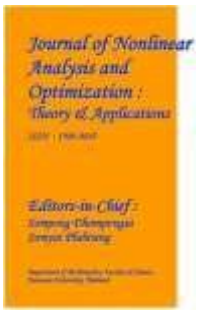
Journal of Nonlinear Analysis and Optimization
Vol. 16, Issue. 1: 2025
ISSN : 1906-9685



A Secure Storage Model With Authentication and Optimal Key Generation Based Encryption

MANNE SRINU[1], Dr. G. SATYANARAYANA[2]

#1 M.Tech Scholar and Department of Computer Science Engineering,
#2 Professor, HOD Department of Computer Science and Engineering, DNR College Of Engineering and Technology, Bhimavaram, AP, India.

Abstract:

The demand for remote data storage and computation services is increasing exponentially in our data-driven society; thus, the need for secure access to such data and services. In this paper, we design a new -based authentication protocol to provide secure access to a remote (cloud) server. In the proposed approach, we consider data of a user as a secret credential. We then derive a unique identity from the user's data, which is further used to generate the user's private key. In addition, we propose an efficient approach to generate a session key between two communicating parties using for a secure message transmission. Session management in distributed Internet services is traditionally based on username and password, explicit logouts and mechanisms of user session expiration using classic timeouts. Emerging solutions allow substituting username and password with data during session establishment, but in such an approach still a single verification is deemed sufficient, and the identity of a user is considered immutable during the entire session. Additionally, the length of the session timeout may impact on the usability of the service and consequent client satisfaction. This paper explores promising alternatives offered by applying s in the management of sessions. A secure protocol is defined for perpetual authentication through continuous user verification. The protocol determines adaptive timeouts based on the quality, frequency and type of data transparently acquired from the user. The analysis is carried out to assess the ability of the protocol to contrast security attacks exercised by different kinds of attackers.

Keywords — Data sharing, understanding controlled encryption, cloud storage, key aggregate encryption

I. Introduction:

Cloud storage is ending up more mainstream these days. In big business circumstances, we see the ascent sought after for data outsourcing, which benefits in the province of shared data and its administration. It is likewise valuable as a center innovation for various online advances for outstanding applications [2]. Cloud computing is known as another option to customary innovation because of its better asset sharing and low-upkeep abilities. The fundamental point of cloud computing is to give superior vitality of computing for different field like military and research association for performing billions of calculations at each second. It is likewise utilized as a part of user situated territories like portfolios to exchange confidential data. In cloud computing, the cloud service providers (CSP), like Amazon, can furnish different services to users with the assistance of intense data servers. Moving the nearby data administration frameworks into cloud servers, users can exploit fantastic services and store critical ventures on their neighborhood foundations. In any case, while sharing data through cloud storage, users are at the same time mindful about the data spillages in the cloud [5]. A standout amongst the most crucial services conveyed by cloud service providers is data storage. Think about a data application. There is an organization which allows its staffs in a similar gathering or division to store and offer records or files in the cloud. Utilizing the cloud, the staffs can be completely discharged from the neighborhood data

storage and upkeep. In any case, it additionally makes a noteworthy hazard to the confidentiality of those put away reports. In particular, the cloud servers controlled by cloud providers are not completely accepted by users while the records put away in the cloud might be s confidential, for example, business thoughts. Recognizable proof of security is most essential issue for wide advancement of cloud computing. Without the verification of personality security users are not prepared to use the cloud services since they would prefer not to uncover their genuine character. To keep up data protection, a fundamental thought is to encode files, and afterward transfer the scrambled data into the cloud. In this paper, we show cryptographic situations for the issue of looking on scrambled data and give consequence of security to the subsequent crypto frameworks [4]. Accessible encryption (SE) plot. In this plan, the data owner scrambles every one of the watchwords which were utilized to encode the data and both the scrambled catchphrase and encoded data were outsourced to the cloud composed. Keeping in mind the end goal to get to the genuine data, the user needs to pass on catchphrase trapdoor on people in general cloud which will be utilized to coordinate a data with a watchword. On the off chance that a match is discovered then the related archive will be recovered, generally the watchword based looking proceeds, until all the catchphrase trapdoor have been tried on the record gathering accessible on the cloud server,. By joining both the cryptographic cloud storage alongside the accessible encryption conspire, the fundamental essential security necessities can be accomplished. Likewise, administration of keys is a difficult issue.. Typically transferred data is scrambled with an alternate encryption key. The quantity of key produced will be corresponding to the quantity of archive files to be scrambled. Likewise, how to send these arrangement of various keys among the different sort of users. In this way, needs to play out the seeking and decoding over the arrangement of archives. These keys must be sent to a user utilizing a protected correspondence channel, likewise by what means can a user store and deal with these keys in their gadgets like cell phones, PCs, PCs, removable gadgets and so forth.

II. Related Work

S. Yu, C. Wang, K. Ren, and W. Lou [2],This framework gives the answer for the issue of fine-grainedness, versatility, and data confidentiality of access control in cloud storage. To address these issues get to approaches are made in view of data characteristics. This paper proposed trait based encryption (ABE), intermediary re-encryption, and sluggish re-encryption methods to accomplish their objective. R. Lu, X. Lin, X. Liang, and X. Shen [3], in this protected provenance SP conspire in light of the bilinear pairings in cloud computing model. This plan is utilized give security and trusted confirmations to data crime scene investigation in cloud computing. Provable security systems are utilized to check the legitimacy of the security. Trusted confirmations for data legal sciences are given by the safe provenance SP plot. X. Tune, D.Wagner, A. Perrig [4], paper proposed the confirmations of security with the assistance proposed cryptographic plan. It underpins looking usefulness without losing the confidentiality of the data. This system is secure for encryption as it gives control seeking over the data. This framework handles the shrouded seeks and additionally inquiry seclusion over the cloud data. This framework additionally underpins arbitrary access unscrambling in which the length of each word likewise should be put away with the word. For Searching procedure encoded Index is utilized when data measure is vast. R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky [5],This paper more grounded security method that is Searchable Symmetric Encryption (SSE). In this system user can store data on remote server and can get to it secretly. To broaden the seeking capacity creators were likewise proposed multi-user SSE. In this framework user minimum the data from huge dataset, Single-database PIR used to recover data from a server containing decoded data. For the protected adjustments new reports can be added to the past archive accumulation. S. Kamara, C. Papamanthou, T. Roeder [6], this paper proposed more grounded security system that is Searchable Symmetric Encryption (SSE). In this system user can store data on remote server and can get to it secretly. To broaden the looking capacity creators were additionally proposed multi-user SSE. SSE is versatile security than picked watchword assaults (CKA2). This framework utilizes reversed file approach. SSE has ability to depict spillage of a database which contains

two tables over word and document identifiers. D. Boneh, C. G, R. Ostrovsky, G. Persiano[7],In this creator alludes component called Public Key Encryption with watchword Search. In this user sends the way to server to recognize that all messages are containing some particular catchphrase without adapting additional data. This framework depends on IBE construction. This approach is for users who claim their data and they wish to transfer that data to an outsider database in which they may not trust. The framework depends on a variation of the Computational Diffie-Hellman issue. C. Dong, G. Russello, N. Dulay [8], in this framework user has its own key which is utilized to scramble and decode the dat a. Consequently it doesn't require any put stock in server for getting to the data. This encryption framework depends on intermediary cryptography in which users share data by means of an un-trusted data storage server. In this server is facilitated by a third gathering. Intermediary cryptography is expand upon the El Gamal encryption plot. To safely scramble watchwords, catchphrase encryption conspire is likewise gotten as a substitute encryption plot. This plan permits user repudiation clearly. F. Zhao, T. Nishide, K. Sakurai [9], data sharing plan in view of property based cryptosystems is proposed by creators. It is fine-grained and in addition adaptable for cloud storage. This plan diminishes the data spillage from catchphrase seek process additionally user disavowal and key refreshing can be effortlessly accomplished. In this framework server recalculate the hash esteems at that point coordinate it with the catchphrase to recover the encoded data. J. W. Li, J. Li, X. F. Chen, et al. [10], this creator gives the data about fluffy catchphrase look strategy in a multiuser framework. It keeps up the watchword protection over the encoded data. Additionally gram-based procedure is used to develop the storage-effective fluffy catchphrase sets. Besides, to enhance the hunt proficiency an image based trietraverse seeking plan is proposed. This framework permits outsourcing cryptographic access control system and furthermore remembers the cost at user side. It bolsters the Interface amongst users and open cloud.

III. Robust Key Aggregate Cryptosystems

In Robust key-Aggregate cryptosystem (RKAC), clients scramble a message under an open key, as well as under an identifier of ciphertext called class. That implies the cipher texts will be further classified into distinctive classes. The key holder holds an expert mystery called expert mystery key, which can be utilized to concentrate mystery keys for distinctive classes. More essentially, the extricated key have can be a total key which is as minimal as a mystery key for a solitary class; however totals the force of numerous such keys, i.e., the decoding force for any subset of cipher text classes. With our illustration, Alice can send Bob a solitary total key through a safe email. Sway can download the scrambled Photographs from Alice's Box.com space and afterward utilize this total key to unscramble these encoded information. The sizes of cipher text, open key, expert mystery key

Also, total key in RKAC plans are all of consistent size. General society framework parameter has size direct in the quantity of cipher text classes, at the same time just a little piece of it is required every time and it can be brought on interest from substantial (non - private) distributed storage.

The information that is transmitted through the total box will be encrypted.

We propose to perform the encryption and decryption

Process using the blowfish algorithm since Blowfish has a64-bit block size and a variable key length from 32 bits up to 448 bits and making it ideal for securing data. It is a variable-length key block cipher. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryption. Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It has been analyzed considerably, and it is slowly gaining acceptance as a strong Encryption algorithm it is much faster when compared to other symmetric algorithms.

IV. Scheme of Robust Key Aggregate Crypto Systems (KRAC)

The information manager makes general society framework parameter through Setup and produces an open/expert mystery key match through KeyGen. Information can be encoded by means of Encrypt by any individual who additionally chooses what

ciphertext class is connected with the plaintext message to be encoded.

Schematic Rules for Robust Key Aggregate Cryptosystems

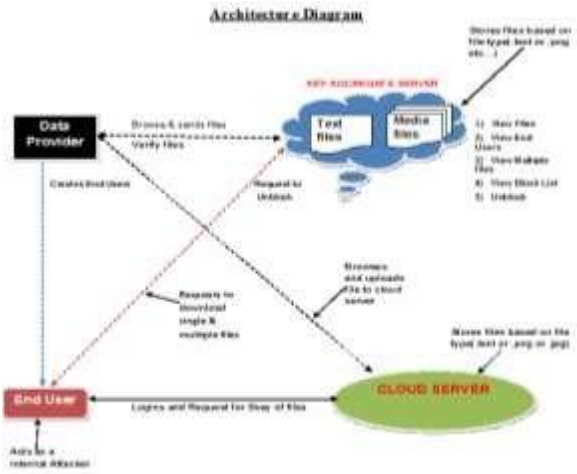
1. Setup (1λ,n) : The Information owner establishes a parameter for public systems via Setup. On input of a security level parameter 1λ and number of cipher text classes n, it outputs the public system parameter param

2. KeyGen: It is executed by information owner to randomly generate a public/M Secret key (Pk,msk)

3. Encrypt (Pk,i,m): It is executed by data owner and for message m and index i, it computes the ciphertext as C

4. Extract (msk,S): It is executed by information owner for attending the decrypting power for a particular set of cipher text classes and it outputs the aggregate key for set S denoted by Ks

Decrypt (Ks,S,I,C): It is executed by a delegate who received, an random key Ks, created by extract. On input Ks, set S, an index I denoting the ciphertext class ciphertext to and output is decrypted result m.



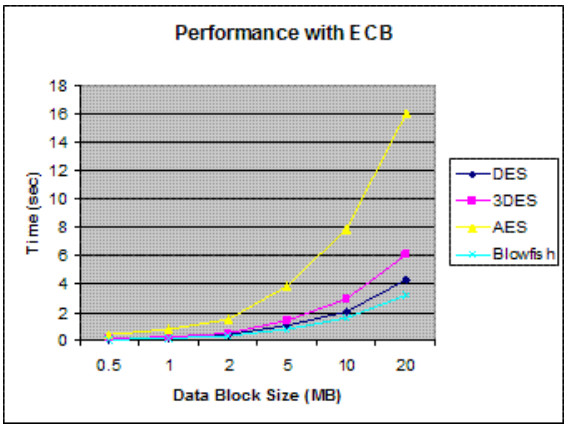


Fig 1. Encryption performance comparison with ECB

The performance speed of the algorithm is also exciting. Chances are high to think that a 448 bit key length is too much. However, when the scrutinizing of the algorithm is done, the effectual throughput of the Blowfish algorithm, we see that even large key lengths result in much faster performance than other encryption algorithms.

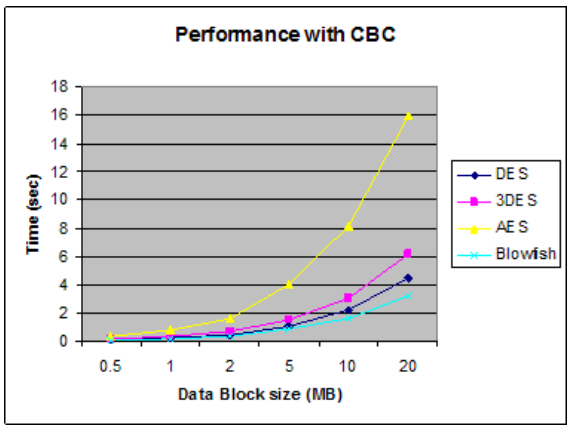


Fig 2: Encryption performance comparison with CBC

Blowfish makes use of a memory size of just over 4 Kilobytes of RAM foe its execution. This constriction is not a crisis even for the very old type of desktops and adaptors, though it does avert use in the tiny embedded systems such as untimely smartcards.

V. Key Aggregate framework:

The proposed system is basically design on the basis of key aggregation encryption. Here we are using two keys to encrypt and decrypt the data

which are secret key and its aggregate key. The data owner creates the public system parameter and generates a secrete key which is public key. Data can be encrypted by any user and he may decides ciphertext block associated with the plaintext file which want to be encrypted.

The data owner have rights to use the secret key from which he can generate an aggregate key which is use for decryption of a set of ciphertext blocks. The both keys can be sent to end user in very secure manner. The authenticated user having an aggregate key can decrypt any block of ciphertext. This project consists of five algorithms which are used to perform the above operations.

These algorithms implementations having following steps are as follow:

Step1. Setup and create the account on the server for sharing of data. This account is generated by data owner.

Step2. KeyGen algorithm is used for the generation of public key. The data owner generates a public secrete key to encrypt the data over cloud. It also creates an aggregate key to access the block of ciphers of limited size.

Step3. Encrypts the data provided by the data owner by using the secrete key. This encrypted data is then share among the cloud.

Step4. The aggregate key is used for extracting the particular block of the ciphers from the cipher file. But other encrypted data remains secure.

Step5. Decrypt: The encrypted data is then decrypted by using the same secrete key which is use for encryption.

VI. Aggregation of Secret Keys:

Introducing a special type of public-key encryption which we call key-aggregate cryptosystem (KAC). In KAC, users encrypt a message not only under a public key, but also under an identifier of ciphertext called class. The key owner holds a master-secret called master secret key, which can be used to extract secret keys for different classes.

More importantly, the extract key can be an aggregate key which is compact as a secret key for a single class, but aggregates the power of many such keys, i.e., the decryption power for any subset of ciphertext classes.

Framework:

Following are different framework activity perform for executing KAC encryption; Step1:The data owner establishes the public system parameter via Setup.

Step2: It generates a public/ master-secret key pair via KeyGen.

Step3: Messages is encrypted via Encrypt.

Step4: Cipher text class is associated with the plaintext message which is to be encrypted. Step5: The data owner uses the master-secret to generate an aggregate decryption key for a set of ciphertext classes via Extract.

Step6: The generated keys is passed to delegates securely through secure e-mails or secure channels.

Step7: Receiver with an aggregate key decrypts any ciphertext provided that the cipher texts class is contained in the aggregate key.

VII. Proposed Work

In this paper, we present a novel receiver-based end-to-end TRE solution that relies on the power of predictions to eliminate redundant traffic between the cloud and its end-users. In this solution, each receiver observes the incoming stream and tries to match its chunks with a previously received chunk chain or a chunk chain of a local file. Using the long-term chunks' metadata information kept locally, the receiver sends to the server predictions that include chunks' signatures and easy-to-verify hints of the sender's future data.

In KAEID user encrypts message under public key cryptosystem. Messages are encrypted by one who decides public key as well as cipher text category. Cipher text is categorized under different "classes". Plain messages which are subset of cipher text class possess few common features. Here all the hosts set up an account on the cloud server. Hosts can login to the

cloud server; they can perform their task and logout of the server. The data owner generates public key/ master key pair. Public key is used for encryption while master key is kept secret. Master key is used for aggregating all the decryption keys. The aggregate key is extracted out of master key and corresponding cipher text class identifier.

This aggregate key is delegated to data recipient. The data recipient compares the set of cipher text classes and decrypts the message. Hence, it also prevents the downloading of unwanted data. Each host in the data sharing system works as IDS. An IDS collects IP address of all hosts in its sub network, and keep eyes on suspicious activities in the network. If any suspicious host is found it is blacklisted. Data sharing with suspicious host is rejected.

1. Our approach can reach data processing speeds over3 Gb/s, at least 20% faster than Rabin fingerprinting.

2. The receiver-based TRE solution addresses mobility problems common to quasi-mobile desktop/ laptops computational environments.

3. One of them is cloud elasticity due to which the servers are dynamically relocated around the federated cloud, thus causing clients to interact with multiple changing servers.

4. We implemented, tested, and performed realistic experiments with PACK within a cloud environment. Our experiments demonstrate a cloud cost reduction achieved at a reasonable client effort while gaining additional bandwidth savings at the client side.

5. Our implementation utilizes the TCP Options field, supporting all TCP-based applications such as Web, video streaming, P2P, e-mail, etc

As shown in Fig. Two hosts data owner and data recipient are accessing the cloud network. Data owner encrypts the data and uploads data on cloud server. Aggregate key is delegated to Data recipient for decryption of requested messages. Hosts involved in communication are also working as IDS. IDS collects and lists IP addresses of corresponding sub network. Monitors the suspicious activities and reject data sharing with the hosts found blacklisted.

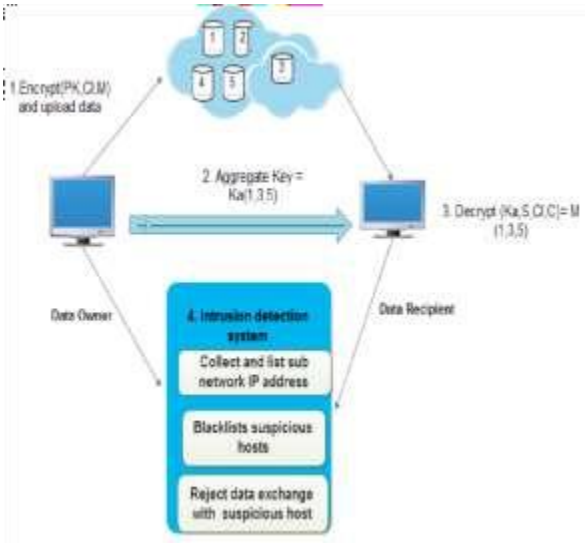


Fig 3-: Proposed Architecture

VIII. Conclusion

Considering the practical problem of privacy preserving data sharing system based on public cloud storage which requires a data owner to distribute a large number of keys to users to enable them to access his/her documents, we for the first time propose the concept of key-aggregate searchable encryption (KASE) and construct a concrete KASE scheme. Both analysis and evaluation results confirm that our work can provide an effective solution to building practical data sharing system based on public cloud storage. In a KASE scheme, the owner only needs to distribute a single key to a user when sharing lots of documents with the user, and the user only needs to submit a single trapdoor when he queries over all documents shared by the same owner. However, if a user wants to query over documents shared by multiple owners, he must generate multiple trapdoors to the cloud. How to reduce the number of trapdoors under multi-owners setting is a future work. Moreover, federated clouds have attracted a lot of attention nowadays, but our KASE cannot be applied in this case directly. It is also a future work to provide the solution for KASE in the case of federated clouds.

References

[1] Baojiang Cui, Zheli Liu_ and Lingyu Wang "Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage" PP: 99 , 2015.

[2]"A Peer-to-Peer Collaborative Intrusion Detection System" Chenfeng Vincent Zhou, Shanika Karunasekera and Christopher Leckie National ICT Australia Department of Computer Science and Software Engineering.

[3] University of Melbourne, Australia 2005 [3] Q. Zhang and Y. Wang, "A Centralized Key Management Scheme for Hierarchical Access Control," in Proceedings of IEEE Global Telecommunications Conference (GLOBECOM 04). IEEE, 2004, pp.

[4] M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies," ACM Transac ormation and System Security (TISSEC), vol. 12, no. 3, 2009tions on Inf.

[5] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," in Proceedings of Advances in Cryptology - EUROCRYPT 05, ser. LNCS, vol. 3494. Springer, 2005, pp. 457473.

[6] S. S. M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters, "Practical Leakage-Resilient Identity-Based Encryption from Simple Assumptions," in ACM Conference on Computer and Communications Security, 2010, pp. 152161.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "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). ACM, 2006, pp. 8998.

[8]J. Li, Q. Wang, C. Wang. "Fuzzy keyword search over encrypted data in cloud computing", Proc. IEEE INFOCOM, pp. 1-5, 2010.

[9] C. Bosch, R. Brinkma, P. Hartel. "Conjunctive wildcard search over encrypted data", Secure Data Management. LNCS, pp. 114- 127, 2011.

[10] C. Dong, G. Russello, N. Dulay. "Shared and searchable encrypted data for untrusted servers", Journal of Computer Security, pp. 367-397, 2011.

Authors

Manne Srinu, Pursing M.Tech in Department of Computer Science and Engineering from D.N.R College of Engineering & Technology, Bhimavaram, Andhra Pradesh ,West Godavari, 534201,India. His area of Interest include Cloud Computing.

Dr. G. Satyanarayana is working as a Professor and HOD in the Department of Computer Science and Engineering, DNR College Of Engineering and Technology, Bhimavaram, West Godavari District, Andhra Pradesh, India.