. A. (2025b). Continuous user authentication on mobile devices. International Research Journal of Advanced Engineering and Science, 10(1), 158–173.
85. Gilbert, M.A., Oluwatosin, S. A., & Gilbert, C.(2024). An investigation into the types of role-based relationships that exist between lecturers and students in universities across southwestern nigeria: a sociocultural and institutional analysis. Global Scientific Journal, ISSN 2320-9186, Volume 12, Issue 10, pp. 263-280.
86. Gilbert, M.A., Auodo, A. & Gilbert, C.(2024). Analyzing Occupational Stress in Academic Personnel through the Framework of Maslow's Hierarchy of Needs. International Journal of Research Publication and Reviews, Vol 5, no 11, pp 620-630.
87. Gill, S. S., Wu, H., Patros, P., Ottaviani, C., Arora, P., Pujol, V. C., ... & Buyya, R. (2024). Modern computing: Vision and challenges. Telematics and Informatics Reports, 13, 100116.
88. Gill, S. S., Xu, M., Ottaviani, C., Patros, P., Bahsoon, R., Shaghaghi, A., ... & Uhlig, S. (2022). AI for next generation computing: Emerging trends and future directions. Internet of Things, 19, 100514.
89. Gu, J. T., Sun, X., Zhang, W., Jiang, Y., Wang, C., Vaziri, M., ... & Xu, T. (2023, October). Acto: Automatic end-to-end testing for operation correctness of cloud system management. In Proceedings of the 29th Symposium on Operating Systems Principles (pp. 96-112).
90. Guo, H., Liang, D., Chen, F., & Shirazi, Z. (2021). Innovative approaches to the sustainable development goals using Big Earth Data. Big Earth Data, 5(3), 263-276.

91. Gupta, I., Singh, A. K., Lee, C. N., & Buyya, R. (2022). Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions. IEEE Access, 10, 71247-71277.
92. Gupta, L., Salman, T., Ghubaish, A., Unal, D., Al-Ali, A. K., & Jain, R. (2022). Cybersecurity of multi-cloud healthcare systems: A hierarchical deep learning approach. Applied Soft Computing, 118, 108439.
93. Gui, Z., Paterson, K. G., & Patranabis, S. (2023, May). Rethinking searchable symmetric encryption. In 2023 IEEE Symposium on Security and Privacy (SP) (pp. 1401-1418). IEEE.
94. Haddadi, M., & Beghdad, R. (2018). DoS-DDoS: taxonomies of attacks, countermeasures, and well-known defense mechanisms in cloud environment. Edpacs, 57(5), 1-26.
95. Harley, K., & Cooper, R. (2021). Information integrity: Are we there yet? ACM Computing Surveys (CSUR), 54(2), 1-35.
96. Harris, S., & Houlihan, B. (2016). Implementing the community sport legacy: The limits of partnerships, contracts and performance management. European sport management quarterly, 16(4), 433-458.
97. Hazela, B., Gupta, S. K., Soni, N., & Saranya, C. N. (2022). Securing the confidentiality and integrity of cloud computing data. ECS Transactions, 107(1), 2651.
98. Hazra, R., Chatterjee, P., Singh, Y., Podder, G., & Das, T. (2024). Data Encryption and Secure Communication Protocols. In Strategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning (pp. 546-570). IGI Global.
99. Herath, H. M. S. S., Herath, H. M. K. K. M. B., Madhusanka, B. G. D. A., & Guruge, L. G. P. K. (2024). Data protection challenges in the processing of sensitive data. In Data Protection: The Wake of AI and Machine Learning (pp. 155-179). Cham: Springer Nature Switzerland.
100. Holko, M., Weber, N., Lunt, C., & Brenner, S. E. (2023, January). Biomedical research in the Cloud: considerations for researchers and organizations moving to (or adding) cloud computing resources. In Pac Symp Biocomput (pp. 536-40).
101. Iezzi, M. (2020, December). Practical privacy-preserving data science with homomorphic encryption: an overview. In 2020 IEEE International Conference on Big Data (Big Data) (pp. 3979-3988). IEEE.
102. Ikwueze, C. (2024). Artificial intelligence as a service: a systematic review of literature from the customer's perspective.
103. Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. Cyber Security and Applications, 1, 100016.
104. Jia, R., Zhang, J., & Lin, Y. (2024). Machine Learning Security Defense Algorithms Based on Metadata Correlation Features. Computers, Materials & Continua, 78(2).
105. Jouini, O., Sethom, K., Namoun, A., Aljohani, N., Alanazi, M. H., & Alanazi, M. N. (2024). A survey of machine learning in edge computing: Techniques, frameworks, applications, issues, and research directions. Technologies, 12(6), 81.
106. Kait, R., & Kumar, T. (2024, May). Insights Into Cloud Computing: Unveiling Trends, Addressing Challenges, and Exploring Opportunities-A Systematic Review. In 2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP) (pp. 593-601). IEEE.
107. Karunamurthy, A., Yuvaraj, M., Shahithya, J., & Thenmozhi, V. (2023). Cloud database: Empowering scalable and flexible data management. Quing: International Journal of Innovative Research in Science and Engineering.
108. Katoch, S., Chauhan, S. S., & Kumar, V. (2021). A review on genetic algorithm: past, present, and future. Multimedia tools and applications, 80, 8091-8126.
109. KEPLER, J. (2024). Advancements and Challenges of Cloud-Based Participatory Learning (Doctoral dissertation, JOHANNES KEPLER UNIVERSITY LINZ).
110. Khalid, M. I., Ehsan, I., Al-Ani, A. K., Iqbal, J., Hussain, S., & Ullah, S. S. (2023). A comprehensive survey on blockchain-based decentralized storage networks. IEEE Access, 11, 10995-11015.
111. Kolthoff, K., Bartelt, C., & Ponzetto, S. P. (2023). Data-driven prototyping via natural-language-based GUI retrieval. Automated software engineering, 30(1), 13.

112. Kommisetty, P. D. N. K., & Nishanth, A. (2024). AI-Driven Enhancements in Cloud Computing: Exploring the Synergies of Machine Learning and Generative AI.
113. Kotha, S. K., Rani, M. S., Subedi, B., Chunduru, A., Karrothu, A., Neupane, B., & Sathishkumar, V. E. (2022). A comprehensive review on secure data sharing in cloud environment. Wireless Personal Communications, 127(3), 2161-2188.
114. Kumar, S., Datta, S., Singh, V., Singh, S. K., & Sharma, R. (2024). Opportunities and challenges in data-centric AI. IEEE Access.
115. Kwame, A. E., Martey, E. M., & Chris, A. G. (2017). Qualitative assessment of compiled, interpreted and hybrid programming languages. Communications on Applied Electronics, 7(7), 8-13.
116. Laalaoui, Y., & Al-Omari, J. (2018). A planning approach for reassigning virtual machines in IaaS clouds. IEEE Transactions on Cloud Computing, 8(3), 685-697.
117. Landoll, D. (2021). The security risk assessment handbook: A complete guide for performing security risk assessments. CRC press.
118. Laxminarayana Korada, V. K. S. (2024). Why are large enterprises building private clouds after their journey on public clouds? European Journal of Advances in Engineering and Technology, 11(2), 49-52.
119. Li, B., Zhong, H., Cui, J., Gu, C., & He, D. (2024). RRMAC: A Multi-data Owner Access Control Scheme with Robust Revocation for Co-owned Data Sharing. IEEE Transactions on Information Forensics and Security.
120. Lodder, M. (2023). Token Based Authentication and Authorization with Zero-Knowledge Proofs for Enhancing Web API Security and Privacy.
121. Mahmood, H. S., Abdulqader, D. M., Abdullah, R. M., Rasheed, H., Ismael, Z. N. R., & Sami, T. M. G. (2024). Conducting In-Depth Analysis of AI, IoT, Web Technology, Cloud Computing, and Enterprise Systems Integration for Enhancing Data Security and Governance to Promote Sustainable Business Practices. Journal of Information Technology and Informatics, 3(2).
122. Mandal, S., & Khan, D. A. (2021). Comprehensive Survey of Security Issues & Framework in Data-Centric Cloud Applications. Journal of Engineering Science & Technology Review, 14(1).
123. Mansouri, Y., Toosi, A. N., & Buyya, R. (2017). Data storage management in cloud environments: Taxonomy, survey, and future directions. ACM Computing Surveys (CSUR), 50(6), 1-51.
124. Marengo, A. (2024). Navigating the nexus of AI and IoT: A comprehensive review of data analytics and privacy paradigms. Internet of Things, 101318.
125. Marinakis, V., Doukas, H., Tsapelas, J., Mouzakitis, S., Sicilia, Á., Madrazo, L., & Sgouridis, S. (2020). From big data to smart energy services: An application for intelligent energy management. Future Generation Computer Systems, 110, 572-586.
126. Mathur, P. (2024). Cloud computing infrastructure, platforms, and software for scientific research. In High Performance Computing in Biomimetics: Modeling, Architecture and Applications (pp. 89-127).
127. Mazumdar, S., Seybold, D., Kritikos, K., & Verginadis, Y. (2019). A survey on data storage and placement methodologies for cloud-big data ecosystem. Journal of Big Data, 6(1), 1-37.
128. Mehta, M., & Shao, C. (2023). A greedy agglomerative framework for clustered federated learning. IEEE Transactions on Industrial Informatics, 19(12), 11856-11867.
129. Miao, Y., Li, F., Jia, X., Wang, H., Liu, X., Choo, K. K. R., & Deng, R. H. (2023). Reks: Role-based encrypted keyword search with enhanced access control for outsourced cloud data. IEEE Transactions on Dependable and Secure Computing, 21(4), 3247-3261.
130. Mimidis-Kentis, A., Soler, J., Veitch, P., Broadbent, A., Mobilio, M., Riganelli, O., ... & Sayadi, B. (2019). The next generation platform as a service: Composition and deployment of platforms and services. Future Internet, 11(5), 119.
131. Mistry, H. K., Goswami, A. M., Chandulalmavani, C., & Patel, R. (2024). Cloud Computing Techniques. Academic Guru Publishing House.
132. Mohamed, E. (2025). Future Trends and Real-World Applications in Database Encryption. Int. J. Electr. Eng. and Sustain., 28-39.
133. Moran, K., Bernal-Cárdenas, C., Curcio, M., Bonett, R., & Poshyvanyk, D. (2018). Machine learning-based prototyping of graphical user interfaces for mobile apps. IEEE transactions on software engineering, 46(2), 196-221.
134. Murthy, J. S., & Kar, R. (2024). Collaborative Cloud: Safeguarding Sensitive Information through Innovative Secure Data-Sharing Practices. In Cloud Security (pp. 1-16). Chapman and Hall/CRC.

135. Murugesan, G. K. (2024). Cloud services—boon or bane: a comprehensive review. SoutheastCon 2024, 108-112.
136. Musa, H. S., Krichen, M., Altun, A. A., & Ammi, M. (2023). Survey on blockchain-based data storage security for android mobile applications. Sensors, 23(21), 8749.
137. Namdev, A., Veeraiah, V., Dhamodaran, S., Islam, S., Patil, T., Pramanik, S., ... & Pandey, D. (2024). Cloud Computing Applications in Biomedicine. In Emerging Trends in Cloud Computing Analytics, Scalability, and Service Models (pp. 291-311). IGI Global Scientific Publishing.
138. Narayanan, U., Paul, V., & Joseph, S. (2022). A novel system architecture for secure authentication and data sharing in cloud enabled Big Data Environment. Journal of King Saud University-Computer and Information Sciences, 34(6), 3121-3135.
139. Navale, V., & Bourne, P. E. (2018). Cloud computing applications for biomedical science: A perspective. PLoS computational biology, 14(6), e1006144.
140. Navale, V., von Kaeppler, D., & McAuliffe, M. (2021). An overview of biomedical platforms for managing research data. Journal of Data, Information and Management, 3(1), 21-27.
141. Nguyen, T. L., Nguyen, L., Hoang, T., Bandara, D., Wang, Q., Lu, Q., ... & Chen, S. (2023). Blockchain-empowered trustworthy data sharing: Fundamentals, applications, and challenges. ACM Computing Surveys.
142. Niu, Y., Ying, L., Yang, J., Bao, M., & Sivaparthipan, C. B. (2021). Organizational business intelligence and decision making using big data analytics. Information Processing & Management, 58(6), 102725.
143. Nocker, M., Drexel, D., Rader, M., Montuoro, A., & Schöttle, P. (2023, March). HE-MAN–Homomorphically Encrypted MAchine learning with oNnx models. In Proceedings of the 2023 8th International Conference on Machine Learning Technologies (pp. 35-45).
144. Nzanywayingoma, F., & Yang, Y. (2019). Efficient resource management techniques in cloud computing environment: a review and discussion. International Journal of Computers and Applications, 41(3), 165-182.
145. Olmsted, A. (2024). Security-Driven Software Development: Learn to analyze and mitigate risks in your software projects. Packt Publishing Ltd.
146. Omer, M. A., Yazdeen, A. A., Malallah, H. S., & Abdulrahman, L. M. (2022). A survey on cloud security: concepts, types, limitations, and challenges. Journal of Applied Science and Technology Trends, 3(02), 101-111.
147. Opoku-Mensah, E., Abilimi, C. A., & Boateng, F. O. (2013). Comparative analysis of efficiency of fibonacci random number generator algorithm and gaussian Random Number Generator Algorithm in a cryptographic system. Comput. Eng. Intell. Syst, 4, 50-57.
148. Opoku-Mensah, E., Abilimi, A. C., & Amoako, L. (2013). The Imperative Information Security Management System Measures In the Public Sectors of Ghana. A Case Study of the Ghana Audit Service. International Journal on Computer Science and Engineering (IJCSE), 760-769.
149. Pan, B., Stakhanova, N., & Ray, S. (2023). Data provenance in security and privacy. ACM Computing Surveys, 55(14s), 1-35.
150. Patel, K. (2024). A review on cloud computing-based quality assurance: Challenges, opportunities, and best practices. Int. J. Sci. Res. Arch, 13(01), 796-805.
151. Peram, P. (2024). ARCHITECTURE: UNDERSTANDING IAAS, PAAS, AND SAA. INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING AND TECHNOLOGY (IJCET), 15(5), 117-128.
152. Prasetio, B. H., Widasari, E. R., Setiawan, A., & Ramadhan, H. M. (2024). Village Data Backup and Disaster Recovery: A Comparative Study of Cloud Solutions with Traditional Methods. Journal of Information Technology and Computer Science, 9(3), 218-235.
153. Radain, D., Almalki, S., Alsaadi, H., & Salama, S. (2021, March). A review on defense mechanisms against distributed denial of service (DDoS) attacks on cloud computing. In 2021 International Conference of Women in Data Science at Taif University (WiDSTaif) (pp. 1-6). IEEE.
154. Radwan, T., Azer, M. A., & Abdelbaki, N. (2017). Cloud computing security: challenges and future trends. International Journal of Computer Applications in Technology, 55(2), 158-172.

155. Rajesh, Y. S., Kumar, V. K., & Poojari, A. (2024). A unified approach toward security audit and compliance in cloud computing. Journal of The Institution of Engineers (India): Series B, 105(3), 733-750.
156. Rajmohan, R., Kumar, T. A., Sandhya, S. G., & Hu, Y. C. (2024). R-GCN: A residual-gated recurrent unit convolution network model for anomaly detection in blockchain transactions. Multimedia Tools and Applications, 1-25.
157. Rani, P., Singh, S., & Singh, K. (2024). Cloud computing security: a taxonomy, threat detection and mitigation techniques. International Journal of Computers and Applications, 46(5), 348-361.
158. Ravi Kumar, Y. V., Basha, N., Kumar KM, K., Sharma, B. M., Kerekovski, K., Ravi Kumar, Y. V., ... & Kerekovski, K. (2019). Best Practices in Oracle Data Guard with Tips and Techniques. In Oracle High Availability, Disaster Recovery, and Cloud Services: Explore RAC, Data Guard, and Cloud Technology (pp. 293-333).
159. Rekeraho, A., Cotfas, D. T., Balan, T. C., Cotfas, P. A., Acheampong, R., & Tuyishime, E. (2025). Cybersecurity Threat Modeling for IoT-Integrated Smart Solar Energy Systems: Strengthening Resilience for Global Energy Sustainability. Sustainability, 17(6), 2386.
160. Renzaho, A. M., Dachi, G., Ategbo, E., Chitekwe, S., & Doh, D. (2022). Pathways and approaches for scaling-up of community-based management of acute malnutrition programs through the lens of complex adaptive systems in South Sudan. Archives of Public Health, 80(1), 203.
161. Rios, E., Iturbe, E., Larrucea, X., Rak, M., Mallouli, W., Dominiak, J., ... & Gonzalez, L. (2019). Service level agreement-based GDPR compliance and security assurance in (multi) Cloud-based systems. IET Software, 13(3), 213-222.
162. Ronquillo, J. G., Erik Winterholler, J., Cwikla, K., Szymanski, R., & Levy, C. (2018). Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information. JAMIA open, 1(1), 15-19.
163. Roozbeh, A., Soares, J., Maguire, G. Q., Wuhib, F., Padala, C., Mahloo, M., ... & Kostić, D. (2018). Software-defined "hardware" infrastructures: A survey on enabling technologies and open research directions. IEEE Communications Surveys & Tutorials, 20(3), 2454-2485.
164. Rosa, L., Foschini, L., & Corradi, A. (2024). Empowering cloud computing with network acceleration: a survey. IEEE Communications Surveys & Tutorials.
165. Sakr, S., Liu, A., Batista, D. M., & Alomari, M. (2011). A survey of large scale data management approaches in cloud environments. IEEE communications surveys & tutorials, 13(3), 311-336.
166. Samha, A. K. (2024). Strategies for efficient resource management in federated cloud environments supporting Infrastructure as a Service (IaaS). Journal of Engineering Research, 12(2), 101-114.
167. Sampson, D., & Chowdhury, M. M. (2021, May). The growing security concerns of cloud computing. In 2021 IEEE International Conference on Electro Information Technology (EIT) (pp. 050-055). IEEE.
168. Sandu, A. K., Pydipalli, R., Tejani, J. G., Maddula, S. S., & Rodriguez, M. (2022). Cloud-Based Genomic Data Analysis: IT-enabled Solutions for Biotechnology Advancements. Engineering International, 10(2), 103-116.
169. Saravanan, A., Bama, S. S., Kadry, S., & Ramasamy, L. K. (2019). A new framework to alleviate DDoS vulnerabilities in cloud computing. International Journal of Electrical & Computer Engineering (2088-8708), 9(5).
170. Sarpatwar, K., Ratha, N. K., Nandakumar, K., Shanmugam, K., Rayfield, J. T., Pankanti, S., & Vaculin, R. (2020). Privacy enhanced decision tree inference. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (pp. 34-35).
171. Sarwar, M. I. (2023). Optimizing Virtualization for Client-Based Workloads in Cloud Computing. International Journal for Electronic Crime Investigation, 7(2).
172. Segun-Falade, O. D., Osundare, O. S., Kedi, W. E., Okeleke, P. A., Ijoma, T. I., & Abdul-Azeez, O. Y. (2024). Evaluating the role of cloud integration in mobile and desktop operating systems. International Journal of Management & Entrepreneurship Research, 6(8).
173. Sehgal, N. K., Bhatt, P. C. P., & Acken, J. M. (2020). Cloud computing with security. Concepts and practices. Second edition. Switzerland: Springer.
174. Seth, B., Dalal, S., Jaglan, V., Le, D. N., Mohan, S., & Srivastava, G. (2022). Integrating encryption techniques for secure data storage in the cloud. Transactions on Emerging Telecommunications Technologies, 33(4), e4108.

175. Shaik, A. F., Meenuga, B., Narahari, V., Harinath, Y., Thanya, R., Shaik, S. T., & Pavani, P. (2024). Sky is the limit, a comprehensive examination of cloud computing's power.
176. Sikos, L. F. (2020). Packet analysis for network forensics: A comprehensive survey. Forensic Science International: Digital Investigation, 32, 200892.
177. Singh, M. M. K., Chandna, M., & Kongala, V. Y. Y. (2024). Risk Management Framework for Cloud Migration and Selection of Suitable Cloud Service Provider. In Advances in Enterprise Technology Risk Assessment (p. 283).
178. Sneider, E. M. (2021). Best Leadership Practices of Multinational Corporations in the use of Automated Migration Tools in Adoption of Commercial Cloud Computing Platforms: A Meta-Analysis (Doctoral dissertation, Purdue University).
179. Soni, P. K., & Dhurwe, H. (2024). Challenges and Open Issues in Cloud Computing Services. In Advanced Computing Techniques for Optimization in Cloud (pp. 19-37). Chapman and Hall/CRC.
180. Sowjanya, M. C. V. N. (2024). Data Science: Exploring Future Trends. Academic Guru Publishing House.
181. Spoorthy, V., Mamatha, M., & Kumar, B. S. (2014). A survey on data storage and security in cloud computing. International Journal of Computer Science and Mobile Computing, 3(6), 306-313.
182. Srivastav, A. K., Das, P., & Srivastava, A. K. (2024). Bioinformatics and Cloud Analytics. In Biotech and IoT: An Introduction Using Cloud-Driven Labs (pp. 285-308). Berkeley, CA: Apress.
183. Steingartner, W., Galinec, D., & Kozina, A. (2021). Threat defense: Cyber deception approach and education for resilience in hybrid threats model. Symmetry, 13(4), 597.
184. Stocker, V., Knieps, G., & Dietzel, C. (2021, August). The rise and evolution of clouds and private networks–Internet interconnection, ecosystem fragmentation. In TPRC49: The 49th Research conference on communication, information and internet policy.
185. Subaveerapandiyan, A. (2023). Research data management practices and challenges in academic libraries: A comprehensive review. Library Philosophy and Practice, 1-106.
186. Sun, P. J. (2019). Privacy protection and data security in cloud computing: a survey, challenges, and solutions. IEEE Access, 7, 147420-147452.
187. Sun, Y., Meehan, T., Schlussel, R., Xie, W., Basmanova, M., Erling, O., ... & Pandit, A. (2023). Presto: A decade of SQL analytics at Meta. Proceedings of the ACM on Management of Data, 1(2), 1-25.
188. Sunyaev, A., & Sunyaev, A. (2020). Cloud computing. In Internet computing: Principles of distributed systems and emerging internet-based technologies (pp. 195-236).
189. Syamsundararao, T., Aswani, D., Prasad, K. L., Babu, G. R., Samatha, B., & Karyemsetty, N. (2022, October). Integrated Cloud Security for Data Storage and Access. In 2022 International Conference on Edge Computing and Applications (ICECAA) (pp. 102-107). IEEE.
190. Wang, Z., & Tabassum, M. (2024). A Holistic Secure Communication Mechanism Using a Multilayered Cryptographic Protocol to Enhanced Security. Computers, Materials & Continua, 78(3).)
191. Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), 9493-9532.
192. Tadapaneni, N. R. (2020). Cloud computing security challenges. International journal of Innovations in Engineering research and Technology, 7(6), 1-6.
193. Talebkhah, M., Sali, A., Marjani, M., Gordan, M., Hashim, S. J., & Rokhani, F. Z. (2021). IoT and big data applications in smart cities: recent advances, challenges, and critical issues. IEEE Access, 9, 55465-55484.
194. Tazi, F., Dykstra, J., Rajivan, P., & Das, S. (2024, May). "We Have No Security Concerns": Understanding the Privacy-Security Nexus in Telehealth for Audiologists and Speech-Language Pathologists. In Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems (pp. 1-20).
195. Thapa, B. (2024). Assessing the Viability of Privacy, Ethics, and Utility in Machine Learning Experiments via Analysis of Structured Data (Doctoral dissertation, Marymount University).
196. Tian, H., Chen, Y., Jiang, H., Huang, Y., Nan, F., & Chen, Y. (2019). Public auditing for trusted cloud storage services. IEEE Security & Privacy, 17(1), 10-22.
197. Tomarchio, O., Calcaterra, D., & Modica, G. D. (2020). Cloud resource orchestration in the multi-cloud landscape: a systematic review of existing frameworks. Journal of Cloud Computing, 9(1), 49.

198. Toyao, T., Maeno, Z., Takakusagi, S., Kamachi, T., Takigawa, I., & Shimizu, K. I. (2019). Machine learning for catalysis informatics: recent applications and prospects. ACS Catalysis, 10(3), 2260-2297.
199. Tsai, P. W., Piccialli, F., Tsai, C. W., Luo, M. Y., & Yang, C. S. (2017). Control frameworks in network emulation testbeds: A survey. Journal of computational science, 22, 148-161.
200. Tyagi, A. K. (Ed.). (2023). Privacy preservation and secured data storage in cloud computing. IGI Global.
201. Uchibeke, U. U., Schneider, K. A., Kassani, S. H., & Deters, R. (2018, July). Blockchain access control ecosystem for big data security. In 2018 IEEE International Conference on Internet of Things (iThings) ... SmartData (pp. 1373-1378). IEEE.
202. Vankayalapati, R. K. (2025). Private clouds: Ensuring control, security. The Synergy Between Public and Private Clouds in Hybrid Infrastructure Models: Real-World Case Studies and Best Practices, 50.
203. Vasconcelos Soares dos Santos, N. (2024). Data Security and User Authentication in Public Cloud Computing Environments.
204. Vasilellis, E., Gkionis, G., & Gritzalis, D. (2024). Press play, install malware: a study of rhythm game-based malware dropping. International Journal of Information Security, 23(5), 3369-3391.
205. Verstraete, M., Bambauer, J. R., & Bambauer, D. E. (2022). Identifying and countering fake news. Hastings LJ, 73, 821.
206. Wang, N., Xue, Y., Liang, H., Wang, Z., & Ge, S. (2019). The dual roles of the government in cloud computing assimilation: an empirical study in China. Information technology & people, 32(1), 147-170.
207. Wang, Z., & Tabassum, M. (2024). A Holistic Secure Communication Mechanism Using a Multilayered Cryptographic Protocol to Enhanced Security. Computers, Materials & Continua, 78(3).
208. Wei, X., Yan, Y., Guo, S., Qiu, X., & Qi, F. (2021). Secure data sharing: Blockchain-enabled data access control framework for IoT. IEEE Internet of Things Journal, 9(11), 8143-8153.
209. Williams, T. (2016). Identifying success factors in construction projects: A case study. Project management journal, 47(1), 97-112.
210. Yan, Y., Tong, X., & Wang, S. (2023). Clustered federated learning in heterogeneous environment. IEEE Transactions on Neural Networks and Learning Systems.
211. Yang, C., Huang, Q., Li, Z., Liu, K., & Hu, F. (2017). Big Data and cloud computing: innovation opportunities and challenges. International Journal of Digital Earth, 10(1), 13-53.
212. Yang, C., Yu, M., Li, Y., Hu, F., Jiang, Y., Liu, Q., ... & Gu, J. (2019). Big Earth data analytics: A survey. Big Earth Data, 3(2), 83-107.
213. Yeboah, T., Opoku-Mensah, E., & Abilimi, C.A. (2013a). A Proposed Multiple Scan Biometric-Based Registration System for Ghana Electoral Commission. Journal of Engineering, Computers & Applied Sciences (JEC&AS), 2(7).
214. Yeboah, D. T., Odabi, I., & Abilimi Odabi, M. C. A. A. (2016). Utilizing divisible load scheduling theorem in round robin algorithm for load balancing in cloud environment.
215. Yeboah, T., Opoku-Mensah, E., & Abilimi, C. A. (2013b). Automatic Biometric Student Attendance System: A Case Study Christian Service University College. Journal of Engineering Computers & Applied Sciences, 2(6), 117-121.
216. Yeboah T. & Abilimi C.A. (2013). Using Adobe Captivate to creative Adaptive Learning Environment to address individual learning styles: A Case study Christian Service University, International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181,www.ijert.org, “2(11).
217. Yeo, L. H., & Banfield, J. (2022). Human factors in electronic health records cybersecurity breach: an exploratory analysis. Perspectives in health information management, 19(Spring), 1i.
218. Yunlong, F., & Jie, L. (2024). Incentive approaches for cloud computing: challenges and solutions. Journal of Engineering and Applied Science, 71(1), 51.
219. Zhang, Y., Xu, C., & Shen, X. S. (2020). Data security in cloud storage (pp. 1-171). Berlin/Heidelberg, Germany: Springer.
220. Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, 9, 29775-29818.