IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Study On Cloud Data Integrity And Security Protection With Improved Cryptography

SEEMA DEVI,[1] Dr. KALPNA MIDHA[2]
Student P.hd,[1] Assistant Professor[2]
Department of Computer Science
Shri Khushal Das University, Hanumangarh, India

Abstract:
Objective: Explores the critical aspects of ensuring cloud data integrity and security through enhanced cryptographic techniques. Emphasizing the need for robust protection in cloud environments, the study delves into improved cryptographic methods as a pivotal means to safeguard sensitive information. The paper highlights advancements in encryption technologies, addressing emerging threats and bolstering data integrity within the dynamic landscape of cloud computing

Method/ Analysis: Present research is concentrated on data reliability and security in cloud environment. In order to achieve this goal improve cryptography mechanism have been considered. It has been observed that there is lack of performance and security in case of conventional approaches. Thus there remains need of advanced security mechanism that should be capable to provide safely to reduce packet dropping rate and improve accuracy that the time of delivery.

Applications/ Improvements: Simulation results conclude that proposed security model is providing better performance and security as compared to conventional AES based encryption mechanism. The future scope of this research is that it would provide significant contribution toward cloud security.

Keywords: Cloud computing, security, cryptography, encryption, decryption

[1] INTRODUCTION

Developing technology cloud computing (CC) has indefinable ties to the GC standard and other major improvements including function computing, distributed computing, and bunch computing. Attaining asset virtualization is the objective of both GC and Cloud. There are significant differences between GC and CC, even if that is not the goal. While increasing the general computing limit is CC's primary emphasis, achieving most extreme computing is GC's primary emphasis. CC also provides a way to handle a broad variety of hierarchical demands by providing more adaptable servers and applications to work with. Companies like Amazon, IBM, "Dropbox," Apple's "iCloud," Google's apps, Microsoft's "Purplish blue," and many more may attract regular customers from all over the globe. CC has introduced a new way of thinking that allows its users to robustly store or construct programs and access them from anywhere at any time via Internet interactions. Cloud Computing provides easy and customizable solutions to access or operate with cloud applications based on customer need. According to the needs of the customer, CC may provide a platform for structural applications, a framework to store and manage the organization's data, and applications to carry out the client's regular tasks. When a customer uses cloud services, data stored in local vaults is transferred to a server farm located far away. With the help of services offered by cloud specialist

firms, this data located in distant places may be accessed or processed. This elucidates that in order for a client to process or store data in the cloud, the data must first be sent to a distant server over a channel (the web). The utmost care must be used while handling and processing this data in order to prevent data breaches.

1.1 CLOUD COMPUTING

The term "cloud computing" refers to a way of running applications, data, and files that makes use of a network of interconnected computers, either privately or publicly accessible, to provide elastic capacity for these tasks. The introduction of this technology has greatly decreased the costs of processing, application hosting, content storage, and distribution. Cloud computing offers a realistic way to see immediate savings, and it may change a data center's setup from a capital-intensive one to a variable-priced one. One of the most basic principles of cloud computing is the reusability of IT capabilities. When contrasted with more conventional ideas like "grid computing," "utility computing," or "autonomic computing," cloud computing ability to expand perspectives beyond organizational boundaries stands out. We provide a high-level architecture of cloud computing that describes many strategies for delivering cloud benefits. Cloud computing offers the chance of cost reduction via enhanced and productive processing, and it improves collaboration, agility, scalability, accessibility, and efficiency. Cloud computing, in particular, represents the use of a collection of decentralized resources, including applications, data, and infrastructure, which are housed in pools of registers, systems, data, and capacity. Infrastructure reflection gives rise to the concept of asset democratization, which allows for pooled assets to be made accessible and available to everyone or anything authorized to use them via institutionalized approaches. This includes infrastructure, applications, and data. Advantage ally located building design: The idea of using these segments in whole or in part, alone or in coordination, gives an administration's planned engineering where assets might be gotten and used standard, as the infrastructure from applications and data output is all around described and in exactly coupled asset democratization. Transporting administration, rather than infrastructural administration, is the primary focus in this paradigm.

Cloud security model

- ✓ **Software as a Service (SaaS):** In this model, a broad application is offered to the customer, as a service on demand. A distinct order of the service runs on the cloud & various end users are overhauled. On the consumers' side, there is no requirement for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted & maintained. Today SaaS is presented by businesses corporations such as Google, Sales force, Microsoft, Zoho, etc.

- ✓ **Platform as a Service (Paas):** Here, a layer of software, or enlargement environment is condensed & accessible as a service, upon which other advanced levels of service can be built. The consumer has the liberty to construct his own applications, which run on the provider's substructure. To see manageability and scalability requests of the applications, PaaS providers proposal a predefined arrangement of OS and application servers, such as LAMP platform (Linux, Apache, MySql and PHP), restricted J2EE, Ruby etc. Google's ,IBM Cloud, Red hat open shift, etc are some of the popular PaaS examples.

- ✓ **Infrastructure as a Service (Iaas):**IaaS offers basic storage and computing abilities as homogenous services over the network. The customer would typically deploy his own software on the infrastructure. Some common examples are Amazon, Go Grid, Tera, etc.

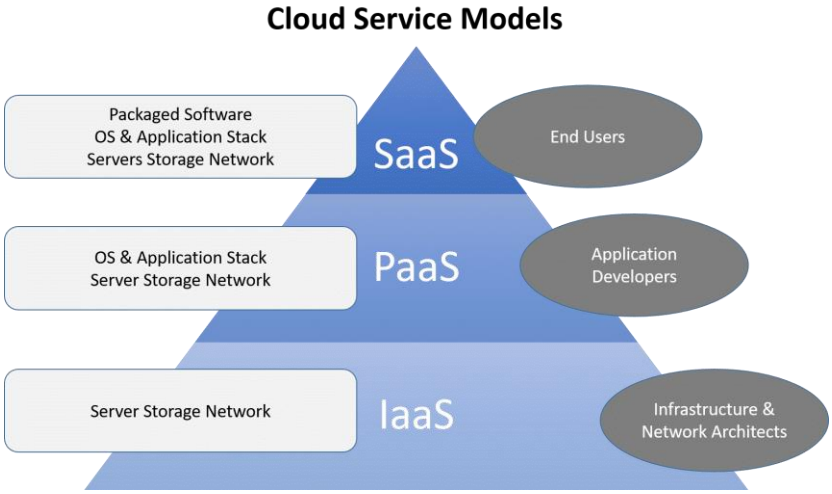


Figure 1.4: Cloud Computing Models

1.2 SECURITY IN CLOUD ENVIRONMENT

To make effective use of the present assets and applications, multi tenancy and virtualization are the main features. Because of virtualization, a single server, data center, office, and operating system may support several users. With this asset sharing concept, a cloud provider may service a large number of consumers. Security concerns arising from multi-occupancy and virtualization in the cloud include data assurance, communication, asset separation, and virtualization.

a) **Data protection**: The cloud computing foundation is shared among various users anytime of time. User data is put away and handled in a common environment that is under supplier's control. User data might be messed with by different malevolent substance. Absence of straightforwardness about the data storage area in the cloud environment, administrative issue because of cross outskirt storage, and so on makes the necessity of data privacy and protection in cloud environment progressively unmistakable. In this way data protection issues including data mystery, respectability and accessibility are key security issues in cloud computing.

b) **Application security**: Application programming running on or being created for cloud computing stages presents distinctive security challenges. Application that is running from the remote ought to be from legitimate supplier and without malware. Adaptability, transparency and public accessibility of cloud foundation are dangers for application security. Safeguarding respectability of applications being executed from remote machines is additionally one of the worries.

c) **Network security**: A cloud computing can be of sort public or private, in light of the sending model. Service and applications are gotten to from remote areas in a cloud environment. Ceaseless accessibility of cloud service with no interruption because of system security issues like refusal of service, and different assaults are significant security challenges.

d) **Virtualization security**: Virtualization innovation presents plausibility of new assaults through the hypervisor and other administration parts. There is no solid way to evaluate security of Virtual servers and applications. Multi-occupancy in cloud basics for distribution physical assets between VMs (Virtual Machine), can offer gradient to man-in-the-centre attack at the time of authorisation for any service. VMs are made and return as and when required in the cloud environment.

e) **Identity administration**: Identities are created at the season of enlistment process for cloud services to get to it. Every user utilizes his identity for getting to a cloud service. Unapproved access to cloud assets and applications is a noteworthy issue. A malignant element can mimic as an authentic user and access a cloud service. Several such vindictive elements secure the cloud resources instigation un-accessibility of

a service for trustworthy user. Likewise it might happen that the user crosses his limit at the season of service use.

If an asset or application's Access Control List is out of date, this might affect their ability to access a certain memory zone or do certain tasks. Consequently, in a cloud computing setting, both users and providers have challenges with the Identity Management framework for granting permission and approval. There is a persistent necessity for supplementary study and investigation in the areas of cloud security.

1.3 CLOUD DATA SYSTEM AND DATA SECURITY

There are a number of advantages to the cloud computing architecture over the more conventional client-server model of service data architecture. Because of the benefits of cloud computing, governments worldwide have begun to use cloud computing models instead of the traditional client-server approach. When it comes to rolling out the cloud computing concept to the whole economy, the government is often the first to do it. Cloud computing solutions tailored to suit clients' unique needs—including but not limited to security, cost sharing, faithful quality, etc.—are now available from several cloud providers. With cloud computing, clients may get foundation, platform, and programming as a service over the web, according to their needs.

Ensuring the availability and criticality of computer hardware, code, and data while protecting them against malicious or inadvertent manipulation is the primary goal of data security. Because of the web's essential features, organizations and governments are compelled to use it. Companies may suffer devastating losses due to a weak data security system, including financial losses, reputational damage, and a decrease in consumer confidence. Data security objectives and assets are monitored, and data security efforts are made to set up properly. The three main concerns for setting up a data security level are availability, transparency, and secrecy.

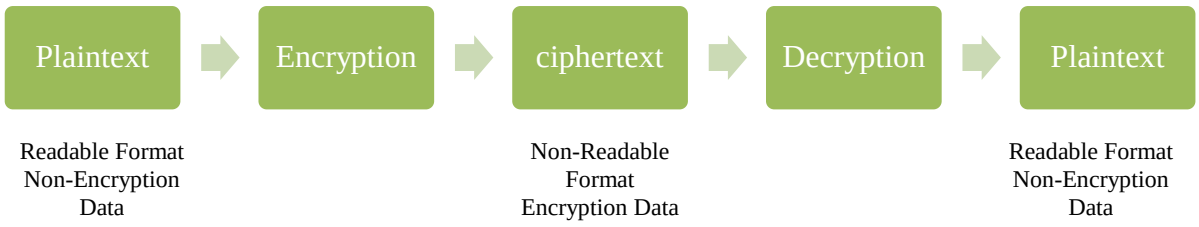
Security goals- Protecting a private or public organization's data and information from intruders and unauthorized users is crucial to protecting this valuable asset. Protecting an organization's data, programs, and hardware against unauthorized access while reducing the likelihood of disclosure, corruption, or unauthorised usage is what data framework security is all about.

- Secret - Secret affirms that just approved users approach data and data of an association. The entrance can be purposeful by the programmer, interlopers or pernicious representative of a similar association to take the data or data for their very own advantage. It very well may be inadvertent because of imprudence or inadequacy of the representative dealing with the data and data of the association. Secret additionally alludes to the component that keeps data and data from unapproved get to. The objective of secret is to utilize some solid user distinguishing proof and validation strategy like user ID and passwords, two variables or multifaceted validation technique to recognize an approved user, and bolster control strategies that limit each distinguished user's entrance to the data framework's assets.
- Validation is the primary prerequisite of data security framework. Appropriate solid validation framework can permit authentic people in, and keep interlopers or unapproved individual out. Any security framework must have an arrangement of controls that limit access to the association's assets as indicated by the approaches of the association. In PC based data framework it is evident to concentrate on disadvantages inside the data arrangement of an association to shield the data from unapproved get to.
- Integrity-Integrity guarantees protection against adjustment of data and data by gatecrashers or unapproved user, or inadvertent alteration of data or data by approved user, and avoidance of inner or outer consistency. Integrity of the profitable data and data of an association is significant; data ought not be changed without need unintentionally or deliberately by unapproved user. It likewise incorporates source integrity that implies that data has originated from the correct individual not from the phony individual, gatecrasher or phony office. Integrity can smooth integrate sincerity and untiring quality of the data, which entails they acquired data, holds the correct records and creates the vague data.

- Security levels- Here are three steps of requisite security intensities: low, modest, and high. An affiliation's operations, assets, and experts are unaffected by a lack of organization and integrity. There is no negative correlation between an association's data availability and its task and asset performance. Level of Direct Security: - All of an affiliation's responsibilities, resources, and representatives suffer greatly when credibility and grouping are compromised.

1.4 Cryptography

The field of study and practice known as cryptography deals with the mathematical algorithms and cryptographic keys used to encrypt data into an unintelligible form known as ciphertext. It is essential for keeping sensitive information, such as conversations, identities, and data, safe from prying eyes.



riginal data, yption. It is necessary to have the secret key that was used for encryption in order to decrypt, which is the act of turning

1. **Encryption and Decryption:** With the use of a cryptographic method and a secret key, the original data,
known as plaintext, may be transformed into ciphertext. This process is known as encryption. It is necessary to have the secret key that was used for encryption in order to decrypt, which is the act of turning
ciphertext into plaintext in reverse.
2. **Ciphertext:** The encrypted data is known as ciphertext since it is in an unintelligible and jumbled state. The only way to crack it and reoccurrence it to plaintext is to have the accurate key.
3. **Cryptographic Algorithms:** The algorithms used for encryption and decryption are mathematical functions. Three popular methods for encryption are DES, RSA, and AES, which stand for Advanced Encryption Standard and Rivest-Shamir-Adleman, respectively.
4. **Cryptographic Keys:** Encryption and decryption are controlled by keys. Two distinct kinds of keys exist:
   - **Symmetric Key:** Encryption and decryption utilize the same key. Secure key distribution is necessary, but it's more efficient.
   - **Asymmetric Key:** It employs a pair of keys, one for encryption and one for decoding, and is also called public-key cryptography.
5. **Key Management:** To keep encrypted data secure, secure key management is crucial. Producing, archiving, assigning, and revocation of keys are all part of it.
6. **Authentication:** Authentication makes use of cryptography to confirm the identification of individuals or systems. One typical method of authentication is the use of digital signatures and certificates.
7. **Hash Functions:** Cryptographic hash functions accept data or messages as input and return digests or hashes of a predetermined size. Data integrity is ensured via these. Two popular hash algorithms are Message Digest 5 (MD5) and Secure Hash Algorithm 256-bit (SHA-256).
8. **Digital Signatures:** To verify the authenticity and accuracy of a document or communication, digital signatures are used. A private key is used for their creation, and the public key is used for verification.
9. **Secure Communication:** Cryptography is used to secure data in transit over networks, such as when using SSL/TLS for secure web browsing, or in Virtual Private Networks (VPNs).

10. **Data-at-Rest Encryption:** Cryptography is applied to protect data stored on devices or servers, making it unreadable to unauthorized users.
11. **End-to-End Encryption:** This make sure that data is encrypted on the sender's device and decrypted on the receiver's device, avoiding arbitrators, together with service providers, from retrieving the plaintext.
12. **Cryptography in Blockchain:** Blockchain technology heavily relies on cryptographic techniques for secure transactions, digital signatures, and data integrity.
13. **Cryptography in Cyber security:** Cryptography is a cornerstone of cyber security, used to protect sensitive data, secure communication channels, and prevent unauthorized access to systems and information.
14. **Legal and Regulatory Considerations:** The use of cryptography is subject to various national and international regulations, with governments often seeking a balance between security and law enforcement concerns.

To keep up with new threats and ensure that digital information remains private, intact, and legitimate, cryptography is a dynamic topic that is always being researched and developed. Protecting digital assets and personal information relies heavily on it, making it an essential part of contemporary information security.

1.4.1 Cryptography in cloud computing

Cryptography plays a decisive role in confirming the security and privacy of data in cloud computing surroundings. Here are several key ways in which cryptography is used in cloud computing:

1. **Data Encryption:**
   - **Data in Transit:** When data is transmitted between a user's device and a cloud server, it is typically encrypted using protocols like SSL/TLS. This ensures that data is protected while in transit, making it difficult for eavesdroppers to intercept or tamper with the information.
   - **Data at Rest:** Cloud providers often use encryption to protect data stored in their data centers. This helps safeguard data in case of physical theft or unauthorized access to the storage infrastructure.
2. **Data Isolation and Multi-Tenancy:** Cryptography is used to enforce data isolation between tenants in a multi-tenant cloud environment. Even if multiple tenants share the same physical infrastructure, their data should remain confidential and inaccessible to others.
3. **Identity and Access Management:** Cryptographic techniques are used to authenticate users and manage access to cloud resources. This officially state that only ascribed users or facilities can access and influence data.
4. **Key Management:** Effective key management is essential in cloud environments. Cloud providers and users must securely generate, store, and distribute encryption keys. Key management systems help protect encryption keys from unauthorized access.
5. **Holomorphic Encryption:** Holomorphic encryption is an forward-looking form of encryption that agrees working out on encrypted data without the requirement for decryption. This technique is useful when users want to perform computations on data stored in the cloud without revealing the data itself.
6. **Secure Cloud Access and Identity Federation:** Federated identity and single sign-on (SSO) solutions often employ cryptography to ensure secure access to cloud services while minimizing the need for users to remember multiple passwords.
7. **Digital Signatures:** Digital signatures are used in cloud environments to verify the authenticity and integrity of data and transactions. They are critical in ensuring the validity of messages and documents shared between users and cloud services.
8. **Secure Containers and Virtual Machines:** Cryptography is used to secure containers and virtual machines in cloud environments, protecting them from tampering or unauthorized access.
9. **Secure Communication Channels:** Secure communication within cloud environments is essential. Cryptographic protocols and mechanisms are employed to establish and maintain secure channels between various cloud components and services.
10. **Compliance and Audit Trail:** Cryptographic techniques are used to establish an audit trail and ensure the compliance of cloud services with industry regulations and standards.

11. **Data Privacy and Compliance:** Cryptography can help organizations comply with data protection regulations, such as the General Data Protection Regulation (GDPR), by protecting the confidentiality and privacy of sensitive customer data.
12. **Secure Cloud Backups:** Cloud backups are often encrypted to protect sensitive data. This confirms that data stored in backup repositories remains secure and confidential.

Cryptography in cloud computing is a acute section of global cloud security. Cloud providers typically offer a range of cryptographic tools and services to help users protect their data and maintain the confidentiality and integrity of information stored and processed in the cloud. However, users must also play a role in properly configuring and managing cryptographic measures to ensure the security of their data and applications in the cloud.

[2] Problem Statement

Using the same tried-and-true procedures that have traditionally been used on other networks is not an option for ensuring the security of the large data since these approaches are no longer sufficient. The transmission of large amounts of data frequently takes place through the use of the protocol-specific port, such as port 21 for FTP or port 80 for HTTP. The percentage of successful assaults increases along with the number of preconfigured ports that are put to use.. The only tier of the stack that the Tradition system protected was the application layer. One channel is used for the communication of all of the facts. It would have been extremely risky if an unauthorized entity were able to decipher the large amounts of data. Because of this, cryptanalysis is able to decrypt it with relatively little effort. A well-defined problem statement is crucial for guiding research, development, and initiatives related to cloud data security.

[3] Proposed Work

An IP filter has been implemented to prevent unauthorized packets from being sent between the server and the client in this case. The improved AES ENCRYPTION module is functional if the packet is genuine. Data transmission process flow has been suggested here. Data must be partitioned, encrypted, sent, decrypted, and then reintegrated across different cloud computing environments. The data port necessary be authenticated though in transportation. Presented below is a detailed outline of the procedure:

1. Data Splitting: Data that requires processing is partitioned into smaller pieces. File size and structure are two of many possible parameters that could inform the data splitting procedure.
2. Encryption at Cloud: Each data chunk is encrypted separately at both the cloud ends. You can use strong encryption algorithms like AES (Advanced Encryption Standard) for this purpose. Each encryption process requires a key, and these keys should be securely managed and shared between the cloud nodes. Ensure that the encryption keys are kept confidential and are not exposed to unauthorized access.
3. Data Transmission: The encrypted data chunks are transmitted from the cloud to the fog and vice versa through a secure network connection. Data transmission should occur over secure channels with proper authentication and data integrity checks.
4. Port Validation: Validate the data port or endpoint to ensure the data is sent and received through the correct communication channel. Implement access control measures to verify that the data transmission occurs over authorized ports.
5. Data Decryption at Receiver End: Upon receiving the encrypted data chunks, each fog node or the fog end decrypts the data chunks using the decryption keys. Simultaneously, the cloud also receives data from the fog and decrypts its respective data chunks using the same keys.
6. Data Reintegration: After decryption, the original data chunks are reassembled into the complete dataset. This may involve merging the data chunks into the correct order and structure.
7. Data Verification: Verify the integrity and authenticity of the data after reintegration to ensure that no unauthorized modifications occurred during transmission.
8. Data Processing: Once the data is fully integrated and verified, it can be processed as needed, whether for analytics, storage, or other applications.

9. Logging and Auditing: Implement thorough logging and auditing mechanisms to keep a record of data transmission activities, including access, encryption, decryption, and port validation.

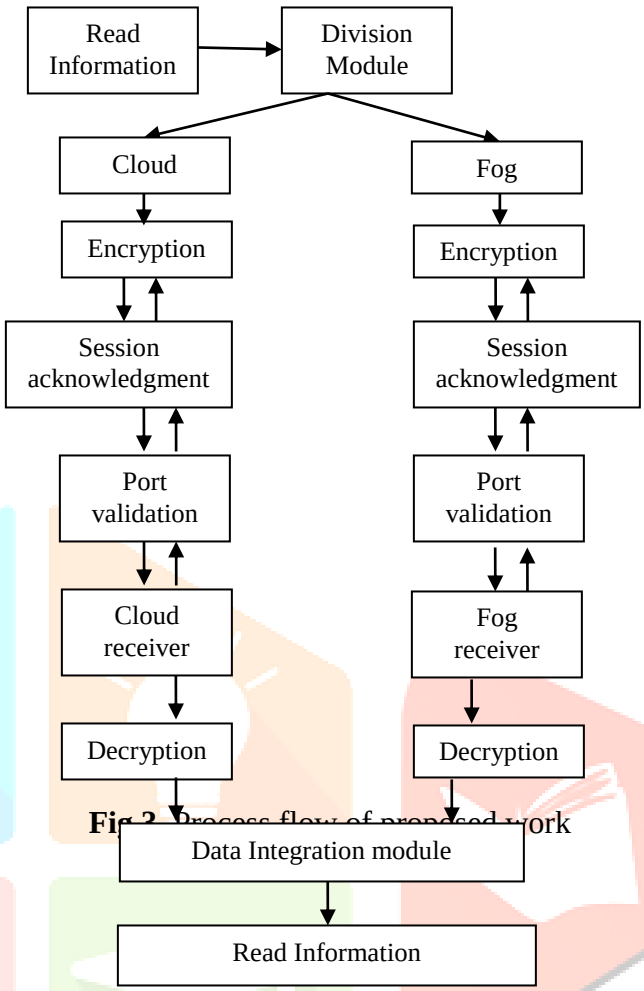


Fig 3 Process flow of proposed work

Data splitting, also known as data sharding or data partitioning, can enhance security in certain scenarios. The security benefits of data splitting primarily revolve around data segmentation and isolation. Here's how data splitting can increase security:

1. Isolation of Sensitive Data: By dividing a dataset into smaller, independent chunks, data splitting allows for the isolation of sensitive or confidential data from other portions of the dataset. This can help contain potential security breaches, limiting the exposure of sensitive information in case of a data breach.
2. Reduced Attack Surface: Splitting data can reduce the attack surface.
3. Rough Access Control: Data splitting facilitates rough access control. You can apply different access policies and permissions to each data shard, ensuring that only authorized users or systems can access specific data portions.
4. Data Redundancy and Backup: In some cases, data splitting can also be part of a data redundancy and backup strategy. When data is replicated and split across multiple locations, it enhances data availability and fault tolerance, contributing to security by ensuring data resilience in case of hardware failures or disasters.

5. Enhanced Data Privacy: For privacy concerns, data splitting can be combined with encryption and anonymization techniques. This further secures sensitive information, making it harder for unauthorized parties to access or identify individuals in the data.

However, it's important to note that while data splitting can enhance security, it's not a one-size-fits-all solution. The effectiveness of data splitting depends on various factors, including the specific use case, the implementation of access controls, and the security measures applied to each data shard. Moreover, data splitting can also introduce complexity and challenges related to data management, especially in terms of data reintegration and ensuring that all components of the dataset remain synchronized. When considering data splitting for security, it's important to carefully design and implement the solution to ensure it aligns with your security goals and doesn't inadvertently introduce new vulnerabilities. The FILE splitter would separate the data into two separate data files, the first of which would be placed on the cloud, while the second would be placed on the fog. A separate location is assigned to the file for the cloud, and another is assigned to the file for the fog. Because of this, the transmission is more reliable and safe to use. An interface for sending files to a server is used. Here you may provide your user ID, password, port number, IP address, and the path of the file that has to be transmitted along with the security token and AES code. In this case, the data would be sent to the server using the GUI for Server. Please input the port number, AES code, and file location to be received below with the security token.

[4] Result and Discussion

It has been mentioned here how the planned work will be implemented and the results it will provide. Using the FILE splitter, the data would be divided into two distinct files: a cloud file and a fog file. The file's name and security code are given, and the file is divided and distributed to two different locations: one for cloud and another for fog, depending on the situation. As a result, communication is more protected and reliable. This is an interface to transfer the file and send the data to server. This is the file transmitter interface, and it's used to send data to the server from a computer. During transmission, both the file path and the security token are taken into account. The sender would send the following file to the receiver. It's possible that it's a text file saved in notepad. The following file would be sent to the recipient's computer. There would be no changes to the file's content since it came from the sender. The file's content was shown here while it was being sent. It's encoded text that can't be decoded. There is no approach somebody could realize it if it were embezzled from him.

Transmission from cloud to end user would be made possible using the transmitter module. There would be no difference between the sender and recipient in terms of port. The IP address of the end user will be shown here. The figure below shows how a cloud-based data transmitter module is designed. Three input boxes are available. Port numbers, IP addresses, and authentication codes are all sent to separate input boxes. The end user section is fragmented into three subdivisions.

1. **Ready to receive from fog:** This factor agrees data to be grouped from the fog side by initial the fog port. Both sides of the port should be able to access it. Data sent from the fog side would be able to be decrypted thanks to the same authentication code.
2. **Ready to accept data from the cloud:** This step allows data collection and transmission from the cloud side by opening the cloud port. Both sides of the port should be able to access it. So that data sent from the cloud may be decrypted, the authentication code would be the same on both ends.
3. **Merge and Decode:** Authentication code is used to combine and decode incoming data at this phase.

Table 1 Comparison of Tradition work and proposed work

Comparison Factors	Traditional Approach	Proposed Work
Integration to fog	They don't make of fog	We make use of fog concept
Security Level	Less security	More secure as splitting the data for transmission
Reliabilty	Less	More
Security layer	They considered application layer only	We considering multiple layer security
Packet dropping	More probability	Less probability
Congestion	More	Fewer chance
Transmission path	Single path	Multiple paths
Port	Predefine	User defined

The end-user module has been divided into three individual segments.

1. You are now ready to accept data from the fog. This step opens the port for the fog and enables data capture that is sent from the fog side. It is necessary for the port to be shared by both parties. The data that has been transmitted from the fog side may have its encryption deciphered if the same common authentication code were used.
2. Prepared to accept data from the Cloud: This part opens the port for the cloud and enables data capture and transmission from the cloud side. It is necessary for the port to be shared by both parties. The data that was delivered from the cloud side may then have its encryption decoded since the same common authentication code would be used.
3. Merge and Decode: This part of the process would combine the data that was received and then decode it based on the authentication code.

Table 2 Comparative Analysis of Packet Dropping

Packets	Traditional	Proposed
100	5	3
200	9	3
300	10	6
400	12	7
500	14	7
600	18	8
700	30	11
800	37	18

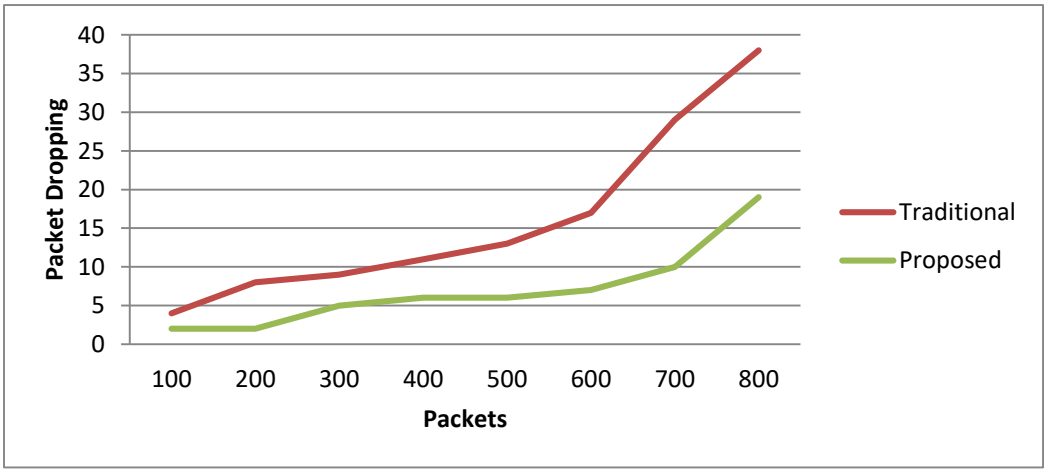


Fig 4

Comparative analysis of packet dropping

Table 3 Comparative Analysis of Accuracy

Packets	Traditional	Proposed
100	90.84%	94.06%
200	90.86%	94.16%
300	90.93%	94.24%
400	90.97%	94.27%
500	91.00%	94.35%
600	91.07%	94.37%
700	91.16%	94.38%
800	91.24%	94.44%

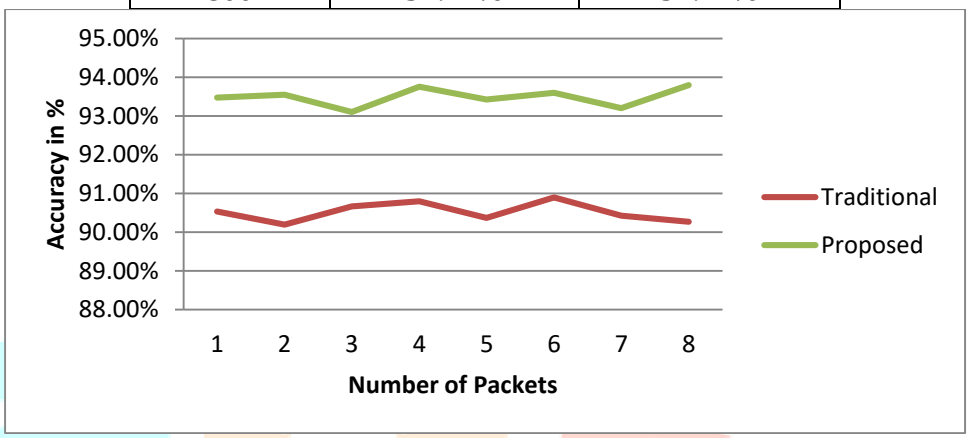


Fig 5 Comparative analysis of Accuracy

[5] Conclusion

Cloud computing and other associated computing paradigms have contributed to acceleration in the rate at which digital transformations are making headway. This technology is beneficial to a wide range of fields and institutions, including academic institutions, healthcare systems, academic institutions, manufacturing facilities, and even governments. Researchers have proposed a variety of distinct computer paradigms during the course of their work. This article proposals a summarizing overview to two of the most contemporary and exciting inventions in the realm of computing: cloud computing. In any case, in addition to that, we have included a concise summary of cloud computing, edge computing, dew computing, and mobile cloud computing and mobile edge computing. When observed from the perception of a inclusive variety of use cases, fog-assisted cloud computing provides a more vigorous platform and a more practical computing solution. One of the greatest imperative distinctions between brink computing and fog computing is the place of the network nodes. Because of this, there has to be a significant amount of research carried out in this field. In this study, some of the challenges and complications related with cloud computing that makes use of fog are explored. The purpose of this essay is, we hope, to shed some light on the nature of computing by providing information that readers will find helpful.

To protect data at the application layer from both active and passive types of attack, a more secure approach has been devised thanks to the suggested implementation, which was described before. Proportional research has been done amongst the proposed approach and the dominant security hypothesis. It has been demonstrated that there is a significantly reduced risk of packet loss when using the proposed approach as opposed to the one that is currently in use. It has been determined that traditional security measures are insufficient. The suggested system makes use of an advanced cryptographic procedure that partitions and encrypts data in order to ensure the confidentiality of user information. Because of the way that this system is set up, there is less of a possibility that any packets will be lost or backed up. In this study, we analyse both active and passive assaults as a means of providing many layers of protection for the network. The proposed method offers improved security for packets by severing them into a greater number of more manageable parts. The inadequacies of these more traditional approaches to security call for the implementation of a contemporary security system.

[6] Future Scope

Data security was only present at the application layer when the process was executed in the conventional manner. There is a provision for the packet's own security in the planned work, and it may be found here. Existing security measures were inadequate, thus it was necessary to develop a whole new system of protection. There was no other choice. A significant decrease in the likelihood of unauthenticated decryption results from this. Protecting yourself against an attacker originating from a different network requires immediate action. With the help of the suggested work, a dependable method of data transfer was created, and the data was divided into many parts to fit this. This approach ensures that the security system can withstand any assaults that crackers or hackers may launch.As the data landscape continues to grow, cloud data security is poised to adapt and tackle new threats and possibilities.

REFERENCES

1. AbdElminaam, D.S., 2018. Improving the security of cloud computing by building new hybrid cryptography algorithms. *International Journal of Electronics and Information Engineering*, *8*(1), pp.40-48.
2. Aikat, J., Akella, A., Chase, J.S., Juels, A., Reiter, M.K., Ristenpart, T., Sekar, V. and Swift, M., 2017. Rethinking security in the era of cloud computing. *IEEE Security & Privacy*, *15*(3), pp.60-69.
3. Al Nasseri, H.M.K. and Duncan, I.M.M., 2016. Investigation of Virtual Network Isolation security in Cloud computing: data leakage issues.
4. Aluyalu, R., Maheshwari, V.U. and Chennam, K.K., 2021. Data Security in Cloud Computing Using Abe-Based Access Control. *Architectural Wireless Networks Solutions and Security Issues*. Springer.
5. Basu, S., Bardhan, A., Gupta, K., Saha, P., Pal, M., Bose, M., Basu, K., Chaudhury, S. and Sarkar, P., 2018, January. Cloud computing security challenges & solutions-A survey. In *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 347-356). IEEE.
6. Bhushan, K. and Gupta, B.B., 2017. Security challenges in cloud computing: state-of-art. *International Journal of Big Data Intelligence*, *4*(2), pp.81-107.
7. Cao, Z., Liu, L. and Li, Y., 2018. Ruminations on fully homomorphic encryption in client-server computing scenario. *International Journal of Electronics and Information Engineering*, *8*(1), pp.32-39.
8. Chen, D. and Zhao, H., 2012, March. Data security and privacy protection issues in cloud computing. In *2012 International Conference on Computer Science and Electronics Engineering* (Vol. 1, pp. 647-651). IEEE.
9. Chinnasamy, P., Padmavathi, S., Swathy, R. and Rakesh, S., 2021. Efficient Data Security Using Hybrid Cryptography on Cloud Computing. Inventive Communication and Computational Technologies. Springer.
10. Coppolino, L., D'Antonio, S., Mazzeo, G. and Romano, L., 2017. Cloud security: Emerging threats and current solutions. *Computers & Electrical Engineering*, *59*, pp.126-140.
11. Cook, A., Robinson, M., Ferrag, M.A., Maglaras, L.A., He, Y., Jones, K. and Janicke, H., 2018. Internet of cloud: Security and privacy issues. In *Cloud Computing for Optimization: Foundations, Applications, and Challenges* (pp. 271-301). Springer, Cham.
12. Dave, D., Meruliya, N., Gajjar, T.D., Ghoda, G.T., Parekh, D.H. and Sridaran, R., 2018. Cloud security issues and challenges. In *Big Data Analytics* (pp. 499-514). Springer, Singapore.
13. Dey, H., Islam, R. and Arif, H., 2019, January. An integrated model to make cloud authentication and multi-tenancy more secure. In *2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)* (pp. 502-506). IEEE.
14. Elsayed, M. and Zulkernine, M., 2019. Offering security diagnosis as a service for cloud SaaS applications. *Journal of information security and applications*, *44*, pp.32-48.
15. Islam, T., Manivannan, D. and Zeadally, S., 2016. A classification and characterization of security threats in cloud computing. *Int. J. Next-Gener. Comput*, *7*(1), pp.268-285.
16. Joshi, B., Joshi, B. and Rani, K., 2017. Mitigating data segregation and privacy issues in cloud computing. In *Proceedings of International Conference on Communication and Networks* (pp. 175-182). Springer, Singapore.

17. JKRSastry, M.T., 2019. Securing SAAS service under cloud computing-based multi-tenancy systems. *Indonesian Journal of Electrical Engineering and Computer Science*, *13*(1), pp.65-71.
18. Ke, C., Huang, Z., Xiao, F. and Liu, L., 2017. Privacy Data Decomposition and Discretization Method for SaaS Services. *Mathematical Problems in Engineering*, *2017*.
19. Krutz, R.L. and Vines, R.D., 2010. *Cloud security: A comprehensive guide to secure cloud computing*. Wiley Publishing.
20. Kumar, P.R., Raj, P.H. and Jelciana, P., 2018. Exploring data security issues and solutions in cloud computing. *Procedia Computer Science*, *125*, pp.691-697.
21. Kumar, R. and Goyal, R., 2019. On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review*, *33*, pp.1-48.
22. Li, P., Li, J., Huang, Z., Gao, C.Z., Chen, W.B. and Chen, K., 2018. Privacy-preserving outsourced classification in cloud computing. *Cluster Computing*, *21*(1), pp.277-286.
23. Liu, S., Yue, K., Yang, H., Liu, L., Duan, X. and Guo, T., 2018, May. The Research on SaaS Model Based on Cloud Computing. In *2018 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)* (pp. 1959-1962). IEEE.
24. Mishra, N., Sharma, T.K., Sharma, V. and Vimal, V., 2018. Secure framework for data security in cloud computing. In *Soft Computing: Theories and Applications* (pp. 61-71). Springer, Singapore.
25. Masala, G.L., Ruiu, P. and Grosso, E., 2018. Biometric authentication and data security in cloud computing. In *Computer and network security essentials* (pp. 337-353). Springer, Cham.