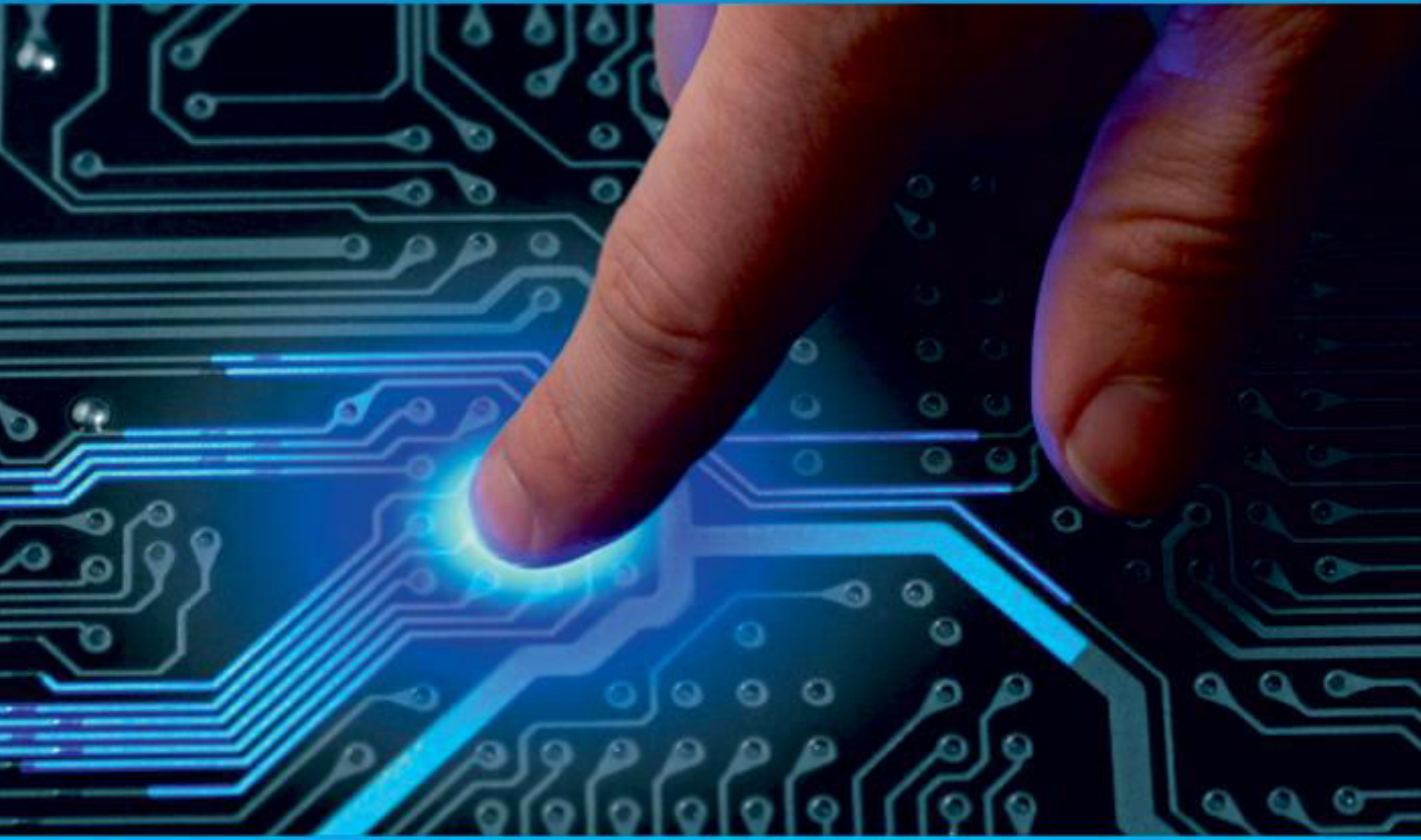
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 3, March 2024

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.379

| DOI: 10.15680/IJIRCCE.2024.1203040 |

Data Transmission Security on Cloud Computing using Algorithm

Sai Lalitha[1], Prof. Rahul Pawar[2]

Student of MCA, Department of CS & IT, Jain (Deemed-to-be) University, Bangalore, India[1]

Assistant Professor, Department of CS & IT, Jain (Deemed-to-be) University, Bangalore, India[2]

ABSTRACT: Cloud computing enables businesses to efficiently store vast amounts of data in the cloud, which can be accessed seamlessly over the Internet without hardware compatibility constraints. However, the transmission of data over the Internet is susceptible to various security threats such as man-in-the-middle attacks, known plaintext attacks, chosen ciphertext attacks, related-key attacks, and pollution attacks. Uploading data to a single cloud service may heighten the risk of compromising confidential information. Prior research has explored several cryptography techniques like SA-EDS, RFDA, and EST to secure data storage across multiple cloud platforms. However, these existing methods exhibit vulnerabilities to various attacks. This article focuses on addressing data security challenges in multi-cloud environments and proposes an advanced approach called Proficient Security over Distributed Storage. PSDS has undergone rigorous testing against multiple attacks, demonstrating its resilience against related-key attacks, pollution attacks, chosen ciphertext attacks, and known plaintext attacks. Additionally, PSDS exhibits reduced computational time compared to existing encryption methods such as STTN and RFD.

KEYWORDS: cloud computing, cryptography, PSDS, encryption, data security

I. Introduction

There are several benefits that cloud computing has over local computer environments. These benefits include lower costs, less administrative work, more flexibility, seamless accessibility, less memory utilisation, and more. Within the cloud computing environment, users have on-demand access to a variety of assets and can take advantage of services like Dropbox, Amazon, and Google Drive that offer backup facilities. Additionally, by providing testing environments without requiring physical infrastructure, cloud computing allows users to cut costs. The user experience is further improved by administrative features like Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Programme interfaces, webmail, and virtual desktops are among the services offered by SaaS, whereas PaaS provides a platform for using tools, libraries, and programming languages. Servers and load balancers are among the online services provided by IaaS. As a result, a growing number of companies, institutions, and people are moving their data to the cloud and using different cloud models—such as private, public, hybrid, and community clouds—to obtain software and infrastructure services.

The investigation of various methods to authenticate data and stop unwanted access, however, is necessary due to the critical concern regarding the security of massive amounts of data stored in the cloud. In order to encrypt data using symmetric or asymmetric keys, cryptography is a fundamental technique in data security. Even though the process of creating asymmetric keys requires a lot of energy and space, the security of this type of encryption—which uses different keys for encryption and decryption—is well recognised. Various levels of security and efficiency are provided by existing cryptographic ideas, such as the Shamir Secret Sharing Scheme and the Advanced Encryption Standard (AES). AES, for example, is widely known for its high-security encryption capabilities, while the Shamir Secret Sharing Scheme uses XOR operations with random integers to encrypt sensitive data before dividing and spreading it over several cloud platforms.

II. Objectives

The principal goal of this research is to apply fuzzy logic, a multivalued logic framework with a range of truth values and changeable ranges. When truth values display gradients from total untruth to absolute truth, fuzzy logic can function. Fuzzy semantic search methods based on logical reasoning improve search experience for the end user by finding and returning results that almost match the search parameters entered by the user. The study also suggests a smart and safe method of data storage that strategically distributes private user information around various cloud servers to reduce the likelihood of compromise and vulnerability. In order to protect both regular and sensitive data from unwanted access or interception, a painstakingly constructed mathematical model is presented together with carefully drafted encryption and decryption techniques.

III. SCOPE

One major worry is how large amounts of data stored in cloud storage will be protected. Many approaches have been developed with the dual goals of verifying information and preventing unwanted access. Cloud computing systems provide significant benefits over on-premises counterparts, including cost savings, decreased administrative workloads, improved flexibility, seamless office accessibility, and optimised memory usage. Users gain from a flexible platform that allows them to request access to a variety of resources. Symmetric key encryption is used by the suggested PSDS algorithm to protect data secrecy even when it is dispersed over several cloud platforms. The suggested solution ensures data resilience and integrity by distributing sensitive data across multi-cloud environments, strengthening protection against unauthorised access and reducing risk exposure in the event of unanticipated situations.

IV. EXISTING SYSTEM

Numerous benefits distinguish cloud computing from local computing, including lower costs, less administration and administrative overhead, greater flexibility, easy access from the workplace, and better memory use. Users that use cloud computing can access a variety of resources on demand thanks to its flexible platform. So, if you upload data to just one cloud provider, you run a higher chance of sensitive data being compromised. Prior studies have discovered a number of cryptographic methods, such as Encryption and Splitting Technique, SA-EDS, and Reliable Framework for Data Administration, that are intended to secure data storage in multi-cloud environment. But there are a lot of attacks that can be made against these current techniques. In addition to outlining the PSDS technique, this essay addresses data security issues in multi-cloud environments.

V. PROPOSED SYSTEM

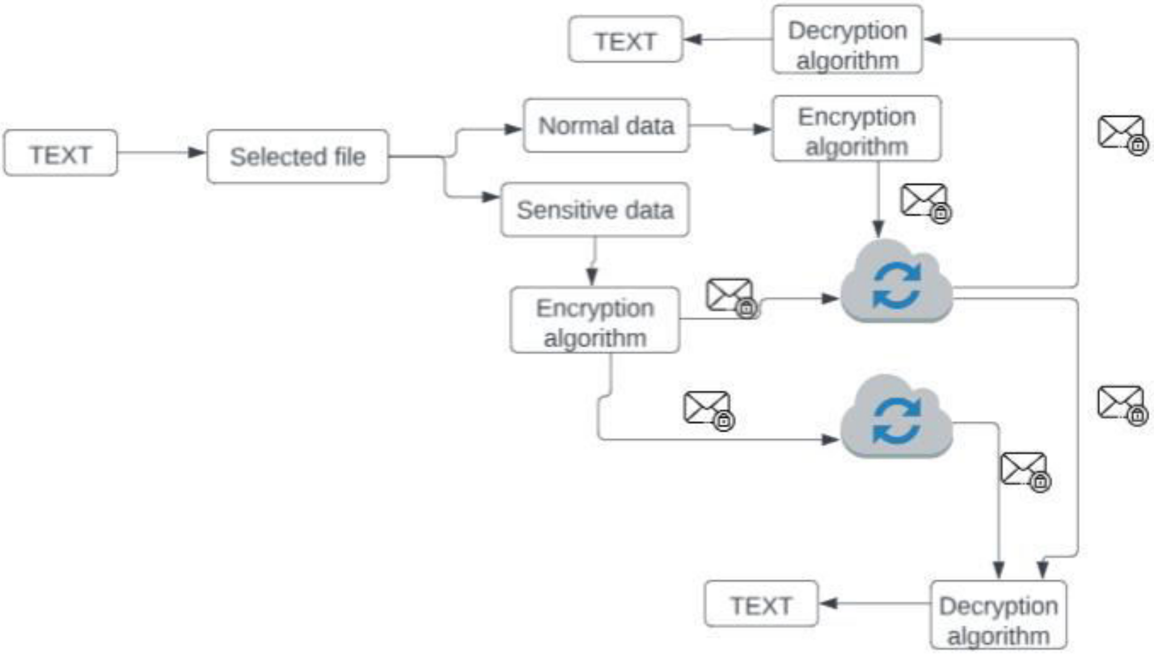
The contributions in general are: To prevent harm and vulnerability, a highly effective and secure data storage strategy has been put out that splits up sensitive user data among several cloud servers. Encryption and decryption methods have been created and presented together with a mathematical model to encrypt and decipher regular and sensitive data. To evaluate the suggested technique's security, it has been examined for protection against a number of known threats. To evaluate its complexity, the computation and communication overhead of the suggested technique has also been examined for both normal and sensitive data. Regarding the overall encryption/decryption time and the computation time for sensitive data, a comparison between the suggested technique and AES, STRRNS, RFDA, and SA-DES has been provided.

VI. SYSTEM DESIGN

The system architecture for the suggested method of file distribution over several clouds consists of user and cloud storage components. In order to upload or download files over the network, a data owner—who is in charge of data file ownership—must go through a login procedure. The data owner can designate the file type after successful authentication. Subject to the policies of various cloud providers, cloud storage functions as a repository that gives users access to storage capacities for their files. An application programming interface (API) is provided by cloud service providers to enable users to communicate with their services. Maintaining data security is still a major challenge, especially when it comes to large amounts of data stored on cloud servers. Numerous techniques have been developed to prevent unwanted access in addition to validating information. Numerous solutions have been offered in the literature to address the issue of data security during information transmission, as highlighted by an analysis of cloud computing and its related applications.

Nonetheless, cryptography is a prominent technique for data encryption that uses symmetric or asymmetric keys. Asymmetric key encryption, which is well known for its strong security, requires a significant amount of energy and space during the key creation process.

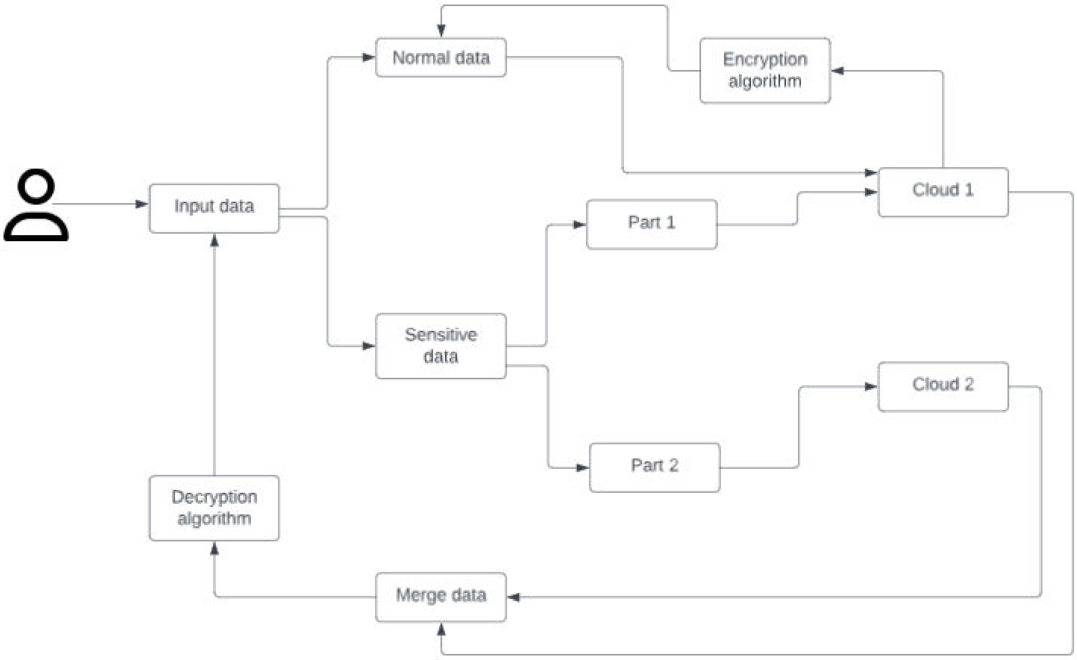
This paper presents Proficient Security over Distributed Storage, a cryptographic solution that protects client data stored in the cloud via symmetric key encryption. It is possible for clients to mark their data as normal or private. Two segments, designated as part1 and part2, are created by splitting up private data. Both segments then go through encryption processes in accordance with the PSDS technique. In order to reduce the possibility of data loss or exposure, the encrypted segments are subsequently transferred individually to two different cloud platforms, cloud 1 and cloud 2. In order to transform ciphertext into plaintext, sensitive data from both clouds is obtained, combined, and put through the decryption process described by PSDS during the decryption phase.



VII. Algorithm

The PSDS method that is being proposed has a distinct operational framework. These components are as follows: Key Generation, which is responsible for creating keys for symmetric encryption in order to protect data confidentiality in cloud storage; an algorithm for splitting sensitive data into smaller segments; and encryption and decryption algorithms that are used to encrypt data during upload and then decrypt it upon owner access. These features function as reference points for evaluating the encryption algorithm's computational effectiveness. Moreover, the encryption time for both regular and sensitive data has been determined in order to assess the effectiveness of the PSDS technique.

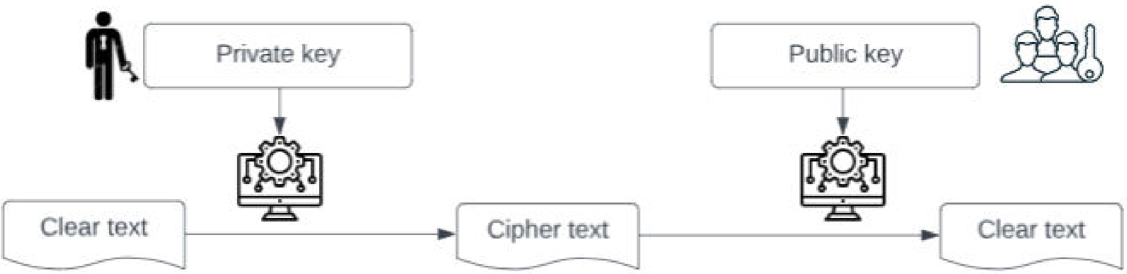
After undergoing extensive testing against a range of attacks, PSDS was found to be resilient to known plaintext assaults, selected ciphertext attacks, pollution attacks, and associated key attacks. In addition, PSDS is more computationally efficient than both STTN and RFD encryption techniques. Users that use cloud computing are provided with a platform that allows them to access various resources on demand. Furthermore, backup options such to those provided by Dropbox, Amazon, and Google Drive are another way that cloud computing provides flexibility. Additionally, by providing environments for application testing without requiring the establishment of physical infrastructures, cloud computing helps clients cut costs.



One major worry with cloud systems is the security of large amounts of data. Many tactics have been developed with the dual goals of preventing unwanted access and verifying information. An introduction to cloud computing is given, along with a list of related applications. While there are several methods suggested in the literature now in publication, data security is still a top priority while transmitting information across computers. However, cryptography remains the principal technique used to encrypt data using symmetric or asymmetric keys.

VIII. Cryptographic Solution

Since the PSDS approach is designed to achieve strong security by dividing private information among multiple clouds, it is flexible. The suggested method shows resistance to several attacks, such as attacks on the chosen ciphertext, associated key attacks, and pollution attacks. Additionally, it prevents cloud service providers from accessing data without authorization.



When the idea of truth encompasses anything from total untruth to perfect assurance, it is used. With a logic foundation, fuzzy semantic search improves the end user's search experience by identifying and obtaining the same data matches that the user submitted for the relevant search query. Further, the model uses semitone similarities to find the closest relevant matches, especially when exact matching are not feasible.

IX. Result and Discussion

This paper explores the main issues surrounding supervised and unsupervised machine learning approaches, explaining the benefits and limitations of each algorithm while taking into account research findings. Dual security measures are available through Data Veracity for Cloud Storage through Dual Protection (DVCSDP) technique. The file is first split up into several parts and sent to several different servers. The Asymmetric Secure Storage Scheme (ASSS), in which the owner of the data splits the file and grants the client authorization by creating a token with the location, login, and password. The amount of data is increasing at an exponential rate due to the rapid growth of technology. Thanks to the widespread use of cloud computing, people may now easily store massive volumes of data to reduce memory utilisation. But data security is the main issue with cloud data storage, which means that data must be converted into ciphertext. In cloud environments, different strategies are used to secure data, with an emphasis on computing efficiency. Because they take a long time to compute, complicated algorithms might not be appropriate for data security, but less complex algorithms could still be dangerous.

To tackle these issues, the Proficient Security over Distributed Storage (PSDS) technique is put forth in this study. Data is categorised into normal and sensitive sections using the PSDS technique. Sensitive data is split into two parts and encrypted before being transmitted to different clouds than normal data, which is uploaded to a single cloud. After these divided sections are recovered, they are combined, and the decryption technique is used to produce plaintext. Protection against a range of attacks is provided by the suggested technique, including man-in-the-middle, related-key, known plaintext, and selected ciphertext instances.

REFERENCES

1. O. Zibouh, A. Dalli, and H. Drissi, ‘‘Cloud computing security through parallelizing fully homomorphic encryption applied to multi-cloud approach,’’ J. Theor. Appl. Inf. Technol 2016.
2. Melhem, M., Alrabaiah, H., & Jararweh, I. (2020). Secure Cloud Storage Using Homomorphic Encryption: A Survey. IEEE Access.
3. Bertino, E., & Sun, D. (2012). Cloud Data Security and Privacy. In Secure Cloud Computing (pp. 1-22). Springer, Boston, MA.
4. Khamis, Z., & Gupta, B. B. (2014). A Survey on Secure Data Storage in Cloud Computing. International Journal of Network Security & Its Applications (JNSA).
5. Erkin, Z., Kirgiz, T., & Toruńczyk, A. (2011). Secure Multi-party Computation over Clouds: Privacy Through Homomorphic Encryption. International Journal of Information Security.
6. Li, J., Huang, W., Tan, X., Xiang, Y., & Wang, R. (2019). Security and Privacy in Cloud Computing: A Survey. Computing Surveys.
7. Ristenblatt, T., & Tromer, E. (2009). Oblivious Computation in the Cloud. In Proceedings of the 2009 ACM SIGSAC Conference on Computer and Communications Security.
8. Popa, R. A., Freeman, J., Mazières, L., & Tanenbaum, A. (2010). SCRUMBLE: Secure Multi-party Computation Three Strikes are Enough. Security and Privacy, IEEE Symposium on, 0-0.
9. Gentry, C. (2009). Fully Homomorphic Encryption Using Ideal Lattices. In Proceedings of the 2009 ACM SIGSAC Conference on Computer and Communications Security.
10. Chen, X., Li, J., Jin, J., & Li, R. (2019). Cryptographic Outsourcing for Big Data Processing in Cloud Computing. IEEE Transactions on Big Data.
11. Yousef, S., Dustdar, S., Wimmer, M., &amp; Leitner, P. (2012).

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details