Advances in Parallel Computing Technologies and Applications
D.J. Hemanth et al. (Eds.)

doi:10.3233/APC210138

A New Approach for Security in Cloud Data Storage for IOT Applications Using Hybrid Cryptography Technique

Pavithra R [a,1], Prathiksha S [a], Shruthi SG [a] and Bhanumathi M [b]
[a] *Undergraduate Student, Department of Computer Science Engineering, Easwari Engineering College, Chennai, India*
[b] *Assistant Professor, Department of Computer Science Engineering, Easwari Engineering College, Chennai, India*

Abstract. The most demanded advanced technology throughout the world is cloud computing. It is one of the most significant topics whose application is being researched in today's time. Cloud storage is one of the eminent services offered in cloud computing. Data is stored on multiple third-party servers, rather than on the dedicated server used in traditional networked data storage in the cloud storage. All data stored on multiple third-party servers is not bothered by the user and no one knows where exactly data saved. It is minded by the cloud storage provider that claims that they can protect the data but no one believes them. Data stored over the cloud and flowing through the network in the plain text format is a security threat. This paper proposes a method that allows users to store and access the data securely from cloud storage. This method ensures the security and privacy of data stored on the cloud. A further advantage of this method is we will be using encryption techniques to encrypt.

Keywords. Cloud, RSA Algorithm, Key Generation, Private key, Public key, Secret key, Authentication, Encryption, Decryption.

1. Introduction

Cloud computing is a technology that uses the Internet and intermediate servers to store data and applications. Cloud computing allows consumers and businesses to use applications without having to install and access their files on any computer with an Internet connection. This technology allows for highly efficient computing by including storage, memory, processing, bandwidth. But where does security fit into all of this? Security analysts and general practitioners say keep it up, but keep an eye out. All the risks of sensitive corporate data associated with external outsourcing apply the cloud computing, and then others. Enforcing security policy and compliance requirements is difficult enough when dealing with third parties and their known or unknown contractors, especially around the world. We suggest how to build a reliable computer cloud computing environment by

[1] Pavithra R, Department of Computer Science Engineering, Easwari Engineering College, Chennai, India. E-mail: bhanuksm@gmail.com.

providing a way to encrypt data on the client-side using a private key before sending it to cloud storage and removing the privacy using that same private key after retrieving it from the cloud storage. All these operations are performed on the client-side using a private key in this way the private key never leaves the client computer and the user is assured of the security of the data stored in the cloud.

2. Literature Survey

Rajat Saxena and Somnath Dey [1], discussed Cloud Audit: How to Verify Data Using Cloud Computing. The proposed system involves multiple and distributed teams (Cloud Audit), which share the bulk of bulk testing among multiple TPAs with load measurement strategies. To perform the load balancing function and perform batch tests, we use multiple TPAs. To measure the effectiveness of the proposed system, the average number of requested data blocks and the total number of data blocks calculated varies by three parameters: probability (Px), file size (Fs), number of audits (A f). This method uses a CBC, PHC, homomorphic tag to ensure data integrity. Ideally, the method is suitable for cloud storage due to the efficient operation of the homomorphic tag and the benefits of PHC. Also, our process supports strong data performance above the minimum. This way, the CSP server does not require additional data structures to manage data performance. It also provides better security in the event of Man In The Middle Attack (MITM), Traffic flow analysis, Impersonation, Dismissal, misuse of data storage servers, due to Paillier's commitment to change small text without distorting clear text and misleading entrants.

The authors of [2] establishes a method to evaluate the latent heat structure based on the percentage of precipitation, space distribution and climatic conditions of the latent heat structure of the deep convective system under different regions and weather conditions and summarizes temporal and spatial distribution of coastal rainfall and typical rainfall characteristics.

Rongzhi Wang [3], discussed research on data security technologies in terms of cloud storage. The data that can be retrieved from the output results of the test module will be stored in a reliable log in the cloud. As one of the two basic modules of system design, R will play an important role in the system. Provides a gauge function and a Tun audit file results to view the operation of the partition, in this way, a reliable third party will carry as little as possible in the audit work without the need to manage a procurement and supply system, making a reliable third-party configuration possible. Users directly from the cloud to get audit results, without the need for a TTP connection. System subsystems, such as the DSBT system or the POR system based on a trusted log, operate not only in one of the roles, but include two or three characters. They play multiple roles and rely on a visual interface to coordinate each other's performance. The program module, therefore, does not depend on the role of the segregation of the body but is based on the fact that the system is subordinate to the concept of segregation.

Xiling Luo et al. [4] discussed An Effective Integrity Verification Scheme of Cloud Data Based on BLS Signature. A remote data integrity protection scheme is proposed that ensures public audibility, privacy protection, and blockless verification. Besides, the scheme may also support batch auditing operations. They introduced and formally defined a ZK-privacy model, where the adversary obtains zero knowledge from the auditing interactions. They proved the privacy-preserving property of our scheme under the

ZK-privacy model. They had also evaluated the performance of the proposed scheme through mathematical analysis and compared it with related schemes in communication and computation overhead. Hence this paper proposes a secure and effective cloud data integrity verification scheme with privacy protection, EoCo, which is based on the BLS short signature .

Yuan Ping et al. [5] discussed the Sustainability of the Public Information Security System. Based on algebraic signature and elliptic curve cryptography, we propose a public verification system that supports effective data validation with low-level communication and computer heads. Besides, the corresponding encryption in the scheme ensures the privacy of the data blocks. To support dynamic renewal, a DCHL-based novel data structure is designed and maintained in TPA to make tasks such as data entry, modification, and deletion easier and more efficient. Using the proposed cloud storage system, security analysis suggests that even a malicious CSP cannot initiate a fraudulent attack, replace attacks and retaliate attacks to pass a guarantee of integrity. At present, the proposed system often exceeds the appropriate data verification schemes for efficiency that is guaranteed by numerical analysis and actual testing.

Yuan Zhang et al. [6] discussed Cryptographic Public Verification of Data Integrity for Cloud Storage Systems. Cruel auditors and external opponents can make SWP work. Most existing social security systems follow SWP, so they have the same framework as the threat model. As a result, these programs also cannot fight external enemies and malicious auditors. An external enemy can make SWP work because there is a clear linear relationship between the evidence information and the data blocks. To counteract external adversities outside of secure channels, a random encryption process was adopted for the compilation of evidence information. Specifically, the authors have used random encryption as a non-line interference code to alter the explicit linear relationship between evidence information and data blocks to non-linear relationships.

Vipul Bornare et al. [7] discussed sharing Data with sensitive information that hides secure cloud storage. The system provides a secure cloud storage system that supports third-party private research better than existing systems. This suggests that security can be increased if construction is converted from a single cloud to a multi-cloud space. The security measures involved in the investigation of third-party information are discussed. Methods are studied to perform research without requiring a local copy of the data and thus significantly reduce communication and computer calculations. Four schemes are being introduced that can be used in many cloud environments to increase security features. Hiding the usage statistics of a single-source provider for one cloud provider is available when the first method is used. Computer and data transfer rates are much lower when using the second method.

RajaniKanth Aluvalu and Lakshmi Muddana [8], discussed A Survey on Access Control Models in Cloud Computing. Every ciphertext is associated with an access policy on attributes in a CP-ABE scheme, and every user's private key is associated with a set of attributes. A user would be able to decrypt a ciphertext only if the set of attributes associated with the user's private key satisfies the access policy associated with the ciphertext. KP-ABE works in the reverse way of CP-ABE. The scheme's access structure or algorithm inherits the same method which was used in KP-ABE to build. The structure built in the encrypted data can let the encrypted data choose which key can recover the data; meaning the user's key with attributes just satisfies the access structure of the encrypted data. The concept of this scheme is similar to the traditional access

control schemes. The encryptor specifies the threshold access structure for his interested attributes while encrypting a message. Based on this, the message of the access structure is then encrypted such that only those whose attributes satisfy the access structure can decrypt it. The most existing ABE schemes are derived from the CP- ABE scheme.

Paul R Rejin and Raj D Paul [9], discussed the verification of data integrity and cooperative loss recovery for secure data storage in cloud computing. For ensuring the correctness of data and preventing data losses, the works split the encrypted data into various cipher blocks and distribute among different service providers. Moreover, the data blocks are distributed equally to all CSPs which leads to a chance of fetching the blocks by any external adversary or malicious CSP in the future. Besides, the integrity of each block was not checked so that there may be a possibility of corrupted blocks. To prevent data access by unauthorized users from cloud storage, a Steganographic Approach using Huffman Coding (SAHC) was applied. For secure data storage in cloud computing, a VDI-CLR technique is proposed. In this approach, CDO encrypts the original file using the CP-ABE scheme and splits it into n/2 cipher blocks, where n denotes the number of CSPs. The randomly selected n/2 CSPs get cipher blocks being distributed to them.

Caiyun Xu [10], discussed Research on Data Storage Technology in computer science. Network storage is a special private data storage server, which can provide platform file sharing functionality. On a LAN, network storage usually takes its place without the need for an application server intervention to allow users to access the data on the network. In this setting, network storage controls and processes all data on the network, removes the load from the business application or server, effectively reduces total costs, and protects user investment. Peer-to-peer network technology, popularly known as peer-to-peer technology (P2P) is a new network technology that relies on computer power and network bandwidth, better than relying on a small number of servers. A clean point network does not have a client or server concept, it has only equal peer points, and ACTS as a client and server for other nodes in the network. P2P networks can be used for many purposes, such as various file-sharing software, real-time news business.

Hasan Omar Al-Sakran [11] discussed ”Finding Protected Data in the Cloud Computing Environment”. Using social media servers to store client data makes secure data sharing a challenge. Protecting the privacy of data stored in public data access policies must be enforced. The cryptographic method proposed in this project solves this problem. Private keys are stored by the data owner. Data must be encrypted before storage on the server, and the only way a client can access data is by providing a corresponding encryption key. Real data encryption and indexing and encryption are done on the owner’s side, and this information is sent to the public cloud service provider. The cloud service provider will create a directory using the owner’s written index that identifies the encrypted data on its site. The service provider cannot access any information from encrypted or indexed data. Clients are looking for blocks that contain specific keywords that encrypt the query on the owner’s site and send it to the service provider’s server. Search is only done on the query reference, and the results are returned to the client

3. System Architecture

There will be a UI where users have the option to upload a file. After uploading a file, clicking the submit button will start storing files in the cloud. If there is an error while

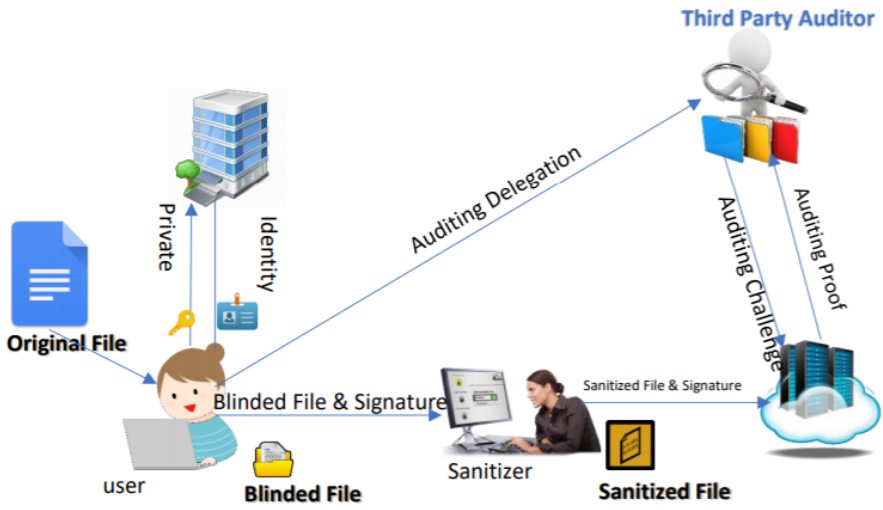

Figure 1. System Architecture

loading, the error will be notified, or else the blinding and cleaning process will take place. Sewage cleaning is called the process of removing/hiding sensitive information in a text. It will keep some parts of the text private and allow other parts to be displayed. After a successful blinding and cleaning process, the files are stored in the cloud. When you need to download a file, the person who will download the files must have the key/password to delete the file and download it.

4. Implementation

This program provides a secure cloud storage system that supports third-party privacy surveys better than existing systems. This suggests that security can be increased if construction is converted from a single cloud to a multi-cloud space. The security measures involved in the investigation of third-party information are discussed. Methods are studied to perform research without requiring a local copy of the data and thus significantly reduce communication and computer calculations. Four schemes are being introduced that can be used in many cloud environments to increase security features. Hiding the usage statistics of a single-source provider for one cloud provider is available when the first method is used. Computer and data transfer rates are much lower when using the second method. The third method provides security such as that one provider may not know the flow of a single application and the cloud provider could not or would not have access to all the data. The fourth method offers the advantage of very low data validation testing to verify file content. It is proved that the third period of the audit is better than the current one.

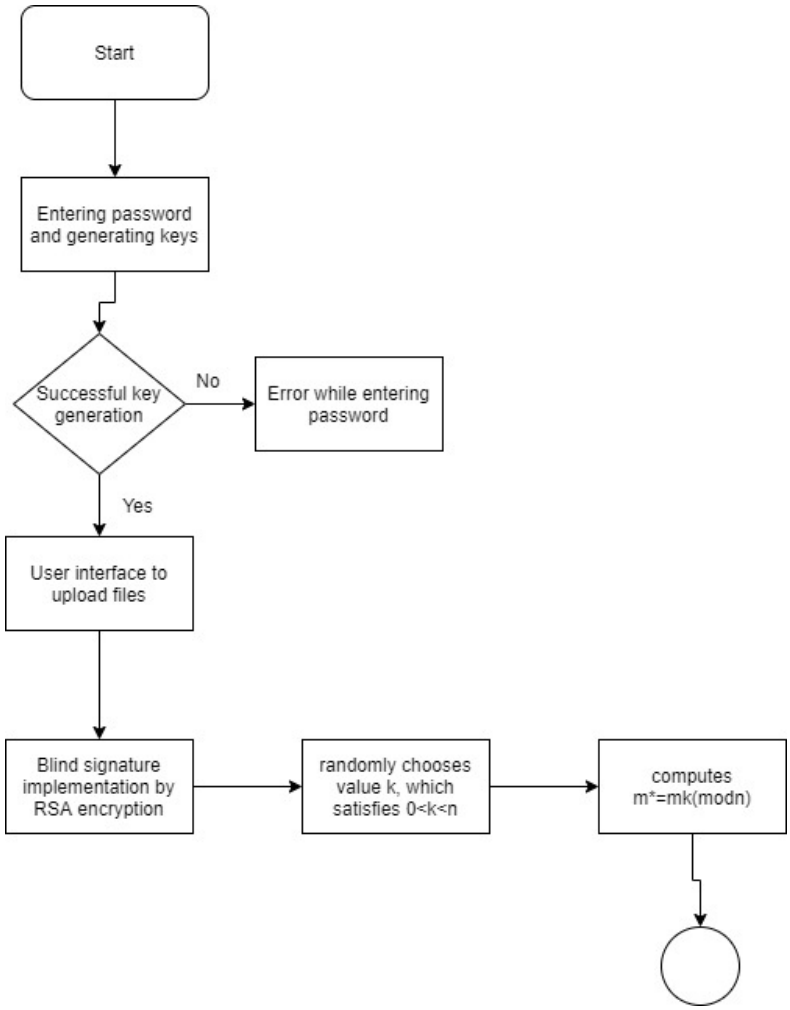

Figure 2. File Blinding Procedure

4.1. Blinding Files

This is the first phase of the module in which users will upload files. After uploading the files, the blinding will start and blind the process where the data is encrypted using the existing Pyycon Python module, which helps protect the contents of the file. Pycrypto allows clients and servers to encrypt customized data and authentication is done accordingly. Pycrypto is a combination of both secure hash functions (SHA256), as well as other encryption algorithms (AES, DES, RSA, ElGamal, etc.). The Pycrypto package is designed and organized in such a way that the installation of new modules is easy. Once blinding is done, the sanitizing phase will begin.

4.2. Sanitizing files

RSA encryption takes effect during this process (file sanitization), which assists in the creation of user keys to access the cloud. RSA uses public-key encryption and is used to protect sensitive data, and is most commonly used when transmitted via an unsecured network such as the Internet. After encryption, a key/password will be generated. A user trying to access these files without a valid key will not be able to view the contents of the file completely.

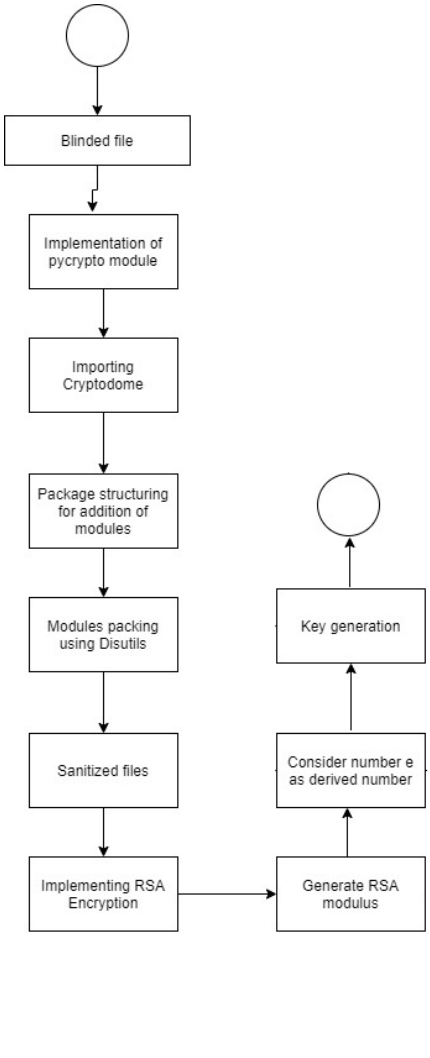

Figure 3. File Sanitation Procedure

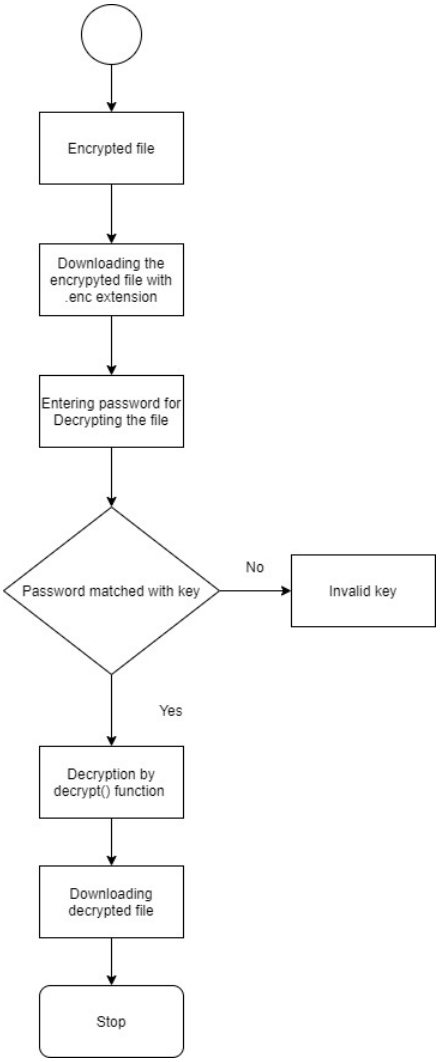

Figure 4. File Download Procedure

4.3. Downloading files

The final module downloads files to the cloud. This user needs to upload the key to a clean file. After that, a stop key will be generated and the user will have to check if it is valid or not. If it works then the user can download the files successfully. If not, the translation key is invalid.

5. Conclusion

We have developed a secure cloud-based data analysis system, which supports data sharing with sensitive information in our system, a file stored in the cloud can be shared and used by others provided that sensitive file data is protected. Cloud storage in rapid development simultaneously also brings a series of negative issues, especially data security issues, which significantly hindered further use of cloud storage.

References

[1] Saxena R, Dey S. Cloud audit: A data integrity verification approach for cloud computing. Procedia Computer Science. 2016 Jan 1;89:142-51.
[2] Chi H. The characteristics of rainfall in coastal areas and the intelligent library book push system oriented to the Internet of Things. Arabian Journal of Geosciences. 2021 Jun;14(12):1-7.
[3] Wang R. Research on data security technology based on cloud storage. Procedia engineering. 2017 Jan 1;174:1340-55.
[4] Luo X, Zhou Z, Zhong L, Mao J, Chen C. An effective integrity verification scheme of cloud data based on BLS signature. Security and Communication Networks. 2018 Nov 19;2018:1-11.
[5] Ping Y, Zhan Y, Lu K, Wang B. Public Data Integrity Verification Scheme for Secure Cloud Storage. Information. 2020 Sep;11(9):1-16.
[6] Zhang Y, Xu C, Li H, Liang X. Cryptographic public verification of data integrity for cloud storage systems. IEEE Cloud Computing. 2016 Nov 11;3(5):44-52.
[7] Bornare V,Nikam K,Khedkar D,Hole S. Data Sharing with Sensitive Information Hiding for Secure Cloud Storage. IJSRD - International Journal for Scientific Research & Development. 2020;8(3):139-41.
[8] Aluvalu R, Muddana L. A survey on access control models in cloud computing. InEmerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India (CSI) Volume 1 2015 (pp. 653-664). Springer, Cham.
[9] Rejin PR, Paul RD. Verification of data integrity and co-operative loss recovery for secure data storage in cloud computing. Cogent Engineering. 2019 Jan 1;6(1):1-12.
[10] Xu C. Research on Data Storage Technology in Cloud Computing Environment. InIOP Conference Series: Materials Science and Engineering 2018 Jul 1 (Vol. 394, No. 3, p. 032074). IOP Publishing.
[11] Al-Sakran HO. Accessing secured data in cloud computing environment. International Journal of Network Security & Its Applications. 2015 Jan 1;7(1):19-28.