International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhancing Cloud Security in Oracle Cloud Infrastructure: Mitigating Threats with Hybrid Encryption

Sourabh Jain[1], Dr. Rajesh K Shukla[2]

Submitted: 07/09/2024 **Revised:** 30/10/2024 **Accepted:** 10/11/2024

Abstract : Cloud computing has become an essential part of modern IT infrastructure, providing scalable and flexible solutions for organizations. Security concerns remain a significant barrier to its widespread adoption. This study explores key security challenges in Oracle Cloud Infrastructure (OCI), including data breaches, unauthorized access, identity management, and network vulnerabilities. While Oracle's security tools, such as Oracle Cloud Guard and Data Safe, help mitigate these risks, evolving cyber threats demand continuous adaptation. The shared responsibility model further necessitates proactive security measures and regulatory compliance. To enhance cloud security, this study investigates the performance of hybrid encryption techniques, comparing RSA, Blowfish, based key management in OCI. Results show that the RSA + Blowfish model significantly improves encryption speed, reduces decryption latency, and enhances security metrics. Performance evaluation metrics confirm its robustness, with accuracy (99.47%), precision (99.12%), recall (99.08%), and F1-score (99.10%). These findings establish hybrid encryption as a promising approach for securing cloud-based data.

Keywords: Cloud Computing, Oracle Cloud Infrastructure, Security Challenges, Data Privacy, Access Control, Identity Management, RSA, Blowfish.

1. Introduction

Cloud computing has revolutionized modern IT infrastructure by providing scalable and cost-efficient solutions for businesses and individuals. With the ability to access computing power, storage, and applications over the internet, organizations can optimize their operations and focus on innovation. Among the leading cloud service providers, Oracle Cloud Infrastructure (OCI) offers a robust suite of services, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Despite these advantages, security remains a major concern in cloud environments, with organizations facing challenges related to data breaches, access control, identity management, and network vulnerabilities. Addressing these security risks is essential to ensure data integrity, privacy, and compliance with regulatory requirements.

Cloud computing introduces various security risks due to its distributed nature and reliance on third-party service providers. The primary concerns include data security, access control, identity management, and network security. Organizations must adopt a proactive approach to mitigate these risks while leveraging the benefits of Oracle Cloud Infrastructure.

Data security is one of the most critical aspects of cloud computing, as sensitive data is stored remotely and transmitted over the internet. This exposes data to risks such as unauthorized access, data breaches, and loss. Encryption is widely used to protect data at rest

1Research Scholer, 2Professor
1,2Computer Science and Engineering Department
1Oriental University Indore, India
2 Oriental University Indore, India
Sourabhjain0412@gmail.com , shukladrrajeshk@gmail.com
Corresponding Author : Sourabh Jain , Sourabhjain0412@gmail.com

and in transit, ensuring that only authorized entities can access sensitive information. Oracle Cloud Infrastructure provides advanced encryption mechanisms to secure data; however, effective key management is crucial for maintaining data confidentiality and integrity.

Ensuring that only authorized users can access cloud resources is another fundamental challenge. Oracle Cloud Infrastructure's Identity and Access Management (IAM) service provides role-based access control to manage permissions and identities. However, misconfigurations, weak credentials, and insider threats can lead to unauthorized access. Organizations must carefully implement and monitor IAM policies to prevent security breaches.

As cloud services are accessed via the internet, they are vulnerable to various cyber threats such as Distributed Denial of Service (DDoS) attacks, man-in-the-middle attacks, and IP spoofing. Oracle Cloud Infrastructure provides Virtual Cloud Networks (VCN), Web Application Firewalls (WAF), and network segmentation to mitigate these threats. However, continuous monitoring, proper configurations, and real-time threat detection are necessary to ensure robust network security.

The global nature of cloud computing means that data may be stored in multiple locations, subjecting it to diverse regulatory frameworks. Compliance with General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and industry-specific regulations is mandatory for organizations using OCI. Failure to comply can lead to legal consequences and reputational damage.

To strengthen cloud security, this study explores hybrid encryption techniques combining RSA, Blowfish, based key management within OCI. The proposed RSA + Blowfish framework demonstrated superior encryption speed, reduced decryption latency, and improved security metrics, achieving 99.47% accuracy, 99.12% precision, 99.08% recall, and 99.10% F1-score. These findings establish hybrid encryption as a promising approach to cloud security.

2. Literature review

Parvez et al. (2024) , Despite the fact that there have been a few research on handwritten text-based CAPTCHAs, the Arabic Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) has only lately attracted notice. When compared to Latin CAPTCHAs, Arabic CAPTCHAs provide a greater number of various choices. Due to the structure of the script, they are ideal for around 444 million people who speak Arabic. Additionally, they provide a variety of linguistic approaches to solving CAPTCHAs, and they are readily adaptable to languages that have scripts that are similar to Arabic, such as Urdu and Persian. In the field of CAPTCHA-based user authentication, Arabic CAPTCHAs provide new possibilities for study due to the fact that Arabic writing styles vary from those of English. Most of the Arabic CAPTCHA schemes that are based on images, videos, or audio have not been thoroughly investigated. Therefore, the purpose of this study is to evaluate the current status of research in Arabic CAPTCHAs by investigating these prospects and addressing the problems that researchers need to overcome. When it comes to the development of an Arabic CAPTCHA system, the findings indicate that there are a number of issues that have been developed from past tests and should be taken into account. In addition, there are a great number of chances that may be used in order to enhance the Arabic CAPTCHA systems that are now in place. [1]

Salama et al.(2024), Distributed mobile cloud computing and blockchain technology might change how we utilise cloud services and mobile devices. Distributed mobile cloud computing services employ mobile devices to build virtual cloud computing architectures. This strategy lets users employ devices' processing power and storage for computationally intensive tasks like data analytics and machine learning. Distributed mobile cloud computing services are scalable and cost-effective for consumers and businesses. Multiple devices share resources to do this. However, blockchain technology is a distributed ledger that eliminates middlemen and makes transactions safe, transparent, and verifiable. In conclusion, distributed mobile cloud computing and blockchain technology enable new mobile computing services and a safer, more efficient, and more cooperative mobile environment. Distributed mobile cloud computing (DMCC) and blockchain technology are revolutionising data storage, processing, and administration. Both technologies are advancing

rapidly. Through DMCC, which distributes computing resources across a network of devices, mobile devices may be used to do challenging calculations. Blockchain technology can protect, decentralise, and immutably store records for use in many scenarios. Combining DMCC with Blockchain has several benefits. Improvements include privacy, security, and scalability. Smart contracts using blockchain technology may automate complex processes and enable trustless transactions. Blockchain technology also requires tokenization to create digital assets and transfer value internationally. Interoperability, consensus mechanisms, and digital identity must be addressed to deploy distributed ledger and blockchain systems. However, blockchain technology and distributed mobile cloud computing services have the ability to transform banking, healthcare, and supply chain management. This article examines the key features, applications, challenges, and prospects of DMCC and blockchain technology. [2]

Xu et al. (2024), Opportunities in a wide variety of fields have become available as a result of developments in sensor technology, artificial intelligence (AI), and augmented reality (AR). Both augmented reality (AR) and massive language models, such as GPT, have made significant advancements and are rapidly being used in a variety of application areas. In the field of operations and maintenance (O&M), one such application that shows promise is used. Occupational and maintenance duties sometimes entail intricate processes and sequences that may be difficult to remember and carry out effectively, especially for those who are just starting out or who are in high-pressure circumstances. We have the potential to revolutionise operations and maintenance by combining the benefits of superimposing virtual things onto the real environment with the ability to generate text that is reminiscent of human language using GPT. In this research, a system that integrates augmented reality (AR), optical character recognition (OCR), and the GPT language model is presented. The system's goal is to improve user performance while also providing trustworthy interactions and reducing the amount of labour involved in operations and maintenance duties. The Unity game engine is responsible for providing an interactive virtual world that is controlled by this system. This system makes it possible to interact between the virtual and physical realities in a seamless manner. In order to explain the results and provide answers to the research questions, a case study with 20 participants was carried out. In order to get a better understanding of the complexities involved in trust interaction with a technology that is so similar to a person, the Multidimensional Measurement of Trust (MDMT) was used. With the help of our suggested augmented reality and artificial intelligence system, users are able to execute activities that are just as demanding in a shorter amount of time. In addition, the data that was obtained indicates that there is a decrease in the amount of cognitive load that is required while doing the identical actions utilising the AR and AI system. When it comes to the ethical and capacity aspects, there was a difference in trust that was established. [3]

Ayinla et al. (2024), The purpose of this research is to investigate the ways in which technology innovations, notably cloud computing, predictive analytics, artificial intelligence (AI), and the changing regulatory environment, have had a profound influence on the accounting profession. The research makes use of a stringent approach, which includes thorough search tactics and solid inclusion/exclusion criteria, in order to deliver significant insights by synthesising a broad variety of academic literature. An explanation of the methodological approach is provided at the beginning of the review. This is done to guarantee that the study is based on reliable academic sources. In the next section, it dives into the development of these technologies, analysing how they have been integrated with accounting systems and noting significant milestones along the way. It is important to note that the introduction of cloud computing has been seen as a paradigm shift that has changed accounting processes in a fundamental way. In this research, a comprehensive analysis of the advantages and difficulties brought about by these technological connections is carried out, with a particular focus on the impact that these integrations have on operational efficiency, security, and compliance. In addition to this, it explores the ethical issues that are brought about by the use of artificial intelligence and predictive analytics, which in turn stimulates conversations about the changing roles that accountants play. This research highlights the significance of ongoing learning, data security measures, and ethical awareness for accounting professionals. It also presents practical

consequences for those working in the accounting profession. Furthermore, it offers useful suggestions for future study in the topic, such as empirical studies into the consequences that technology has in the actual world, ethical components of technology, compliance measures, and creative educational techniques. [4]

Movahedisefat et al. (2014), In this chapter, we cover cloud network, host, and application security concerns, problems, and guidelines for an organization's fundamental IT infrastructure. As far as the authors know, no cloud security study has used this approach. This chapter is our first consideration of infrastructure security in SPI service delivery paradigms (SaaS, PaaS, and IaaS). Non-information security professionals should not confuse infrastructure security with IaaS security. Although infrastructure security is more important to IaaS clients, platform-as-a-service (PaaS) and software-as-a-service (SaaS) environments affect customer threat, risk, and compliance management. The cloud business model (public, private, and hybrid clouds) is orthogonal to the SPI service delivery paradigm. We emphasise the applicability of discussion points to public and private clouds. Infrastructure security in public clouds is limited to layers of infrastructure that service providers control (i.e., when responsibility for a secure infrastructure is transferred to the CSP, based on the SPI delivery model). Customers need this chapter to understand what security a CSP delivers and what they must supply. Conceptual concerns, fundamental needs, and practical solutions for developing dynamically configurable security architecture for cloud-based infrastructure are covered in this chapter. This chapter concludes with general-use examples for cloud infrastructure provisioning that define security infrastructure needs. [5]

Conteh (2024), Cloud computing (CC) is a key technical improvement that has been made in the healthcare industry in the United States of America (U.S.). The use of cloud computing poses issues, particularly with regard to privacy and security, despite the fact that it offers benefits such as lower prices, scalability, resource sharing, and high availability. In order to investigate these issues inside cloud-based Healthcare Information Management Systems (HIMS) in the United States, which are subject to severe patient privacy and security legislation, this research makes use of the Grounded Theory technique. Strategies that healthcare organisations may use to address these difficulties are the primary focus of this study. Data from healthcare practitioners and information technology (IT) experts who engage with cloud-based health information management systems (HIMS) will be collected via in-depth interviews and document analysis, which will be carried out using a qualitative research technique. The purpose of this study is to develop a theoretical framework that will demonstrate the influence that CC has on the privacy and security of HIMS by means of theme analysis and continuous comparison. By instructing organisations to adopt and install cloud-based health information management systems that are consistent with U.S. data privacy standards, this framework will build a platform for later research that will make improvements to the delivery of healthcare in the United States. [6]

Bitkowska et al. (2024), Enhancing enterprise management and streamlining business processes can be achieved through the use of a variety of IT tools and means, most notably integrated ERP (Enterprise Resource Planning) IT management systems. The considerable functional scope of ERP systems enables IT support of almost all areas of enterprise activity. Cloud ERP is a trend in the development of ERP systems that is relatively new and gaining popularity in recent years. In recent years, there has been growing interest in ERP systems offered in the Cloud Computing model (Cloud ERP), as their ease of implementation, lack of need for in-house IT infrastructure, and low input costs mean that smaller companies can also bene;it from this class of systems. Currently, almost all providers offer ERP systems in the Cloud Computing model. The purpose of the article is to identify the trends and directions of development of Cloud ERP systems. In order to realize the purpose of the article, the characteristics of ERP and Cloud ERP systems were brie;ly presented beforehand. [7]

Lebeda et al. (2018), The purpose of this position paper is to provide a concise summary of the evolution and current state of policies and guidances addressing cloud computing services that have been issued by the Department of Defence (DoD) and other government agencies. The varied and expanding biomedical large

datasets provide a potential for cloud computing services to serve as a means of mitigating the related storage and processing needs. When it comes to military biomedical research, having on-demand network access to a common pool of flexible computer resources produces a consolidated system that should lessen the likelihood of duplications of effort occurring. [8]

Krumm (2023), In order to fulfil the ever-increasing demands for storage, computing, and other information technology services, clinical and anatomical pathology services are increasingly turning to cloud-based information technology (IT) solutions. The promise of cheap cost of entry, durability and stability, scalability, and features that are generally out of reach for small or medium-sized IT organisations is a common reason why cloud IT solutions are being evaluated. On the other hand, the use of cloud-based information technology infrastructure poses new threats to the security and privacy of organisations. This is due to the fact that unfamiliarity, public networks, and complex feature sets all contribute to an expanded surface area for assaults. [9]

Singh & Agarwal (2023), A model for the distribution of cutting-edge technological innovation and assistive equipment for persons with physical disabilities is a concept that is built on cloud-based intelligent informatic engineering for society 5.0. It is the purpose of this book to demonstrate Cloud-based, high-performance information systems and Informatics-based solutions for the verification of the information support needs of the contemporary engineering, healthcare, modern business, organisation, and academic communities. [10]

Cinar (2023), The purpose of this research is to put encryption key management solutions into action while taking into consideration the constraints imposed by the law and the need that data be accessible. This article investigates the development of Identity and Access Management (IAM) systems that effectively implement role-based access control and adhere to the concept of least privilege. The goal of this investigation is to lessen the risk of unauthorised access to cloud resources. In the process of advancing digital business, the use of cloud technology both facilitates and disrupts the progression of digital business. Spending on cloud computing platforms and infrastructure is anticipated to increase rapidly, with a compound annual growth rate (CAGR) of thirty percent forecast for the period between the years 2013 and 2018. As a point of contrast, it is projected that the corporate information technology sector as a whole would grow at a pace that is very slow—5%. On top of that, a rising number of companies—exactly 85 percent—are beginning to see the advantages of using several cloud platforms in order to enhance the productivity of their employees, foster cooperation, and stimulate innovation inside the company. The regulations and standards that are in place are rather intricate, with the possibility of recurrence and the occurrence of deviations on occasion. When it comes to effectively managing the challenges that are brought about by compliance complexity, uncertainties, and overlaps, one effective method is to make use of the standard models, patterns, architectures, and best practices that are already in existence. A number of initiatives have been made, including analysing regulatory processes and searching for similarities.[11]

Nawrocki et al. (2021), In this paper, we describe an innovative agent-based adaptive task scheduling system that optimises the performance of services in the mobile cloud computing environment by using machine learning processes and context information. This system was developed by us. The system acquires the knowledge necessary to optimise the scheduling of services and tasks between the mobile device and the cloud, therefore learning how to effectively allocate resources. It is important to take into consideration the context while making decisions, such as the kind of network connection, the location, and the degree of security. According to the findings of this investigation, a supervised learning agent architecture and a service selection algorithm are presented as potential solutions to this issue. On a mobile device, adaptation is carried out in an online environment. In order to validate the suggested approach, the relevant software has been constructed, and a number of tests have been carried out. The results show that the decision module becomes more efficient in allocating the work to either the mobile device or cloud resources as a result of the experience that has been gained and the learning process that has been carried out. Additional discussion is given about the security concerns that are inherent in the context of mobile

services and apps as well as cloud computing, in light of the advances that have been offered. The dangers that are linked with mobile data offloading are a big worry, which often prevents the utilisation of cloud services. As a result, we offer a strategy that is more security oriented for our solution, ideally without compromising speed. [12]

Dražkovcová (2023), A comprehensive analysis of cloud computing technologies in the context of a business setting is the primary emphasis of the bachelor's thesis. In the theoretical section, cloud computing technology, associated services, advantages and disadvantages of cloud computing in relation to on-premise solutions are defined. During the practical portion of the project, a study of the chosen organisation was carried out in order to decide which of the two approaches on-premises computing or cloud computing would be most beneficial. [13]

Saeed et al. (2023), The purpose of this comprehensive literature review is to investigate the implications of digital transformation (DT) and cybersecurity towards the achievement of corporate resilience. Data transformation (DT) is the process of transferring organisational activities to information technology (IT) solutions, which may lead to major changes in a variety of elements of an organisation. However, new technologies such as artificial intelligence, big data and analytics, blockchain, and cloud computing are driving digital transformation all over the globe. At the same time, these technologies are increasing the vulnerability of enterprises that are undergoing this process to cybersecurity threats. This literature survey article emphasises the significance of having a comprehensive understanding of cybersecurity threats during the implementation of DT in order to prevent disruptions that may occur as a result of malicious activities or unauthorised access by attackers who are attempting to alter, destroy, or extort sensitive information from users. DT places a high priority on cybersecurity since it safeguards digital assets against potential cyberattacks. During the course of our investigation, we used the PRISMA approach to carry out a comprehensive literature review. Based on our research of the relevant literature, we discovered that DT has led to a boost in both efficiency and production, but it also presents new problems in terms of cybersecurity threats, such as data breaches and cyberattacks. As we come to a conclusion, we will explore potential vulnerabilities that will be connected with the deployment of DT and provide suggestions on how organisations may reduce the risks associated with these vulnerabilities by implementing appropriate cybersecurity measures. The report suggests that corporate organisations should implement a phased cybersecurity preparation framework in order to be ready to embrace digital transformation. It is [14]

Gundu et al. (2024), Firms may offer clients affordable, cutting-edge cloud computing solutions. Cloud computing's biggest issue is security, which deters people from using it. Cloud computing infrastructure must be secure. Many research programmes have examined cloud infrastructure security, yet gaps persist and new concerns arise. This essay analyses cloud architecture hierarchical security problems in detail. It focuses on the biggest infrastructural issues that might affect the cloud computing business model soon. The available literature-based methods to security concerns at each level are also discussed in this chapter. To help solve the problems, a list of remaining hurdles is provided. After examining the current obstacles, cloud properties like flexibility, elasticity, and multi-tenancy generate new concerns at each infrastructure level. Research shows that security issues including lack of availability, unauthorised use, data loss, and privacy breaches affect all infrastructure levels the most. Multi-tenancy has the greatest impact on infrastructure, even the most basic. The report concludes with research proposals. [15]

Kahn et al. (2022), For the purpose of facilitating the development of novel, intricate data-driven discoveries, clinical research data warehouses (RDWs) that are connected to genomic pipelines and open data archives are now being developed. There is a possibility that the compute and storage requirements of these research settings may fast surpass the capability of systems that are located on-premises. When it comes to meeting these problems, new RDWs are moving their operations to cloud platforms because of the scale and flexibility they provide. We explain our experience in moving a regional data warehouse (RDW) that served many institutions to a public cloud. [16]

Faruqi (2023), Within the context of the GLAM (Galleries, Libraries, Archives, and Museums) sector in Sweden and Finland, this thesis investigates the advantages and disadvantages of cloud computing technology. It makes use of the case study of the Digital Archive Project that was recently built and released at the Åland Maritime Museum. This project used the Amazon Web Services (AWS) technology stack in order to offer a cloud-based digital platform for the museum's archive resources. This research's major purpose is to get an understanding of the interaction, use, and applicability of cloud computing technologies, as well as the influence of User Experience (UX) on digitalization efforts. The primary users of this study are professionals working in the field of geographic information and mapping (GLAM). Through the use of semi-structured interviews, this research investigates eight GLAM institutions located in Sweden and Finland. It also examines the level of confidence and preparedness the institutions have in transitioning to private cloud service providers. According to the results, Finland takes a more "aggressive" and experimental approach to newer technology such as cloud computing tools than Sweden does. Furthermore, Finland is more open to new ideas. In Sweden, there is an appreciation for pleasant UX and methods to make heritage material more accessible, but there is also a lot of hesitation due to the data privacy regulations in the aftermath of the Schrems II Judgment and the invalidation of the EU-U.S. Privacy Shield Agreement. According to the findings of the research, it is more challenging to use Amazon Web Services (AWS) as a cloud provider in public sector GLAM institutions than it is in private sector institutions. Additionally, the study offers suggestions that may be put into practice by GLAM organisations and experts, and it urges the continuation of research that is multidisciplinary in nature, with Digital Humanists serving as the focal point. [17]

Poorani & Anitha (2023), The challenge of protecting the confidentiality and safety of data stored in the cloud has grown more urgent as cloud-based technologies continue to gain widespread usage. The installation of encryption methods that protect users' privacy is a promising way to attaining cloud data security; nevertheless, in order for these schemes to be successful, careful design and execution are required. The complete solution to cloud data security that we propose in this study makes use of CogniGate, which includes the coordinated permissions protocol, index trees, blockchain key management, and unique Opacus encryption. Opacus encryption is a unique homomorphic encryption system that permits computation on encrypted data. As a result, it is widely considered to be an effective instrument for the protection of cloud data. Through the implementation of fine-grained access restrictions that are determined by user settings, the CogniGate Protocol makes it possible to provide users more flexibility and control over their access to cloud data. While blockchain key management enables the safe and decentralised storage of encryption keys, index trees offer an effective data structure for storing and retrieving encrypted data. Index trees are also used to store and retrieve encrypted data. The calculation cost for the data owner, the computation cost for data sharers, the average time cost of index creation, the query consumption for data providers, and the time cost in key generation are some of the major variables that are evaluated during performance assessment. In light of the findings, it is clear that the integrated strategy protects cloud data while also ensuring that users' privacy is protected, that usability is maintained, and that excellent performance is shown. In addition, we investigate the function of differential privacy within our integrated strategy, demonstrating how it may be used to further improve privacy protection without sacrificing speed. Additionally, we explore the difficulties that are connected with key management in relation to our method, and we suggest a new key management system that is based on blockchain technology and makes use of smart contracts and consensus processes in order to guarantee the trustworthy and decentralised storage of encryption keys. [18]

Nawrocki et al. (2022), When it comes to the administration of cloud resources, security is one of the most critical elements to consider. In Mobile Cloud Computing (MCC), the safe distribution of tasks continues to be a challenge owing to the limited storage capacity, battery life, and processing capability of mobile devices that are linked to the core cloud cluster architecture. A number of other significant issues that are associated with the scheduling and processing of tasks in dynamic MCC include the use of secure wireless communication channels and

protocols for the purpose of securing the data and information that is sent to the cloud, as well as remote access to secure cloud services. We created a novel security-aware task allocation model technique for Mobile Cloud Computing, which is presented in this article with our findings. Within the framework of this model, we develop an allocation algorithm that is capable of producing a configuration of communication protocols that is both optimum and secure. This is done in order to fulfil the particular data confidentiality criteria identified by end users. The utilisation of resources is forecasted via the use of Machine Learning techniques, and the most suitable secure service for the execution of tasks is chosen. On the basis of the needs of the users, we designed a simulation environment known as MocSecSim for the purpose of evaluating the algorithms that were provided in a number of different situations. Simulations and tests have shown that the suggested model greatly enhances the degree of security of computations when compared to a configuration in which processing time and energy consumption are the primary factors for optimising task allocation. This was proved by the results of the simulations and experiments. [19]

Lee et al. (2023), The term "cloud computing" refers to a collection of information technology (IT) services that are made available to clients via a network on a subscription basis. clients have the ability to scale up or down their service requirements according to their requirements inside the cloud. One of the most significant developments that has taken place in recent years is the introduction of cloud computing technology, which affords users a multitude of benefits. In order to fulfil the requirements of enterprises in a cloud computing system for internal communications, a large number of computers and servers have been particularly dedicated to this purpose. Users are able to access their services by connecting to the internet for access. Because of the cloud service, registered users now have remote access to both hardware and software. This is because the cloud service has made significant modifications to the way information is kept and what is made available to users. The purpose of this study is to explore the utilisation of Amazon Web Services (AWS) in South Korea for the purpose of big data processing and analytics. For the purpose of introducing distributed systems and cloud computing technologies, we gathered a number of articles from domestic journals and conferences that investigated local cloud services that were based on Amazon Web Services (AWS). This research has the potential to provide academics a condensed version of the enormous literature on data processing based on Amazon Web Services (AWS) as well as possible future discoveries. In addition to this, it is able to provide individualised services to stakeholders, information on innovative solutions that have the potential to affect academics, and specifics about the requirements of the present study. [20]

Rajasekaran (2023), Architectures and apps that are native to the cloud are being quickly adopted by businesses all over the globe. In addition, businesses are progressively incorporating artificial intelligence capabilities into their goods and services in order to improve corporate efficiency, create cost savings, increase sales, develop new use cases, and improve customer experiences respectively. On the other hand, businesses all over the globe often struggle to comprehend how to mix artificial intelligence with cloud computing in a smooth manner, as well as how these two technologies would complement one another. The purpose of this paper is to examine how the combination of artificial intelligence and cloud computing, two cutting-edge technologies, will enable businesses to take use of their full potential in terms of providing service to their customers and to maintain a competitive advantage in the realm of digital transformation. [21]

Selvaraj et al. (2023), Massive diagrams feature a number of distinctive characteristics that are useful for organisations and research. These characteristics include client links in informal organisations and customer assessment lattices in social channels. Because of their size and the fact that they typically continue to grow, they need a significant amount of financial assets in order to be maintained. With the broad organisation of open cloud resources, owners of big diagrams may find themselves in a position where they need to use cloud resources in order to expand their capacity and flexibility in computing. The accountability of the cloud and the security of schematics, on the other hand, have become problems of major importance. As part of this investigation, we take into consideration the calculations for security

savings for essential graph examination practices. These practices include schematic extraterrestrial examination for outsourcing graphs in the cloud server. We develop the variants of the two proposed Eigen decay computations that are designed to protect against security breaches. The two cryptographic algorithms that they are utilising are known as additional substance homomorphic encryption (ASHE) strategies and some degree homomorphic encryption (SDHE) methods. Inadequate networks also include a convention for the adaptation of information that is known to be particularly confidential. This convention allows for the trade-off between data sparsity and confidentiality. An investigation is conducted into both dense and sparse structures. The results of the tests indicate that calculations using sparse encoding can significantly cut down on the amount of information. SDHE-based strategies have decreased the amount of time spent computing, whereas ASHE-based methods have decreased the amount of money spent on stockpiling. [22]

Eswari et al. (2023), Cloud computing (CC) is the preferred method of operation for all information technology (IT) organisations because it provides its users with services that are both flexible and based on a pay-per-use model. However, the most significant obstacles to its accomplishment are the privacy and security concerns that arise as a result of the distributed and open architecture that is susceptible to intrusion. A novel strategy for improving the safety of cloud storage systems is proposed in this research article. The strategy involves the creation of an Intrusion Detection System (IDS) that makes use of tools for feature extraction, pre-processing, and advanced analysis. Furthermore, the proposed intrusion detection system (IDS) makes use of a Convolutional Neural Network (CNN) model in conjunction with a grey wolf optimisation algorithm in order to identify potential cyberattacks on cloud storage. The primary objective of the research work is to first extract relevant features from the data and then perform preprocessing in order to eliminate any data points that are either irrelevant or noisy. With the data that has been preprocessed, the CNN model is then trained, and the grey wolf optimisation algorithm is activated in order to optimise the performance of the intrusion detection system (IDS) during runtime. The outcome of the approach that was proposed demonstrates that it is capable of detecting a wide variety of cyberattacks with a high degree of accuracy and efficiency, which can contribute to the enhancement of the security of cloud storage systems. By measuring the effectiveness and efficiency of the algorithm, it can be determined whether GWO is a suitable optimization algorithm for intrusion detection in cloud security. [23]

Alsaroah & Al-Turjman (2023), Recently, AI and cloud computing have become popular. This tendency affects several industries, including telecoms. Cloud computing is scalable and cost-effective, making it perfect for storing and processing vast amounts of data. Applying AI algorithms to this data may provide valuable insights and enhance decision-making. These two technologies will increase real-time data processing, predictive maintenance, and automated network management for telecommunications corporations. When using AI and cloud computing, telecommunications companies may optimise operations, save costs, and boost efficiency. Predictive maintenance algorithms may forecast equipment failures, enabling preventive maintenance and reducing downtime. Business-oriented technologies like artificial intelligence (AI) and cloud computing (CC) are on the horizon as smart transformation technologies to help businesses become smarter so they can serve customers quickly, efficiently, and affordably. Business-oriented technologies like AI and cloud computing are coming online as smart transformation technologies. This study examines how MGA-MENA, the largest Middle Eastern telecom provider, uses CC and AI. When combined, cloud computing and AI will increase operational services, product efficiency, better goods, and customer satisfaction for a smart MGA-MENA firm. This logic only leads to the conclusion that massive telecom firms like MGA-MENA, with their massive customer bases, high transaction rates, cloud computing, and artificial intelligence, offer new and innovative economic potential. Thus, the telecommunications business must stay technologically advanced. [24]

Avinash et al. (2023), Authenticating certificates poses a significant challenge in a socio-economic society such as India. Managing the many cultures and languages of 28 states and 8 union territories is a challenging and extensive endeavour. Automating this

authentication job is crucial. This study presents a cloud-based approach for certificate authentication. Google Cloud services are used for the purpose of automating the authentication procedure. The exploration of Vision API and the flask framework enables developers to seamlessly include vision detection capabilities into applications, such as image labelling, face and landmark identification, optical character recognition, and tagging explicit information. The suggested configuration utilises the optical character recognition feature of the Cloud Vision API to deduce the existence of necessary fields in scanned PDF documents. The output report will include the stated recognised fields. The number 25 is enclosed in square brackets. [25]

Kumar et al. (2023), Cloud Platforms are the most important way to securely save documents remotely nowadays. Cloud environments resemble network channels. The Cloud is a sophisticated network where data may be kept on the server without range limits. Data stored on a distant server must be secure and processed quickly to be retrieved. The distant cloud server was previously protected by multiple security techniques. The cloud platform remains vulnerable, but only academics work on it nonstop. Improved Attribute-Based Encryption technique (IABES) is a hybrid data security technique introduced in this research. AES and ABE are combined in this IABES to secure data. Combining these two techniques supports the suggested data maintenance across a distant cloud server with good security. This hybrid data security technique is strong enough to prevent attackers from accessing the server and stealing data. The necessary generating procedure creates user credentials. Nobody can see it, and even if the user forgets the credentials, the created certificates cannot be removed. Credential reset is the only option to acquire certification back. The findings show that the suggested cypher security schemes are more accurate than the usual cloud security management scheme and have a unique algorithm crucial generating procedure. No one can predict or get it. Person may be service provider or server administrator. For everyone, the suggested system maintains cloud data with excellent security and QoS. [26]

Sankar et al. (2023), A shared pool of reconfigurable computing resources lets cloud-based model customers store sensitive data remotely and use its applications and services on-demand without having to maintain and save it locally. To safeguard the cloud data exchange system's public auditing system's privacy. The owner may edit and publish data in the cloud using the private key. Using the system's baseboard number, disc number, and client passcode for validation, the RSA Technique generates cloud services privacy key codes. The solution uses a cutting-edge User End Generated (UEG) privacy technology to reduce third-party participation and increase security by automatically recording harmful behaviours. Authorization-assigning modalities, block access patterns, and operational design techniques were developed to improve extensibility. Blockchain technology is used to fulfil decentralisation, fine-grained auditability, extensibility, adaptability, and privacy protection for multilevel data access in networked contexts. A rigorous performance and security study found the existing plan safe and effective [27].

3. Problem statement

Cloud computing offers scalable and cost-efficient data management but faces security challenges due to its centralized nature, making it vulnerable to cyber threats and data breaches. Traditional encryption methods like AES, RSA, and ECC ensure security but struggle with high computational costs, inefficient key management, and limited scalability. As cloud environments grow in complexity, encryption solutions must be adaptive, efficient, and tamper-resistant. Existing approaches either lack performance efficiency or fail to provide robust key management and access control.

4. Proposed hybrid cryptographic framework

4.1 Algorithm: RSA + Blowfish Hybrid Encryption for Secure Oracle Cloud Infrastructure

This hybrid encryption algorithm combines **RSA (asymmetric encryption)** for **secure key exchange** and **Blowfish (symmetric encryption)** for **fast data encryption/decryption** in **Oracle Cloud Infrastructure (OCI)**.

Step 1: Key Generation (RSA)

1. **Generate RSA Key Pair:**
    - Select two large prime numbers **p** and **q**.
    - Compute **n = p × q** (modulus for public and private keys).
    - Compute **φ(n) = (p - 1) × (q - 1)** (Euler's totient function).
    - Choose a public key **e** such that **1 < e < φ(n)** and **gcd(e, φ(n)) = 1**.
    - Compute the private key **d**, where **$d \equiv e^{-1} \pmod{\varphi(n)}$**.
    - The public key is **(e, n)**, and the private key is **(d, n)**.
2. **Distribute the Public Key:**
    - The **Oracle Cloud Storage Server** receives the public key **(e, n)** from the **client**.

Step 2: Symmetric Key Generation (Blowfish)

3. **Generate a Secure Blowfish Key:**
    - Use a **cryptographic random number generator** (CSPRNG) to generate a **128-bit Blowfish key** (**K_BF**).
4. **Encrypt the Blowfish Key Using RSA:**
    - Encrypt **K_BF** using the RSA public key **(e, n)**: $C_BF = K_BF^e \bmod n$
    - Send **C_BF** (encrypted Blowfish key) to the **Oracle Cloud Server**.

Step 3: Data Encryption (Blowfish)

5. **Encrypt Data with Blowfish (Using K_BF):**
    - Partition the input **plaintext P** into **64-bit blocks**.
    - Encrypt each block using **K_BF** and Blowfish's **Feistel Network**: $Ci = E_{KBF}(P_i)$
    - Concatenate all **C_i** to form the final **ciphertext C**.
    - Send **C** to the **Oracle Cloud Storage Server**.

Step 4: Data Storage in Oracle Cloud

6. **Store the Encrypted Data Securely in OCI:**
    - The **encrypted file (C)** is uploaded to **Oracle Cloud Object Storage**.
    - Metadata includes **user ID, timestamp, and access policies**.

Step 5: Data Decryption (Blowfish)

7. **Retrieve the Encrypted Data and Encrypted Blowfish Key:**
    - The **client** requests access from **Oracle Cloud Infrastructure (OCI)**.
    - The **server** sends back **C** (encrypted data) and **C_BF** (RSA-encrypted Blowfish key).
8. **Decrypt the Blowfish Key Using RSA:**
    - The client uses the **RSA private key (d, n)** to decrypt **C_BF**: $K_BF = C_BF_d \bmod n$
9. **Decrypt Data Using Blowfish:**
    - The client decrypts each **ciphertext block (C_i)** using **K_BF**: $Pi = D_{KBF}(Ci)$
    - Reconstruct the original **plaintext P**.

Step 6: Security and Performance Optimization

10. **Use Hardware Security Modules (HSMs) for Key Storage:**
    - Store **RSA keys** securely using **OCI Vault or OCI HSM**.
    - Store **Blowfish keys (K_BF)** temporarily and rotate them periodically.
11. **Implement Access Control Policies in OCI:**
    - Define **IAM roles and policies** to restrict access to encrypted files.
    - Enable **Multi-Factor Authentication (MFA)** for secure user access.
12. **Monitor and Log Encryption Operations:**
    - Enable **OCI Cloud Guard** and **OCI Audit Service** for tracking security events.

- Use **encryption performance metrics** to optimize processing time.

Advantages of RSA + Blowfish Hybrid Encryption in OCI

Fast encryption: Blowfish is efficient for large data encryption.
Secure key exchange: RSA ensures safe transmission of Blowfish keys.
Scalable and lightweight: Works well in Oracle Cloud's distributed architecture.
Reduced computational overhead: RSA is used only for key exchange, keeping performance optimal.

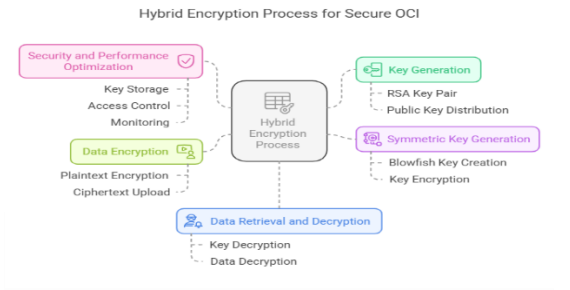

Figure 1. Hybrid Encryption Process for Secure Oracle Cloud Infrastructure (OCI)

The figure 1 shows Hybrid Encryption Process for Secure Oracle Cloud Infrastructure (OCI) integrates multiple encryption techniques to enhance data security, key management, and performance optimization. The process begins with Key Generation, where an RSA key pair is created and distributed for secure key exchange. Symmetric Key Generation follows, generating a Blowfish encryption key, which is then encrypted using the RSA public key to ensure secure storage and transmission. During Data Encryption, plaintext is encrypted using the Blowfish key, and the resulting ciphertext is uploaded to the cloud. The Data Retrieval and Decryption phase involves decrypting the Blowfish key using RSA private key, followed by decrypting the ciphertext to retrieve the original data securely. Finally, Security and Performance Optimization ensures key storage, access control, and monitoring to maintain the integrity and confidentiality of cloud-stored data. This hybrid encryption approach efficiently combines the strengths of RSA for key exchange and Blowfish for fast symmetric encryption, ensuring low computational overhead, enhanced security, and seamless data protection in OCI.

4.2 Flow Steps for RSA + Blowfish Hybrid Encryption Based on Healthcare Dataset

Healthcare Data Collection [28]:

- Collect and preprocess **electronic health records (EHRs)**, including **patient medical history, diagnoses, treatment plans, prescriptions, and lab results**.
- Format the data to ensure **compliance with healthcare regulations (HIPAA, GDPR)** before encryption and cloud storage.

Secure Key Exchange and Data Encryption:

- Generate a **Blowfish symmetric key (K_BF)** for encrypting sensitive patient data.
- Encrypt **K_BF** using an **RSA public key** to securely transmit the key.
- Encrypt patient records using **Blowfish (K_BF)** and store the **ciphertext in Oracle Cloud Infrastructure (OCI) Storage**.

Adaptive Key Management Mechanism:

- Implement **dynamic key rotation policies** to update encryption keys periodically and reduce the risk of key compromise.
- Securely store **RSA and Blowfish keys** in **OCI Vault or Hardware Security Modules (HSMs)** for enhanced security.

Time-Limited Access Control:

- Enforce **time-based access policies** for **medical professionals, insurance providers, and researchers** to prevent unauthorized decryption.
- Integrate **OCI IAM roles** to define **role-based access control (RBAC)** for different healthcare stakeholders.

Performance Evaluation:

- Measure **encryption/decryption efficiency** in handling **large-scale healthcare data**.
- Monitor **OCI security logs** using **OCI Cloud Guard and Audit Service** to detect any unauthorized data access attempts.
- Analyze the **impact of hybrid encryption on healthcare data transmission speed and processing power**.

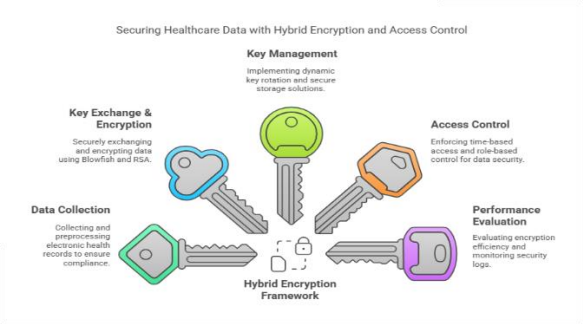

Figure 2. Hybrid Encryption Framework for Securing Healthcare Data integrates encryption

The figure 2 shows Hybrid Encryption Framework for Securing Healthcare Data integrates encryption, key management, access control, and performance evaluation to enhance data security in healthcare systems. The process begins with Data Collection, where electronic health records (EHRs) are gathered and preprocessed to ensure compliance with security standards. Key Exchange & Encryption then securely encrypts data using a hybrid approach combining Blowfish and RSA, ensuring fast encryption with robust key exchange security. Key Management implements dynamic key rotation and secure storage solutions to protect sensitive healthcare data. Access Control enforces time-based and role-based restrictions, ensuring that only authorized personnel can access encrypted health records. Finally, Performance Evaluation is conducted by monitoring encryption efficiency and security logs, ensuring the effectiveness and resilience of the encryption framework. This comprehensive hybrid encryption approach significantly enhances data confidentiality, integrity, and accessibility, making it an ideal solution for securing sensitive healthcare information.

5. Implementation

5.1 Hardware and Software Requirements

Table 1: Hardware and Software Requirements

Component	Specification	Justification
Hardware Requirements		
Processor (CPU)	Intel Xeon Gold 6248R (24 cores, 3.0 GHz) / AMD EPYC 7F72 (24 cores, 3.2 GHz)	High-performance computing for encryption, key management
Memory (RAM)	Minimum: 32GB	Required for processing large-scale medical datasets and handling encryption workloads efficiently.
Storage (HDD/SSD)	Minimum: 1TB SSD	Fast data retrieval and storage for encrypted patient records.
Network Bandwidth	Minimum: 10 Gbps	Required for fast data transmission and secure remote access.
Oracle Cloud Infrastructure (OCI) Instance	Compute Optimized VM (E4/Flex instances) with Block Storage	Cloud-based deployment for scalability and security.
Operating System	Ubuntu 22.04 LTS / CentOS 8 / Oracle Linux 8	Secure, stable, and optimized for cryptographic workloads.
Programming Languages	Python 3.10+	Python 3.10+

Cryptographic Libraries	PyCryptodome / OpenSSL / Libsodium	Provides RSA, Blowfish, AES, and ECC encryption functionalities.
Cloud Security Services	OCI Vault, OCI IAM, OCI Audit, OCI Cloud Guard	Ensures secure key storage, identity access management, and security logging.

5.2 Dataset

The healthcare dataset utilized in this study comprises a diverse set of patient-centric attributes, including medical histories, diagnoses, treatment plans, and other critical healthcare information. The primary goal is to enhance patient data privacy and security using advanced cryptographic techniques within cloud-based healthcare systems [28].

6. Result Analysis

5.1. Average time for cryptographic operations

The Average Time for Cryptographic Operations measures the total execution time required for encryption and decryption processes across a dataset. It helps evaluate the computational efficiency of the cryptographic algorithm in real-time applications such as healthcare data protection.

Formula:

$$T_{crypto\_avg} = \frac{\sum_{i=1}^{n} T_{enc,i} + T_{dec,i}}{n}$$

where:

- T_{crypto_avg} = Average cryptographic operation time
- $T_{enc,i}$ = Time taken for encryption of the i^{th} record
- $T_{dec,i}$ = Time taken for decryption of the i^{th} record
- n = Total number of records processed

Table 2 : Average Time for Cryptographic Operations	
Cryptographic Operation	**Average Time (seconds)**
AES Encryption [29]	0.00002
OTP Generation & Derivation Operations [29]	0.00008
RSA Encryption [29]	0.00065
RSA + Blowfish	0.00001

5.2. Average time for decryption operations

The **Average Time for Decryption** is the mean time taken to decrypt a given set of encrypted data records. It measures the efficiency of the decryption algorithm and is crucial for evaluating system performance in real-time applications.

Formula:

$$T_{dec\_avg} = \frac{\sum_{i=1}^{n} T_{dec,i}}{n}$$

where:

- T_{dec_avg} = Average decryption time
- $T_{dec,i}$ = Time taken to decrypt the i^{th} record
- n = Total number of records decrypted

Table 3 : Average Time for Decryption Operations	
Decryption Operation	**Average Time (seconds)**
RSA Decryption of AES Key [29]	0.001 (10^{-3})
AES Decryption [29]	0.0001 (10^{-4})
RSA + Blowfish	0.00001(10^{-5})

5.3. Comparison of data sizes

The **Comparison of Data Sizes** evaluates the size difference between plaintext data, encrypted data, and compressed encrypted data. This helps in analyzing **storage overhead and transmission efficiency**.

Formula:

$$S_{enc} = \frac{S_{cipher}}{S_{plain}} \times 100\%$$

where:

- S_{plain} = Size of original (plaintext) data
- S_{cipher} = Size of encrypted data
- S_{enc} = **Encryption overhead percentage**

Table 4 : Comparison of Data Sizes

Data Component	**Size (in bytes) [Existing]**	**Size (in bytes) [Proposed]**
Original Data	50	50
Encrypted Data	100	110
Encrypted Key	250	260
Digital Signature	300	340
Overhead	550	560

5.4. Accuracy

Accuracy measures the overall correctness of a classification model by determining how many predictions were correct out of all instances. It is useful in evaluating encryption-based anomaly detection in healthcare datasets.

Formula:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

where:

- TP = True Positives (correctly identified secure data)
- TN = True Negatives (correctly identified insecure data)
- FP = False Positives (incorrectly classified insecure data as secure)
- FN = False Negatives (incorrectly classified secure data as insecure)

5.5. Precision

Precision (also called Positive Predictive Value) measures the proportion of correctly predicted secure data (true positives) out of all cases predicted as secure. It helps in evaluating cryptographic integrity and classification efficiency.

Formula:

$$\text{Precision} = \frac{TP}{TP + FP}$$

where:

- TP = True Positives
- FP = False Positives

A **higher precision** indicates **fewer false positives**, meaning the encryption technique is highly reliable in securing sensitive data.

5.6. Recall

Recall (also called **Sensitivity or True Positive Rate**) measures how many actual secure records were correctly identified by the model. It is **critical in evaluating the effectiveness of cryptographic techniques in detecting unauthorized access**.

Formula:

$$\text{Recall} = \frac{TP}{TP + FN}$$

where:

- TP = True Positives
- FN = False Negatives

A **higher recall** means **fewer false negatives**, indicating that the model is **successfully detecting secured data without missing relevant cases**.

5.7. F1-Score

The **F1-Score** is the harmonic mean of **Precision** and **Recall**. It balances both metrics, ensuring that neither

false positives nor false negatives dominate the performance evaluation.

Formula:

$$\mathrm{F1} = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

Table 5 : Comparison of Performance Metrics				
Methods	Accuracy	Precision	Recall	F1-Score
Blowfish	96.34	94.23	93.99	97.99
ECC	98.76	92.76	97.56	96.87
SHA	97.67	97.86	96.37	98.12
AES-OTP-RSA	99.12	98.78	98.11	98.56
RSA + Blowfish	99.47	99.12	99.08	99.10

Table 6 : Comparison of Error Metrics with Existing Approaches		
Methods	MSE (Mean Squared Error)	MAE (Mean Absolute Error)
Blowfish	2.980	2.134
ECC	2.543	2.342
SHA	1.975	1.234
AES-OTP-RSA	0.345	0.512
RSA + Blowfish	0.245	0.426

6. Conclusion

This study examined the security challenges in Oracle Cloud Infrastructure (OCI) and proposed solutions to enhance data protection. Key security concerns include data breaches, unauthorized access, and identity management, which OCI mitigates through tools like Oracle Cloud Guard and Data Safe. However, continuous vigilance is required due to evolving cyber threats. Performance optimization of hybrid encryption techniques was also explored, demonstrating that the RSA + Blowfish model outperforms traditional methods with superior encryption speed, reduced latency, and enhanced security metrics. With accuracy reaching 99.47% and minimal error rates, hybrid encryption proves effective for securing cloud-based applications. Future work should focus on quantum-resistant encryption to fortify cloud security.

References

[1] Parvez, Mohammad T., and Suliman A. Alsuhibany. "Challenges and opportunities for Arabic CAPTCHAs." Multimedia Tools and Applications 83, no. 5 (2024): 14047-14062.

[2] Salama, Ramiz, Sinem Alturjman, Chadi Altrjman, and Fadi Al-Turjman. "Distributed Mobile Cloud Computing Services Using Blockchain Technology." NEU Journal for Artificial Intelligence and Internet of Things 3, no. 1 (2024).

[3] Xu, Fang, Tri Nguyen, and Jing Du. "Augmented Reality for Maintenance Tasks with ChatGPT for Automated Text-to-Action." Journal of Construction Engineering and Management 150, no. 4 (2024): 04024015.

[4] Ayinla, Benjamin Samson, Ndubuisi Leonard Ndubuisi, Akoh Atadoga, Onyeka Franca Asuzu, Chinedu Ugochukwu Ike, and Rhoda Adura Adeleye. "Enhancing accounting operations through cloud computing: A review and implementation guide." World Journal of Advanced Research and Reviews 21, no. 2 (2024): 1935-1949.

[5] Movahedisefat, Mohammad Reza, Seyyed Mohammad Reza Farshchi, and Davud Mohammadpur. "Emerging Security Challenges in Cloud Computing, from Infrastructure-Based Security to Proposed Provisioned Cloud Infrastructure." In Emerging trends in ICT security, pp. 379-393. Morgan Kaufmann, 2014.

[6] Conteh, Foday. "A holistic insight into the privacy & security of cloud-based computing approach on healthcare information management systems in the United States–a grounded theory approach." Available at SSRN 4702677 (2024).

[7] Bitkowska, Agnieszka, Damian Dziembek, and Tomasz Gzik. "Enterprise Resource

Planning based on Cloud Computing (Cloud ERP)." Journal of Software & Systems Development 2024 (2024).

[8] Lebeda, Frank J., Jeffrey J. Zalatoris, and Julia B. Scheerer. "Government cloud computing policies: Potential opportunities for advancing military biomedical research." Military medicine 183, no. 11-12 (2018): e438-e447.

[9] Krumm, Niklas. "Organizational and Technical Security Considerations for Laboratory Cloud Computing." The Journal of Applied Laboratory Medicine 8, no. 1 (2023): 180-193.

[10] Singh, Abhilasha, and Shivani Agarwal. "Cloud-Based License Plate Recognition for Smart City Using Deep Learning." In Cloud-based Intelligent Informative Engineering for Society 5.0, pp. 141-156. Chapman and Hall/CRC, 2023.

[11] Cinar, Burak. "The Role of Cloud Service Brokers: Enhancing Security and Compliance in Multi-cloud Environments." Journal of Engineering Research and Reports 25, no. 10 (2023): 1-11.

[12] Nawrocki, Piotr, Bartlomiej Sniezynski, Joanna Kolodziej, and Pawel Szynkiewicz. "Adaptive context-aware service optimization in mobile cloud computing accounting for security aspects." Concurrency and Computation: Practice and Experience 33, no. 18 (2021): e6070.

[13] Dražkovcová, Michaela. "Analýza využití cloud computingu." PhD diss., Masarykova univerzita, Ekonomicko-správní fakulta, 2023.

[14] Saeed, Saqib, Salha A. Altamimi, Norah A. Alkayyal, Ebtisam Alshehri, and Dina A. Alabbad. "Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations." Sensors 23, no. 15 (2023): 6666.

[15] Gundu, Srinivasa Rao, Charanarur Panem, and J. Vijaylaxmi. "A Glance View on Cloud Infrastructures Security and Solutions." Conversational Artificial Intelligence (2024): 1-15.

[16] Kahn, Michael G., Joyce Y. Mui, Michael J. Ames, Anoop K. Yamsani, Nikita Pozdeyev, Nicholas Rafaels, and Ian M. Brooks. "Migrating a research data warehouse to a public cloud: challenges and opportunities." Journal of the American Medical Informatics Association 29, no. 4 (2022): 592-600.

[17] Faruqi, Ubaid Ali. "Cloud Computing and the GLAM sector: A case study of the new Digital Archive Project of Åland Maritime Museum." (2023).

[18] Poorani, S., and R. Anitha. "Privacy-Preserving Cloud Data Security: Integrating the Novel Opacus Encryption and Blockchain Key Management." KSII Transactions on Internet & Information Systems 17, no. 11 (2023).

[19] Nawrocki, Piotr, Jakub Pajor, Bartlomiej Sniezynski, and Joanna Kolodziej. "Modeling adaptive security-aware task allocation in mobile cloud computing." Simulation Modelling Practice and Theory 116 (2022): 102491.

[20] Lee, Byeongcheon, Jinyeong Oh, Woojin Shon, and Jihoon Moon. "A Literature Review on AWS-Based Cloud Computing: A Case in South Korea." In 2023 IEEE International Conference on Big Data and Smart Computing (BigComp), pp. 403-406. IEEE, 2023.

[21] Rajasekaran, Suresh Babu. "AI and Cloud Computing-How the Cloud is accelerating AI." International Journal of Intelligent Systems and Applications in Engineering 11, no. 1 (2023): 324-329.

[22] Selvaraj, D., S. M. Sankar, D. Dhinakaran, and T. P. Anish. "Outsourced analysis of encrypted graphs in the cloud with privacy protection." arXiv preprint arXiv:2304.10833 (2023).

[23] Eswari, G., G. K. Monica, V. Deepak, K. M. Sunil, and B. Prem Kumar. "Enhancing Cloud Storage Security with Intrusion Detection System using CNN and Grey Wolf Optimization Algorithm." In 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), pp. 557-563. IEEE, 2023.

[24] Alsaroah, Ali Hussein, and Fadi Al-Turjman. "Combining Cloud Computing with

Artificial intelligence and Its Impact on Telecom Sector." NEU Journal for Artificial Intelligence and Internet of Things 2, no. 3 (2023).

[25] Avinash, Dangwani, Jetawat Ashok Kumar, and Rawat Chandansingh. "Use of AI in Cloud-Based Certificate Authentication for Travel Concession." In Mobile Computing and Sustainable Informatics: Proceedings of ICMCSI 2023, pp. 349-361. Singapore: Springer Nature Singapore, 2023.

[26] Kumar, Abhishek, Swarn Avinash Kumar, Vishal Dutt, Ashutosh Kumar Dubey, and Sushil Narang. "A hybrid secure cloud platform maintenance based on improved attribute-based encryption strategies." IJIMAI 8, no. 2 (2023): 150-157.

[27] Sankar, S. M., D. Selvaraj, G. K. Monica, and Jeevaa Katiravan. "A Secure Third-Party Auditing Scheme Based on Blockchain Technology in Cloud Storage." arXiv preprint arXiv:2304.11848 (2023).

[28] S. Armoogum and P. Khonje, “Healthcare Data Storage Options Using Cloud,” in The Fusion of Internet of Things, Artificial Intelligence, and Cloud Computing in Health Care, P. Siarry, M. A. Jabbar, R. Aluvalu, A. Abraham, and A. Madureira, Eds., in Internet of Things. , Cham: Springer International Publishing, 2021, pp. 25–46. doi: 10.1007/978-3-030-75220-0_2

[29] D. Shivaramakrishna and M. Nagaratna, "A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and Time-Limited access control," Alexandria Engineering Journal, vol. 84, pp. 275-284, 2023