Securing a Cloud Environment by Adopting Novel Cryptographic Techniques

Dr K Madan Mohan,
Associate Professor,
Department of CSE(AI&ML),
Malla Reddy College of Engineering,
madan.keturu@gmail.com

Abstract. Built-in cloud computing, which cloud customers may make use of to percentage statistics, is a whole and functional technique. Cloud Service Providers (CSPs) may also transmit server offerings to cloud buyers via powerful information facilities. The authentication of cloud customers protects information, and CSPs might also have outsourced records record- sharing safety ensures. The constant shift in cloud users, mainly unauthenticated users or 1/3 events, affords a sizable trouble in maintaining statistics privacy. The multipurpose sharing of data even as safeguarding facts and private safety from unwanted or other 1/3-party users remains hard. Cloud computing has emerged as the next renewable technology in the field of data generation. While many cloud safety evaluations are actually available, there may be still a large discrepancy among the best mapping of problems and their associated remedies. Cloud information storage is brief, but the records we shop have to be secure, and cloud carrier companies or cloud caregivers should keep the data stored inside the cloud. The information proprietor is worried approximately the integrity and dependability of records saved within the cloud. In this text, a thorough comparative analysis of numerous schemes and "cryptography algorithms" used to cozy statistics thru the public cloud will be executed, and a clear overview of diverse strategies and their obstacles might be given in tabular style.

Keywords: Cloud Computing Security, Data Security, PKCS, Data Sharing, Cryptographic algorithms, NIST.

1. Introduction

The scenario underscores the rapid growth of cloud-based wireless networks and sensor community systems, which offer enhanced software capabilities, on-demand data access, and server services. Both individuals and organizations extensively utilize cloud storage services, enabling remote access to a wide array of shared applications and services under the cloud computing paradigm. Conversely, personal computers have inherent limitations in storage capacity, while the cloud provides scalable solutions, facilitating outsourcing of sensitive data such as health records, personal photos, videos, etc. However, ensuring the security of cloud-stored data against privacy breaches remains a critical challenge for social network applications. Consequently, safeguarding cloud storage data becomes imperative for owners, necessitating solutions like encrypted data interchange [12], secure search functionalities for encrypted data, and data audits for outsourced information [4]. This study aims to analyze and address the data privacy and security concerns faced by users in cloud storage environments. It also investigates encryption methodologies, evaluates performance metrics, and compares features and computational complexities among existing schemes relevant to dynamic group data sharing. The research methodology explores strategies for enhancing data security in outsourced cloud environments.

1.1 Data Sharing in Dynamic Groups

Data sharing has become increasingly significant across various sectors including real-world organizations, governments, and corporations [2]. Groups of data owners (users) authorized as a network must be acknowledged, with memberships governed by dynamic rules that accommodate individuals joining and leaving the group based on specific user attributes [3]. Cloud infrastructure embodies a distributed setup comprising virtual machines dynamically allocated to meet client-specific resource demands. Service Level Agreements (SLAs) delineate the parameters governing this collaboration between cloud providers and consumers [1]. Defined by the National Institute of Standards and Technology (NIST), cloud computing offers ubiquitous network access to configurable computing resources (e.g., servers, storage, applications) that can be rapidly provisioned and released with minimal management effort or service provider intervention [2]. The evolving cloud technology landscape delivers a spectrum of services to consumers at competitive costs, albeit with paramount attention to cloud data security and computer integrity. This involves applying principles such as confidentiality, authentication, data integrity, non-repudiation, intrusion detection, and operational efficiency [3].

1.2 Cryptographic Methods for Securing Cloud Storage

The security of public cloud storage relies extensively on cryptographic techniques.

Three primary approaches are employed:

1. Symmetric and asymmetric key encryption transforms plaintext into ciphertext.
2. Substitution methods alter plaintext characters with alternate characters, numbers, or symbols.
3. Transposition techniques protect data integrity via permutations of the actual document.

Confidentiality ensures that information is transmitted solely between the sender and intended recipient, preventing unauthorized access by third parties. Data integrity safeguards stored information from unauthorized alteration or corruption, ensuring consistency across cloud infrastructure. Availability guarantees that users have uninterrupted access to systems, applications, and data, safeguarding against denial-of-service attacks that aim to restrict access to network resources.

2. Cloud Computing

The term "Cloud" in cloud computing refers to a cloud service provider. Over the past three decades, significant advancements in computing and data technology have paved the way for the adoption of cloud computing [5]. Key developments include the construction of robust Internet backbones, widespread adoption of wireless Internet connectivity, the establishment of extensive server networks and data center storage, breakthroughs in high-performance and flexible computing technologies for data centers and the web, among others.

According to the International Data Corporation (IDC), sales from cloud computing products such as servers, public cloud storage, and private cloud grew by 8.1% year-on-year to $8.4 billion in the third quarter of 2016. The annual growth rate of public cloud is projected to be seven times that of total IT expenditure growth, reaching $53.1 billion by 2019 and globally
$203.4 billion. Major companies like Amazon, Google, Microsoft, and others are rapidly expanding their cloud computing platforms and infrastructure to cater to a large number of users. The success of these companies has spurred many others, including Media Temple, Mosso, Joyent, and others, to enter the cloud computing market.

Cloud computing utilizes three service models: SaaS, PaaS, and IaaS, providing users with infrastructure, platforms, applications, and software as services. SaaS allows users to run applications on cloud provider infrastructure, accessible via web browsers. PaaS service models enable customers to rent existing applications or develop and test new ones using provided hardware, operating systems, storage, and networking capabilities. IaaS provides clients with access to storage, networking, and other computing resources, allowing them to manage arbitrary applications.

3. Cloud Service Models

Cloud service providers utilize three primary models to deliver their services: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

3.1 Software as a Service (SaaS)

Also referred to as Application Cloud or Service Cloud, SaaS is a software-as-a-service paradigm where software is provided as a service to multiple cloud users over the Internet. Users access the software through a web browser on various client devices.

3.2 Platform as a Service (PaaS)

PaaS is a virtual platform that enables the development, deployment, and maintenance of applications using cloud-based architecture principles. It provides a web-based environment where cloud service providers manage underlying infrastructure including networks, servers, operating systems, and storage. Users are granted control over the application-hosting environment, including deployment software and configuration settings. PaaS offers enhanced security and accessibility compared to traditional IaaS methods, typically at a lower cost.

3.3 Infrastructure as a Service (IaaS)

IaaS delivers virtualized computing resources over the internet. It provides users with essential computing resources such as storage, servers, and networking components, allowing them significant control over their software development environment. Physical infrastructure is also a requirement in IaaS, although the provider manages the virtualization, storage, servers, and networking software components. Essentially, IaaS delivers infrastructure in the form of a service.

4. Literature Review

Recent reviews on secure cloud data sharing have emphasized essential requirements rather than sharing of group-based data in the cloud. The study of secure cloud data sharing is increasingly important with the rise of Cloud Computing and the growing need for data exchange. Analytical surveys and papers in this domain can be categorized into group key supervision, cumulative key searchable encryption, and group signature and proxy re-encryption. Group Key Supervision (GKS) primarily involves key creation, distribution, and revocation among group members. The Group Controller (GC) manages key operations, while the Key Server (KS) handles key storage and distribution (Menezes et al., 1996).

Menezes et al. describe Group Key Management (GKM) as a set of techniques for developing and managing shared key groups among group members, ensuring secure data exchange in cloud environments. Primary group management in cloud data exchange is categorized into GKS central protocols, decentralization, and distribution. A proposed GKS approach for cloud systems supports dynamic group data sharing, reducing memory usage for rekeying messages and eliminating communication overheads and storage burdens (Menezes et al., 1996).

Liu, Kumar, and others proposed a secure data sharing method based on the SE Key Aggregate Scheme, utilizing limited data storage smart cards for secure data storage and transmission. Their comprehensive security assessment validated its effectiveness in practical cloud data sharing scenarios (Liu et al., 2013).

Goyal et al. advocate Attribute-Based Encryption (ABE) for fine-grained access control in cloud storage, offering superior granularity compared to Access Control Lists (ACL). ABE associates data elements or users with specific attributes, granting access based on defined Access Management Policies (AMPs) (Goyal et al., 2006).

Yu et al. introduced a method combining Key-Policy Attribute-Based Encryption (KPABE) with Proxy Re-Encryption (PRE) for secure and scalable data access control in the cloud. Their approach meets fundamental security requirements and enhances user access rights protection (Yu et al., 2010).

Proxy Re-Encryption (PRE), proposed by Strauss and Sahai, enables secure data sharing by transforming data encrypted with a delegator's public key into a format that can be decrypted using a delegate's private key, without exposing sensitive data or private keys (Strauss & Sahai, 2002).

Qin et al. emphasize the importance of dependable, efficient, and secure data exchange in the cloud using Proxy Re-Encryption (PRE) techniques, particularly for handling large datasets with rapid encryption and decryption requirements (Qin et al.).

5. Cloud Development Models:

Cloud computing serves as a web network-based infrastructure, facilitating the shared computation of statistics and assets on demand for computer systems and numerous gadgets. It affords get entry to commonplace computing resources, inclusive of servers, garage, running structures, software program, and management, which can be immediately managed and accessed with reduced manage. Cloud garage and capability agreements empower IT groups and customers to shop and procedure their statistics from third-birthday celebration data facilities worldwide, counting on resource sharing to attain stability and financial scale. This is pushed through the improvement and adoption of modern technology and exemplary models, aiming to empower consumers to leverage most important advancements in cloud computing without the need for giant expertise.

In this phase, we discuss the critical features inside cloud frameworks deployed by way of Cloud Service Providers (CSPs). These capabilities encompass a comprehensive array of offerings handy over the internet. Virtualization plays a pivotal role in cloud deployment, allowing the creation of multi-tenant environments with several users or clients who may not engage or percentage every other's records. Cloud storage is maintained, controlled, and “sponsored up at far flung places”. It likely refers to being financially supported or backed in ventures or activities that take place in distant or remote locations, reachable over a network for clients to retrieve statistics. The hypervisor, a massive element for virtualization, enables the execution of a couple of Virtual Machines (VMs) on a unmarried hardware host, administering and handling various working systems walking on a shared physical machine. The National Institute of Standards and Technology (NIST) similarly categorizes cloud computing into 4 implementation models primarily based on the suitability and particular purpose of purchaser clouds.

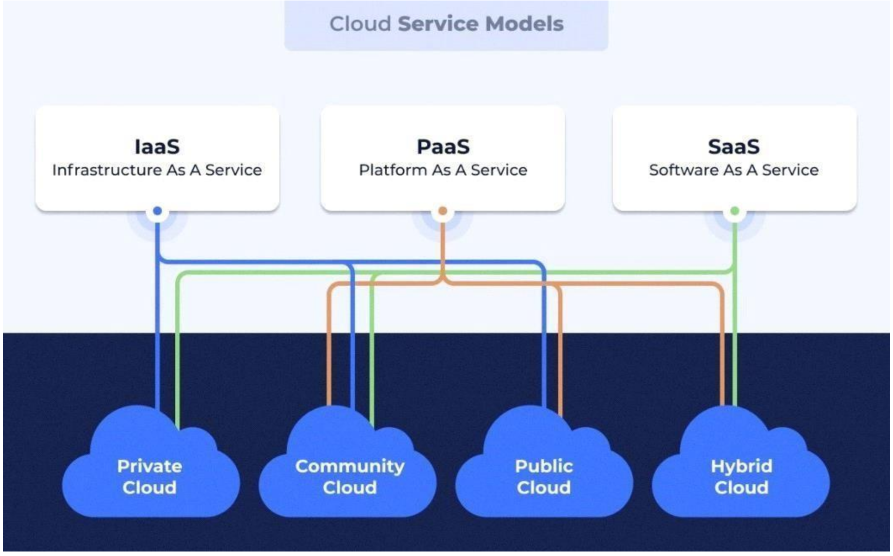

Figure-1: Various Cloud Development Models

5.1 Public Cloud:

Public cloud provides infrastructure available to the general public, owned, controlled, and operated by a business, educator, government organization, or combination thereof. It allows anyone to access computational resources.

Example: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP). These platforms offer a wide range of services accessible over the internet, including virtual machines, storage, and databases.

5.2 Private Cloud:

Private cloud is cloud computing implemented exclusively by a single organization or multiple users within that organization (e.g., distinct business units). Private clouds prioritize security and control.

Example: VMware's vSphere, IBM Cloud Private, OpenStack. These platforms enable organizations to build and manage their own cloud infrastructure tailored to their specific needs, ensuring greater control over data and compliance with security requirements.

5.3 Community Cloud:

Community cloud infrastructure is accessible only to a specific group of users who share common concerns such as security requirements, policies, or missions. It can be hosted on-premises or off-site.

Example: Government network clouds, where multiple government agencies share a common cloud infrastructure to collaborate on projects while adhering to strict security and compliance policies.

5.4 Hybrid Cloud:

Hybrid cloud is a cloud environment that integrates two or more distinct cloud networks (private, community, or public) using standardized or proprietary technology. It offers benefits of both public and private clouds, including scalability and cost- effectiveness, while addressing concerns like data security and integrity.

Example: A company using a private cloud for sensitive internal operations and a public cloud for less critical workloads or for scalability during peak periods. For instance, a financial institution might use a private cloud for secure transactions and a public cloud for customer-facing applications.

6. Security Issues

Cloud computing encounters two primary challenges: Security and Reliability. Due to the nature of cloud storage, where multiple clients' data coexist, security concerns arise as any client's data could potentially be accessed by unauthorized parties. This vulnerability opens doors for hackers to exploit, attempting to steal sensitive data, manipulate information, or disrupt services. To mitigate these risks, various security measures are employed in cloud environments, such as Encryption, Authorization, and Authentication.

Cloud security risks can be classified into those affecting cloud customers and those concerning cloud service providers. These risks include Data Leakage, Data Breaches, Hacking, Denial of Service (DoS) attacks, malicious insider threats, and shared technology vulnerabilities. Cloud service providers are responsible for implementing robust security measures to safeguard against such risks. Key security factors such as Authentication, Authorization, and Data Protection need to be addressed by providers to ensure the confidentiality, integrity, and availability of information.

The trustworthiness of a cloud service provider (CSP) and its services significantly influences a client's decision to migrate to a cloud platform or adhere to traditional frameworks. Establishing trust involves assessing whether the CSP assumes responsibility for various risks, including data protection, virtual machine (VM) security, and compliance with regulatory requirements. The Confidentiality, Integrity, and Availability (CIA) model serves as a foundational framework for evaluating cloud system security. This model ensures that security requirements align with the essential principles of safeguarding information in modern cloud infrastructures.

7. Confidentiality and Privacy

Protecting business belongings from unauthorized access involves ensuring confidentiality. In a cloud environment, unauthorized users may attempt to access data stored within the same database, posing a risk to both the cloud service provider (CSP) and its clients. Moreover, the CSP itself may employ unethical individuals who could potentially access or tamper with sensitive client records.

7.1 Confidentiality & Privacy Concerns in Cloud Computing Encompass Various Factors:

1. Many cloud storage services transmit content via internet folders containing customer information.
2. The geographic location where a customer's data is stored can also impact its security.

While cloud services are generally considered reliable, occasional anomalies occur. Providers may request detailed information about personal data files and user privilege data, raising concerns about data privacy. Consequently, business owners should devise robust access control protocols to mitigate potential breaches. These protocols are critical for protecting customer data and ensuring confidentiality in cloud environments.

8. Integrity in Cloud Computing

Integrity is a critical security property that ensures an asset remains unchanged by unauthorized individuals, thus maintaining its accuracy and correctness according to the owner's intentions. Any operations related to insertion, deletion, or modification are assumed to compromise the integrity of the asset. In the context of cloud computing, where customers access resources through internet browsers, numerous web attacks pose widespread threats to the integrity of records, databases, virtualized storage, and even WSDL files.

- **Several data security problems related to integrity within the public cloud are addressed below:**

8.1 Data Outsourcing

Outsourcing data to the cloud service provider (CSP) presents an immediate challenge to data integrity. The CSP may possess the capability to delete legitimate customer data tuples, which the client may not be able to recover.

8.2 Insecure API

Using insecure APIs sourced from obscure origins poses a significant threat. Attackers can exploit vulnerabilities in these APIs, potentially gaining unauthorized access using leaked API keys.

8.3 Collision Attack

A collision attack involves merging multiple copies of media or files to create a new, potentially compromised version. This technique encompasses various tasks, including data averaging, substitution, and linear data mixing, among others.

8.4 Wrapping Attack

A wrapping attack is a common network attack, particularly prevalent in cloud systems. During SOAP translation in the Transport Layer Service (TLS) layer, attackers may duplicate text and signatures, presenting them to the server as genuine user inputs.

Addressing these integrity-related concerns is paramount for ensuring the security and trustworthiness of data stored and processed within the public cloud environment. Implementing robust security measures and protocols is crucial to mitigate the risks posed by potential attacks and breaches.

9. Availability

Availability is one of the most crucial elements that a Cloud Service Provider (CSP) must maintain. Numerous businesses rely upon cloud-based technology to serve their clients, and ensuring uninterrupted availability of these services is paramount. Even minor downtime can result in significant, irrecoverable financial losses.

A standard Service Level Agreement (SLA) outlines the commitments made by the provider concerning service availability and responsiveness to demand. For instance, the SLA may specify that the service will be operational 99.99% of the time and that additional resources can be dynamically allocated if utilization exceeds 80% of the capacity provided. This ensures that the services remain accessible and responsive to customer needs, thereby maintaining client satisfaction and trust in the cloud service provider.

9.1 Comparison of Cryptographic Methods

Table 1 compares various cryptographic methods for protecting cloud data based on several analytical criteria. The factors under examination include key size, block size, round number, runtime, key utilization, and memory consumption. Both the advantages and drawbacks are also noted.

Advanced Encryption Algorithms (AEAs) are essential for safeguarding personal digital information, cybersecurity, and government computer privacy. In response to this need, the US government developed and implemented the Advanced Encryption Standard (AES). Unlike AES with a block size of 128 bits, the small block size of Blowfish (64 bits) renders it more vulnerable to birthday attacks.

AES has been extensively tested on a variety of file types, including pictures, audio, video, text, documents, and portable document format (PDF), and has consistently yielded stable results.

Each encryption algorithm mentioned possesses its own strengths and weaknesses. The evaluation of different encryption algorithms' effectiveness is based on selected parameters, including encryption time, decryption time, avalanche effect, and memory consumption.

10. Comparative Analysis Of Cryptographical Security Algorithms

TABLE 1: Comparison between various cryptographic Algorithm

Algorithm	**AES**	**RSA**	**Blowfish**	**IDEA**	**DES**
Key used	Encryption and Decryption same key used.	Two keys, one for encryption and one for decryption, were	Encryption and Decryption same key used.	Encryption and Decryption same key used.	Encryption and Decryption same key used.
Execution Time	Rapid	Slowest	Fast	Slow	Same as AES
Data encryption Capacity	Large quantity of data	Tiny data	Lower than AES	Tiny data	Less than AES
Security	Strong	Considered to be safe	Considered secure	Inarticulate	Inarticulate
Key size	128,192 or 256 bits	>than 024 Bits	32-448bits	128 bits	56 bits out of 64 bits
Block size	128,192 or 256bits	Irregularity	64bits	64bits	64bits
Rounds	10, 12 or 14 depending on key size	1	16	8.5	16
Encryption Type	Symmetric	Asymmetric	Symmetric	Symmetric	Symmetric
Benefits	Most reliable, less memory, more powerful key size, good speed and time	Probably easier to share your public key.	Less memory, good speed,	Comp lex round s, large key size	Low encryption time, good power consumption and it was throughput.
Drawbacks/ Limitations	Brute force attack, the implementation of the software is complicated.	Challenged by man-in- the-middle attack.	Throughput, key management	There have been so many activities.	Initial and final permutation not clear

10.1 Key Exchange and Public Key Infrastructure (PKI):

- **Key Exchange:** Assess the suitability of algorithms for securely exchanging cryptographic keys.
- **PKI Compatibility:** Ensure algorithms integrate seamlessly with PKI systems for secure communication.

10.2 AES Alternatives: Serpent

Type: Symmetric key block cipher.

Security and Simplicity: Highly secure, straightforward design. Structure: Substitution-permutation network (SPN). Key Sizes: 128, 192, 256 bits. Block Size: 128 bits.

Rounds: 32 (128-bit key), 48 (192-bit key), 64 (256-bit key).

10.3 RSAAlternatives: Elliptic Curve Cryptography (ECC)

Type: Public key cryptography.

Mathematics: Based on elliptic curves. Key Sizes: 256-bit, 384-bit, 521-bit.
Efficiency: Strong security with shorter keys, ideal for constrained environments.

Public Key Cryptography: Widely used for secure key exchange and digital signatures.

10.4 Blowfish Alternatives: Twofish Type: Symmetric key block cipher. Developer: Bruce Schneier.
Security and Efficiency: High. Structure: Feistel network.
Key Sizes: 128, 192, 256 bits. Block Size: 128 bits.
Rounds: 16 for all key sizes.

Key Expansion: Uses key-dependent S-box.

10.5 IDEAAlternatives: RC6

Type: Symmetric key block cipher.

Designer: RSA Security.

AES Finalist: Flexible and high performance. Key Sizes: 128, 192, 256 bits.
Block Size: 128 bits.

Rounds: Typically 20 for all key sizes.

Word Size: Operates on variable word sizes based on key size.

10.6 DES Alternatives: Triple DES (3DES) and AES

- **3DES:**

Type: Symmetric key block cipher. Enhancement: Improved DES.
Key Options: 56-bit, 112-bit, 168-bit (effective sizes: 168, 336, 504 bits). Block Size: 64 bits.
Operation: Applies DES three times with different keys.

AES:

Type: Symmetric key block cipher. Standard: Replaces DES.
Structure: Substitution-permutation network (SPN). Key Sizes: 128, 192, 256 bits.
Block Size: 128 bits.

Security and Efficiency: Enhanced compared to DES.

10.7 Camellia Algorithm

Type: Symmetric key block cipher. Block Size: 128 bits.
Key Sizes: 128, 192, 256 bits.

Strength Factors: Secure and robust design for various encryption needs.

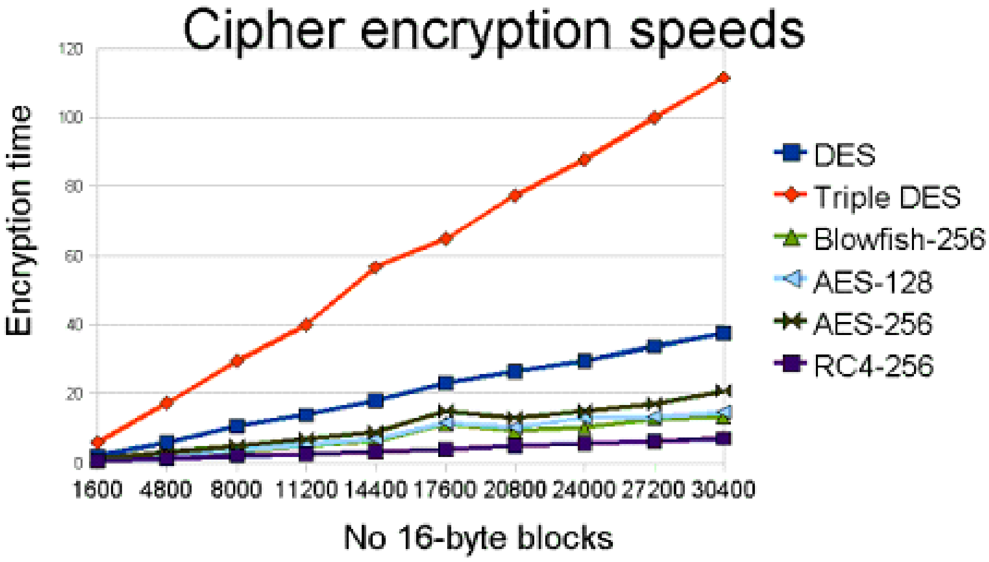

FIGURE 2: Encryption time Versus Plaintext of multiple symmetric encoding algorithms

Figure 2 illustrates the overall encryption times for various algorithms. Additionally, it is noted that RSA requires the largest amount of memory, while Blowfish consumes the least for device usage. Table 2 presents the memory usage for the specified algorithms' processing units.

TABLE 2: Memory consumed units' operation

Algorithm	**Memory consumed (KB)**
DES	18.4
3DES	20.5
AES	14.7
Blowfish	9.40
RSA	30.50

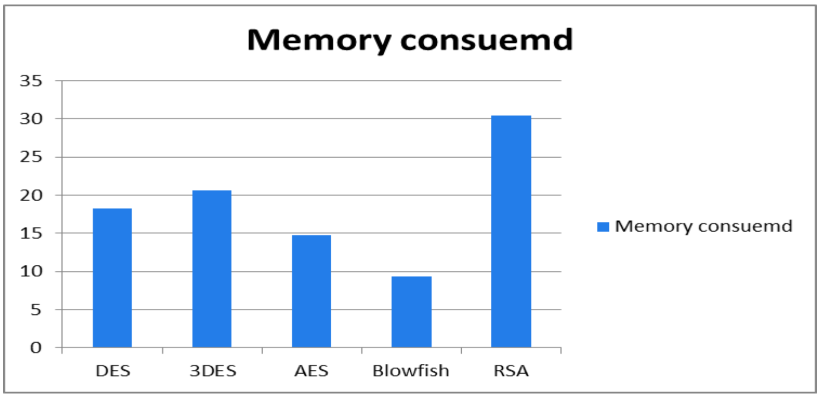

FIGURE 3: Memory consumed by cryptographic algorithm

10.8 Avalanche Effect in Cryptography

The avalanche effect in cryptography is a desired property of encryption algorithms. It means that a small change in the plaintext (like changing a single character) should result in a significantly different ciphertext. This helps ensure that the encryption is secure because it makes it harder for someone to predict how changes in the input affect the output.

10.8.1 Measuring the Avalanche Effect

To measure the avalanche effect, we use something called the Hamming distance. This involves comparing the binary representations (0s and 1s) of the plaintext and the ciphertext.

10.8.2 Steps to Measure the Avalanche Effect

10.8.2.1 Convert to ASCII: First, convert each character of the plaintext and ciphertext to their ASCII values. ASCII is a standard way to represent characters as numbers.

10.8.2.2 Convert to Binary: Convert these ASCII values into binary form.

10.8.2.3 Calculate Hamming Distance: Compare the binary values of the plaintext and the ciphertext using the XOR operation. The XOR operation compares two bits and returns 1 if they are different, and 0 if they are the same.

10.8.2.4 Count the 1s: The result of the XOR operation will be a binary number. Count the number of 1s in this binary number. This count is the Hamming distance.

10.8.2.5 Calculate Avalanche Effect: Divide the Hamming distance by the length of the document (number of characters) to get the avalanche effect.

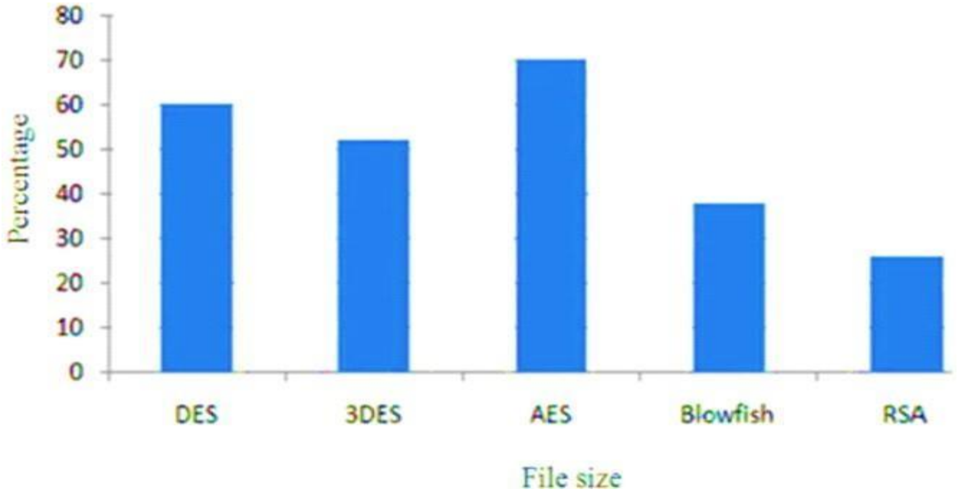

FIGURE 4: AES has highest Avalanche effect whereas RSA shows least Avalanche effect

11. Conclusion

Cloud computing has accelerated advancements in security technologies and significantly increased the use of internet services. Stable data sharing is a critical concern in cloud-based communities. The main areas of concern are data security, traceability, access control, and account cancellation. Utilizing cloud infrastructure to decrease costs and improve service efficiency for end-users is very beneficial to e-commerce applications and social networking sites. However, many variables influence net profit, such as the geographical dispersion of member locations, the available internet structure in these geographical zones, the changing presence of usage patterns, and the adaptation or reconfiguration of cloud services. Cloud computing has emerged as an important field of study. The cloud provides many benefits to consumers by offering services such as pay-per-use, cost-effective services, and rapid internet connection. The cloud has enormous potential, but many consumers are still hesitant to embrace it due to obvious issues that have yet to be resolved. While many solutions have been proposed, none have addressed all the issues.

Several researchers have highlighted various security issues and concerns, such as data leakage, data loss, unsecured API, collusion attack, wrapping assaults, unclear risk profile, and many more, as significant barriers to consumers adopting cloud data security. Another major issue is trust, as service providers are often hacked, leaking critical data via hostile agents, causing them to lose their reputation. Cryptography techniques are used to ensure the secrecy and integrity of data. Several systems and encryption techniques are utilized to protect privacy and user data from internal and external threats. This article covers a range of public cloud security issues and describes the encryption methods and strategies employed by various authors in a tabular format.

According to the comparison study, symmetric algorithms are more powerful and trustworthy. Table 3 shows that the AES and Blowfish algorithms require less encoding time and memory usage than other methods. Future improvements to public cloud security will be pursued. Protecting data on untrustworthy cloud services is difficult, and effective encryption methods are essential. Future suggestions include combining additional security techniques with cryptography. Future studies will also explore more efficient methods to handle data security and cloud privacy concerns. Integrating current data access control methods into this research could yield a helpful real-world framework. New cryptographic solutions are anticipated to achieve a balance between security and usability to reduce computing complexity. Another possibility is to enhance data operation flexibility by integrating the proposed method with other cryptographic primitives, such as homomorphic encryption, to enable calculations without decrypting encrypted data.

12. References:

1. Buyya, R., Yeo, C., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25(6), 599-616.

2. Mell, P., & Grance, T. (2009). The NIST definition of cloud computing. National Institute of Standards and Technology, Tech. Rep.

3. Thakkar, B. (2020). A Survey for Comparative Analysis of various Cryptographic Algorithms used to Secure Data on Cloud. International Journal of Engineering Research and, 9(08).

4. Popli, M., & Deep, G. (2018). A Critical Analysis on Cloud Security. International Conference on Innovations in Computing (ICIC 2018), 19-23.

5. Kim, W. (2009). Cloud Computing: Today and Tomorrow. The Journal of Object Technology, 8(1), 65.

6. Voorsluys, W., Broberg, J., & Buyya, R. (2011). Introduction to Cloud Computing. In Cloud Computing: Principles and Paradigms (pp. 1-44). New York, USA: Wiley Press.

7. More, S., & Chaudhari, S. (2016). Third Party Public Auditing Scheme for Cloud Storage. Procedia Computer Science, 79, 69-76.

8. Meenakshi, I.K., & George, S. (2014). Cloud server storage security using TPA. International Journal of Advanced Research in Computer Science & Technology (IJARCST).

9. Dave, D., Meruliya, N., Gajjar, T.D., Ghoda, G.T., Parekh, D.H., & Sridaran, R. (2018). Cloud security issues and challenges. In Big Data Analytics (pp. 499-514). Springer, Singapore.

10. Patel, K. (2019). Performance analysis of AES, DES and Blowfish cryptographic algorithms on small and large data files. International Journal of Information Technology, 11(4), 813-819.

11. Advani, N., Rathod, C., & Gonsai, A.M. (2019). Comparative study of various cryptographic algorithms used for text, image, and video. In Emerging Trends in Expert Applications and Security (pp. 393-399). Springer, Singapore.

12. Ali, M., Dhamotharan, R., Khan, E., Khan, S., Vasilakos, A., Li, K., & Zomaya, A. (2017). SeDaSC: Secure Data Sharing in Clouds. IEEE Systems Journal, 11(2), 395-404.

13. Journal of E-Governance. (2011). Guidelines on Security and Privacy in Public Cloud Computing. Journal of E- Governance, 34(3), 149-151.

14. Berger, S., Cáceres, R., Pendarakis, D., Sailer, R., Valdez, E., Perez, R., Schildhauer, W., & Srinivasan, D. (2008). TVDc. ACM SIGOPS Operating Systems Review, 42(1), 40-47.

15. Ashokkumar, S., Karuppasamy, K., Srinivasan, B., & Balasubramanian, V. (2010). Parallel Key Encryption for

CBC and Interleaved CBC. International Journal of Computer Applications, 2(1), 21-25.

16. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Group key management for secure multicast communication: An overview. Network Protocols.

17. Liu, X., Kumar, P., Zhang, J., & Others. (2013). Secure data sharing in cloud computing using revocable-storage identity-based encryption. IEEE Transactions on Cloud Computing, 6(4), 750-762.

18. Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06) (pp. 89-98).

19. Yu, S., Wang, C., Ren, K., & Lou, W. (2010). Achieving secure, scalable, and fine-grained data access control in cloud computing. In Proceedings of the 29th IEEE International Conference on Computer Communications (INFOCOM '10) (pp. 1-9).

20. Strauss, M. J., & Sahai, A. (2002). Proxy re-encryption. In Proceedings of the 8th ACM Conference on Computer and Communications Security (CCS '02) (pp. 16-25).

21. Qin, J., Wang, Y., & Li, X. (Year). Title of the paper. In Proceedings of the conference name, page numbers.