MAINTAINTING SECURITY OF- DATA ACCESS IN CLOUD COMPUTING

[1]Prof. Pushpmala Nawghare, Seema Sagar, Sakshi Ughade, Asmita Surve
ZES"s ZCOER, Narhe, Pune

Abstract: Now a day"s people are using their smart phones for various purposes like uploading data, sharing data, use of online services, etc. along with their primary functions, but the problem with smart phones is that they are having limited computational power and storage space. Cloud computing along with mobile computing environment, solve this problem and also increases the capacity of mobile devices. The major problem of using cloud is the privacy issue, which also becomes the problem in mobile cloud computing environment. This paper gives light-weighed cryptographic machinery a proxy re-encryption to solve the data integrity, data security issues in which users has to keep only short secret keys for all cryptographic operations in mobile cloud without involvement of any trusted third party.

Keywords: Anonymous authentication, Advanced-Encryption-Standard, Elliptic-curvecryptography, sync traffic, reduplication, key Aggregation.

1. Introduction

Cloud-Computing refers to manipulate, configuring, and access the hardware and software possessions closely. It gives online data storage space, road and rail network, and submission. Cloud-computing provides display place independency, as the software is not compulsory to be installed in the neighbour hood on the PC. Consequently, the Cloud Computing is making our profitable and reliable-business applications mobile and collaborative. To save data on cloud, cryptographic machinery a proxy re-encryption system provides many benefits, like less cost, authenticity and availability, but the data privacy issues result into security and truthiness problems. Since portable cloud computing combines the techniques of portable computing and cloud computing, many users can upload there data on cloud through cell phones. This paper gives an idea of well-organized data circulation system in dynamic environment which gives flexibility to transportable users to strongly accumulate their data in cloud storage armed forces, and share their information with acquaintances. System given in this paper is several cryptographic prehistoric to release data space to yourself, data integrity, dynamical data adjustment and scoring from commencement to end, and stretchy data circulation. Also allows the dataset admin to anytime change and remove his data.

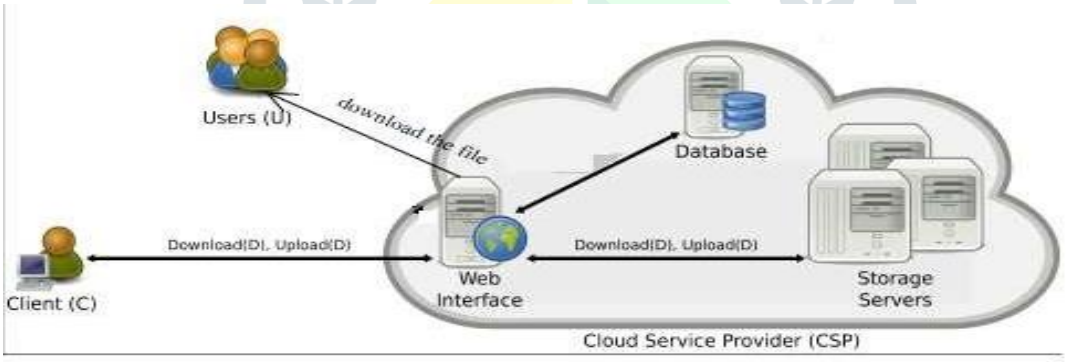

Fig 1. Basic Structure

In fig.1 the basic structure there are two categories/modules, first is user (admin) and second is client. Here, user and client both will get access of a file. The owner/ user accessing the all categories like upload, download, delete, accept request, remove request etc. Client has access only for upload, download, and send request to owner for accessing file. User or admin have fully access about the data accessing but client required the permissions for accessing the data. For that the client send request to the owner or admin for data accessing after accepting the request admin gives permission to client for access the file/data which is warehoused in the cloud. The data which remains stored in various storage servers and through the web interface user or client can store and access the data from cloud.

2. Existing Work

The interconnected employment on mysterious validation plans can be comprehensively ordered into open key cryptosystems (PKC) based plans [3]–[4], uniqueness founded cryptosystems investigation of STASIS and LSA. These proportions of semantic closeness can be connected to short messages for use in Conversational Specialists (CAs). CAs are PC programs that associate with people through regular language discourse [5]Tara"s Finikov proposed a system in which influence of transformation processes in higher education to lower academic standards, changes and deformation in ethical field of global and national higher education. We considered the genesis and

modern standards of academic integrity [6]. Schemes, pen names plans [7], [8], consolidated plan utilizing both character based encryption and pen names, application situated plans. Mysterious verification plans dependent on PKC in [9], [10] were infeasible for versatile systems in light of the computational assets required by PKC secluded exponentiation, which expend a greater number of assets than what a cell phone can offer. To limit the computational prerequisites, different unknown confirmation plans dependent on elliptic bend cryptosystem (ECC) encompass been wished-for [11]–[12], which have in good health execution in view of the littler key size utilized in ECC. The execution of ECC based plans are upgraded by personality based cryptosystems over ECC. Not at all like the conventional PKC, the character based cryptosystems abuse open personality, for example, ID or email address as the client's open key to dispose of the cost identified with the administration of open key endorsements, which is frequently attractive in versatile situations.

2.1 Motivation:

- To secure information. Furthermore, add protection to information verification.
- To minimize paper work.
- To prevent data from unauthorized access.

3. System Architecture

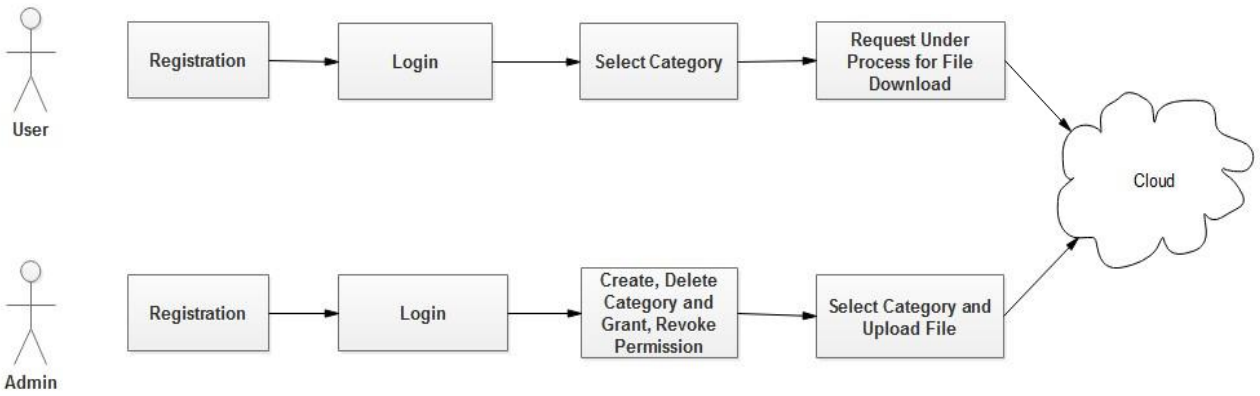

Fig 2: System Architecture

In this architecture, the dataset admin will divide his private dataset into several classes. The data holder protects his dataset in each class with an individual method by using the TB-PRE scheme. A safe and sound symmetric encryption is in employment to cipher the files for each dataset class, and then the TB-PRE proposal is used to cipher the symmetric reserved key. In examination of result, that all data classes may surround number of dataset files, the dataset admin also generates a Merkle Hash Tree (MHT) for every dataset grouping and with only provisions that the sub-data having the origin of the MHT consequent to all grouping at admin private home storing. Above and beyond, the Boneh–Lynn–Shacham signature pattern used to substantiate the extraction of the MHT such that the documents purchaser cloud also confirms the truthfulness of the information documentation plus substantiate the characteristics of the documentation shoulder. System architecture of wished-for system is shown in Fig.2. In this data allocation system basically three modules are available, specifically, cloud module, the data possessing module and the dataset user module. The dataset admin is not a static user who supplies his personal private dataset in the obscure (by several classes), and allows the dataset client to admittance his confidential data (of few grouping) from the storage that is cloud. The cloud is separate, that provides luggage compartment facilities and also responsible to give assistance the dataset admin to allocate the own dataset (belongs to one of the grouping) to the information purchaser. The dataset customer is a person, who initially gets data admittance acquiescence (of one of the dataset grouping) from the dataset possessing module (and same procedure continued once per dataset) .Data discretion: All stakeholders (along with the cloud) not having admission permission also cannot be in cahoots with to view the confidential data of the dataset admin. Dataset truthfulness: Both the dataset admin and the dataset client can check the truthiness of the datasets. Dataset substantiation: The dataset client can substantiate the dataset admin uniqueness. Dynamic dataset maneuver: The dataset admin can perform information adjustment and remove operations without heartwarming the privacy, truthiness and confirmation characteristics. Drill Down data allocation: The dataset purchaser may read the confidential dataset belong to a grouping only then he achieves the authentication to that specific dataset class from the dataset admin.

3.1 Decryption Technique

Here in this process we are performing decryption at the time of file download to get data in original form.

3.2 AES (Advance Encryption Standard)

AES is an iterative rather than Feistel secret message. It is centered on „replacement transformation network". It includes of a succession of connected operation, selected of which engross changing inputs by unambiguous productions (substitutions) and others involve slouching bits approximately (variations). Fascinatingly, AES executes all its computation on bytes to a certain degree than bits. Subsequently, AES treats the 128 bits of a unique content square as 16 bytes. These 16 bytes are prearranged in four segments and four columns for administration as a framework −Unlike DES, the numeral of rounds in AES is eccentric and relies upon the length of the key. AES utilizes 10 rounds for 128-piece keys, 12 rounds for 192piece keys and 14 rounds for 256-piece keys. Every one of these rounds utilizes an alternate 128piece round key, which is open from the creative AES key.

3.3 ECC (Elliptic curve cryptography)

In this algorithm we are generate a signature for categorizer to save the data discretion. That signature will be association to file. Public key and confidential or conventional distinctiveness based cryptography that has some individuality fundamentals that fit well in the prerequisite of cloud computing. This work aims at humanizing cloud computing surrounded by Cloud Organizations with encryption unconsciousness based on Elliptic Curve Cryptography.

4. Mathematical Model:

- S = {s, e, X, Y, I}
- s = Start of the Program
- Register/Login into the system
- Provide user file
- e = End of the program
- X = Input of the program
- I = user text file
- Y = Output of program = categories file

First, user provide text file that might be of our system categories file into deferent categories and use AES to convert readable file into non readable format

F= {F1, F2, ..., Fn}

5. System Outcomes

The system will provide decrypted files when user request to download particular files of different category. User will get an authentication key on their mail i.e., called as BLS Signature. This key will be different for different users so that main key will not get hacked.

6. Future scope

Further, we could develop a flexible system which can work with real time data. In the future we will consider mp3, mp4 data and PDF files also and we can design the BLS Signature more accurately.

7. Conclusion

We proposed a system in cell cloud computing which doesn"t included some other confidential service. Also it gives many features like document integrity, authentication, modification, deletion, with access control policies as well as drill down access control. Outcome of this is a new more powerful and tested confidential proxy re-encryption scheme and also ensuring the security.

Reference:

[1] Jiang Zhang, Zhenfeng Zhang, and Hui Guo "Towards Secure Data Distribution Systems in Mobile Cloud Computing", vol.14, 2017

[2] Ghassan O. Karame, Claudio Soriente, Krzysztof Lichota, Srdjan Capkun, "Securing Cloud Data under Key Exposure", vol.13, 2017

[3] J. Zhu and J. Ma, "A new authentication scheme with anonymity for wireless environments," IEEE Trans. on Consumer Electron., vol. 50, no. 1, pp. 231–235, Feb. 2004.

[4] G. Horn and B. Preneel, "Authentication and payment in future mobile systems," Computer. Security – ESORICS 98, pp. 277–293, 1998.

[5] W. Lei, Y. Li, Y. Sang, and H. Shen, "A secure anonymous authentication scheme for electronic medical records system," in Proc. 13th Int. Conf. on e-Business Engineering, Nov. 2016, pp. 48–55.

[6] V. Sucasas, G. Mantas, A. Radwan, and J. Rodriguez, "An oauth2-based protocol with strong user privacy preservation for smart city mobile ehealth apps," in Proc. IEEE Int. Conf. on Commun., May 2016, pp. 1–6.

[7] R. Fernando, R. Ranchal, B. An, L. B. Othman, and B. Bhargava, "Consumer oriented privacy preserving access control for electronic health records in the cloud," in Proc. IEEE 9th Int. Conf. on Cloud Computing, Jun. 2016, pp. 608–615.

[8] A. Mehmood, I. Natgunanathan, Y. Xiang, G. Hua, and S. Guo, "Protection of big data privacy," IEEE Access, vol. 4, pp. 1821–1834, Apr. 2016.

[9] H. Xiong, J. Tao, and C. Yuan, "Enabling telecare medical information systems with strong authentication and anonymity," IEEE Access, vol. 5, pp. 5648–5661, 2017.

[10] X. Li, S. Tang, L. Xu, H. Wang, and J. Chen, "Two-factor data access control with efficient revocation for multi-authority cloud storage system," IEEE Access, vol. 5, pp. 393–405, 2017.

[11] C. Yang, W. Ma, and X. Wang, "Novel remote user authentication scheme using bilinear pairings," Lecture Notes in Compute. Science, vol. 4610, p. 306, 2007.

[12] P. E. Abi-Char, A. Mhamed, and E.-H. Bachar, "A fast and secure elliptic curve based authenticated key agreement protocol for low power mobile communications," in Proc. Int. Conf. on Next Generation Mobile