As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 9(SI01): 103-107, 2023
Copyright © 2023 International Journal for Modern Trends in Science and Technology
ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST09SI0120
Available online at: http://www.ijmtst.com/vol9si01.html

Investigation into a Management System for Key Combinations, Centered Around Identity Authentication

P.Madhavi, CH.Deepika, J.Kannamma, Salma Samreen

Department of Computer Science and Engineering, Vijaya Institute of Technology for Women, Enikepadu, Vijayawada.

To Cite this Article
P.Madhavi, CH.Deepika, J.Kannamma, Salma Samreen. Investigation into a Management System for Key Combinations, Centered Around Identity Authentication. International Journal for Modern Trends in Science and Technology 2023, 9(SI01), pp. 103-107. https://doi.org/10.46501/IJMTST09SI0120

Article Info
Received: 26 January 2023; Accepted: 22 February 2023; Published: 26 February 2023

ABSTRACT

Because of the high volume of enormous information, Cloud Computing is powerful solution for storing huge amounts of information in the cloud, as the cloud can reserve and handle a high volume of clients.ABE is a promising way to make sure that huge amounts of information in the cloud are safe. A minor execution gives the person who owns the information a chance to get it back, freeze it under the new access rules, and then send it back to the cloud. Additionally, we propose various strategy calculations for access strategies.Also, we suggest a smart and safe way for the people who own the data to check if the cloud server has updated the figure messages correctly

1.INTRODUCTION

The general and simple way of protecting cloud outsourced files is to encrypt data files before uploading them to cloud storage.Despite the fact that the data file encryption algorithms do seem to be publicly available, the data files seem to be secure since this key used only for encryption and decryption is kept under wraps. As an outcome, key generation & distribution were indeed crucial issues in cloud computing. The key should always be extremely safe so that nobody can reach the transmitted data files.Encryption of the entire cloud would also secure the data by encryption and decryption with a key. Still, it will only prevent a few limited people from access and it can't be secure if the private key is leaked to unwanted people who will lead to the disclosure of a secret file in the cloud.

[16]Cloud computing is where the owner of the data stores the large scale of data for subsequent processing.The data should be encrypted using the cryptographic method where owners need to maintain full authority over security keys.Using an encryption management tool before encrypting your data will help protect data from data loss.The encryption keys should be kept secret from cloud providers.

Key Management is in which data is encrypted and decrypted using the use of encrypted keys.Keys make sure the safe data transmission across the internet.Security requirements for key management are

1.Access: only authorized users can access encryption keys.

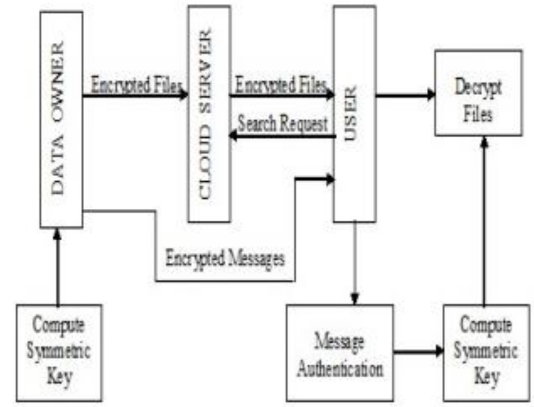
2.the data should be protected from swindling

3.Unintended use of keys: these keys should be used for specific functions

The proper management of cryptographic keys is essential to the effective use of encryptions. As a result, managing these cryptographic keys is a difficult security issue. Only the authorized user has full access to the data if he or she has the secret key. The symmetric keys provide confidentiality to protect the information. So, the symmetric key must be shared with the user very secretly.We came up with a plan for auditing the security of cloud storage based on the user's identity.

2. SYSTEM MODEL

Since the architecture requires a security model to visualize the Securities and Exchange Commission Cloud Life Cycle model, the security mechanism includes two components: a tunnel with SSL security, and static Security is improved by using SSL to create a secure tunnel.. The file hosted on a remote host is always accessible to the on-demand cloud model. It is important to look into the security parameters of such hosts and the queries that are used to get data from the model. Here, the data and key prefixes are swapped using an encrypted sequence and the enc and dec schemes. There are two parts to the architecture: enc and dec. [17] The data and key are acknowledged and then sent enc. The prefix is also sent with the data to be enc to the HADOOP preprocessing step.The scheme is being used in the case to process the secure file transmission in conjunction with the remote host. Remote threats are never possible because the technique is entirely routed using SSL. The owner generates the secret key / symmetric key using a hierarchical tree-based mechanism before outsourcing the files. The file will then be uploaded using the key. The data holder is responsible for producing the message digest for 'n' sample messages, encrypting them with private key, and transferring them to the user. The user must first decrypt the texts and compute the message digest for each message. If the digest provided by the owner matches, the hierarchy tree algorithm is used to generate the symmetric key.When the user gets the files, he decrypts them with this symmetric key.



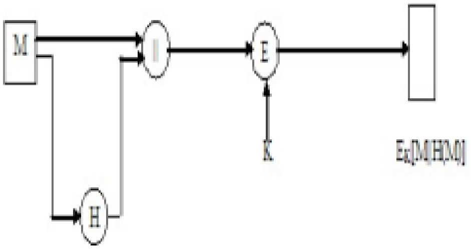
Key Management System Model

3. GENERATION SYMMETRIC KEY

We feed "n" messages into a tree-based hash algorithm to generate the encryption key. Following that, the process produces the root value, which provides the symmetric key for the key-based algorithm.

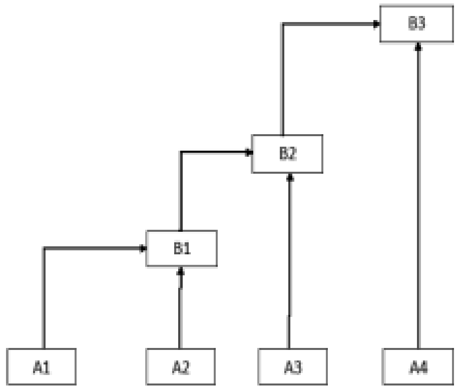
3.A. Key Generation Algorithm

```
Step 1: Start making an empty stack.
Step 2:PUSH(ni).
Step 3: While the stack is still not empty, perform the following steps:
    ● Step 3.1 : PULL(Top);
    ● Step 3.2 : PULL(Top+1);
    ● Step 3.3 :Top hash = H(Top|| Top+1);
Step 3.4 :PUSH (Top hash);
Step 4:Return the top hash.
```

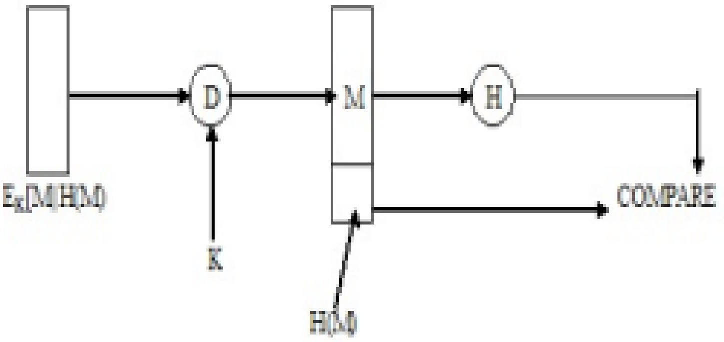


3.B. Message Authentication

In the method to generate a key,Messages will then be delivered to the user.. As a result, before calculating the symmetric key, the user must ensure that the messages received have not yet been tampered with. The data owner uses to calculate the ciphertext using the SHA1 method before encrypting the messages. So, the private key is used to encrypt the message digest, and then the message digest is sent to the user.



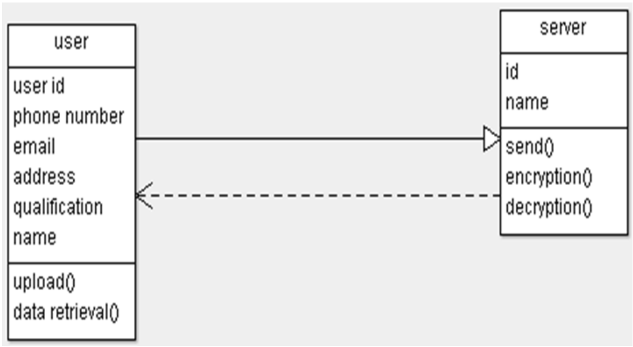
3.B.(i). Authorization by owner



3.B.(ii). Authorization by owner

3.C. Identification

Connections should always be uniquely identified instead of encrypted in several cases.Such that, both members must be aware of the identity of the other. Before granting access to resources, we must first establish and validate identity. One of the most common approachesto verification is through the use of a simple password verification mechanism. A user name is used, followed by a password. Then it verifies a password lookup table to see whether the passwords match. Because the same password is used for each login, this is considered a reusable password.One major problem is that if someone succeeds to crack the technique, they can easily grab the entire password file. When storing data on a device, using a one-way hash function is preferable to storing it in plaintext. We can now have a file with passwords that are encrypted and can't be read. When you type in a password, the system just encrypts it and compares it to the encrypted password.If both passwords are encrypted to the same string, the system will accept them both.



Identification Hash function table

4. DERIVATION SYMMETRIC KEY

The user should first decrypt the encrypted messages using the owner's public key. The message is then determined and compared to one sent by the owner. Then if this matches, then the user uses the hierarchy tree approach to find the symmetric key.

4.A. Key Derivation Algorithm

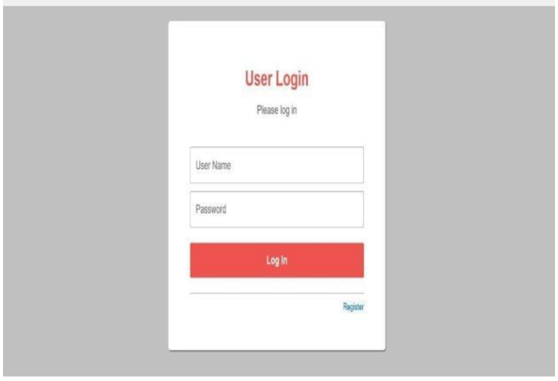
```
AlgorithmKeyDerivation
(ni mean ciphered messages)
Step 1: mi= DECRYPT (ni) pk
Step 2: Make an empty stack.
Step 3: PUSH (mi).
Step 4: : While the stack is not empty, perform the following steps:
    Step 4.1: PULL (Top);
    Step 4.2: PULL (Top+1);
    Step 4.3: Tophash=H(Top|| Top+1);
    Step 4.4: PUSH (Top hash);
Step 5: Return an top hash.
```

Whereas if information is updated, the user requests the data, and the owner sends back the messages.

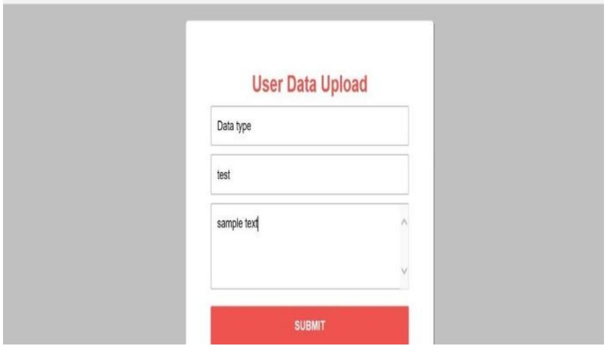
5. EXPERIMENTAL RESULT

We created an identity-based data integrity auditing scheme for secure cloud storage in this study,where it enables data exchange while hiding private information. According to our technique, as long as the confidential material in the file is protected, the file stored on cloud can be distributed and was used by others.Moreover, remote data integrity auditing is still possible and efficient.The security proof as well as experimental results prove that the proposed accomplishes levels of security and performance.

6. OUTPUTS



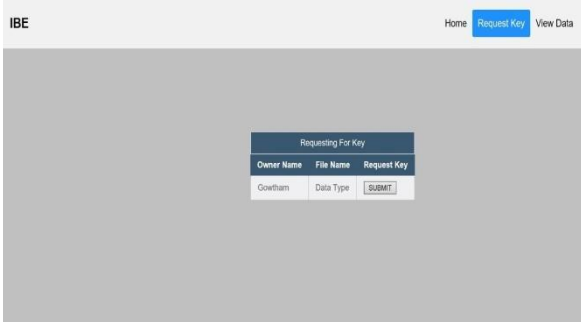
a)Register and login in as owner.



test

sample text

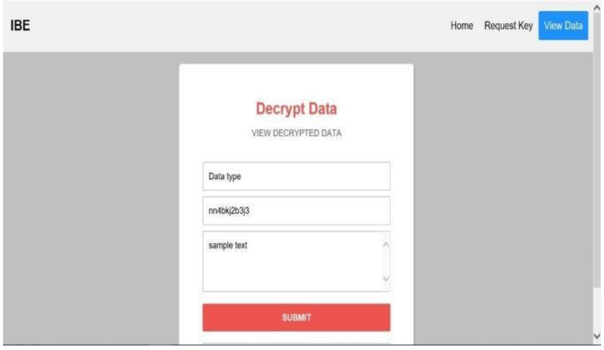
b)Upload data as owner.



Requesting For Key

Owner Name	File Name	Request Key
Gowtham	Data Type	SUBMIT

c)login in as a user and request the data.



nn4bkj2b3j3

sample text

d)key is sent to the user'sregistered details.

7. CONCLUSION

The proposed key management strategy is safer and more efficient in terms of symmetric key generation and distribution. Because the whole method is tunneled through SSL, attacks from afar are never possible. One of the hardest things about cloud computing is making sure that data is correct. The goal for the future is to come up with a new and effective way to check the integrity of data in the cloud.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” IEEE Internet Computing, vol. 16, pp. 69–73, Jan. 2012.

[2] D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in Security and Privacy, 2000. and 2000. Proceedings. 2000 IEEE Symposium on, pp. 0–44, 2002.

[3] E. J. Goh, “Secure indexes,” Cryptology ePrint Archive, HTTP:// eprint.iacr.org/2003/216., 2003.

[4] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: improved definitions and efficient constructions,” in ACM Conference on Computer and Communications Security, pp. 79– 88, 2006.

[5] J. Li, Y. Shi, and Y. Zhang, “Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage,” International Journal of Communication Systems, vol. 30, no. 1, 2017.

[6] Y. Miao, J. Ma, X. Liu, X. Li, Q. Jiang, and J. Zhang, “Attribute-based keyword search over hierarchical data in cloud computing,” IEEE Transactions on Services Computing, vol. PP, no. 99, pp. 1–1, 2017.

[7] A. Swaminathan, Y. Mao, G. M. Su, H. Gou, A. L. Varna, S. He, M. Wu, and D. W. Oard, “Confidentiality-preserving rank-ordered search,” in ACM Workshop on Storage Security and Survivability, Storage 2007, Alexandria, Va, USA, October, pp. 7–12, 2007

[8] C. Wang, N. Cao, K. Ren, and W. Lou, “Enabling Secure and efficient ranked keyword search over outsourced cloud data,” IEEE Transactions on Parallel and Distributed Systems, vol. 23, pp. 1467–1479, Aug.2012.

[9] S. Zerr, D. Olmedilla, W. Nejdl, and W. Siberski, “Zerber +r: top- k retrieval from a confidential index,” in International Conference on Extending Database Technology: Advances in Database Technology, pp. 439–449, 2009.

[10] P. Golle, J. Staddon, and B. Waters, “Secure conjunctive keyword search over encrypted data,” Lecture Notes in Computer Science, vol. 3089, pp. 31–45, 2004.

[11] B. Dan and B. Waters, “Conjunctive, subset, and range queries on encrypted data,” in Theory of Cryptography Conference, pp. 535–554, 2007.

[12] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, “Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption,” in International Conference on Theory and Applications of Cryptographic Techniques, pp. 62–91, 2010.

[13] Y. Miao, J. Ma, X. Liu, X. Li, Z. Liu, and H. Li, “Practical attribute-based multi-keyword search scheme in mobile

crowdsourcing," IEEE Internet of Things Journal, vol. PP, no. 99, pp. 1–1, 2017.

[14] Y. Miao, J. Ma, X. Liu, Q. Jiang, J. Zhang, L. Shen, and Z. Liu, "Vcksm: Verifiable conjunctive keyword search over mobile e-health cloud in shared multi-owner settings," Pervasive and Mobile Computing, vol. 40, pp. 205–219, 2017.

[15] C. Chen, X. Zhu, P. Shen, J. Hu, S. Guo, Z. Tari, and A. Zomaya, "An efficient privacy-preserving ranked keyword search method," IEEE Transactions on Parallel and Distributed Systems, vol. 27, pp. 951–963, Apr. 2016.

[16] Parvathi, D. S. L., Leelavathi, N., Ravikumar, J. M. S. V., & Sujatha, B. (2020, July). Emotion Analysis Using Deep Learning. In 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 593-598). IEEE.

[17] Kumar, J. R., Sujatha, B., &Leelavathi, N. (2021, February). Automatic Vehicle Number Plate Recognition System Using Machine Learning. In IOP Conference Series: Materials Science and Engineering (Vol. 1074, No. 1, p. 012012). IOP Publishing."