TEST Engineering & Management

March - April 2020
ISSN: 0193-4120 Page No. 11405 - 11407

Data Security for Cloud Mechanisms and Identity Using Cloud Authority

***[1]D. Vishnu Vardhan Reddy, [2]K. Jaisharma**

*[1]UG, [2]Assistant Professor, [1,2]Saveetha Institute of Medical and Technical Sciences,
Saveetha School of Engineering, Chennai, India
*[1]vishnuvardhan67634@gmail.com, [2]jaisharmak@saveetha.com

Article Info
Volume 83
Page Number: 11405 - 11407
Publication Issue:
March - April 2020

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 15 April 2020*

Abstract

Data security for cloud mechanisms and identity is a new encryption technique .In this technique we encrypt the data by using user personal files such as name, emailid, phone number, date of birth etc. Even though there are many encryption techniques the main uses of this one is it is going to reduce the storage of data and hence authorisation time is going to reduce. In this scheme there are three main parts .First one is user, the user requests the data that is present in the cloud. Second one is Admin, if the user is valid hegrants the permission and also he moniters every request time to time and grants the permission .Third one is Data owner he uploads the data. This scheme does doesn't have the computational overhead. Due to its uniqueness the efficiency is very high and reliable. The sql database is connected in order to store the keys and data. If u compare with diffehellman key exchange it provides more security and decreases the access time .We also can use different types encryption and decryption techniques like vinegar cipher, playfair cipher in order to encrypt the unique files.

Keywords: *public key, private key, cipher text, plain text, Crypto algorithms, user personal files.*

1. Introduction

Data security for cloud mechanisms and identity is a new encryption technique to encrypt the data by unique data of user .when ever user requests the data, The admin checks whether the requested person is valid or not if the request is valid .he sends the password to the users registered mail .Then the user takes the password and gets the data from the cloud .The encryption of data like email id ,phone number ,name ,data of birth is done by using different types of encryption techniques like vinegar cipher, rsa algorithm, playfair cipher etc. This encryption helps in generating unique key and these keys can be used again and again for sending data .We can use sql server for storing the data in the database and these database contains users personal files, keys. The javascript is used to create the webpages of user, dataowner and admin .This encryption and decryption technique is done by three people .First one is user ,the user requests the data that is present in the cloud .Second one is Admin ,if the user is valid he grants the permission and also he moniters every request time to time and grants the permission .Third one is Data owner he uploads the data. It provides high efficiency and there by computational overhead decreases .If we want to provide additional security to our files we can use extra algorithms for security .With the help of cloud Data owner can upload the data anytime he ever want .The most interesting thing this the user gets the password to his mail. so that he can access the data that is present in the cloud. Local host plays an important role in sending the password to the mail. All the things we have discussed so far are done in the local host. This technique is useful for getting unique keys for every encryption, Unless having different keys for every time .For n number of users it takes only n keys .it reduces storage and hence access time reduces and performance increases.

Public Key: It is a key that is known to everyone.
Private Key: It is a key that is known to only the person who is using.
Plain Text: It is a text that is before encryption.
Cipher Text: It is a text that is after encryption.

March - April 2020
ISSN: 0193-4120 Page No. 11405 - 11407

User Personal Files: These files may be phone number, dob, email, name etc.

2. Literature Review

[1]K.REN et al suggested that data security is the most important thing now a days. in order to secure our data we need the algorithm that provides security .All these algorithms that are proposed are have high complexity and having high storage .if we use these algorithms for n number of users we need 2n or n^2 number of keys .the makes the databases full and the access time will be very high .In order to overcome these problems we are having new algorithm which provides high security with less storage. In this we take using user personal files such as name, emailid, phone number ,date of birth and encrypt them using vineger or playfair cipher and then we gets the encrypted key. In this technique for n number of users only n keys are used. This makes it the more efficient algorithm that is never before. it also provide low access time due to the lesser number of keys .this makes the algorithm to be more efficient..

[2]J.LI et al told that Cloud helps in accessing data at anywhere and at anytime. In this algorithm we are having three major parts First one is user ,the user requests the data that is present in the cloud .Second one is Admin ,if the user is valid he grants the permission and also he moniters every request time to time and grants the permission .Third one is Data owner he uploads the data. The uploaded data can be accessed anywhere by the user if he requests the data. the admin sends the key to the users mail. So that he can access the data anywhere and at anytime. There are many applications of this technique it is user friendly and it sis understandable and it also provide good security. In order to store the data we need sql and for webpages we need javascript. first the user needs to register .in this the keys are very less this is because we are generating the keys by using the users own personal data which is unique .The cloud on the other hand stores all the data that is uploaded by the owner and encrypts them. We use local host as a server .these local host helps in sending mail to the user. Many reallife applications use these technique. it is better than differ hellman key exchange and if we need we can provide additional security by using AES and Des etc.

3. Proposed system

In this system we have data owner, user and cloud authority.

1. Data Owner:

The owner is the person that decides whether to upload the data or not. He has the full knowledge of the uploaded content, he uploads the data to the server. whenever some user requests the data admin grants the permission and gets the data. The money regarding the data will we gone to the data owner account.

2. End User: The user first registers to the cloud account and the request for the data.

3. Cloud Admin: The admin moniters all the data that is uploaded in the cloud and then grants permission who ever requests for the data if he is a valid person

Implementation Code: IT has three parts

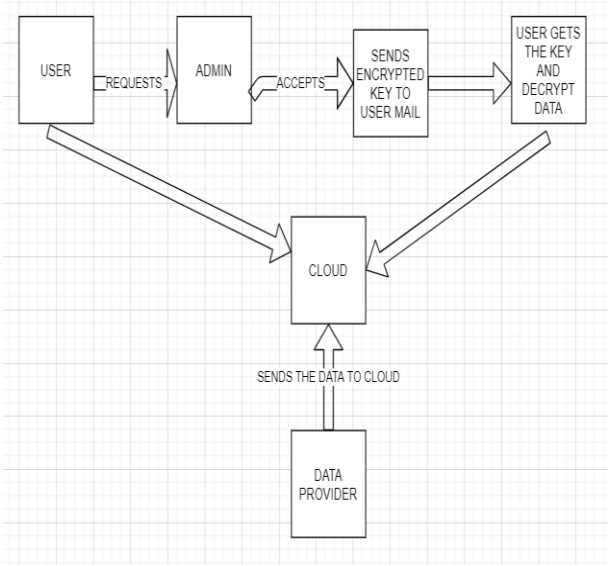
They are owner, user, admin:

Admin: Admin controls the data and decide whether the user is valid person or not.

Owner: owner encrypts the data and upload the content.

User: user can request the data and receive passcode in mail

System Architecture: system architecture says that how plain text is converted into cipher text by the ide encryption .It also shows how the things will work diagrammatically.

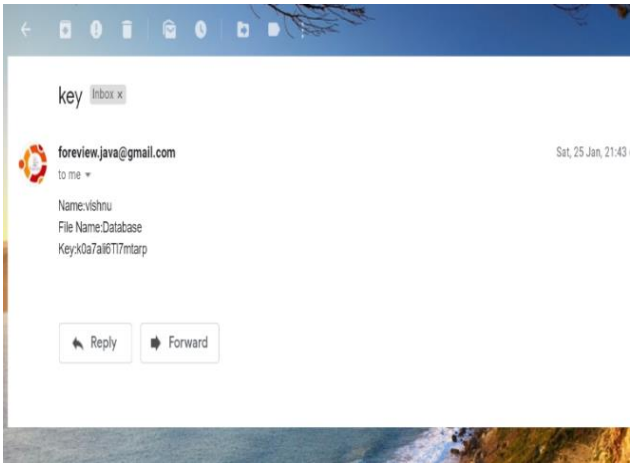


4. Results

Whenever user requests for the data the admin verifies the request and sends the key to the requested mail .He then takes that key and access the data. we also have the results for sizes of encryption, decryption keys etc

EXISTING KEY DATA	ALGORITHM(ENCRYPTION)	RESULT OF ENCRYPTED KEY	COMPUTATION TIME	NUMBER OF KEYS REQUIRED B/W TWO PARTIES
Vishnuvardhan,9790876123,21/08/1999	AES/DES	3abzrtyucagdk	1.34ms	1
Abc,696275469764587,09/7/2000	AES/DES	Vgsg7tryrryrb	1.28ms	1
Xyz,687368755,03/8/2000	AES/DES	B672fduwiss	1.26ms	1

March - April 2020
ISSN: 0193-4120 Page No. 11405 - 11407



5. Conclusion

The system that is proposed is totally based on providing high security with unique identity of a person .This helps in producing less number of keys and there by access time and computational time is going to reduce drastically. The most important thing is cloud which provide access at any time and any place. The three persons data owner, cloud, user plays a very important role in providing security and good low computational time.

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. SandP 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, Storagess 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.