Computer Networks and Communications
https://ojs.wiserpub.com/index.php/CNC

UNIVERSAL WISER PUBLISHER

Research Article

An Analysis of Different Security Models and the Obstacles of Ensuring Security and Privacy while Storing Data on the Cloud

Shahid Naseem[1*], **Salbia Sidrat**[2], **Muhammad Mueed Hussain**[2]

[1] Department of Information Sciences, Division of Science & Technology, University of Education, Township, Lahore, Pakistan
[2] Department of Computer Science, The Institute of Management Sciences, Lahore, Pakistan
E-mail: shahid.naseem@ue.edu.pk

Received: 16 April 2024; **Revised:** 28 August 2024; **Accepted:** 29 August 2024

Abstract: Every day, cloud computing—which stores user data online—becomes more and more popular. Instead of being aware of security risks, the main goal of a cloud-based system is to use the internet as a storage medium. Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are the three primary categories of cloud computing models. But as cloud computing has gotten more popular, security has grown to be a major worry. The difficulties with data storage in various cloud computing scenarios are examined in this research. It suggests using the Internet Protocol Security (IPsec) architecture as the foundation for the Security Encryption Privacy (SEP) paradigm. To improve security and stop assaults on cloud storage, it generates and encrypts data using the RSA algorithm and public key cryptography. In addition, our suggested approach is contrasted with alternative security models. This study's primary goal is to comprehend cloud computing.

Keywords**:** RSA algorithm, public key cryptography, SEP, encryption, IaaS, PaaS, SaaS

1. Introduction

"Cloud computing" is described by the National Institute of Standards and Technology (NIST) as "a cloud computing model" that facilitates resource pooling, ubiquitous on-demand access, and ease of delivery across many service providers [1]. Over the past few years, there has been a rise in demand for both wider infrastructure and internet usage. Instead of using a computer, smartphone, or other device to store data on the cloud, a cloud-based ecosystem tries to occupy an ambiguous area on the internet. In addition to helping their clients get rid of physical hard drives and licensed software, this quickly developing technology has also allowed its users to save money and time.

The rapid evolution of cloud computing has ushered in transformative era, marked by unprecedented advancements in technology, infrastructure, and service delivery. As organizations increasingly migrate their operations to cloud environments, the paradigms governing this dynamic landscape continue to evolve, shaping the future of computing. This study offers a comprehensive exploration of these transformative shifts, focusing on three pivotal aspects: security, efficiency, and innovations. Security stands a cornerstone in the realm of cloud computing, with the omnipresent concerns surrounding data protection, privacy, and the integrity of digital assets. Efficiency, the lifeblood of any computing ecosystem, emerges as a second critical dimension in our exploration. In this study, we delve into the intricate web of

DOI: https://doi.org/10.37256/cnc.2220244762

security challenges and solutions, dissecting the robust measures that could providers employ to fortify their platforms against the ever-growing spectrum of cyber threats.

The use of cloud computing represents the cutting edge of several technologies, including distributed processing, grid computing, and “service-oriented architecture (SOA)”. Grid computing is less adaptable than cloud computing, though. These days, banks, healthcare providers, and educational institutions are migrating their data to the cloud [2]. The amenities that cloud environments provide their customers are the primary factor in this decision. These facilities offer a range of services and applications, including networking, databases, data storage, and data storage capacity that may be adjusted in accordance with the services the user purchases. The customer must pay for the service they use, such as postpaid services offered by cell operators, based on the storage capacity and consumption. Service providers eliminate the hassle of customers having to carry physical storage devices in addition to their computers or mobile phones by storing the data remotely on servers and enabling users to access it from anywhere in the globe [3].

In this article, we present an improved storage data solution that maintains storage security and privacy concerns by applying the cloud’s IP sec architecture. We tackle privacy issues with encryption approaches, while RSA is employed to thwart assaults. The interconnectivity of several levels is the foundation of cloud computing’s overall architecture. Through the World Wide Web, the cloud computing architecture offers on-demand access to data with scattered resources. Additionally, it created a standardized architecture that allowed several users to connect to and utilize a single pool of resources, including servers, storage, and applications.

As seen in Figure 1, its framework normally consists of three levels: a front-end layer that gives consumers an interface to access services, a back-end layer that includes server infrastructure and storage, and a network layer that connects the various parts. Cloud service providers allow customers to continuously access computing resources without requiring any infrastructure facilities using a variety of approaches, including Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [4].

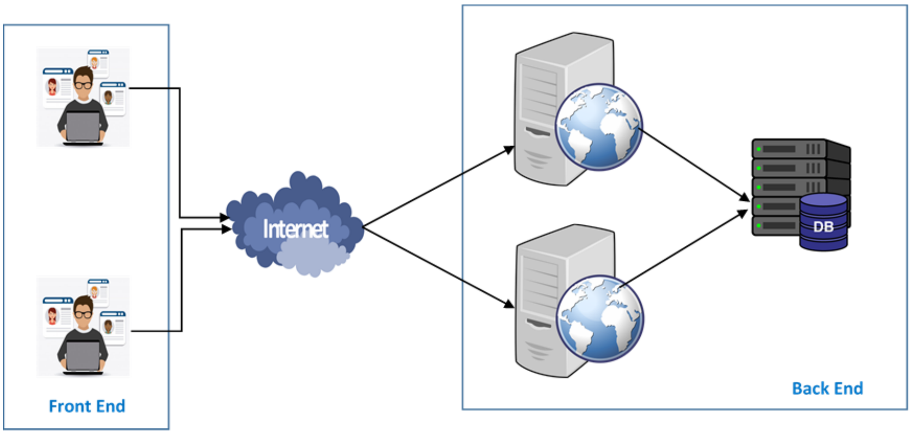


Figure 1. Cloud computing architecture

1.1 *Risks in cloud computing infrastructure*

Notwithstanding all of the benefits of cloud computing, maintaining its privacy and safeguarding customers’ sensitive and personal data on the cloud presents a significant barrier for all service providers today. One type of assault against cloud computing infrastructure is denial of service, which prevents the authorized user from accessing their account. Service hijacking, eavesdropping, unprotected virtual machines, distributed technology vulnerabilities, and many more are examples of different threats. Brute force assaults, improper usage of cloud services, and malevolent cloud users can all seriously damage the system [5]. This article’s core thesis is that, while cloud data storage has many positive effects, there are also serious security risks and difficulties that must be addressed. With the massive growth of data in recent years, cloud computing security issues have become one of the biggest concerns. Given that we have no idea where our data is kept or how it has been handled, security needs to be a top priority. Data breaches, credential breaches, malware injection attacks, faulty authentication, compromised interfaces and APIs, and account hijacking have all happened as a result of privacy and confidentiality issues. The following are the primary security threats that should be considered while implementing and managing cloud data. There are other approaches to address these issues, including as how the data transitions from one encryption level to the next generation level. However, in this article, we examine a few strategies to guarantee that these worries are at least mitigated.

The structure of this article is as follows: IPsec Architecture is briefly discussed in Section 2. Cloud data storage security concerns and solutions are covered in Section 3, along with work relating to Sections 4 and 5 methodology and its application. Section 6: Discussions and Results 7 Final thoughts and next projects.

2. IPsec architecture

Three typical services are provided to clients by cloud service providers: "Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)." Cloud service providers host browser-based apps under SaaS. In PaaS, a service provider makes services easier for their customers by developing software solutions for certain issues. In Infrastructure as a Service (IaaS), the cloud service provider provides services to their customers via virtual computers so they may improve their business acumen. The Cloud Security Alliance (CSA) lists data loss, illegal access, and data breaches as some of the most significant dangers to cloud data security. A few of these frequently happen in cloud systems. Purchasers of cloud services need to understand the dangers of data leaking as well as how susceptible their data is to various assaults and threats. The danger of a data breach rises when a cloud user stores their data online and, if not managed and secured effectively, they lose faith in both the cloud storage provider and the business. Due to the various problems and difficulties associated with cloud security, there are numerous areas of study in the field of cloud data storage. Research subjects that are in demand include loss of control, multi-tenancy, data leakage, and vendor lock-in. Prominent companies in the cloud computing space include Amazon, Samsung Cloud, Google Apps, iCloud, and Microsoft Azure [6].

2.1 *IPSEC architecture and its components*

The main functions of the security protocol known as IPsec (Internet Protocol Security) are to authorize and encrypt IP connections. The two main components of the latter's architecture are the Encapsulating Security Payload (ESP) and the Authentication Header (AH). While ESP provides privacy through encryption, AH detects and verifies the total validity of underlying data packets in a unique way. IPsec may operate in two modes: tunnel mode, which encodes and combines all of the data packets into a single dynamic IP packet, and transit mode, which encrypts the payload. Various encryption methods and key management protocols can be implemented by IPsec based on the security needs of the user.

IPsec also includes essential administration software for managing cryptographic keys and secure connections, as well as a defensive policy repository. Given that IPsec provides a flexible and secure architecture for encrypting Internet protocol communications, it is inevitable that IPsec is an essential component of modern information security. The packet's integrity is maintained and the transmitter of the packet is digitally signed by the authentication header. This suggests that every disruption to the packet during transmission will be detected. AH employs a keyed hash function that is supplied in the header to determine the integrity check value (ICV) for the packet. By guaranteeing the confidentiality, integrity, and authenticity of the sent data, the Encapsulating Security Payload protects it. Similar to AH, ESP encrypts the data payload of the packet and may also provide integrity and verification. ESP creates an ICV using a keyed hashing method and uses a symmetric encryption mechanism to encrypt the network packets. In addition to the aforementioned essential elements, IPsec offers a crucial administrative structure for efficiently exchanging credentials needed for authentication and encryption. The IPsec keys seen in Figure 2 are generated and maintained using the Internet Key Exchange (IKE) protocol. Together, these modules provide a wide range of security protocols for IP communications, ensuring network-wide data confidentiality, integrity, and authentication [5, 6].

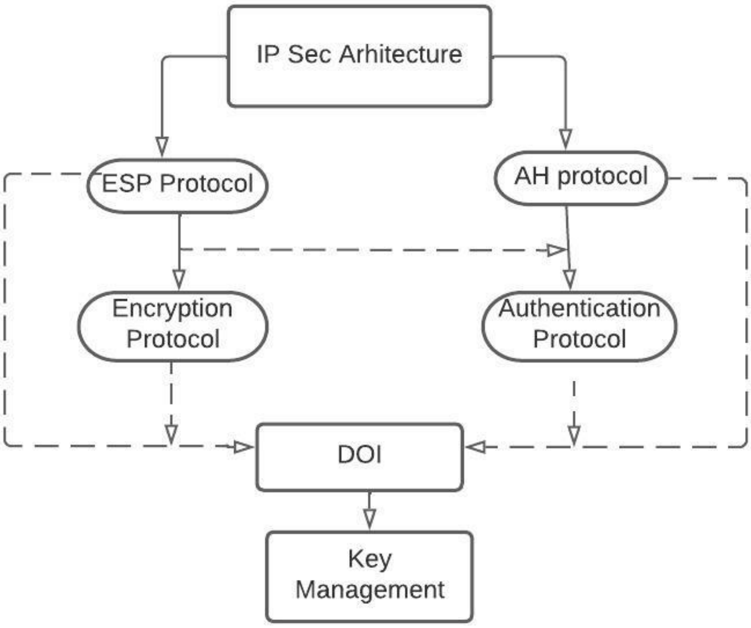


Figure 2. IP sec architecture

3. Present issues and solutions in the security of cloud data storage

The purpose of this essay is to give readers a general understanding of cloud storage's foundations and security issues. Cloud storage is no different from any other study subject when it comes to the importance of security and privacy. Data privacy and integrity, data recovery and vulnerability, inadequate media sanitization, appropriate third-party engagement, and backup are the primary security concerns with cloud storage. Cloud computing gives cloud service providers total access to data, which might lead to illegal actions such data copying, modification, deletion, and destruction. There are more security problems as a result of the restricted access. Threats, prospective assaults, external hostile activity, unequal service distribution, data loss, data leakage, and multitenancy problems are the main obstacles to cloud storage [7]. According to [8], This article highlights important aspects such data privacy, protection, security, and loss issues to provide readers a thorough grasp of security and privacy concerns in cloud storage. The author specifically highlights the problems with data storage that most clients face.

3.1 *Cloud storage issues*

The issues of privacy, integrity, data recovery, and vulnerability that come with storing data on cloud platforms are listed below Figure 3.

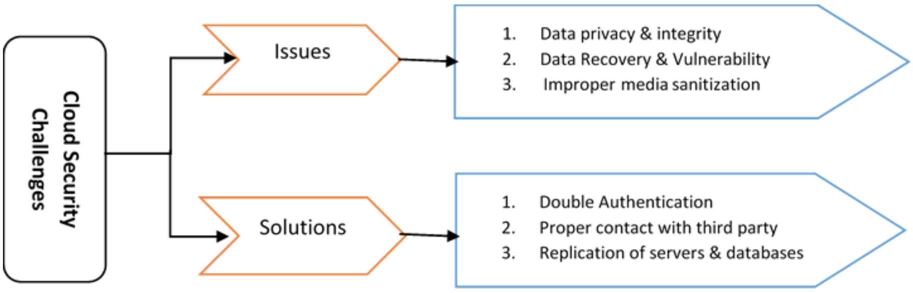

Cloud Security Challenges
Issues
1. Data privacy & integrity
2. Data Recovery & Vulnerability
3. Improper media sanitization
Solutions
1. Double Authentication
2. Proper contact with third party
3. Replication of servers & databases

Figure 3. Challenges in cloud storage

3.1.1 *Data privacy and integrity*

By keeping data on cloud servers rather than local PCs, cloud computing increases the risk of data loss and breaches. The big databases that are utilized to hold data are the main source of these risks. Nonetheless, these problems may be resolved by upholding security precautions and putting the CIA (Confidentiality, Integrity, and Availability) architecture into practice [9]. A few advantages of cloud computing are enhanced performance, economic viability, and effective resource management. Nevertheless, even with security precautions in place, there are always security risks. There are two kinds of risks associated with cloud computing. The first category consists of possible intruder activity and the unreliability of client service providers (CSPs). Adversary assaults fall into the second category and include things like the illicit alteration, removal, or destruction of user data. These assaults may result in data breaches, which is a serious issue with cloud storage.

Problems like time gaps between servers can also cause failure, which further jeopardizes user data security. Malicious activity using cloud computing can result in data loss, privacy difficulties, and other problems. Because of the potential for harmful attacks stemming from the previously listed hazardous scenarios, adherence to fundamental cryptographic standards is necessary in order to guarantee cloud computing performance. Algorithms for cryptography can aid in reducing dangers and hazards [10].

3.1.2 *Vulnerability and data recovery*

Although there are many benefits to using cloud computing, there is a risk that data may be compromised by unauthorized users during periods of high traffic flow. These malevolent operations employ a variety of methods to obtain data from prior users. Although well-known websites like Amazon and Ali Express have had this problem, they have often been able to retrieve their data. This presents a significant risk to private user data.

3.2 *Cloud storage solutions*

Suggested remedies to the above-described problems, including data sanitization and backups, include the following [11].

3.2.1 *Data sanitization*

One of the most important steps in solving storage-related issues is sanitization. To avoid duplication, sensitive data must be removed. All information needs to be real and true. When there is a disk shift, a maintenance problem, or subpar service, sanitation is required. Priority reduction and advanced resource allocations can be utilized to overcome this issue.

3.2.2 *Backups of data*

In the event that data is accidentally or inadvertently deleted, having a backup is essential. A grading system, ranging from 1 to 10, was presented by the author to help users assess the security, sensitivity, and data integrity requirements for their data. CSPs utilize a grading system on a scale of 1 to 10 in order to guarantee the security, sensitivity, and data integrity of the stored data. The security level is established and routine data backups are kept up to date based on this grade. It is necessary to adhere to certain standards and norms in order to stop malevolent actions like incursion.

3.2.3 *Common attacks in cloud storage*

Network-based attacks, application-based attacks, and storage-based assaults are the three categories into which cloud storage attacks fall. Figure 4 displays an extensive list of various assaults [12]. In the event that data is accidentally or inadvertently deleted, having a backup is essential. A grading system, ranging from 1 to 10, was presented by the author to help users assess the security, sensitivity, and data integrity requirements for their data. CSPs utilize a grading system on a scale of 1 to 10 in order to guarantee the security, sensitivity, and data integrity of the stored data. The security level is established and routine data backups are kept up to date based on this grade. It is necessary to adhere to certain standards and norms in order to stop malevolent actions like incursion.

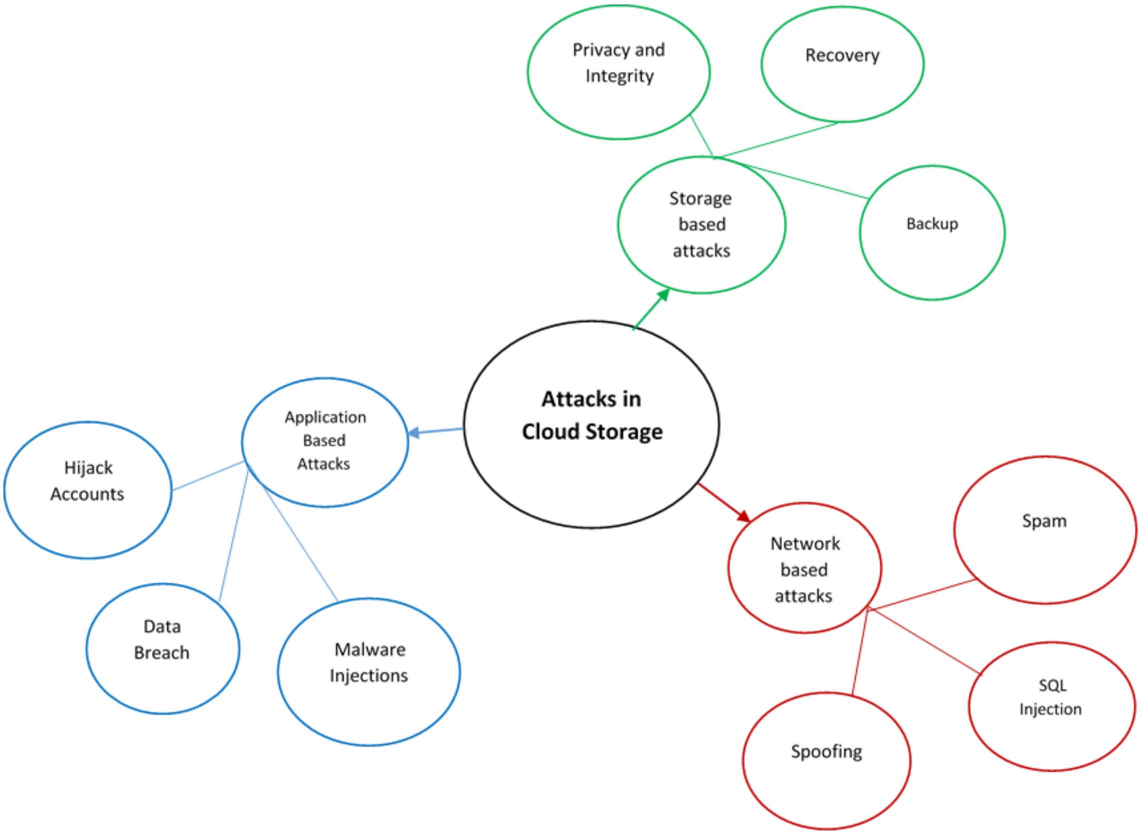


Figure 4. Attacks in cloud storage

3.3 *Data security in dropbox*

The public cloud service Dropbox was created in 2007 by two MIT students, Arash Ferdowsi and Drew Huston. Drew came up with the concept as he kept forgetting his flash drive at home. Dropbox protects data while it is in transit between Dropbox applications and other servers using secure sockets layer (SSL) and transport layer security (TLS). These provide a safe tunnel that is secured by advanced encryption standard (AES) encryption of 128 bits or more. Dropbox files that are not in use are secured using a 256-bit advanced encryption standard to safeguard critical user information against ransomware, malware, brute-force assaults, and data breaches. Since then, Dropbox has had success. The cloud provider develops, manages, and maintains the infrastructure; all users need is an internet connection. Users only have access to the application. When data is stored in the cloud under this service paradigm, the user has no control over it. Dropbox protects user accounts against unauthorized login attempts via two-factor authentication, user and device management, and a zero-knowledge password manager. Aside from that, sophisticated sharing restrictions that assist guarantee that only authorized individuals have access include password security, expiration dates, and simple revocation of files and folders. For many of the data processing and file storage requirements of users, Dropbox complies with international regulatory standards. This includes support for HIPAA compliance for teams and GDPR compliance [13].

3.4 *Data security in NextCloud*

Frank Karlitschkek and a group of seasoned engineers and business owners created NextCloud, a private cloud service, in 2016 to regain control over user data and information. It is an open-source, free collection of client-server programs that also provides information and data. NextCloud employs a number of outside penetration testers and specialists and states that security and privacy are its top priorities. Additionally, they provide financial incentives to those who identify and disclose vulnerabilities through their bug bounty program. When NextCloud was created, they have seen a significant amount of acceptance. NextCloud served both small businesses and private people [14].

3.5 *Data security in SharePoint and OneDrive*

In a time when the value of individual privacy is eroding, it is more crucial than ever to keep the information private. The most crucial factor to take into account when selecting a cloud collaboration platform is cloud provider confidence. Security, privacy, compliance, and transparency are the cornerstones of gaining and preserving confidence, and they apply to Microsoft SharePoint and OneDrive for Business. They are your files if you use OneDrive and SharePoint. You command and possess them. Despite the strength of the cloud computing idea, many consumers in this day and age are unaware that their cloud storage provider may use or send their information to other parties. Though most users don't give security and data protection on the cloud much attention, cloud storage is widely used these days. OneDrive from Microsoft is a highly well-liked cloud storage service that allows you to save files online. The user must log into their Microsoft account in order to view their data. Surprisingly, the user does not always have access to all of their OneDrive files using File Explorer while logging onto a separate Windows 10 computer. OneDrive effortlessly saves and recovers data from any device, and it functions well with Microsoft files. OneDrive is swiftly rising to the top of the personal cloud storage market [15].

4. Literature review

Sec Cloud, a data privacy technique proposed by Wei et al. [16], offers third-party pairing, encryption, and signature verification to protect cloud services. Using methods like multiplicative and additive groups, cyclic groups, and other approaches, the protocol creates keys for encryption and decryption. The Diffie-Hellman technique is used to produce session keys, which are then compared to the previously generated key and its signature. For security, the protocol uses hash trees (Markle) to verify data storage. The suggested solutions don't deal with availability concerns, even though they offer secrecy, integrity, and privacy. To address storage security issues, Yang [17] proposed the File Assured Deletion (FADE) technique. Data integrity, security, and privacy are guaranteed by this protocol. The program provides encryption, guaranteed deletion, and secret sharing, among other trusted party services. Similar to the Wei et al. work, it addresses confidentiality, integrity, and privacy issues but leaves availability out.

Q. Liu [18], The author suggested a time-based plan to address storage problems in cloud computing. Using the ABE algorithm, which is renowned for its capacity to transfer data securely, the system entails re-encryption. The approach provides robust privacy protection and safe cloud data exchange. The plan makes use of attribute-based encryption and proxy re-encryption with a clear focus on privacy and secrecy. This work, a survey by R Barona et al. [19], examines the different security risks and problems with data breaches that occur in cloud computing settings, as well as the research fields associated with data breaches. The writers talk about the main reasons why data breaches happen, such as technological problems, malevolent attacks, intrusions without stealing information, human mistake, and online cyber theft. They talk about the difficulties and reasons behind data breaches and provide security solutions to lessen these challenges and their drawbacks. Among the techniques covered are:

- Homomorphic cryptography;
- High confidence offsite server attestation
- A range of tools include features including real-time data traffic detection and future forensic audit trails.

The author of Mouna et al. [20] described a method intended to assess the dangers of cloud providers' data breaches based on previously established security service level agreements (Sec-SLA). Cloud provider security flaws are found using a tree-based structure, and the system may serve as a decision support tool by determining the origin of an attack and forecasting the consequences of an attack route. Algorithms for key creation, shared vital generation, encryption, key recovery, and proxy recovery are also covered in the article. The authors show that their system can combine data error localization and guarantee storage correctness by introducing homomorphic tokens, so fulfilling the aim of the study. Future research, according to the authors, should focus on fine-grained data localization and dynamic data storage. Jaydip Kumar has carried out a thorough analysis of several techniques for data storage security [21]. The author investigated many techniques for protecting raw data sets, including naïve Bayes, K-NN, K-means, and evolutionary algorithms, along with associated pseudo codes and functions. The study also makes various recommendations for cloud-based security measures, such as encryption, data masking, access control, one-time password authentication, intrusion detection system (IDS) software, and access control. To guarantee safe cloud data storage, the author emphasizes the necessity for more study on novel security techniques. Even with the advent of new security technologies, the author of that report [22] examined three critical security issues: account hijacking, multitenancy, and data breaches. The report also covered the many kinds of clouds and their offerings. The study emphasizes how data breaches impact IaaS, SaaS, and PaaS, the three categories of cloud services. The author recommends employing encryption and fundamental management strategies to protect against data intrusions. By using techniques like mutual authentication, passwords and smart cards, and biometric authentication, data breaches can also be lessened from account hijacking. Proposed countermeasures to multitenancy include segmentation and virtual machine introspection, but because of their complexity, they still need to be extensively deployed.

Yunqi examined the dangers of cloud storage and virus assaults on data in his study [23]. They suggested a strategy to deal with this problem, which entails adopting data partitioning techniques by splitting data objects into partitions and spreading them among servers, as well as building the data on the cloud using a hybrid or replication approach. The partitioning technique was implemented using the TLA, and the testing findings shown that it could offer a user-perceived update response latency that was better than, and in some cases much better than, previous ways. Given the circumstances, this is a favorable outcome and a major improvement. Rosado examined security risks with cloud computing data in his work [24] noting that a high number of services are contracted out to other parties, raising the possibility of outside assaults and non-compliance problems. Cloud computing strengthens data security against external hostile assaults by leveraging Web 2.0 and SOA technologies. The researcher put out a workable plan to deal with these problems.

4.1 *Research gap*

For many users, data security in cloud storage has been a major concern and an important problem. Ensuring data security is even more important now that there are more assaults targeting cloud storage. As a result, the data in cloud storage needs end-to-end protection from the application developers. Numerous investigations have been carried out to assess cloud storage's security performance under diverse conditions. To the best of our knowledge, however, research has not yet been done on how well cloud storage performs when IP sec is included in order to achieve end-to-end security and authentication.

5. Proposed model

Data breaches, multi-tenancy, and data loss concerns are addressed by the Security Encryption Privacy (SEP) paradigm, which combines one or more hybrid, private, or public clouds. Many organizations share the suggested model in order to prevent security risks. This kind of cloud model is often run by an outside company or internally. While the private cloud is less expensive than the communal cloud, the public cloud is more expensive than the latter. The security risks associated with cloud computing have become a competitive advantage for cloud providers, who are aware of these vulnerabilities. Increased cloud storage and security might be achieved by using a reliable network and platform. By safeguarding data and making its high-performing services available to the customer, a secure cloud offers a dependable solution.

It is divided into several stages, each of which has a specific purpose, such as data creation or encryption. All three cloud computing service models—Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)—have cloud security as their top priority. Ensuring application security is crucial for SaaS implementations. Effective SaaS application security, for example, is facilitated by secure coding techniques, ongoing vulnerability assessments, and thorough application testing. During deployments, PaaS security considerations will include every SaaS domain. However, as a PaaS user, you should be aware of a few minor variations. For instance, there are more choices available to set up the protection of data and the rights of users to access it. As such, you can be tasked with managing user permissions. However, certain PaaS providers could have integrated tools and systems for controlling user access. Similarities exist between IaaS security during cloud deployment and application and software security. For instance, the hypervisor or virtualized layer is managed by the cloud provider, while the customers are in charge of everything else. Certain security technologies that are effective for SaaS may not be appropriate for IaaS due to disparate deployment patterns.

The concept makes use of public key cryptography—more precisely, the RSA algorithm—to improve security and thwart various kinds of cloud storage assaults. With its ESP protocol ensuring secure data transfer and traffic, the IPsec architecture keeps data on the cloud. Ensuring the accuracy and consistency of the data is the main goal of the model. By inputting their registered credentials, users may access the cloud services and data, which are encrypted for total internet security using the RSA method. IPsec, or Internet Protocol Security, offers an encrypted and authenticated architecture for protecting IP (Internet Protocol) traffic. In IPsec, the following actions are usually performed in order to accomplish encryption: Choose an encryption algorithm. Choosing an encryption algorithm is the first step in achieving encryption in IPsec. AES (Advanced Encryption Standard), DES (Data Encryption Standard), and 3DES (Triple Data Encryption Standard) are only a few of the encryption methods that IPsec supports. The DES is a block cipher, which uses a 64-bit ciphertext key with permutation and substitution to apply a cryptographic key and algorithm concurrently to a data block rather than one bit at a time, as seen in Figure 5.

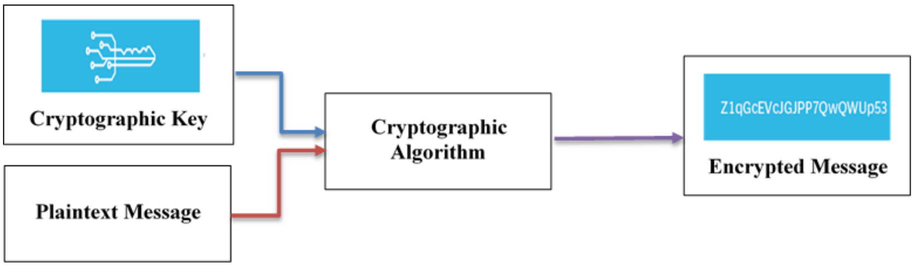


Figure 5. Data encryption standard architecture

64 bits of plain text are fed into DES as an input, and 64 bits of ciphertext are output. DES is a block cipher that encrypts data in blocks of 64 bits each. With a few small variations, the same key and algorithm are utilized for both encryption and decryption. There are 56 bits in the key. We discard bit locations 8, 24, 32, 40, 48, 56, and 64. The key length in the DES standard is 64 bits, or 8 bytes, with a parity check bit in each byte. The stages of the DES algorithm are as follows: An initial permutation (IP) function receives the 64-bit plain text block at the start of the operation. After then, the plain text is subjected to the first permutation [25].

i. Left Plain Text (LPT) and Right Plain Text (RPT) are the two parts of the permuted block that are created by the first permutation.

ii. The encryption procedure consists of sixteen cycles for each LPT and RPT.

iii. Finally, the LPT and RPT are reunited, and the newly combined block is subjected to a Final Permutation (FP).

iv. This procedure yields the intended 64-bit ciphertext.

$$IP(X) = L_0R_0 \tag{1}$$

$$L_{i-1} = R_{i-1} \tag{2}$$

$$R_i = L_{i-1} \bigoplus f(R_{i-1},\, K_i) \tag{3}$$

$$Y = IP^{-1}(R_{16}\, L_{16}) \tag{4}$$

Equation (1) gives the 64-bit plain text block to an initial Permutation (IP) function. On plain text, the first permutation is carried out. Equation (2) states that the round generates L_i and R_i, which advance to the following round (or final permutation box), using L_{i-1} and R_{i-1} from the previous round (or the initial permutation box). The left and right halves of the text are switched in Equation (3). The XOR function makes the mixer invertible. Within the function f (R_{i-1}, K_i), all noninvertible elements are gathered. Equation (4) displays the text encrypted. Finally, LPT and RPT are reconnected, and the combined block is subjected to a Final Permutation (FP). This procedure yields 64-bit ciphertext as its output. The U.S. government selected the symmetric block cipher Advanced Encryption Standard (AES) to safeguard sensitive data. Sensitive data is encrypted using AES in hardware and software all across the world. It is crucial for cybersecurity, electronic data protection, and government computer security. Data breaches and cyber-attacks have become all too common, and the consequences can be devastating. Not only risk financial lost, but the trust of their customers and partners can be severely damaged. Data protection has become a top priority for businesses of all sizes. With the increasing reliance on cloud technology, the need to safeguard sensitive information has never been more crucial. Cloud security assessments are a systematic and thorough evaluation of an organization's cloud security measures. They involve a comprehensive review of security controls, policies, and procedures to assess their effectiveness in protecting sensitive data. During a cloud security assessment, various aspects of cloud security are examined, including data encryption, access controls, network security, and incident response procedures. The assessment may also include a review of compliance with industry regulations and best practices.

AES includes three block ciphers:

- AES-128 encrypts and decrypts a block of messages using a 128-bit key length.
- AES-192 encrypts and decrypts a block of messages using a 192-bit key length.
- AES-256 encrypts and decrypts a block of messages using a 256-bit key length.
- Each cipher uses cryptographic keys of 128, 192, and 256 bits, respectively, to encrypt and decode data in blocks of 128 bits.

One 128-bit key has ten rounds in AES, a 192-bit key has twelve rounds, and a 256-bit key has fourteen rounds. A round comprises many processing stages, such as mixing, transposition, and replacement of the input plaintext to create the final ciphertext output seen in Figure 6.

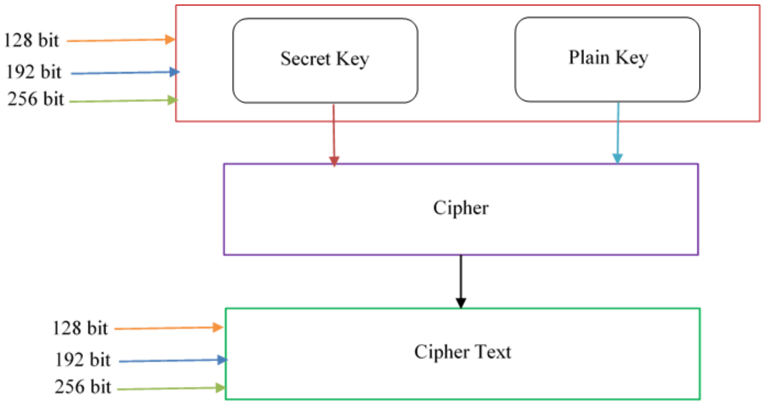
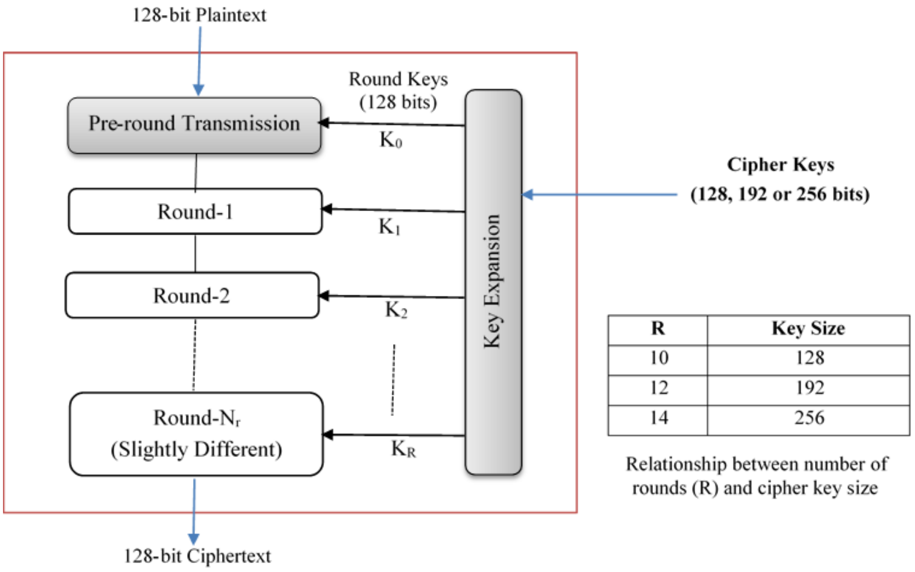


Figure 6. Advanced encryption standard architecture

In AES encryption, each round comprise of four sub-processes as shown in Figure 7.



R	Key Size
10	128
12	192
14	256

Figure 7. Encryption process in AES

The steps of the AES algorithms are mentioned below:

i. The plain text is divided into blocks.

ii. Implement the byte substitution.

iii. Each row is shifted a specific number of times.

iv. Matrix multiplication is performed, where each column is multiplied with a matrix.

v. Add round key.

IPsec generates and exchanges encryption keys between the communicating parties using a key exchange protocol, such IKE (Internet Key Exchange). Set up IPsec policies: The security guidelines for IP traffic are specified by IPsec policies. These regulations include authentication techniques, key exchange protocols, and encryption. Create security associations for IPsec: Security associations (SA) are in charge of IP traffic authentication and encryption. The security parameters specified in the IPsec rules are part of the security association that is established when two parties wish to connect securely. Encrypt IP traffic: After the security association has been formed, IP traffic can be encrypted with the encryption keys and agreed-upon encryption technique. Next, the encrypted data is sent across the network. Decrypt IP traffic: Using the matching decryption key, the encrypted data is unlocked upon receipt. Following decryption, the receiver may receive and process the data. An overview of the fundamental stages involved in achieving encryption in IPsec is given in [26]. The suggested model entails several phases, such as:

5.1 *Generation of data*

This approach starts with data generation, which is analogous to ownership. Data flow is facilitated by the ESP protocol, in which the user actively participates. The flow of data in companies is frequently directed. Users need to be aware of the ownership restrictions and maintenance procedures before storing any data in the cloud. Users may access their data and information, and the data owner is aware of the information that has been gathered. Additionally, users are entitled to request that their data and information be deleted.

5.2 *Data encryption*

Encrypting created data with the public key of the intended receiver is the first step towards data security. By ensuring that the data stays secret and confidential between the users, this encryption technique helps to avoid a number of security problems.

5.3 *Data transfer*

Once encrypted data has been gathered, it has to be sent. Although it is encrypted as a precaution, organizations usually do not need to encrypt data communication. To make sure that hackers cannot access the data or use it for illegal purposes, the major priority is protecting its confidentiality and integrity. Nevertheless, user identification is also required for data integrity, meaning that encryption is not enough to provide security. According to our suggested architecture, authentication is the first line of defense against any security issues down the line. These fundamental procedures protect the data during transport from illegal access and guarantee consistency and correctness. Integrity and confidentiality are essential aspects of cloud storage while transferring data.

5.4 *Usage of the data*

In the following stage, it is crucial to make sure the sent data is used appropriately. For example, encryption is a smart choice when the data is kept on a basic storage medium that doesn't change, like Amazon. Encryption is not appropriate for static data in cloud apps that are deployed using PAAS and SAAS models, and there are issues with inconsistent data that is not able to be encrypted because of indexing. Concerns regarding unencrypted data are raised by the fact that other users' data is kept alongside the user's due to the multi-tenant capability in the cloud. The security and privacy of data are seriously threatened by this. It is the data owner's obligation to do security checks on the supplied private information in order to resolve this issue. Users are responsible for making sure that the information they provide is accurate and consistently used for the intended purpose. Without authorization, no personal information is disclosed to unaffiliated third parties, such CSPs.

5.5 *Sharing the data*

In the subsequent stage, users' consent is required for data sharing; nonetheless, it is the data owner's duty to impose limitations and limits on the sharing of personal data. To distribute the data to registered users, the owner must grant access to a reliable third party. Upon receiving the data, users can use their private keys to decode it. Additionally, network, storage, and application-based assaults can be stopped using the RSA algorithm. The following is the RSA algorithm [27]:

$$n = (p \times q) \tag{5}$$

$$\varphi(n) = (p-1) \times (q-1), where\ \varphi(n) \lessdot n \tag{6}$$

$$1 < e < \varphi(n),\ where\,\gcd(\varphi(n), e) = 1 \tag{7}$$

$$d = e^{-1}\ mod\ \varphi(n),\ where\ d = decryption\ and\ e = encryption\ key$$

$$where\ (e \times d)\ mod\ \varphi(n) = 1 \tag{8}$$

$$E = D^{e}\ mod\ n \tag{9}$$

$$D = E^{d}\ mod\ n \tag{10}$$

Equation (5) shows the first part of the public key. Equation (6) shows the decrypt process. Equation (7), *e* shows the encryption key. '*e*' must be co-prime of phi and smaller than pi. Equation (9) illustrates the encryption process. This implies that the data owner has access to just one party, and that party is not permitted to disclose private information to third parties without the owner's consent. Equation (10) illustrates the decrypt procedure, so users need to make sure they follow the guidelines and stick to the sequence when sharing data with outside parties. They should also take precautionary measures to guarantee that data security is maintained. '*E*' displays the encrypted data, and '*e*' displays the encryption key. In a similar vein, '*d*' displays the decryption key and '*D*' the decrypted information.

5.6 *Storage of data*

Various strategies are needed for data storage, depending on the kind of data and the storage environment. While cloud-based data is usually kept in PaaS or SaaS systems, simple storage data is frequently employed in IaaS setups. Data security is always the major concern, regardless of the storage technique, and the CIA triad—confidentiality, integrity, and availability—is the main framework for doing this. Using public key encryption, which generates keys and uses encryption algorithms to protect data, is frequently the best way to guarantee secrecy. Public key cryptography is best suited for large-scale cloud computing systems since it is faster and more efficient than private key encryption. Furthermore important is data integrity, and customers may find it challenging to understand where their data is kept due to contemporary cloud computing capabilities. Data integrity may be ensured by using encryption and security algorithms such as RSA, AES, DES, and Diffie-Hellman to handle this problem. Lastly, because it is vulnerable to external threats, data availability is crucial. As seen in Figure 8, the RSA method may be utilized as a security-based solution to shield cloud data from different dangers and thwart these attacks.

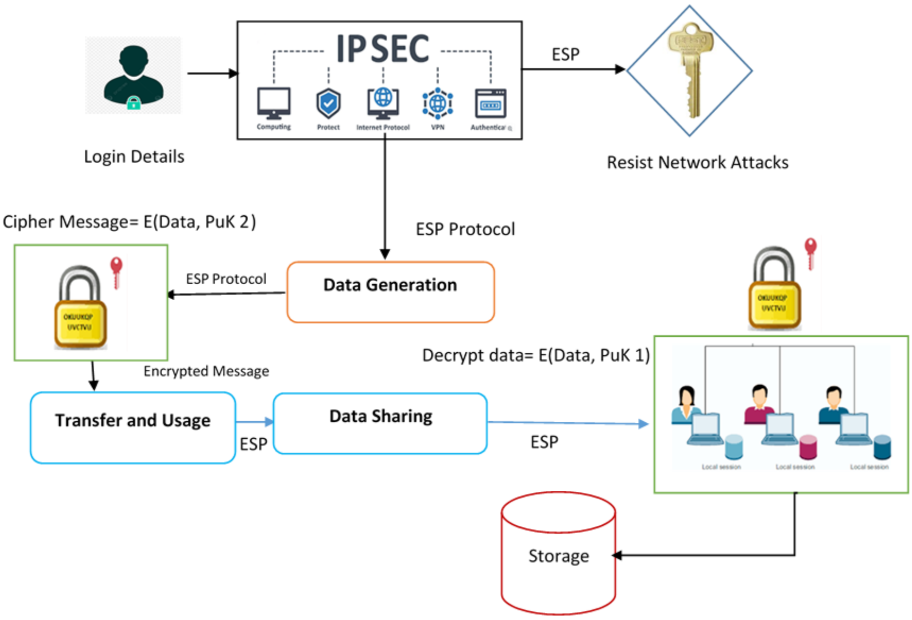


Figure 8. Proposed model

6. Evaluation and discussion

Encryption and the CIA trinity (confidentiality, integrity, availability) are frequently employed to guarantee the security of communication and information networks. The common cryptographic formulas and methods listed below are employed in secure communication to accomplish these goals [28, 29, 30].

6.1 *Encryption*

As seen in Figure 6, asymmetric encryption, commonly referred to as public-key cryptography, is an encryption system that employs two keys for encryption and decoding. When utilizing asymmetric encryption, the sender encrypts a message using the public key of the receiver. The recipient uses their private key to decode the message [31].

$$C = E(D, PuK2) \tag{11}$$

$$C = E(D, PuK1) \tag{12}$$

For safe communication, encrypted data may be computed using Equations (11) and (12). As seen in Table 1 and Figure 9, the bar graph contrasts several security models and shows that IP Sec has a better percentage of data security than the other security protocols, such as FADE, Time PRE, Sec-Cloud, and Local Storage [32].

Table 1. Data encryption percentage of different models

Sr. No.	Model	Data Encryption (%)
1	IPSEC	83
2	Local	60
3	Time Pre	63
4	FADE	71
5	Second Cloud	75

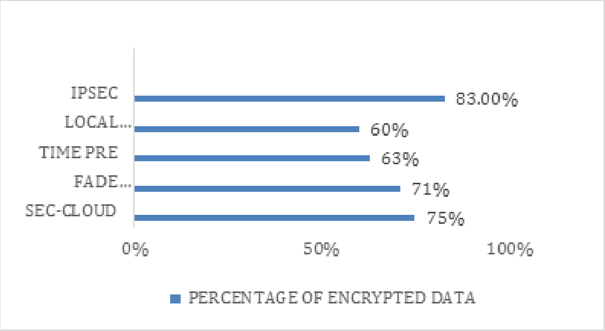


Figure 9. Percentage of different models for data integrity

6.2 *Confidentiality*

It speaks about preventing unwanted disclosure of information while maintaining its privacy. Secrecy may be attained by using cryptographic methods like encryption, as seen in Figure 7. Equation (13) is used in cryptography [33]:

- The cipher text is C.
- The function for encryption is E.
- The encryption key is K.
- The message in plaintext is M.

Table 2 and Figure 10 illustrate that in Equation (14) for decryption, M is the plaintext message, D is the decryption function, K is the decryption key, and C is the cipher text.

$$C = E(K, M) \tag{13}$$

$$M = D(K, C) \tag{14}$$

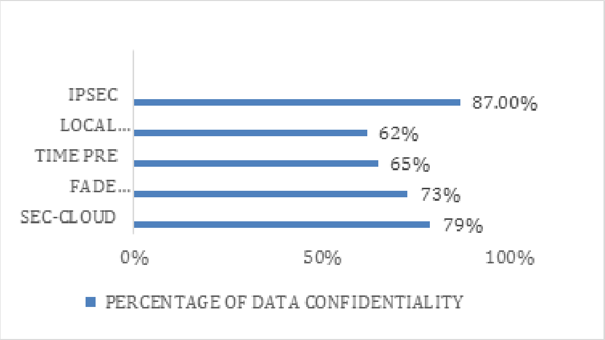


Figure 10. Percentage of different models for data confidentiality

Table 2. Data confidentiality percentage of different models [34]

Sr. No.	Model	Data Confidentiality (%)
1	IPSEC	87
2	Local	60
3	Time Pre	65
4	FADE	73
5	Second Cloud	79

6.3 *Integrity*

As seen in Figure 8, it guards against unauthorized change or deletion of information that is accurate and full. Integrity can be attained by using cryptographic methods like digital signatures and message authentication codes (MACs). MAC is represented by Equation (15), where T stands for MAC tag, MAC for MAC function, K for MAC key, and M for message. The digital signature is represented by S in Equation (16), the signature function is represented by Sign, the private key is represented by K, and the message is represented by M. As illustrated in Table 3 and Figure 11, Equation (17) for signature verification uses V as the verification result, verify as the verification function, K as the public key, M as the message, and S as the signature [35].

Issuing Digital Signatures for Integrity and Authentication of Digital Documents

$$T = MAC(K,M) \tag{15}$$

$$S = Sign(K,M) \tag{16}$$

$$V = Verify(K,M,S) \tag{17}$$

Table 3. Data integrity percentage of different models

Sr. No.	Model	Data Integrity (%)
1	IPSEC	89
2	Local	60
3	Time Pre	65
4	FADE	74
5	Second Cloud	77

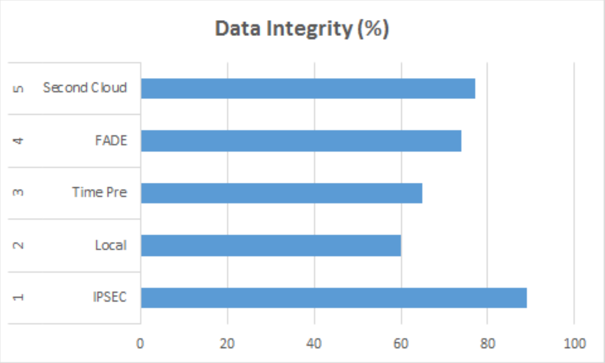


Figure 11. Percentage of different models for data integrity

6.4 *Availability*

As seen in Figure 9, it relates to making sure that information and communication systems are available to and useable by authorized users. Availability may be attained through the use of cryptographic techniques like key exchange and secure communication protocols. Key exchange equation: KE is the primary exchange function, while $K1$ and $K2$ are the shared keys. The cipher text C in Equation (19) is the same as the plaintext message M, the encryption function E is the same as the shared key $K1$, and the safe communication equation is represented by Equation (18). As seen in Table 4 and Figure 12, Equation (20) for secure communication decryption uses M for the plaintext message, D for the decryption function, $K1$ for the shared key, and C for the cipher text [36].

$$K1 = KE(K2) \tag{18}$$

$$C = E(K1, M) \tag{19}$$

$$M = D(K1, C) \tag{20}$$

Table 4. Data availability percentage of different models

Sr. No.	Model	Data Availability (%)
1	IPSEC	91
2	Local	59
3	Time Pre	62
4	FADE	75
5	Second Cloud	79

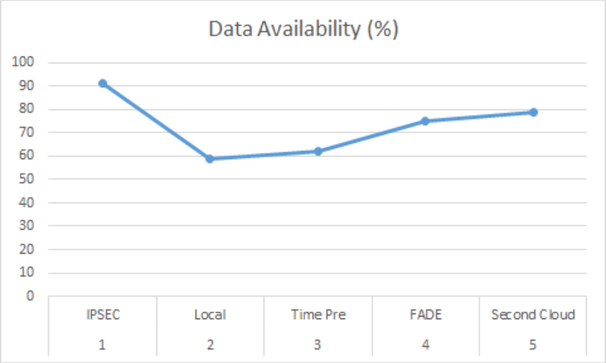


Figure 12. Percentage of different models for data availability

In conclusion, cryptographic methods and equations, such as encryption, decryption, MACs, digital signatures, key exchange, and secure communication protocols, may be used to accomplish encryption, confidentiality, integrity, and availability in secure communication [37]. Compared to previous protocols, our suggested SEP approach delivers higher levels of data encryption and CIA triad security. In terms of efficiency, cost-effective analysis in SEP is helpful as it guarantees the efficient use of limited cloud computing resources while reducing expenses. As a result, this strategy has several benefits, including financial savings and the avoidance of needless raw material waste. On the other hand, access control features of information security technologies have been shown to be successful and effective in maintaining the confidentiality of sensitive data. Using stochastic Petri nets models, the advantages of deploying a DRM product in businesses are measured and contrasted with the security requirements of an organization and possible implementation costs. A company's capacity to make wise security investment decisions may be strengthened by using this process. A method was developed that can quantitatively assess the advantages and disadvantages of deploying information security technology, helping security investors to make informed investment decisions. A case study centered on the implementation of the MS IRM system.

By utilizing less resources and requiring less maintenance, the suggested approach has the ability to achieve the CIA trinity bond (Confidentiality, Integrity, and Authentication) in addition to encryption and authentication. Full data security; threats are identified and thwarted. Additionally, it enables you to use the security algorithm to identify the assault. By utilizing less resources and requiring less upkeep, our suggested methodology has the ability to accomplish the CIA trinity bond (Confidentiality, Integrity, and Authentication) in addition to encryption and authentication. Complete data security is ensured, and assaults are identified and thwarted. With an emphasis on security, efficiency, and cutting-edge trends, a thorough examination of the cloud computing environment explores the changing paradigms that have shaped the industry's current state and provides insights into the opportunities and problems that will arise as technology develops. Addressing the crucial issues of data privacy, integrity, and access control in cloud systems revolves on security. In an era characterized by cyber threats and vulnerabilities, the study emphasizes the significance of strong security frameworks by examining the most recent security procedures and protocols put in place to protect sensitive information. Another important component of security is efficiency, which is assessed through a study that looks at scalability issues, resource allocation techniques, and performance optimization tactics.

Table 5. Comparisons with different security models

Authors	Proposed Scheme	Services	Privacy	Integrity	Availability	Confidentiality
L. Wei, H. Zhu [27]	Sec-Cloud, a solution aimed at enhancing the security of data stored in the cloud	Encryption: Secure encoding Bilinear pairing: Efficient cryptographic pairing Signature verification: Authentication validation Trusted third party: Reliable intermediary	Yes	Yes	No	Yes
Y. Tang, Lee, Lui [28]	FADE, a protocol designed to ensure the confidentiality and authenticity of data	Encryption: Secure data encoding Trusted third party: Reliable intermediary Assured deletion: Guaranteed data erasure Threshold secret sharing: Distributed secret management	Yes	Yes	No	Yes
Q. Liu, G.Wang [29]	Time PRE, a secure data sharing scheme designed for use in cloud environments.	Proxy re-encryption: Third-party key exchange Attribute-based encryption: Access control by attributes	Yes	No	No	Yes
Z. Tari [30]	Approach to ensuring the security of data stored locally	Erasure correcting code: Error-correcting code for data recovery Data redundancy: Duplication of data for fault tolerance	No	Yes	Yes	Yes
Purposed model	IPsec (Internet Protocol Security) protocol is a suite of cryptographic protocols used for securing Internet Protocol (IP) communications.	Authentication Header (AH): Provides data integrity and authentication without encryption Encapsulating Security Payload (ESP): Provides data confidentiality, integrity, and authentication through encryption Security Associations (SA): Negotiates and manages the security parameters for IPsec communications Key Management: Provides secure key exchange and management for the encryption and authentication mechanisms used by IPsec.	Yes	Yes	Yes	Yes

7. Conclusions and future work

Since cloud computing has emerged as the most preferred choice for consumers, worries over the security of data kept there have grown. This document has identified and addressed a number of security risks. A novel framework, dubbed the "Security Encryption Privacy Model," has been put out to examine the security challenges present in the three different cloud model types—SaaS, PaaS, and IaaS. Data production, transmission, consumption, sharing, storage, and encryption utilizing encryption keys are all secured by security encryption. For this purpose, an RSA security algorithm is utilized to mitigate various data threats, risks, and attacks in different cloud models. After applying this algorithm, the security encryption technique ensures that the data stored in the cloud is reliable, secure, and hidden from unauthorized users, which was a significant challenge for cloud security providers in the past. In the future, some innovative solutions will be introduced to improve cloud storage's scalability, reliability, and efficiency.

Conflict of interest

The authors declare no conflict of interest.

References

[1] A. Rashid, "Cloud computing characteristics and services: a brief review," *Int. J. Comput. Sci. Eng.*, vol. 7, no. 2, pp. 421–426, 2019.

[2] M. Alouffi, "A systematic literature review on cloud computing security: threats and mitigation strategies," *IEEE Access*, vol. 9, pp. 57792–57807, 2021.

[3] P. Sharma, "Analysing the adoption of cloud computing service: A systematic literature review," *Global Knowl. Mem. Commun.*, vol. 70, pp. 114–153, 2020.

[4] B. Abdurachman, "Survey on threats and risks in the cloud computing environment," *Procedia Comput. Sci.*, vol. 161, pp. 1325–1332, 2019.

[5] M. Esper, "Implementing Protection on Internal Networks using IPSec Protocol," in *Proc. 2022 8th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Coimbatore, India, Mar. 25–26, 2022, pp. 378–383.

[6] R. Kumar, "Encryption and Authentication of Data Using the IPSEC Protocol," in *Proceedings of the Fourth International Conference on Microelectronics, Computing and Communication Systems: MCCS 2019*, Singapore: Springer, 2021, vol. 4, pp. 855–862.

[7] P. Rakesh, "Distributed scheme to authenticate data storage security in cloud computing," *Int. J. Comput. Sci. Inf. Technol. (IJCSIT)*, vol. 9, 2017.

[8] J. Yang, "Data security and privacy protection for cloud storage: A survey," *IEEE Access*, vol. 8, pp. 131723–131740, 2020.

[9] J. Sun, "Privacy protection and data security in cloud computing: a survey, challenges, and solutions," *IEEE Access*, vol. 7, pp. 147420–147452, 2019.

[10] P. Ravi Kumar, "Exploring Data Security Issues and Solutions in Cloud Computing," in *Proc. 6th Int. Conf. Smart Comput. Commun.*, Kurukshetra, India, Dec. 7–8, 2017.

[11] M. Kadam, "A Comprehensive Overview of Privacy and Data Security for Cloud Storage," *SAMRIDDHI: A J. Phys. Sci., Eng. Technol.*, vol. 14, pp. 296–300, 2022.

[12] P. Suryateja, "Threats and vulnerabilities of cloud computing: a review," *Int. J. Comput. Sci. Eng.*, vol. 6, pp. 297–302, 2018.

[13] A. Olaosebikan, T. Dissanayaka, and A. Mailewa, "Security & Privacy Comparison of Next Cloud vs Dropbox: A Survey," in *Proc. Midwest Instr. Comput. Symp. (MICS)-2022*, Milwaukee, WI, USA, Apr. 1–2, 2022.

[14] D. Mailewa, et al., "A review of MongoDB and Singularity Container security in regards to HIPAA regulations," in *Proc. 10th Int. Conf. Utility Cloud Comput.*, Austin, TX, USA, Dec. 5–8, 2017.

[15] F. Aqus and H. Dhika, "Analyzing Data Encryption Efficiencies for secure cloud storages: A case study of Pcloud vs OneDrive vs Dropbox," *Fakt. Exacta*, vol. 12, no. 1, pp. 1–20, 2019.

[16] V. Sharmila, “Security and Privacy for Storage and Computation in Cloud Computing,” *Int. J. Sci. Res. (IJSR)*, vol. 4, pp. 525–527, 2020.

[17] Y. Wang, “A Review on Assured Deletion of Cloud Data Based on Cryptography,” *Procedia Comput. Sci.*, vol. 187, pp. 580–585, 2021.

[18] J. Liu, “Time-based proxy re-encryption scheme for secure data sharing in a cloud environment,” *Inf. Sci.*, vol. 258, pp. 355–370, 2014.

[19] M. Barona, “A survey on data breach challenges in cloud computing security: Issues and threats,” in *Proc. 2017 Int. Conf. Circuit, Power Comput. Technol. (ICCPCT)*, Kollam, India, Apr. 20–21, 2017, pp. 1–7.

[20] A. Jouini, “A security framework for secure cloud computing environments,” in *Cloud Security: Concepts, Methodologies, Tools, and Applications*, Pennsylvania, PA, USA: IGI Global, 2019, pp. 249–263.

[21] J. Kumar, “Cloud computing security issues and its challenges: a comprehensive research,” *Int. J. Recent Technol. Eng.*, vol. 8, pp. 10–14, 2019.

[22] S. Pericherla, “Cloud Computing Threats, Vulnerabilities and Countermeasures: A State-of-the-Art,” *ISC Int. J. Inf. Sec.*, vol. 15, pp. 1–58, 2023.

[23] M. Celesti, “Towards hybrid multi-cloud storage systems: Understanding how to perform data transfer,” *Big Data Res.*, vol. 16, pp. 1–17, 2019.

[24] M. Abdulsalam, “Security and privacy in cloud computing: technical review,” *Future Internet*, vol. 14, p. 11, 2021.

[25] A. Sadiqa and K. Majid, “New extension of data encryption standard over 128-bit key for digital images,” *Neural Comput. Appl.*, vol. 33, no. 3, pp. 1–14, 2021.

[26] P. Gupta, “A Review on Cryptography based Data Security Techniques for the Cloud Computing,” in *Proc. 2021 Int. Conf. Adv. Comput. Innov. Technol. Eng. (ICACITE)*, Greater Noida, India, Mar. 4–5, 2021, pp. 1039–1044.

[27] U. Musa, M. Adebivi, O. Aroba, and A. Adebivi, “RSA and Elliptic Curve Encryption System,” *Int. J. Inf. Sec. Privacy*, vol. 18, no. 1, pp. 1–27, 2024.

[28] R. Belguith, “Enhancing data security in cloud computing using a lightweight cryptographic algorithm,” in *Proc. 11th Int. Conf. Autonomic Autonomous Syst.*, Rome, Italy, May 24–29, 2015, pp. 98–103.

[29] S. Kishore, “RSA Algorithm: A Theoretical study and implementation,” *Int. Res. J. Modernization Eng. Technol. Sci.*, vol. 2, pp. 834–840, 2020.

[30] S. Saroj, “Threshold Cryptography Based Data Security in Cloud Computing,” in *Proc. 2015 IEEE Int. Conf. Comput. Intell. Commun. Technol.*, Ghaziabad, India, Feb. 13–14, 2015, pp. 202–207.

[31] V. Kalashnikov, V. Avramenko, N. Kalashnikova, and J. Kalashnikov, “A Cryptosystem Based Upon Sums of Key Functions,” *Int. J. Combinatorial Optim. Problems Inform.*, vol. 8, no. 3, pp. 31–38, 2017.

[32] P. Yang, N. Xiong, J. Ren, “Data Security and Privacy Protection for Cloud Stroage: A Surve,” *IEEE Access*, vol. 1, no. 1, pp. 31–45, 2020.

[33] N. Alsulami, A. Eman, and M. Mostafa, “A Survey on Approaches of Data Confidentiality and Integrity Models in Cloud Computing Systems,” *J. Emerg. Trends Comput. Inf. Sci.*, vol. 6, no. 3, pp. 188–195, 2015.

[34] P. Somasundaram and P. Iaeme, “Encryption Techniques and Access Control to Achieve Secure Transmission of Phi in the Cloud,” *Int. J. Inf. Technol. Manag. Inf. Syst.*, vol. 14, no. 2, pp. 31–38, 2023.

[35] A. Hassan, J. Ismael, A. Alaa, and R. Xunhuan, “Issuing Digital Signatures for Integrity and Authentication of Digital Documents,” *Al-Mustansiriyah J. Sci.*, vol. 34, no. 3, pp. 50–55, 2023.

[36] W. Shuaib, F. AreeJ, Y. Aun, and S. Farhan, “Encryption Techniques and Algorithms to Combat Cybersecurity Attacks: A Review,” *VAWKUM Trans. Comput. Sci.*, vol. 11, no. 1, p. 295305, 2023.

[37] R. Kumar, “A Systematic Review of the Security in Cloud Computing: Data Integrity, Confidentiality and Availability,” in *Proc. 2020 IEEE Int. Conf. Comput. Power Commun. Technol. (GUCON)*, Greater Noida, India, Oct. 2–4, 2020, pp. 334–337.