The Importance of Cryptography in Cloud Computing

Assist Lect. Saja Alaam Talib
Department of Control and Systems Engineering,
University of Technology, Baghdad, Iraq.
Email: sajaalaam@yahoo.com

أهمية التشفير في الحوسبة السحابية

م. م. سجى علام طالب
قسم السيطرة و النظم-الجامعة التكنولوجبية، بغداد \ العراق

المستخلص

نمت الحوسبة السحابية كمفهوم مقبول على نطاق واسع في وقت واحد، مثل أجهزة الإنذار لأمن البيانات والمعلومات. تسعى هذه الورقة إلى تحديد الأدوار الشاملة للتشفير في معالجة هذه المشكلات في البيئة السحابية. تبدأ الدراسة بالخلفية التاريخية للتشفير ثم تنتقل لتحليل الاتجاهات في تكنولوجيا المعلومات قبل مناقشة التحديات التي تواجه الأمن في الحوسبة السحابية. والهدف من نشره هو تسليط الضوء على أهمية استخدام تقنيات التشفير لحماية سرية المعلومات وسلامتها والامتثال لها. تم تطبيق الجمع بين مراجعة الأدبيات وطريقة دراسة الحالة، واستخلاص المعرفة من أمثلة الاستخدام الجيد للتشفير والدروس المستفادة من الانتهاكات الأمنية. وهي تكشف مدى أهمية علم التشفير في تعزيز الأمن والحفاظ على ثقة العملاء. يتم تشجيع ممارسي تكنولوجيا المعلومات الرئيسيين على عدم التخفيف من حذرهم واعتماد استراتيجية أمنية متكاملة لدرء الهجمات المستقبلية. اختتام الدراسة هو تجميع للتحليل اللاحق، مما يسلط الضوء على استمرار تطبيق التشفير لأمن نظام المعلومات السحابية.

الكلمات المفتاحية: التشفير، الحوسبة السحابية، أمن البيانات، التشفير، المعلومات.

Abstract

Cloud computing has grown as a widely accepted concept simultaneously, as the alarms for the security of data and information. This paper seeks to establish the comprehensive roles of cryptography in tackling these issues in the Cloud environment. The study begins with the historical background of cryptography and then moves on to analyze trends in information technology before discussing on the challenges to security in cloud computing. The goal of its publication is to highlight the importance of using cryptographic technologies for the protection of information confidentiality, its integrity and compliance. The combination of literature review and the case study method was applied, pulling knowledge from examples of good cryptographic use and the lessons learned from breaches in security. They reveal how cryptology is crucial in the furthering of cloud security and in maintaining customers' faith. Key information technology practitioners are encouraged not to relax their guard and adopt an integrated security strategy to ward off future attacks. Conclusion of the study is in synthesis of the subsequent analysis, highlighting the continued applicability of cryptography for Cloud Information System security.

Keywords: Cryptography, Cloud Computing, Data Security, Encryption, Information.

1. Introduction

As a relatively new development in the IT disparate and complex area, cloud computing has revolutionized the way information and data is hosted and managed by organizations and consumers. This is an innovative method that enhances capability, versatility, and economic utility by allowing computing resources to be hosted remotely by a third party. Nevertheless, like any other solution, clouds have certain risks and concerns that are largely related to security issues and, therefore, require the application of appropriate security measures [1].

It's for this reason that cryptographic techniques remain fundamental approaches for curbing the threat of data corruption and unauthorized access of data in cloud computing. These techniques work effectively ensuring confidentiality of the data transfers and data stored regardless of their location and are thus crucial in developing guarded paths between the users and cloud services. This paper approaches the role played by cryptography in the field of cloud computing, and its ability to tackle numerous security issues, as a multifunctional tool. Starting from creating secure methods for data encryption to handle both keys and users, elementary aspects of cryptography lay a solid foundation for cloud computing. When arguing about the use of cryptographic applications in the cloud, their advantages and disadvantages, and the potential risks in this sphere, it is possible to conclude about the significance of indicating the fact that, in order to provide the effective usage of cloud computing services, as well as to avoid certain threats, it is crucial to gain detailed knowledge of these techniques for both providers and consumers of cloud services.

Concerning this exploration, it is intended to explain the necessity of cryptography in terms of risk management and maintaining the latter in compliance with the prescribed rules to build credibility and have a more secure cloud computing platform [2].

With the increase in the growth of using various organizations' assets in cloud infrastructures, the matter of protecting it has become an issue of increasing concern. The importance of cloud computing is that most companies and people are storing their information on cloud environments, and this opens new risks such as hacking others' information, data theft, and more. According to these challenges the following is deemed necessary because the information that is being sought to be stored on a cloud may be personal information or even sensitive business information [3].

Consequently, this work intends to highlight the importance of cryptography as an essential approach toward the protection of information in cloud computing. With cloud adoption at an all-time high, it is crucial to outline the use of cryptographic methods to manage the threats arising from improper use of these services which may compromise the privacy and data integrity. This study aims at contributing as to how cryptographic elements are used in cloud computing as a system, while emphasizing the fact that data security is achieved at different sub-phases throughout transfer, storage, and processing. In this way, the research aims not only to contribute to the existing knowledge of the precautions required for the formation of a stable cloud computing climate [4], but also to provide the foundation for forming a secure one. The cloud computing application diagram is highlighted in the figure below, Figure 1.

Figure 1 Cloud computing application diagram

2- Literature Review

Historical Evolution of Cryptography

Effective communication requires that data transmitted through communications channels remain secure meaning cryptology is the science of secure communication since its early beginnings to present times illustrates this struggle. Due to this, encryption in early civilizations was viewed as a technique that would facilitate the passing of messages while at the same time ensuring that none of the civilians had any clue as to what was going on. With time, the idea of cryptography developed, and there were several inventions at some specific periods of time; especially during a war; for instance, the Enigma machine in the Second World War [5]. The new starter came with changes by moving from symmetric key systems to a new public key cryptography system. The Italian communication protocol that was established based on this theory

is the key enabling process of this shift, while the work of Whitfield Diffie and Martin Hellman in the 1970s paved the way for the advancement by making possible to exchange cryptographic keys over insecure channels. To continue with the new evolution in generation, the RSA algorithm, which was developed by Ron Rivest, Adi Shamir, and Leonard Adleman, offered the much-needed practical approach to implementing public key cryptography [6].

The practice of cryptographic standards emerged during the last 20 years of the twentieth century, and institutions such as NIST were actively defining preferable algorithms. The advanced encryption standard (AES) Symmetric Key Cryptography Algorithm became a global standard in the year 2001 which eventually initiated the development of other cryptographic practices. In total then, the past developmental history of cryptography shows that this discipline has been dynamic in its capacity to address the problems of protecting information in various timelines. From the earliest modes of protecting the sending and receiving messages from unauthorized third parties to the evolution of contemporary cryptographic techniques, this journey makes us rich in understanding as to how the science of cryptography has evolved over the time and how much it continues to be important in the world of information security. This is something that is very important to understand to grasp the extent of the cryptographic techniques that are employed even in the current generation technologies and especially when it comes to personal data security within cloud-computing architectures [7]. The following is the Cryptography block diagram as depicted in Figure 2 below.

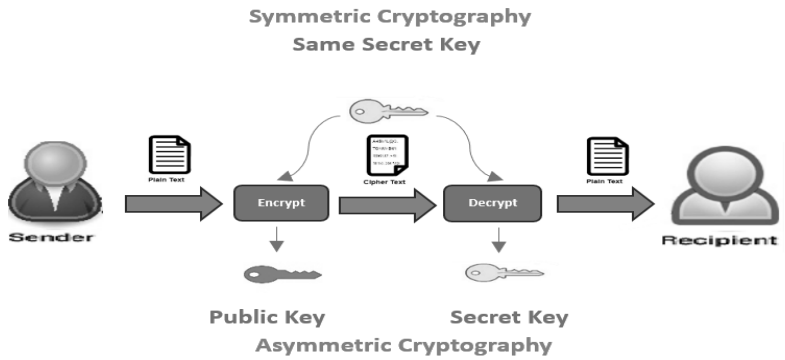

Figure 2 Cryptography block diagram

Cryptography in Information Technology

Cryptography plays a critical function in Information Technology as IT has become mankind's lifeline in contemporary society as regards the provision of information using the internet and other related media. Cryptography plays crucial roles in the information technology domain as a key component of protecting information confidentiality and secure transmission in numerous applications. Scholars have identified several elements to specifically illustrate that cryptography is central in Information Technology [8].

- Secure Communication Protocols: Cryptographic protocols set the foundation of secure communication that is Major in Information Technology. There are several protocols that are currently employed to set up secured tunnels whereby information exchange is consequential; SSL/TLS is one of the most famed protocols used in creating encrypted connections between clients and servers to facilitate secure network communication and prevent leakage of information [8].

- Data Encryption: cryptography is used to describe the secure encoding of information in preventing it from being accessed by entities that are unauthorized to do so. Essentially, cryptographic ciphers can be employed in converting the concerned information into a form that is quite comprehensible to humans and computers, which helps in offering a degree of security to both the data in motion and the data in storage [8].
- Digital Signatures: Digital signatures are also known as digital signatures, which is the cryptographic techniques that are employed in the identification and identification of the communication or message of digital communication. This assures the recipient the authenticity of the sender and that the content has not been interfered with in the middle [8].
- Hash Functions: It's used to easily convert a large message or any input of any size to a fixed-size output referred to as the hash or message digest. In IT hash functions are employed in checking and ensuring the integrity of data, password security and even in investigation and solving of cyber-crimes. A small modification in the input leads to the fluctuation of the hash value output, which is very helpful for detecting changes [7].
- Key Management: Effective key management is essential for the secure implementation of cryptographic systems. Cryptographic keys are used for encryption and decryption processes, and proper key management practices are crucial for maintaining the security of encrypted data [9].

- Authentication Mechanisms: Cryptography plays a pivotal role in user authentication systems. Secure authentication protocols, often based on cryptographic principles to ensure that the authorized systems gain access to sensible resources.

In the context of Information Technology, cryptography provides the tools and techniques necessary to address security challenges and protect data from various threats. As technology continues to advance, the role of cryptography in IT remains indispensable for maintaining the confidentiality, integrity, and authenticity of digital information [9].

Security Challenges in Cloud Computing

The rapid adoption of cloud computing has ushered in transformative benefits for organizations, but it has also given rise to a unique set of security challenges. Understanding and addressing these challenges are crucial for maintaining the integrity and confidentiality of data in cloud environments. The literature highlights several key security challenges associated with cloud computing [10].

- Data Breaches: Cloud environments store vast amounts of sensitive data, making them attractive targets for malicious actors. Incidents of data breaches or unauthorized access can have extreme sequels, including the exposure of sensitive information and potential legal ramifications [10].
- Insider Threats: The shared multi-tenant nature of cloud services introduces the risk of insider threats. Unauthorized access by individuals within the cloud provider's organization or by co-tenants poses a significant challenge, emphasizing the need for robust access monitoring and controls mechanisms [10].

- Compliance and Legal Issues: Different industries and regions have specific regulatory requirements governing the storage and processing of certain types of data. Ensuring compliance with these regulations in a cloud environment can be challenging, especially when data is stored across geographic locations [9].
- Insecure Interfaces and APIs: Cloud services often rely on interfaces and APIs (Application Programming Interfaces) for interactions between different components. Insecure interfaces or APIs can become potential points of vulnerability, allowing attackers to exploit weaknesses in the system [9].
- Lack of Transparency: Cloud users may have limited visibility into the security measures implemented by the service provider. The lack of transparency regarding security practices, incident response procedures, and data handling processes can lead to uncertainty and concerns about the overall security posture [10].
- Data Loss and Recovery: Cloud users entrust service providers with their data, but the possibility of data loss due to various factors, such as hardware failures or accidental deletion, is a significant concern. Ensuring robust data backup and recovery mechanisms is critical to mitigating the impact of such incidents [10].
- Identity and Access Management: Managing user identities and access controls is complex in cloud environments, especially when dealing with many users and diverse services. Issues such as weak authentication, improper access controls, or inadequate identity management can compromise the overall security of the cloud infrastructure [11].

- Shared Resources: Multi-tenancy, a key feature of cloud computing, means that resources are shared among multiple users. This introduces the risk of one tenant impacting the security or performance of another, intentionally or unintentionally.

Understanding these security challenges is essential for developing effective strategies and implementing robust security measures in cloud computing environments. Cryptography, as a foundational element of cloud security, plays a critical role in addressing many of these challenges, providing encryption, authentication, and other mechanisms to ensure the integrity of cloud-based systems and protect data [11]. Figure 3 below clarifies Cloud security module.

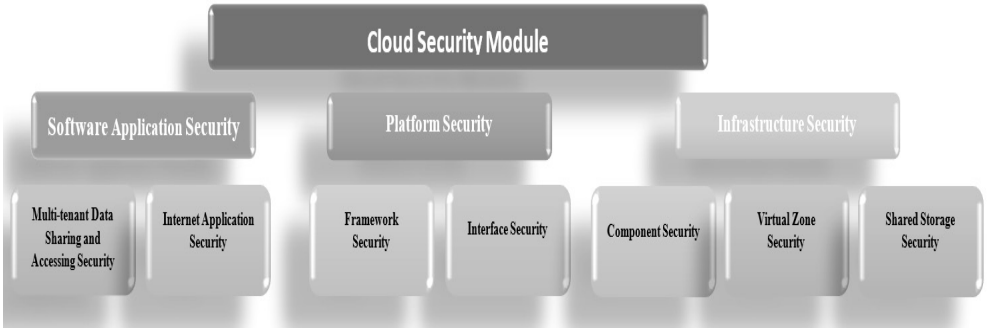

Figure 3 Cloud security module

Existing Cryptographic Solutions in Cloud Environments

As the security challenges in cloud computing continue to evolve, researchers and practitioners have proposed and implemented various cryptographic solutions to mitigate risks and ensure the confidentiality and integrity of data in cloud environments. The literature highlights several key cryptographic solutions tailored for the specific challenges posed by cloud computing [6].

- Data Encryption: Encryption remains a fundamental cryptographic solution for protecting data in cloud environments. Both data in transit and at rest can be encrypted, providing an additional layer of security. The algorithms of Advanced encryption, such as AES (Advanced Encryption Standard), are widely employed to safeguard sensitive information [8].
- Homomorphic Encryption: It is an innovative cryptographic technique that allows to perform computations on the data that is encrypted only without decryption process. This enables secure data processing in the cloud while preserving the confidentiality of sensitive information [8].
- Secure Key Management: Effective key management is critical for maintaining the security of encrypted data. Cryptographic solutions for secure key generation, distribution, and storage help prevent unauthorized access to encryption keys, ensuring the overall integrity of the encryption process [10].
- Digital Signatures and Authentication Protocols: Digital signatures play a crucial role in authenticating the origin and integrity of data in cloud environments. Authentication protocols, such as OAuth and OpenID Connect, leverage cryptographic mechanisms to verify the identity of users and entities accessing cloud services [10].
- Tokenization: Tokenization involves replacing sensitive data with unique tokens, reducing the risk associated with the exposure of actual data. Cryptographic tokenization solutions are employed to protect sensible data, such as credit card numbers or personally identifiable information (PII), stored in the cloud [9].

- Multi-Party Computation: Multi-party computation (MPC) is a cryptographic approach that enables multiple parties to jointly compute a function over their inputs while keeping those inputs private. This technique is valuable in scenarios where collaborative computations are required without revealing individual data sets [9].
- Quantum Cryptography: With the advent of quantum computing, researchers are exploring quantum cryptographic solutions to address potential threats posed by quantum algorithms that could break classical cryptographic schemes. Quantum key distribution (QKD) is one such approach that leverages the principles of quantum mechanics for secure key exchange [11].
- Secure Cloud Storage Protocols: Cryptographic protocols designed for secure cloud storage focus on ensuring the confidentiality and integrity of data stored in the cloud. Techniques like convergent encryption and proxy re-encryption enhance the security of cloud-based storage solutions.

These existing cryptographic solutions demonstrate a concerted effort to address the specific security concerns in cloud computing. As the field continues to advance, ongoing research and innovation in cryptography will be essential for staying ahead of emerging threats and ensuring the sustained security of data in cloud environments [11].

3- Objectives

To evaluate the extent of Cryptography in supporting data security and confidentiality in Cloud computing

The main aim of this work is to Map out the extent to which cryptography can be useful to ensure data security with emphasis on cloud computing. This entails an articulate discussion on how cryptographic tools, for instance, encryption and its associated protocols, offer mechanisms of protecting volatile and critical data at different angles of data processing, storing, and communication within clouds. The specific focus is to analyze how cryptography functions as one the key building blocks in maintaining the data confidentiality and to discuss threats related to cloud computing that has emerged as a major concern in the contemporary information technology setting. This way the research hopes to shed light on the applicability and effectiveness of cryptographic schemes to ensure the privacy and security of data in cloud-based environments.

To evaluate the effectiveness of cryptographic algorithms in preserving data integrity of data hosted in cloud environments.

This research project focuses on assessing and explaining the impact of cryptographic algorithms on data reliability in the context of cloud computing. The objective includes the definition of the role of cryptography which covers such elements as hash functions and digital signatures, in achieving the goal of accuracy, consistency, and reliability of cloud data storage, processing, and transfer. In evaluating the outcomes of the different cryptographic algorithms being employed, the study aims at determining the level of success these algorithms may have in ensuring that changes, interference, or data corruption within the cloud system, are effectively addressed to improve

the assurance level of the integrity of information within the developed systems. As to the specific objectives of the assessment made within the framework of the study, it is expected to contribute to a better understanding of the importance of cryptographic algorithms in maintaining data integrity within the context of cloud computing [12].

Discussion on the topicality of cryptographic methods in terms of securing the data both in transit and at rest in the cloud.

The key concern of this research study is understanding the importance of cryptography for information protection in contexts of cloud computing when data is in transit as well as while stored. The objectives of the research include analyzing cryptographic systems and protocols due to the increase in data transmission security over networks and storing of data in cloud storage systems. Therefore, in exploring the application of cryptographic techniques to both these areas of contemporary information technology usage, the present study aims to present a more comprehensive understanding of how cryptographic return and associated security features and protocols support the process of shielding sensitive information across the complex and interconnected framework of cloud computing infrastructures. Thus, this research seeks to provide deeper insights into the multiple roles that cryptography plays in raising the level of security in data transmission and in storage within the cloud [13].

4. Methodology

Research Design

The chosen research design for this study involves a two-fold approach [14]:

Literature Review:

- Carry out a literature review of previous work on cryptographic techniques used in maintaining security in cloud computing with regards to data privacy and protection.
- Conducting a literature review of the published research articles, books, conference papers and other documents that serves to understand the theoretical background and practical implications of cryptographic techniques for implementing availability in cloud computing models.
- Outlining major trends, issues, and innovations in the context of cryptography as an IT field while providing cloud computing services.

Case Study Analysis:

- Case studies to analyze the practical applications of cryptographic tools and technologies in Loa-based cloud computing deployments.
- Considering appropriate industry types and CSPs in the choice of cases to gather a wider base for cryptographic use.
- Herein, methodical understanding of the concrete cryptographic algorithms, protocols, and strategies utilized in these cases to provide data confidentiality and integrity.
- Applying the lessons learned and the best practices tested in the case studies to assemble tips and guidelines for action.

This research design can be regarded because of joining detailed literature review which will identify existing approaches and key ideas with the case study analysis which will highlight how these ideas can be applied in the practical environment. The use of both theoretical and empirical strategies is expected to offer insights and comprehensive coverage of the part played and effect brought by cryptography in safeguarding information in the cloud environment. The triangulation of theoretical and practical data provides for the credibility and validity of the practical findings drawn from the various cases under study.

Data Collection

The data collection process for this study involves [15]:

Literature Analysis:

- Conducting a literature review in professional periodicals, scientific journals, conferences papers, and other books that are aimed at investigating the effectiveness of cryptography in maintaining the confidentiality and integrity of data in cloud environment.
- In this phase, the author should systematically analyze the available literature to come up with unique research concepts, theoretical concepts, and practical applications of cryptographic solutions in cloud context.
- Filtering out the important facts which ones can be considered as the main key points for understanding the research objectives in terms of data, trends, possible and existing challenges, and developments.

White Papers Review:

- By gathering white papers from reliable cloud service offering firms, security firms, together with other stakeholders that are operating in the cloud computing technology fields to gain their vivid opinions on the application of cryptographic approaches in cloud settings.
- Looking at various reviews of the white papers and generally understanding the kind of information that is presented in the papers; specifically focusing on the technicality part of the papers that contains specifications, recommended approaches, and practical implementation of cryptography to secure data in the cloud.

Case Studies:

- To achieve a wider variety of case studies, I chose cases from several different industries, different cloud service models, and different cryptographic solutions used.
- Analyzing the case studies of the given organizations in order get the details of the exact cryptographic algorithms, protocols, and strategies used for securing data while in transit and when stored in the cloud.
- Upon identifying key areas and tasks of interest within the selected case studies, the next step is to note patterns, difficulties, and triumphs that occurred in the implementation across the different cases.

Such approaches are defined to chart the process of data collection, with special emphasis placed on using quality sources to obtain accurate and reliable information. Thus, while conducting the study, the author sought to use both journal materials, white papers and their practical case,

as the goal of the study was to consider the role and significance of cryptography in protection of data in cloud computing systems and approaches from various sources.

Data Analysis

While trying to establish the research results for this study, the analysis will entail a qualitative method. The analysis will encompass the following key steps [2]:

Thematic Coding:

- Using a more practical thematic coding approach to sort the information found during literature review and analysis of white papers and case studies.
- Detecting the cyclical motifs, patterns, and ideas concerning the application of cryptography to provide confidentiality and data integrity in the context of the cloud computing business.

Pattern Recognition:

- In this step, the collected data is analyzed to identify patterns of the application of cryptographic algorithms and protocols under different cloud computing contexts.
- To establish the prospects and challenges within the several industries as well as different CSPs, in their execution of cryptographic solutions.

Contextual Understanding:

- Building up a situation-aware conception of the real-life applications as well as the threats linked with cryptology in cloud security.

- Analyzing the trade-offs of cryptographic techniques, focused requirements of different industries, and the development of cloud solutions.

Case Study Synthesis:

- Summarizing the general lessons, success stories, and possible lessons learnt and the strengths and weaknesses on the application of cryptography in cloud security, based on the case studies observed.
- Making a comparison of what has been discerned in the literature with regards to the theoretical frames and what has been observed in the case studies.

Narrative Synthesis [15]:

- In the process of work carried out, it is necessary to create a logical and unified story that would include information obtained during the literature review and case study analysis.
- The importance of realizing an emancipatory/phenomenology understanding of contemporary security approaches and cryptography, focusing on its role in cloud systems with an emphasis on confidentiality and integrity.

Choice of qualitative data analysis approach will help in achieving the study objective as follows; Thus, the study aims at providing meaningful insights on the topics and trends that were identified using a broad spectrum of sources and show the real-life applicability of using cryptographic solutions.

5. Significance of cryptography in cloud computing

Ensuring Data Confidentiality

The usefulness of cloud computing to accrue maximum returns on investment in cloud technology through sturdiness and flexibility can only be complemented by the relevance of cryptography as a paramount tool in defense of data privacy. Several key aspects highlight the crucial role that cryptographic measures play in safeguarding sensitive information within cloud environments: The following factors explain the light at which cryptographic measures can be used to enhance security of data that is stored in the cloud:

- Encryption for Data in Transit: Integrity of data during transfer is another aspect protected with the help of protocols, in particular Secure Socket Layer/Transport Layer Security. Encryption procedures work some type of data manipulation that makes the data non-readable by anyone who is not particularly allowed to understand it. This ensures that even if the information, which was transmitted reached the unauthorized recipient, its confidentiality cannot be violated [16].
- Protection of Data at Rest: Regarding distributed data repositories, decryption methods are used for encoding the data. This can essentially be attributed to the fact that encryption such as AES has the function and capacity of a warrant to safeguard data at rest in a way that makes it nearly impossible to violate the access of the information in question. This is particularly relevant where the application is deployed on a multi-tenant public cloud [15].

- User Authentication and Access Control: Cryptography is also used to aid in providing methods for user authentication in the process and make sure only worthy dignitaries can access certain information. Some of the broad range measures that can be employed by cloud service providers to promote security include the use of cryptographic protocols for the purpose of user authentication, restricting the access to information within cloud by employing cryptographic key and credential [16].
- Secure Key Management: The use of key means protection of the key plays the most-significant role in the confidentiality of data and therefore requires proper management. According to cryptographic solutions it can be possible to investigate proper formation, data transmission, and storage of encryption key. Robust key management practices provide protection to those assets and permit only the intended recipients to carry with them the keys to permit them deciphering of the information [15].
- Homomorphic Encryption for Secure Computation: This created additional security whereby computation can be made on encrypted data without necessarily exposing the raw data. This increases data privacy during the processing phase to enable computations to be processed in the cloud safely without the crucial details being revealed [17].
- Protecting Against Insider Threats: Another important aspect of cryptography is that restriction of insider by cryptographic permissions. The use of cryptography access mechanisms allows individual tenants or users of the same Cloud environment the ability to access and decrypt only data contained in their own tenancy domain [17].

- Compliance with Privacy Regulations: There is an increased demand for privacy regulations and the protection of information and data in many industries. Cryptography enables cloud service providers as well as clients to stick to these regulations by enabling them to implement effective techniques for the protection and proving the confidentiality of such data [18].
- Data Segmentation and Isolation: This makes it easier to segment and isolate data to make sure that one string of information does not directly have access to the other string of information since there is always separate keys encrypting each string of data. This also enhances data security as opposed to data masking, which, besides hiding specific values within a dataset, does not protect data from unauthorized access even if the intruder gets access to a particular segment of the data [18].

In summary, we have established that cryptography occupies a central role in the protection of data within the cloud computing environment. Its many uses in preserving security in data in transit, and security in data and information at rest, are helps in making the cloud secure and reliable. It is therefore important for organizations and users of cloud services, where the information can be processed and/or stored, to grasp the importance of cryptography as the chief tool in ensuring data confidentiality.

Securing Data Integrity

One of the key necessities of trustworthy and dependable operating model for cloud computing is data integrity. Cryptography plays a pivotal role in preserving the accuracy, consistency, and reliability of data, addressing several key dimensions of securing data integrity within the cloud [1]:

- Cryptographic Hash Functions: Cryptographic hash is a modern technique for creating virtual fingerprints or digital identification numbers usually of a small size from data. These hash values serve as unique identifiers for the original data. They contain signatures or descriptors. It has been proposed that hash values can be compared before and after transmission or storage of data in the cloud where changes can be quickly and easily identified, thus maintaining data integrity [1].
- Digital Signatures: Digital signatures offer a sound way of authenticating digital messages in the manner that guarantees their authenticity with automatic checks on their integrity. In cloud computing, information is tagged, and the tag ensures the sender that the information being received has not been tampered with in the process. Cloud users can check the validity of the data and confirm that the data has not been modified by anyone since it was generated by encrypting the message with the public key of the recipient [3].
- Secure Communication Protocols: Different cryptographic protocols used in secure communication like SSL/TLS, do not only encrypt it but also check whether the content is intact or not. The protocols employ necessary measures such as message authentication codes (MACs) to identify alterations in the data as it is passed through the network [3].
- Checksums and Error Detection: Data integrity employs cryptographic checksums and error-detection codes with an aim of identifying and possibly correcting errors that are likely to affect data integrity. These

techniques are of more importance when transporting large volumes of data and storing it in cloud storage [6].

- Blockchain Technology: IT security is also one area that is addressed by blockchain as certain cloud applications, for instance by enabling distributed ledgers or decentralized systems utilize cryptographic hash function to ensure data authenticity. Thus, each block records a hash of a previous block within blocks, making the system's sequence tamper-evident and secure [1].
- Cryptographic Time Stamping: Identifying time sequences with cryptographic technology enables the creation of protected timestamps for data, thus proving the data's authenticity at a certain time. This is important for auditing and any previous records stored in the cloud should be intact without modifications [1].
- Preventing Unauthorized Modifications: Cryptography also plays a crucial role in maintaining checkpoint access to the altered data by employing access control measures hand checking the data integrity through necessary cryptographic measures. This is important when it comes to ensuring that the information contained has a set level of consistency and accuracy, especially in multi-user cloud platforms [4].
- Secure Multi-Party Computation: It is done using cryptographic techniques like secure multi-party computation, where the symbols are inputted by two or more parties and the output is a function of the input data without exposing the data. This helps to maintain data integrity in that even at a time when computations involve collaboration client data is kept safe [4].

In summary, there is Valeur general des cryptographies and cloud computing, worth of data integrity in general cryptographic applications. By applying the mentioned techniques, CSPs and consumers could build a sound framework for proving and sustaining data genuineness, accessibility, and availability through the entire cloud data life cycle. It also makes cloud-based systems more reliable ad trustworthy in comparison to traditional system.

Protection of Data in Motion and Storage

Cryptography has a critical role in ensuring solution security in their networks and Cloud's data transmission and storage (Data In-Transit & Data At-Rest). The significance of cryptographic measures in protecting data in these two states is critical for maintaining overall security and confidentiality:

Data in Transit [5]:

Encryption of Communication Channels: Those protocols that may include SSL/TLS encrypt data during its transit between the users and cloud services. This makes that information that is transferred over the networks to be retained secure and private, thereby eliminating indirect listening and other unlawful invasions of privacy.

- Secure Sockets Layer (SSL) and Transport Layer Security (TLS): These cryptographic protocols thus afford secure encryption between clients' and servers' stations. They employ mathematical formulas to ensure that data that is transmitted through the cloud is safe by being encrypted, this adds in on the security of the data transmitted on the cloud.
- Message Authentication Codes (MACs): These include MACs that are applied to data in transit, with the purpose of ensuring the

received data has not been altered in transit. This is good because it assures the data has not been interfered with while in transit across different networks.

Data at Rest [5]:

- File and Disk Encryption: Cryptographic solutions to data intended to be stored in Cloud repositories or physical devices involve encryption of these data. Other technologies such as AES (Advanced Encryption Standard) are utilized by safeguarding data that is stored, which means even if unauthorized personnel gain access, data stored would be on encryption and so cannot be accessed.
- Secure Key Management: Cryptographic systems help adopt secure key management policies for data that is archived. Data that is stored needs to be encrypted, and the keys used for decryption of stored data need to be created, distributed, and protected so that improper access to data that is stored cannot be gained.
- Homomorphic Encryption: Modern encryption algorithms such as homomorphic encryption enable arithmetic operations to be conducted directly without use of decryption. This is especially useful when data stored in the cloud needs to be retained secure and intact in storage while still requiring computations.

Unified Approach [5]:

The field of cryptography is a fundamental one that deals with securing the data in the instances of its transmission and storage, thus providing an integrated line of protection during data flow and storage. It also makes security more thorough as it covers possible security threats regardless of whether data is sent from one point to another or stored and waiting for a signal to be active.

Compliance and Privacy Assurance [17]:

The protection of data that is in motion or stored temporarily in a system is equally important especially as it seeks to meet industry standards or regulatory requirement as well as personal preferences. These aspects are served by cryptographic measures to ensure users and organizations that their information is protected using the highest standards of confidentiality and security. All in all, the application of cryptographic techniques to protect data in motion and data stored in cloud computing significantly enhances the level of cloud security. Through such measures as encryption, secure communication protocols, and state-of-the-art cryptographic approaches, CSPs and consumers can effectively unleash the complexities of securing data across its evolutionary life cycle in the context of a cloud system.

Compliance with Regulatory Requirements

Thus, cryptography is a paramount means for safeguarding cloud computing environments against non-compliance with legal statutes and regional or domain-specific standards. The significance of cryptographic measures in achieving regulatory compliance is particularly pronounced in the following aspects [4]:

- Data Confidentiality and Privacy: By using relevant strong encryptions, cryptography meets regulatory requirements covering the secrecy and privacy of organizational information. There are many regulated sectors where the protection of personal and financial data is a crucial issue, for instance, the healthcare or finance industry. Some measures are as follows: encryption of the data transmitted and stored on the cloud as well as in-transit

encryption fulfilling the privacy requirements for cloud service providers and users [4].

- Secure Data Handling and Storage: The law sometimes provides legal standards in the care and storage of data. Cryptography, in part through storing data at rest, guarantees that, even if an unauthorized entity breaches the physical perimeter, the information remains protected. The rules of using personal data are set by the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), etc., and can be fulfilled with the help of cryptographic security measures [16].
- Identity and Access Management: Cryptography helps SOPs for identity and access management to be secure and aligns the organization to requirements set by various authorities concerning user Authentication and authorization. With the help of cryptographic methods in protected login, access control, and multi-factor authorization, cloud environments can meet the requirements of regulation and protect users' identities adequately [16].
- Audit Trails and Accountability: This is useful for things like digital signatures and cryptographic time stamping to assure the audit trail and accountability. The specificity of the compliance requirements means that the programs need to allow tracking and auditing of activities done on the sensitive data. Audit trail is a method used for tracking activities, and it ensures that records are protected with the help of cryptographic measures to conform to the regulatory auditing standards [17].

- Secure Communication Protocols: The safe transfer of data is highlighted in many regulatory frameworks used in organizations today. Policies such as SSL/TLS, which secure the flow of line, also help in meeting the compliance as they safeguard data from being intercepted by unauthorized parties [17].
- Protection Against Data Breaches: It is important to have secured applications to avoid leakage of sensitive information and especially when such instances attract stringent penalties. It is for these performances that utilization of encryption to data in status simplification secures cloud environments' invulnerability against undue access and conceivable invasions in consonance with requirements stipulated by regulations on safety of data [18].
- Cross-Border Data Transfer: It helps in protecting the data while moving from one country to another, thus helping to meet the ideals of some regulatory authorities on data transfer across borders. Inasmuch as data security is concerned, encryption protocols help to ensure that information remains secure as it passes through various networks of organization in different international boundaries to ensure they meet the set legal requirements on transfer of data between nations [18].
- Adherence to Industry Standards: Use of cryptography makes it possible for cloud service providers and their users to observe industry specific cryptographic standards set down by regulatory authorities. Adhering to standard cryptographical methods makes the security feature robust and puts into consideration the regulator's requirement [19].

Altogether, the use of cryptographic measures is essential in cloud computing to ensure its compliance with existing regulations. In this regard, cryptography provides important inputs that help in the development of the secure and compliant cloud model which touches on the areas of data confidentiality, storage security, and access controls and auditability. This is especially important for industries that are dealing with sensitive data or are within confined regulations. The following figure 4 elaborates on the Cryptography model for secure data sharing over cloud [18].

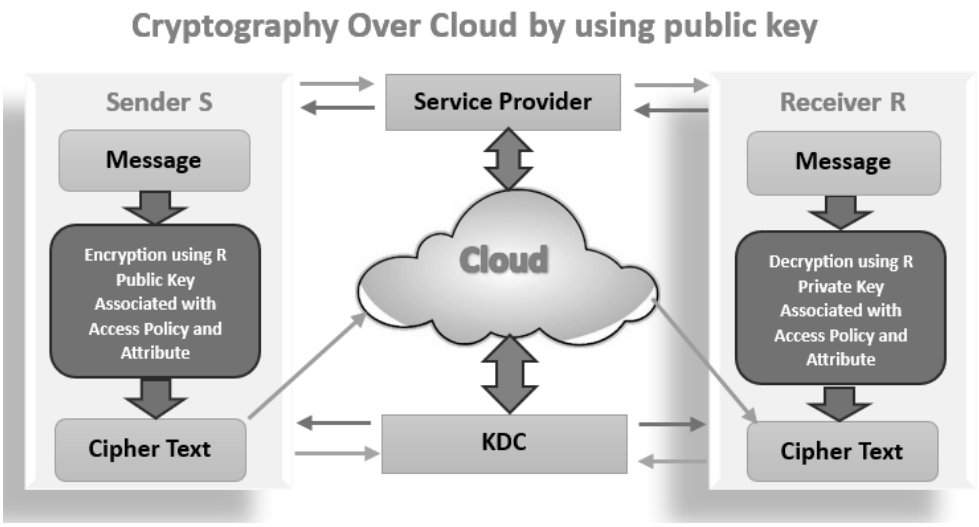

Figure 4 Cryptography model for secure data sharing over cloud

6. Challenges and Solutions

Key Management Issues in Cloud Cryptography [2]

Cryptographic keys are some of the valuable assets needed for the operational security and efficiency of cryptographic systems in cloud computing. However, key management in the cloud introduces specific challenges that need to be addressed:

. Challenges

- Scale and Complexity/ Challenge: Cloud deployment commonly results in a big number of users, services, and connected devices. These kinds of operations can be challenging at this scale to manage cryptographic keys, and issues can arise with the distribution, rotation or revoking of keys.
- Multi-Tenancy/ Challenge: Multitenancy is normally common with cloud services so they may be more shared in nature. Key management becomes an issue of concern as one tenant may require frequent access and issuance of keys while another will not require them frequently and the keys need to be isolated and properly managed to avoid cross –contamination.
- Lifecycle Management/ Challenge: The management of cryptographic keys used for encryption, distribution, and security purposes has proven daunting during the cloud computing lifecycle, especially in terms of generation, distribution, rotation, or destruction. Failure at any of the four stages results in the generation of security threats.

- Secure Key Storage/ Challenge: Of particular concern is storing and protecting cryptographic keys when deploying applications in a cloud computing model. Some of the potential risks associated with the access of key storage include exposure of the keys so that the data might be leaked.
- Compliance and Legal Issues/ Challenge: The main issue arising with the integration of meeting regulatory requirements associated with key management in different regions. Cloud service providers that want to protect implementation implementations of cryptographic keys are legally bound to adhere to various legal systems.
- Key Revocation and Rotation/ Challenge: The security of systems requires that key sharing should be done in a timely manner and keys be updated or replaced periodically. Revocation and rotation of keys is also complex in cloud environments as any disruption of services may severely affect services in many organizations.

· Solutions

- Automated Key Management Systems/ Solution: Designed for key management within a large and complex cloud environment, the automated systems used must be also capable of handling the scale and tasks required. Automation enables the most vital copy key generation and its distribution and timely rotation.
- Tenant-Specific Key Management/ Solution: Businesses that lease computing resources should follow specific control measures to meet the multiple tenancy challenge. It means that to ensure different requirements are met, proper divisions of the key management procedures and accesses controls are done.

- Robust Lifecycle Management Policies/ Solution: Creating effective frameworks and procedures for critical key lifecycle, when it is necessary to describe key creation, distribution, updating, and deletion. The proper checklist that can be recommended from time to time can make sure that the company complies with the set down policies.
- Hardware Security Modules (HSMs)/ Solution: HSMs for storage of keys Implementation of HSMs has been adopted by many organizations as a way for storing keys securely. HSMs offer specific hardware designed to securely manage cryptographic keys, improving key-level security.
- Continuous Monitoring and Auditing/ Solution: Stringent measures of monitoring and auditing, the key areas of access control which are tailored for revealing unauthorized access or any malicious events related to key management. This is because it helps the business to achieve and remain in compliance with legal and regulatory standards.
- Key Revocation and Rotation Strategies/ Solution: Key revocation and rotation are efficient techniques that must be employed appropriately without causing inconveniences that may negatively affect the quality of the services delivered. This may entail providing a framework for convoluted key transition that may require key rotations with little interruption.

To tackle key management challenges in cloud cryptography we need to consider the technological solutions, the policies which need to be equipped and set up for the key management and of course following the

best practices most recommended by the industries. Hence, strong key management practices of key associated issues can help cloud environments to strengthen the cryptographic systems' security and reduce risks inherent to key-related issues.

Overcoming Performance Challenges [6]

· Challenges

- Computational Overhead/ Challenge: The security solutions that use strong encryption are likely to affect processing in the cloud either at the framework level or for the services to the clients.
- Latency in Secure Communications/ Challenge: The adoption of such safe communication measures like SSL/TLS may entail a certain level of latency, thus causing problems when it comes to the interactivity of applications and services in the cloud models.
- Resource Consumption/ Challenge: Cryptographic processes are computationally demanding, especially in cases of large amounts of data to be encrypted; and they often collaterally translate into considerable resource utilization and performance drawbacks.

· Solutions

- Algorithmic Optimization/ Solution: It is imperative to make sure that mathematical algorithms are refined, and the size of the computer required greatly reduced but the security of the data remains unaltered. This entails choosing friendly and appropriate algorithms and refreshing the cryptographic protocols.
- Hardware Acceleration/ Solution: Utilize hardware related advancements like dedicated cryptographic hardware or GPUs as a

tool of hardware acceleration to reduce some amount of processing of cryptographic computations.

- Caching and Pre-Computation/ Solution: It is important to utilize cache memory and pre-calculation methods to decrease the amount of effort for commonly executed cryptographic functions, which will enhance efficiency of operations in cloud environments.

Addressing quantum Computing Threats [12]

· Challenges

- Quantum Computing Vulnerabilities/ Challenge: The emerging new technology in the computing environment, the quantum computing, is seen to be a real threat to the traditional cryptographic algorithms, notably the public-key cryptography since they can be vulnerable to quantum cryptanalysis attacks.
- Post-Quantum Transition/ Challenge: Issues that surround post-quantum cryptography particularly when preparing to migrate from the current state involve choice and implementation of cryptographic algorithms that will not be affected by quantum computers as well as maintaining compatibility with already established systems.

· Solutions

- Post-Quantum Cryptography Adoption/ Solution: The next step is to maintain awareness of the progress of post-quantum cryptography and start implementing the quantum-resistant algorithms. Quantum development means cloud systems have been prepped in anticipation of quantum threats.

- Quantum Key Distribution (QKD)/ Solution: Introduce and integrate Quantum Key Distribution (QKD), which allows to develop secure communication channels according to the theory of quantum mechanics to minimize the risks of a quantum attack.

User Awareness and Education Increase [20]

· Challenges

- User Negligence/ Challenge: This implies that occasional user may be naïve in security related practices and may unknowingly act in a manner that poses a threat to the security of its data that is stored in cloud.
- Phishing and Social Engineering/ Challenge: Phishing attacks and use of social engineering exploits vulnerabilities that users have. This is because apart from not recognizing these types of tactics, the users may be easily duped always.

· Solutions

- User Training Programs/ Solution: To enhance the security of consumers, initiate extensive user awareness programs to teach the consumers about the right behavior and precautions they should take when they are using the cloud services; for instance, proper password management, detecting and avoiding of phishing scams, and the need for data encryption.
- Multi-Factor Authentication (MFA)/ Solution: Promote and ensure compliance with multi-factor authentication (MFA) process so that password is not the only access that is granted meaning reducing instances of unauthorized access.

- Regular Security Awareness Campaigns/ Solution: Another security recommendation would be to constantly remind users through seminars, articles, and other forms of advertisement about the positivity of security concerns, potential threats that linger in the environment of cyberspace, and the significance of adhering to secure practices in the use of Cloud Computing technology.
- Transparent Security Policies/ Solution: Certainly, the developers must transparently convey the security policies to the users and define the paradigm around data protection in the cloud.

Enhancing user awareness and education, along with addressing emerging technological challenges, is essential for building a resilient and secure cloud computing environment. A holistic approach that combines technological solutions with user empowerment contributes to a more robust defense against potential threats. (Schneier, 1996).

7. CASE STUDIES

Successful Implementations of Cryptography in Cloud Environments [18]

Case Study: Analysis of Cloud Service Provider X

· Background:

- Overview: The case of Cloud Service Provider X has established cryptographic solutions as security measures to its cloud services.
- Cryptography Applications:
- Ensured data in-transit is encrypted by building an encrypted end-to-end mechanism based on TLS protocols.

- Used appropriate AES-256 algorithm to encrypt data that are stored in cloud.
- Ensured sound key management strategies, and even key management techniques such as key cycling were followed.

· Results:

- Enhanced Data Security: The application of cryptographic functions contributes greatly to increasing the security of customer data through protection during transfer and storage.
- Compliance Assurance: The cryptographic solutions enabled its adherence to industry regulation and standards, making customers assured on protection of their data.

· Lessons Learned:

- Holistic Approach: It could be inferred that the implementation success was due to the adoption of a comprehensive strategy that fevered the protection of data in transit and at rest. Proofs revealed that encryption coupled with key management policies were successes.
- Regular Audits: The continuing review of the cryptographic implementations also helped in the steady monitoring and non-deviation in compliance to the set standards with attention being focused on the areas that needed constant enhancement.

Lessons Learned from Security Breaches in Cloud Computing [18]

Case Study: Here follows some major types of Security Breach Incident Y that individuals can face in their daily lives.

· Background:

- Overview: Negative example: Company Y had recently undergone a security risk where its cloud computing setting was violated, and confidential information leaked.
- Root Cause Analysis:
- Weak Authentication: The break in was made easy since the attackers exploited poor user authentication measures such that many of the users had their accounts and passwords stolen.
- Lack of Encryption: Cloud data retrieved by the outfitter was not well encrypted, thus it was easy for unauthorized personnel to access sensitive information.
- Insufficient User Education: One is users become the prey of phishing attack because of poor or lack of security consciousness.

· Lessons Learned:

- Multi-Factor Authentication (MFA): MFA could have also been adopted to add another layer of security that would have minimized the effect if the credentials were compromised.
- Encryption Best Practices: It is therefore very desirable to adopt encryption best practices for data at rest by using formats that make it virtually impossible to accessible by anyone other than the rightful owner even in cases where the system has been compromised.
- Continuous User Education: A notable point for raising the bar in perspective is the growing need for regular and comprehensive user education programs to mitigate the risks of social engineering attacks.

In these case studies, early identification, and aggressive execution of security measures for cloud computing is illustrated. Cryptography successes help protect data, meet laws and standards, and build and sustain customer trust, while security failures drive home key lessons about the necessity for strong authentication, encryption, and of promoting awareness in cloud-based settings.

8. Recommendations

Best practices for implementing Cryptography in Cloud Computing [19]

- Holistic Encryption Strategy: It is recommended when implementing encryption to take a more comprehensive strategy to data protection, which also involves protecting data during transfer and while stored. For the channel we must employ the recommended encryption protocols, which in this case are SSL/TLS while for the storage, one must employ good algorithms like AES among others.
- Key Management Excellence: Implement secure key management procedures and ensure proper management of symmetric keys such as creation, distribution, updating and decommissioning of keys. These procedures can be made more efficient with key control automation systems.
- Regular Security Audits: For checked cryptographic ’s realization, carry out periodical security auditing. This ranges from basic checks on the type of encryption used in a network, the management of keys and other measures put in place as checked against standard code of practice.

- User Education Programs: Continued awareness of users via seminars and other training methods is also instrumental in improving security standards. Teach users how to identify phishing scams, when to use and when not to use strong authentication measures and what are the meaning and importance of encryption.
- Post-Quantum Readiness: Closely monitor activities in the post-quantum cryptography arena and plan for a migration toward quantum-soup algorithms. To address this issue, cryptographic protocol designers should monitor the threats and periodically design and adjust cryptographic protocols based on these threats.
- Hardware Security Modules (HSMs): Discuss the following use cases for the improvement of cryptographic storage: Hardware Security Modules (HSMs). HSMs offer security by dedicating fixed and secure hardware processing elements for cryptographic key management.
- Compliance Adherence: Reliability of cryptographic implementations in terms of regulations and standards: Adopt proper standard conformities of cryptographic implementations for the appropriate industry standards. Cryptography: Conduct the literature review for cryptographic measures based on the growing compliance needs and update it periodically.
- Multi-Layered Security: Secure it with multiple layers of security measures including encryption, firewall, DDoS protection, intrusion detection and access control mechanisms among others. It also increases resistance in various ways against the different security threats.

Future Research Directions [20]

- Quantum-Safe Cryptography: Organizations should commit resources towards research and deployment of post-Quantum cryptographic algorithms to protect their networks and structures. Find out measures that can be taken to avoid susceptibility to potential threats brought about by future advancements in quantum computers.
- Advancements in Homomorphic Encryption: Information derived from homomorphic encryption is an enabler that will reverse the process of putting encrypted data into usable form in other algorithms. There are two aspects that need to be addressed as part of the current and future development of the app that will effectively add to this capacity; The capacity of the app must be enhanced to justify the growth in the number of users.
- Dynamic Key Management Solutions: Further analysis of predesigned and selected Dynamic KM technologies that can be utilized in dynamic cloud environments. Some of these are, namely: specifying cryptographic algorithms, self-updating protocols, and key management methods.
- User-Friendly Cryptography Interfaces: The cryptographic software itself also was presented with new interfaces that are comfortable for the user. Through reminding consumers of criminal and security issues and guiding them to make correct and safe decisions, adaptive interfaces assist in promoting safe and correct behaviors.
- Integration with Emerging Technologies: Simplify the cryptographic products and discuss them with reference to contemporary

technologies like artificial intelligence and ailing blockchain. Assess how these technologies can be used to supplement eventual cryptographic approaches for improved security.

- Resilience Against Advanced Persistent Threats (APTs): Consider such advanced concepts and issues of cryptology and develop cryptographic methods for counteracting APT. Enhance the resilience of cryptographic systems at a time where threats classes are diverse, and resilience and creativity are rife with new cunning threats.
- Standardization of Cryptographic Protocols: As all the protocols entail that some of them need to be designed or are still under design, involve the industry partners to assist in designing standard cryptographical protocols. Standardization contributes to the achievement of these objectives: Integrated systems: Through standardization, various cloud environments are more easily compatible since everyone must follow certain laws.

9. Conclusion

In conclusion, this paper highlights the need to embrace cryptography as a primary solution in the cloud computing security space. First, the results of the work put emphasis on the multi-faceted significance of cryptographic procedures in support of data secrecy and the given integrity, as well as applicable rules compliance. CISOs and other information technology professionals should employ layered security measures, become alert to new attacks like quantum computing, and invest in security awareness training for cloud environments to enhance protection.

The role of cryptography in providing security standards remains significant even as cloud computing presents the future of technology. This study also demonstrates that rather than being a component, cryptography is rather a powerful force that defines and drives the reliability and dependability of cloud computing technology. It is crucial to be constantly on the lookout for trends and threats, to adjust strategies and behaviors as necessary, and to employ sound cryptographic policies to confidently protect a cloud from various threats and preserve the sanctity of its information.

References

[1] Asha, & Ismail, S" Security issues and solutions in cloud computing a survey" Int. J. Comput. Sci. Inf. Secur. (IJCSIS), 14(5), pp. 309-315, 2016.

[2] Jaber, A, N, & Fadli, M "Use of cryptography in cloud computing," 2013 IEEE International Conference on Control System, Computing and Engineering, Penang, Malaysia, pp. 179-184, 2013. https://doi.org/10.1109/ICCSCE.2013.6719955

[3] Sasikumar, K, & Nagarajan, S "Comprehensive Review and Analysis of Cryptography Techniques in Cloud Computing" in IEEE Access, vol. 12, pp. 52325-52351, 2024. https://doi.org/10.1109/ACCESS.2024.3385449

[4] Garg, D, Sidhu, J, & Rani, S " Emerging Trends in Cloud Computing Security: A bibliometric Analyses" IET Software, 13(3), pp. 223-231, 2019. https://doi.org/10.1049/iet-sen.2018.5222

[5] Zissis, D, & Lekkas, D "Addressing Cloud Computing Security issues" Future Generation Computer Systems, 28(3), pp. 583-592, 2012. https://doi.org/10.1016/j.future.2010.12.006

[6] Agarwal, V, Kaushal, A, K, & Chouhan, L "A Survey on Cloud Computing Security Issues and Cryptographic Techniques" In Social Networking and Computational Intelligence: Proceedings of SCI-2018, pp. 119-134, 2020.

[7] Bhargav, A, J, S, & Manhar, A "A Review on Cryptography in Cloud Computing" International Journal of Scientific Research in Computer Science Engineering and Information Technology, 6(6), pp. 225-230, 2020. https://doi.org/10.32628/CSEIT206639

[8] Modi, C, Patel, D, Borisaniya, B, Patel, H, Patel, A, & Rajarajan, M "A Survey of Intrusion Detection Techniques in Cloud" Journal of Network and Computer Applications, 36(1), pp. 42-57, 2013. https://doi.org/10.1016/j.jnca.2012.05.003

[9] Wang, C, Wang, Q, Ren, K, Cao, N, & Lou, W "Toward Secure and Dependable Storage Services in Cloud Computing" IEEE Transactions on Services Computing, 5(2), pp.220-232, 2011. https://doi.org/10.1109/TSC.2011.24

[10] Agarwal, P "Cryptography Based Security for Cloud Computing System" International Journal of Advanced Research in Computer Science, 8(5) , 2017.

[11] Akbar, H, Zubair, M, & Malik, M, S" The Security Issues and Challenges in Cloud Computing" International Journal for Electronic Crime Investigation, 7(1), pp.13-32, 2023. https://doi.org/10.54692/ijeci.2023.0701125

[12] Subashini, S, & Kavitha, V "A Survey on Security Issues in Service Delivery Models of Cloud Computing" Journal of Network and Computer Applications, 34(1), pp. 1-11,2011. https://doi.org/10.1016/j.jnca.2010.07.006

[13] Ali, I, Sabir, S, & Ullah, Z "Internet of Things Security, Device Authentication and Access Control: A Review". ArXiv Preprint ArXiv:1901.07309, 2019.https://doi.org/10.48550/arXiv.1901.07309

[14] Christensen, C "Review of Cryptography and Network Security: Principles and Practice" Cryptologia, 35(1), 97-99, 2010. https://doi.org/10.1080/01611194.2010.533253

[15] Kaleem, M, Mushtaq, M, A, Jamil, U, Ramay, S, A, Khan, T, A, Patel, S, & Hussain, S, K "New Efficient Cryptographic Techniques for Cloud Computing Security" Migration Letters, 21(S11), pp. 13-28, 2024.

[16] Gupta, K, Gupta, D, Prasad, S, K, & Johri, P" A Review on Cryptography Based Data Security Techniques for the Cloud Computing" In 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), pp.1039-1044, 2021. https://doi.org/10.1109/ICACITE51222.2021.9404568

[17] Thabit, F, Alhomdy, S, Al-Ahdal, A, H, & Jagtap, S "A New Lightweight Cryptographic Algorithm for Enhancing Data Security in Cloud Computing" Global Transitions Proceedings, 2(1), pp. 91-99, 2021. https://doi.org/10.1016/j.gltp.2021.01.013

[18] Alemami, Y, Al-Ghonmein, A, M, Al-Moghrabi, K, G, & Mohamed, M, A "Cloud Data Security and Various Cryptographic Algorithms" International Journal of Electrical and Computer Engineering, 13(2), 2023. https://doi.org/10.1109/ACCESS.2024.3385449

[19] Yong, P, E, N, G, Wei, Z, H, A, O, Feng, X, I, E, Dai, Z, H, Yang, G, & Chen, D, Q "Secure Cloud Storage Based on Cryptographic Techniques" The Journal of China Universities of Posts and Telecommunications, 19, pp. 182-189, 2012. https://doi.org/10.1016/S1005-8885(11)60424-X

[20] Chinnasamy, P, Padmavathi, S, Swathy, R, & Rakesh, S" Efficient Data Security Using Hybrid Cryptography on Cloud Computing" In Inventive Communication and Computational Technologies: Proceedings of ICICCT 2020, pp. 537-547, 2021. https://doi.org/10.1007/978-981-15-7345-3_46

Received ..... 23 July 2024

Revised..... 16 Sept. 2024

Accepted.....28 Sept. 2024