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

Automated Data Security Model Using Cryptography Techniques in Cloud Environment

[1]Mada Prasad, [2]M. Jagadeeshwar, [3]Dr. D. Shanthi

Submitted: 28/01/2024 **Revised**: 06/03/2024 **Accepted**: 14/03/2024

Abstract Cloud computing, a highly debated research frontier, offers the dual advantage of cost reduction and enhanced scalability and flexibility in computing services. Its widespread adoption spans diverse sectors such as the military, healthcare, industry, and education, facilitating the storage of vast datasets. Users can access shared resources, including software and information, at their convenience from any location. However, the security of cloud-stored data, categorized as private, public, or sensitive, poses challenges, especially when entrusting third-party providers with confidential information. Acknowledging that security is a joint responsibility of both enterprises and customers, even industry giants stress the need for a collaborative approach. Encrypting information stored in the cloud becomes imperative from the client's standpoint to prevent unauthorized access. Numerous challenges arise in cloud data storage, necessitating innovative solutions, and various algorithms have been developed to address these issues. This study employs cryptographic techniques to address security concerns, with a focus on the Asymmetric Key Cryptography with Related Key Set (AKC-RKS) technique. The paper introduces novel safety mechanisms using the AKC-RKS technique, comparing the proposed model with traditional encryption methods. The results demonstrate a high level of data security in the proposed model, showcasing the efficacy of cryptographic techniques in fortifying data security within cloud environments.

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

1. Introduction

The current focus of research centers around the security aspects of cloud computing. As traditional data storage gives way to cloud-based alternatives, users gain the ability to access their data from any location at any time [1]. However, data security remains a significant hurdle hindering the widespread adoption of cloud computing in enterprises. This research proposes a multi-level cryptography-based approach to enhance security in cloud computing [2].The proposed algorithm leverages asymmetric key cryptography for data encryption and decryption within cloud environments [3]. A key feature of this security model is its emphasis on fostering awareness between cloud users and service providers, aiming to mitigate security risks [4]. The model's design prioritizes maximizing data security to its fullest extent. Cloud computing represents a recent trend in the computing landscape, reshaping traditional paradigms. Technological advancements have led to increased internet usage and augmented costs associated with hardware and software [5]. The pay-per-utilization model in cloud computing allows clients to pay for the resources and services they consume, contributing to its popularity due to its convenience and cost-effectiveness [6]. The Cloud offers users a range of resources, including networks, servers, and storage, presenting services such as webmail, online business applications, social media platforms, and internet file storage [7]. With a simple internet connection, users can access these resources and support functions. One of the primary advantages of Cloud Computing lies in its abstraction, eliminating the need for customers to possess expertise in managing the infrastructure. Technologies like Virtualization, Utility Computing, Service-Oriented Computing, Multi-tenant environments, and Load Balancing contribute to the success of Cloud Computing [8]. Despite its numerous advantages, Cloud Computing faces obstacles to widespread adoption. The transfer of users' and businesses' data to a publicly accessible website raises concerns as it involves relinquishing control to a third party, potentially making it vulnerable to unauthorized access. In cloud services, information is dispersed across various resources, leaving clients with minimal control. A critical concern in cloud computing revolves around safeguarding customer data and securely delegating tasks to external cloud service providers [9]. Security issues arise from the fact that cloud service providers transmit information over the Internet, creating opportunities for adversaries to compromise it. To address these concerns, appropriate security measures must be implemented within the cloud environment. Key sharing, specific

[1]*Research Scholar, Department of Computer Science, Chaitanya Deemed to Be University, Warangal Urban. Email ID: mp4unix@gmail.com*
[2]*Prof. M. Jagadeeshwar, Department of Computer Science, Chaitanya Deemed to Be University, Warangal Urban*
[3]*Dr.D.Shanthi, Associate Professor, Department of Information Technology, Maturi Venkata Subba Rao Engineering College, Hyderabad.*

cryptographic techniques, blind processing, and delegation to third parties have proven effective in preventing security vulnerabilities [11]. Encryption/decryption and other security measures are actively being explored to secure information during accumulation, transmission, and utilization [12]. Cloud computing offers three fundamental service types: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), each with its own set of advantages and disadvantages. IaaS facilitates scalable and automated computing services, allowing access and monitoring of various resources, including computers, networks, and storage [13]. Enterprises can procure services online and on demand, avoiding the need to invest in hardware entirely. Certain program components can be provided through IaaS [14]. PaaS provides programmers with a foundation to build and customize their applications. Users can outsource servers, storage, and networking while retaining control over their applications [15]. Cryptography in the cloud involves studying secure communication networks to protect private data, information, and messages from unauthorized access [16]. Current cryptography focuses on data confidentiality, authenticity, and identification, all integrated into the technique [17]. With sensitive data stored in the cloud and accessible globally over the internet, security is a major concern. Cryptography plays a crucial role in ensuring safe data transmission, securing digital media, and protecting web storage and transport [18]. Various techniques, including Encryption Algorithms like DES and AES, Identity-Based Cryptography, and the RSA Algorithm, safeguard the encryption and decryption of data in cloud computing [19]. The following Figure 1 illustrates the basic cryptography process.

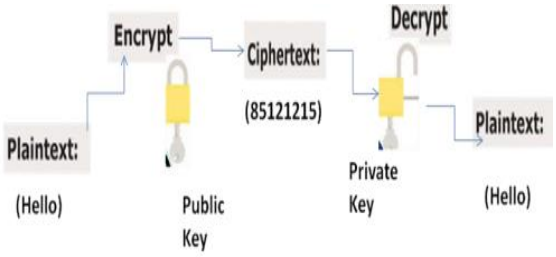

Fig 1: Basic Cryptography Process

Data is now encrypted using a variety of different cryptographic algorithms. Data integrity, authentication, & availability have never been more protected with cryptography than they are now. As shown in Figure, the most basic kind of cryptography encrypts plaintext with an encryption key and decrypts the cypher text with a decryption key [20].Generally there are three basic uses of cryptography:

As Block Ciphers

A block cipher is a technique for encrypting the data where another decryption key & algorithm are deployed to a data block rather than one bit at a time. As a result of this method, it is ensured that identical blocks of text will not be encrypted identically. Encrypted blocks are typically decrypted using the same cipher text that was used in the previous block. The cipher text is created by encrypting these data blocks with an encryption key [21]. The block cipher mechanism is shown in Figure 2.

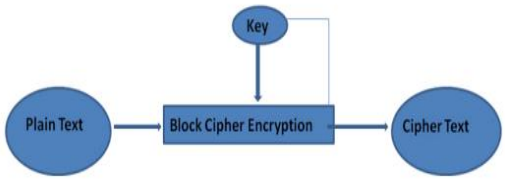

Fig 2: Block Cipher Mechanism

As Stream Ciphers

Since it relies on the current state of cipher, this encryption method is known as state cipher. Instead than encrypting blocks of data, this method encrypts each and every bit. Every item of data is encrypted using a unique encryption key and technique [22]. Because of their minimal hardware complexity, stream ciphers typically present more quickly than block ciphers. However, if this approach is not used appropriately, it might lead to serious security issues as shown in Figure 3.

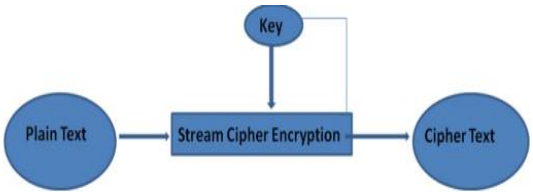

Fig 3: Stream Cipher Mechanism

Fig 3: stream cipher encryption process

As Hash Functions

The input text is transformed into an alphabetic string using a mathematical process known as a hash function. In most cases, the generated alphanumeric string has a fixed length. Using this method, it is ensured that no two sentences will produce the same alphanumeric string. Still, even if the input words are somewhat different from one other, the output strings produced from them could be vastly different [23]. The Figure 4 represents the cryptography hash function.

$F(y) = y \bmod 10$ (1)

Fig 4: Cryptographic Hash Function Mechanism

Securing data in the cloud involves the utilization of a diverse array of methods and techniques, including those outlined above and numerous others. The selection and application of these approaches depend on the specific circumstances. It is strongly recommended to employ any method that enhances data security within cloud services [24]. This paper adopts the Asymmetric Key Cryptography with Related Key Set (AKC-RKS) technique, introducing novel safety mechanisms. The proposed model generates a key set designed to facilitate both the encryption and decryption of data intended for storage in a cloud environment.

2. Literature Survey

Recent research in cloud security has concentrated on mitigating potential hazards. Fursan Thabit et al. proposed the use of a trusted third-party auditor to ensure the integrity of data stored on a remote cloud server [1]. Trusted third parties are advocated as expert agents in the context of data auditing. A primary function of these third-party agents is to retrieve and verify signatures on file tags before concluding their tasks. In a similar vein, Hadisukmana et al. presented a technique for encoding data using the AES and Blowfish methods, specifically in the context of the third-party auditor (TPA) [2]. This method involves the cloud provider recording a document on a computer and actively reporting it to the agent for correctness verification. The agent then requests a fresh hash for the file from the cloud provider and receives it back for validation. Chittibabu et al. [4] proposed a new way to ensure the integrity and confidentiality of data. Using a different method, this approach also makes advantage of user-based encryption software and third-party cloud (TPC) services. First, the owner must enable some actions over his data, such as encrypting the file, computing a hash value with each block, appending it, and lastly uploading this to the cloud. The TPC role in government data audit appears later. Using the provider's encrypted blocks and each signature appended and formed in the cloud, the TPC verifies the data's authenticity by calculating the hash value. Finally, the third party compares the two signatures to see if the cipher text has been altered. This approach has been hampered by TPC issues and also increases customer workload. Cloud computing security has received a lot of attention in the past few years. A number of authors have come up with a variety of ways to ensure that users' safety is their first priority. Tamimi et al. [6] developed a paradigm in which counter propagate neural networks are used for both encryption and decryption. It's a step above from the standard security setup. Improved information security is the focus of three-level authentication systems discussed in this article. The proposed approach also includes real-time monitoring of system and the functioning of the investigative virtual machine. Kumar et al. introduced an advanced multi-level encryption and decryption technique aimed at enhancing cloud security [7]. Unlike decrypting data solely at the lowest level, this method mandates decoding at various levels, increasing the complexity and rendering it more resilient against potential attacks. Cryptographic algorithms such as Data Encryption Standard (DES), Rivest-Shamir Adleman (RSA), and Advanced Encryption Standard (AES) are employed at each encryption level with the primary objective of thwarting unauthorized access to the data. Addressing the concerns of cloud computing privacy and security, Hamadah et al. proposed the use of Ubuntu Corporate Cloud (UCC) as a solution [9]. UCC implements encryption and decryption of data, ensuring that administrators, serving as service providers, do not have unrestricted access to the client's data while fulfilling their responsibilities. Cyber attacks on cloud data confidentially can be reduced using a model proposed by Tao et al. [11]. They suggest client-end authentication and authorization management as a means to this end. There's a new way of doing cryptography that combines chaos theory and neural cryptography. Rather than relying on the randomness of the input noise to increase the strength of encryption keys, this method depends on chaotic random noise. Data security in the Cloud is addressed via an algorithm developed by Anjana et al. [12]. Keys are generated using an alphanumeric encryption table. Primary authentication is performed using these keys. This algorithm protects data against unauthorized access. Data availability, integrity, and security are addressed by Moulika Bollinadi et al. [13]. Their first plan is public auditing. In this design, the Third Party Authenticator (TPA) is Homomorphic Linear Authenticator (HLA). Their second approach involves threshold cryptography. While the initial strategy ensures that the Trusted Third Party (TPA) remains unaware of crucial data during the auditing process, the second method provides assurance that stored data is impervious to exploitation by any unauthorized user. Yang et al. proposed a hybrid approach that integrates Blowfish, RSA, and SHA-2 for this purpose [17]. In this case, both symmetric and non-symmetric algorithms are combined into one. Blowfish is used for data confidentiality, RSA for authentication, and SHA2 for data integrity. This model's data transfer via the internet is protected by a high level of security. Rohit Bhadauria et al. introduced a Hybrid Cipher Scheme [20], utilizing a biometric approach to authenticate and verify the authenticity of each user. SHA, RSA, and three DES techniques are among the many employed in this paper. SHA and Symmetric encryption are utilized to upload information securely, whereas 3DES cryptography is employed for secure data transport. This design will ensure a secure communications environment and avoid illegal access. Elliptic Curve Cryptography is proposed by Mosola et al. [21]. The model can only be decoded after it

has been downloaded in this case. In addition, the user authenticates himself at the moment of login by providing certain input parameters. These techniques are used in conjunction with the Elliptic Curve algorithm for additional security. Visual cryptography has been proposed by AL-Museelem Waleed et al. [23] as a solution to the problem of data storage security because of its smaller key size and higher security. Stored in encrypted form on data servers, user authentication is a prerequisite for the service provider to release access keys for the shared image. Subsequently, users are required to transpose the shared image with this encrypted key to access the secret key, which serves as the key to the information. Singh et al. proposed a method that amalgamates the RSA Partial homomorphic hashing algorithm with MD5 [25]. In this approach, data is initially encrypted using the RSA Partial method before being uploaded to a cloud server, and this method is subsequently employed for decrypting the encrypted data. Afterwards, the MD5 Hashing algorithm creates the hash value using the algorithm. It is in charge of ensuring the safety of your data.

3. Proposed Methodology

In our suggested framework for enhancing data security and privacy, we apply an automated random cryptography technique. This encryption method is unique in that it encrypts individual data blocks. To be more specific, a randomly generated t is created for every block of data.

Algorithm AKC-RKS: It is done in the cloud environment to identify the normal users and malicious users. The cloud user registration involves in allocation of unique number to the user.

Algorithm AKC-RKS:

Step-1: The cloud user registration:

$$CUreg[U] = \sum_{u=1}^{M} G(i) + Time + A(i)$$

$$Unum\big(CUreg(i)\big) = \sum_{u=1}^{M} addr\big(CUreg(i)\big) + Th + rand(1, count(CUreg))$$

Here

G is the user information for communication,

Time is the instant time during registration,

A is the sensitive information of the user,

Th is the threshold value by the service provider.

Step-2: The trust factor calculation:

$$Trfactor\big(CU(i)\big) = \frac{count(CUreg)}{Th} + \sum_{u=1}^{M} \tau - \delta(CU(i)) + B(i) + \sqrt{addr\big(CU(i)\big) + \frac{\beta}{\tau}}$$

Here

τ is the maximum users in server groups,

δ is the registered users in the cloud server group,

β is the behaviour levels of the node as normal and attacker user.

(The trust factor for all the registered nodes is done in the cloud environment. The trust factor is used to identify the user behaviour during the data transmission process.)

Step-3: Key pair generation:

M=getValue()

N=getValue()

K=(M $\oplus$ N)<<2

$$Kset = Th + \max(Trfactor\big(CU(i)\big), Trfactor\big(CU(i+1)\big) + K$$

$$Key_x = M * K - Th \oplus \text{Kset} + \min(\text{Trfactor}(\text{CUreg}(i))$$

$$Key_y = N + K - \left(\frac{M}{2}\right) + pow(K, 4) \oplus \text{Key}_x + \max(\text{Trfactor}(\text{CUreg}(i))$$

$$RKP = \{Key_x : Key_y\}$$

(In the cloud, the generation of related key pairs is carried out to secure the data for encryption and decryption processes.)

Step-4: The user authentication:

$$CUauth[K] = \sum_{i=1} Unum(CU(i)) \varepsilon CUreg \left\{\frac{if\ Unum\ \epsilon\ CUreg\ then\ 0}{else\ 1}\right\}$$

(The user authentication: is done for allowing the access to data to store or to access in the cloud setup. Cryptography models are employed to execute the encryption and decryption processes among authenticated users.)

Step-5: The authenticated user's encryption:

$$\text{CP} = 1 + \text{TI}$$

$$PT = \frac{CP}{2} - K$$

$$RS = PT\ mod\ K$$

$$CipherT = RS + K + M + N$$

(The authenticated user's encryption: are allowed to perform the encryption process using a key in a key pair that encrypts the user data and then stored in cloud. The encryption is performed as)

Step-6: The decryption process:

$$DP = 1 + TI$$

$$DT = DP \ mode \ K$$

$$MesgT = DT - K + M - N$$

(The users request a key for decryption to access the original content. The authenticated users can access the content by the use of a key in the related key pair set.)

4. Results

People, gadgets, and sensors all contribute to the creation of data. When dealing with data, users have to deal with a crucial idea that impacts all scientific fields. The fundamental role of cloud computing is to guarantee the security and reliability of data. When numerous users share the same resources, there is a potential for data misuse. As a result, protection for data access and processing are a must. The most frequent method of protecting data in the cloud is to utilise cryptography techniques. An issue with cloud computing cryptography is securing the data using related keys. This solution protects encrypted information and ensures that only authorised individuals may acquire the keys.

The primary goal of cloud computing is to provide users with swift and user-friendly access to computational and storage resources. Representing a newer form of on-demand computing, cloud computing encompasses a diverse array of resources at a more cost-effective price. Furthermore, cloud computing is dedicated to delivering efficient and accessible computing and data storage services within a cloud environment. While challenges and risks persist within the cloud computing system, the popularity of cloud computing services in the computer world is driven by the pursuit of solutions to enhance security, such as encryption. Only the intended recipient of the cipher text can decipher the concealed message, which is accomplished by encrypting the data or message before it is sent. Cryptology is a mathematical method for the management of security information, including encryption, data quality, and authentication. There are a number of more secure approaches that can be used in conjunction with cryptography. Implemented using Python and executed in Google Colab, the proposed model is based on Asymmetric Key Cryptography with Related Key Set (AKC-RKS). A comparative analysis is conducted between the proposed model and the traditional Genetics Techniques and Logical-Mathematical Functions (GT-LMF) Model.

In order to create a cloud account, a user must fill out a registration form, or profile page. As a component of the user registration procedure, individuals are generally asked to furnish a username and password, in addition to responding to supplementary security questions for an enhanced security framework. Figure 5 illustrates the user registration accuracy levels of both the proposed and conventional models.

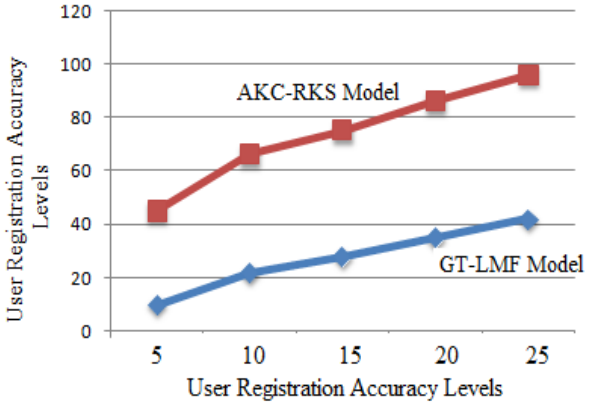

Fig 5: User Registration Accuracy Levels

An expansion of Prime Matchmaking, which allowed users to connect their account details so that they could only play with other confirmed accounts, is Trust Factor. In the realm of cloud computing, trust plays a pivotal role in determining the choice of a cloud service provider and identifying trusted nodes for data communication. The time taken for trust factor calculation is explicitly depicted in Figure 6.

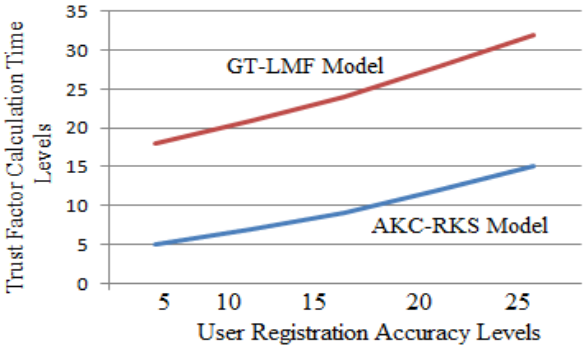

Fig 6: Trust Factor Calculation Time Levels

Assurance and accountability are the two most common strategies for building trust in cloud computing. By giving consumers with cues of cloud service provider, trust, and friendliness as well as some degree of consistency, standards, training, and communication tactics strive to ensure them. Maximum data protection can be achieved by using cloud storage. Because they're stored in the cloud, user files are encrypted and under constant surveillance for potential threats to their confidentiality and integrity. To ensure data preservation in case of emergencies, user data is duplicated, securing a backup copy. Figure 7 depicts the accuracy levels of trust factor calculations.

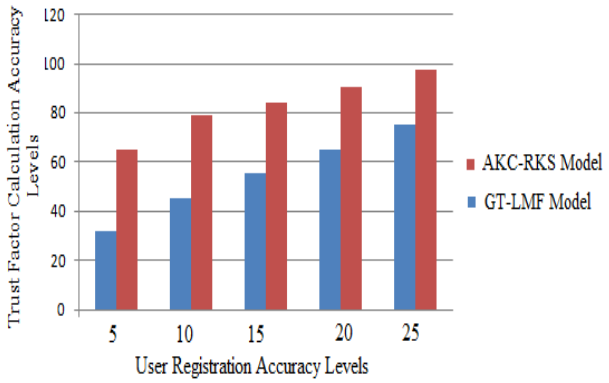

Fig 7: Trust Factor Calculation Accuracy Levels

In cryptography, key generation involves the creation of new keys. A key generator, commonly referred to as software that produces keys, is employed for this purpose. Cryptography utilizes a variable value known as an encryption key, which is applied to a specific piece of text for encoding or decoding. The complexity of deciphering the message depends on the length of the encryption key. The proposed model generates a related key pair for the encryption and decryption process, with the time levels for related key pair calculation represented in Figure 8.

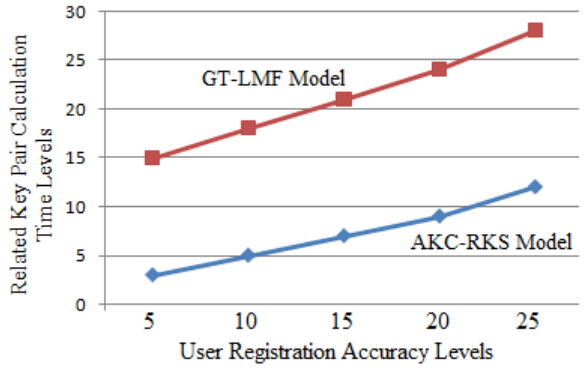

Fig 8: Related Key Pair Calculation Time Levels

Encoding data is the goal of the cryptographic procedure known as encryption. With this method, information that was originally represented as plaintext is transformed into ciphertext. In an ideal world, a ciphertext can only be deciphered back to plaintext by authorised parties, preventing unauthorised individuals from seeing the original data. Figure 9 clearly illustrates the accuracy levels of encryption for both the proposed and traditional models.

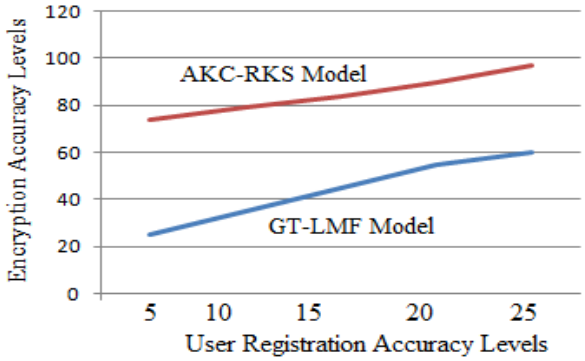

Fig 9: Encryption Accuracy Levels

Decryption involves transforming encrypted data back to its original state, typically through a reversal of the encryption procedure. The decryption of encrypted data requires a secret key or password, ensuring that only authorized users can perform the decryption process. The related key pair is used to perform both the encryption and decryption. The decryption accuracy levels are shown in Figure 10.

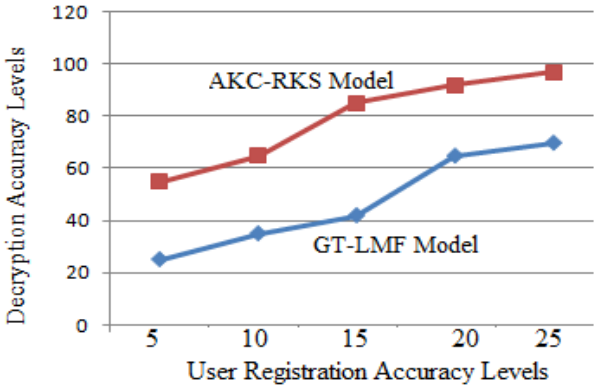

Fig 10: Decryption Accuracy Levels

Data security entails safeguarding against unauthorized access and data corruption throughout the entire lifecycle of content. Utilizing a diverse set of data security measures such as encryption, hashing, tokenization, and key management is crucial to guarantee the protection of sensitive data across various applications and platforms. Figure 11 depicts the data security levels of the proposed model.

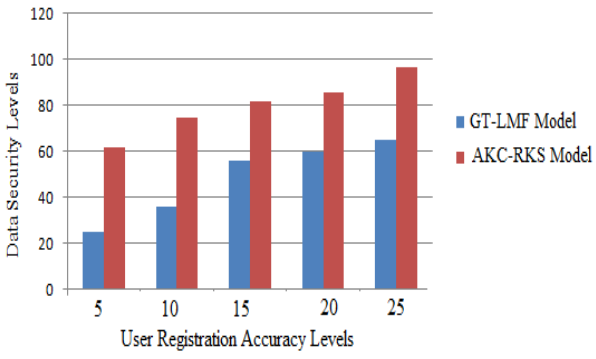

Fig 11: Data Security Levels

5. Conclusion

Data security emerges as a critical concern in the realm of cloud computing, prompting numerous companies to shift their data storage to cloud platforms. This research delves into a spectrum of security considerations in various cloud computing scenarios. After uploading data to the public cloud, this study encrypts it at the client side, decrypting it at the receiver side to establish an additional layer of data protection. The incorporation of Asymmetric Key Cryptography with Related Key Set enhances cloud storage security. Compared to existing cryptography-based methods, it elevates data security levels in the cloud. While the test focused on encrypting and decrypting a text file, the versatility of the proposed strategy allows for potential exploration of other file types. The outcomes indicate secure communication of encrypted and decrypted results to authorized recipients. The model's adaptability and efficiency render it suitable for diverse organizations with varying goals, objectives, and requirements in domains such as finance and health The discussed measures contribute to preserving the confidentiality, privacy, and integrity of cloud data. The achievement of the research's purpose, enhancing cloud data security and privacy through cryptography, is evident. Nevertheless, further research is warranted to refine the combination and provide enhanced protection for multimedia data. This technique maximizes data security while significantly reducing the time required for uploading and downloading a text file in the cloud environment. Future iterations of this model could integrate Artificial Intelligence approaches to bolster cloud service security.

6. Acknowledgements

We acknowledge the support provided by Chaitanya Deemed to be University for this research endeavor. Special thanks go to:

Jagadeeshwar M, Professor, Department of Computer Science, Chaitanya Deemed to Be University, Warangal Urban, for their invaluable assistance in shaping the study on automated data security model using cryptography techniques in cloud computing environment within the domain of cloud security.

Shanti D, Associate Professor, Department of Information Technology, Maturi Venkata Subba Rao Engineering College, Hyderabad, for their insightful comments and suggestions that significantly enhanced the quality of the manuscript.

Their contributions were instrumental in the development and refinement of this research work.

References

[1] Fursan Thabit, Sharaf Alhomdy, Sudhir Jagtap, A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions, International Journal of Intelligent Networks, Volume 2, 2021, Pages 18-33, ISSN 2666-6030, https://doi.org/10.1016/j.ijin.2021.03.001.

[2] Hadisukmana, R.N. An Approach of Securing Data using Combined Cryptography and Steganography. Int. J. Math. Sci. Comput. 2020, 6, 1–9.

[3] Alegro, J.K.P.; Arboleda, E.R.; Pereña, M.R.; Dellosa, R.M. Hybrid schnorr, rsa, and aes cryptosystem. Int. J. Sci. Technol. Res. 2019, 8, 1770–1776.

[4] Chittibabu, P.; Kannan, M.; Priya, C.; Vaishnavisree, S.; Scholar, R. A Comparative Analysis of Des, Aes and Rsa Crypt Algorithms for Network Security in Cloud Computing. J. Emerg. Technol. Innov. Res. 2019, 6, 574–582.

[5] Alsaffar, D.M.; Almutiri, A.S.; Alqahtani, B.; Alamri, R.M.; Alqahtani, H.F.; Alqahtani, N.N.; Alshammari, G.M.; Ali, A.A. Image Encryption Based on AES and RSA Algorithms. In Proceedings of the 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 19–21 March 2020; pp. 1–5.

[6] Tamimi, A.A.; Dawood, R.; Sadaqa, L. Disaster recovery techniques in cloud computing. In Proceedings of the 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), Amman, Jordan, 9–11 April 2019; pp. 845–850.

[7] Kumar, L.; Bandal, N. A review on hybrid encryption in cloud computing. In Proceedings of the 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 18–19 April 2019.

[8] Khan, I.A.; Qazi, R. Data Security in Cloud Computing Using Elliptic Curve Cryptography. Int. J. Comput. Commun. Netw. 2019, 1, 46–52.

[9] Hamadah, S. Cloud-based disaster recovery and planning models: An overview. ICIC Express Lett. 2019, 13, 593–599.

[10] Zaghloul, E.; Zhou, K.; Ren, J. P-MOD: Secure Privilege-Based Multilevel Organizational Data-Sharing in Cloud Computing. IEEE Trans. Big Data 2019, 6, 804–815.

[11] Tao, Y.; Xu, P.; Jin, H. Secure Data Sharing and Search for Cloud-Edge-Collaborative Storage. IEEE Access 2019, 8, 15963–15972.

[12] Anjana; Singh, A. Security concerns and countermeasures in cloud computing: A qualitative analysis. Int. J. Inf. Technol. 2018, 11, 683–690.

[13] Moulika Bollinadi, Vijay Kumar Damera, "Cloud Computing: Security Issues and Research Challenges" in Journal of Network Communications and Emerging Technologies (JNCET) Volume 7, Issue 11, (2017).

[14] Anshika Negi, Mayank Singh, Sanjeev Kumar, "An Efficient Security Framework Design for Cloud Computing using Artificial Neural Networks" in International Journal of Computer Applications (0975 – 8887) Volume 129 – No.4, (2015).

[15] A Venkatesh, Marrynal S Eastaff, "A Study of Data Storage Security Issues in Cloud Computing", in International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 3-No 1, (2018).

[16] Y Z An, Z F Zaaba & N F Samsudin, "Reviews on Security Issues and Challenges in Cloud Computing", International Engineering Research and Innovation Symposium (IRIS), Conf. Series: Materials Science and Engineering 160 (2016).

[17] J. Yang and Z. Chen, "Cloud Computing Research and Security Issues," 2010 International Conference on Computational Intelligence and Software Engineering, Wuhan, 2010, pp. 1-3.doi: 10.1109/CISE.2010.5677076.

[18] Deepanshi Nanda, Sonia Sharma, "Security in Cloud Computing using Cryptographic Techniques", International Journal of Computer Science and Technology Vol. 8, Issue 2, (2017).

[19] Adnaan Arbaaz Ahmed, Dr.M.I.Thariq Hussan, "Cloud Computing: Study of Security Issues and Research Challenges" in International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 7, Issue 4, ISSN: 2278 – 1323 (2018).

[20] Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki, Sugata Sanyal, "A Survey on Security Issues in Cloud Computing" in ACTA TEHNICA CORVINIENSIS – Bulletin of Engineering Tome VII [2014] Fascicule 4 ISSN: 2067 – 3809.

[21] N.N Mosola, M.T Dlamini, J.M Blackledge, J.H.P Eloff, H.S Venter, "Chaos-based Encryption Keys and Neural Key-store for Cloudhosted Data Confidentiality", in Southern Africa Telecommunication Networks and Applications Conference (SATNAC) (2017)

[22] Shakeeba S. Khan, Prof.R.R. Tuteja, "Security in Cloud Computing using Cryptographic Algorithms", in International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 1, (2015)

[23] AL-Museelem Waleed, Li Chunlin, "User Privacy and Security in Cloud Computing", in International Journal of Security and Its Applications Vol. 10, No. 2 (2016), pp.341-352

[24] Dr. Ramalingam Sugumar, K. Raja, "EDSMCCE: Enhanced Data Security Methodology for Cloud Computing Environment" in International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 3 | Issue 3 | ISSN: 2456-3307(2018).

[25] Reshma Suryawanshi, Santosh Shelke, "Improving Data Storage Security in Cloud Environment Using Public Auditing and Threshold Cryptography Scheme", in International Conference on Computing Communication Control and Automation (ICCUBEA),(2016).