International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Secure Proxy Server Data Sharing Scheme in Hybrid Cloud

[1]Reshma Sultana, [2]Dr. Md Ateeq-Ur-Rahman

[1]Department of Computer Science & Engineering, Shadan College of Engineering & Technology, Hyderabad, Telangana, India
[2]Professor, Department of Computer Science & Engineering, Shadan College of Engineering & Technology, Hyderabad, Telangana, India

ABSTRACT

Security is the major concern for users willing to store their own information in any remote server. Public Data Storage is available for all the users accessing cloud servers. For public clouds, there will be no authentication for data as the information is available and accessible to everyone on network. However, Personal contents need security attention from data storage service providers and we call it as Cloud Service Providers. As the cloud server is untrusted, data owners hesitate to store their personal contents from their devices like PCs, laptops, smart devices etc to cloud servers. There exist a large vary of security problems within the distributed computing. This paper depends on the examination after effects of proxy cryptography, personality based open key cryptography and remote information honesty checking out in the open cloud. Now and again, the cryptographic operation will be appointed to the outsider for instance proxy. In this way, we need to utilize the proxy cryptography. Proxy cryptography is an essential cryptography primitive. Expecting the proxy server will act as a security agent in between data owners and cloud service providers. Adding proxy server will make application security to the next level. In order to realize the performance of the application, the proxy servers are best as they rely totally on client requests. Data owners' data is secure through integrity keys which are generated and maintained by auditors.

Keywords : Proxy public key cryptography, remote data integrity checking, cloud computing, identity-based cryptogaphy.

I. INTRODUCTION

In organization's data storage is becoming a major problem. cloud data storage can be solution to this problem ,but security issues rises .As the cloud server is untrusted data owners hesitate to store their personal contents from their devices like PCs, laptops, smart devices etc. to cloud servers. . However Personal content need security attention from data storage service providers we call it as Cloud Service Providers In Public cloud condition, most customers transfer their information to PCS and check their remote information's respectability by Internet. In any case, the supervisor won't trust others can play out the remote information honestly checking. Public checking will acquire some risk of releasing the protection. There exist a wide range of security issues in the distributed computing. This paper depends on the examination after effects of proxy cryptography, personality based open key cryptography and remote information honesty checking out in the open cloud. Now and again, the cryptographic operation will be appointed to the outsider, for instance proxy. In this way, we need to utilize the proxy cryptography. proxy cryptography is an essential cryptography primitive.

In PKI (Private Key Infrastructure), remote information trustworthiness checking convention will play out the certificate administration. At the point when the director assigns a few substances to play out the remote information trustworthiness checking, it will bring about significant overheads since the verifier will check the certificate when it checks the remote information respectability.

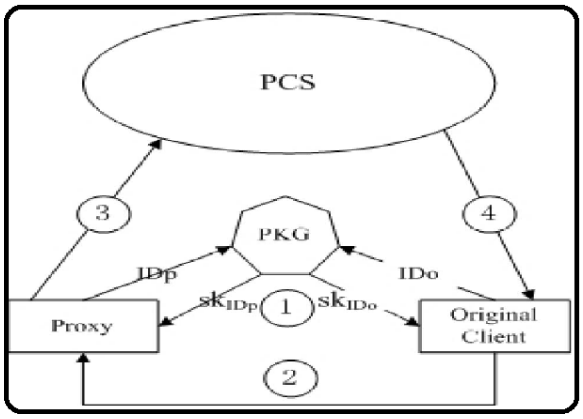


Figure 1. Proposed system

II. EXISTING AND PROPOSED SYSTEM

2.1 Existing System

In 2013, Yoon et al. proposed an ID-based proxy signature plot with message recuperation. Chen et al. proposed an proxy signature plot and an edge intermediary signature conspire from the Weil blending. By joining the proxy cryptography with encryption strategy, some proxy re-encryption plans are proposed.

Out in the open cloud, remote information honesty checking is a vital security issue. Since the customers' monstrous information is outside of their control, the customers' information might be ruined by the vindictive cloud server paying little heed to purposefully or inadvertently. Keeping in mind the end goal to address the novel security issue, some efficient models are introduced.

2.1.1 Disadvantages of Existing System

Power Consumption was expectedly more. Cloud Infrastructure was degrading the performance of the application. As every time clients' needs to directly interact with the cloud server. Key Distribution task for cloud server was a hectic job. sometimes same key can be reused for same file next time to download.

2.2. Proposed System:

In this paper cloud server totally rely on proxy for client requests.Client first interacts with Proxy server for data storage, key generation, data download etc,
To overcome drawbacks of existing system in this paper one more user plays an important role for distribution of keys throughout the application data processing called as auditor.

Crypto Proxy Identity based Data Processing (CPIDP) is our scheme where client's data gets encrypted while outsourcing from the client at proxy server.

Furthermore, proxy server will communicate with auditors for data verification and auditing task. This paper depends on the exploration consequences of proxy cryptography, character based open key cryptography and remote information uprightness checking out in the open cloud.

In open cloud, this paper concentrates on the personality based proxy arranged information transferring and remote information trustworthiness checking. By utilizing personality based open key cryptology, our proposed CPIDP convention is effective since the testament administration is wiped out. CPIDP is a novel proxy arranged information transferring and remote information trustworthiness checking model in broad daylight cloud. We give the formal framework model and security display for CPIDP convention. At that point, in light of the bilinear pairings, we planned the main solid CPIDP convention. We propose a productive CPIDP convention for secure information transferring and capacity benefit in broad daylight mists.

Bilinear pairings method makes personality based cryptography pragmatic. Our convention is based on the bilinear pairings. We initially audit the bilinear pairings**.**

2.2.1Advantages of Proposed System

Data Owners did not need to worry about security their data as crypto proxy will handle the security issues. Proxy Servers encrypts the data at client side before outsourcing by using AES Encryption algorithm High Performance can be noticed in this scheme from proxy servers.

Reliability can be achieved as it is accessible from anywhere using any device.

III. Implementation & Results

This paper depends on the exploration consequences of proxy cryptography, character based open key cryptography and remote information uprightness checking out in the open cloud.

In open cloud, this paper concentrates on the personality based proxy arranged information transferring and remote information trustworthiness checking.

We propose a productive CPIDP convention for secure information transferring and capacity benefit in broad daylight mists.

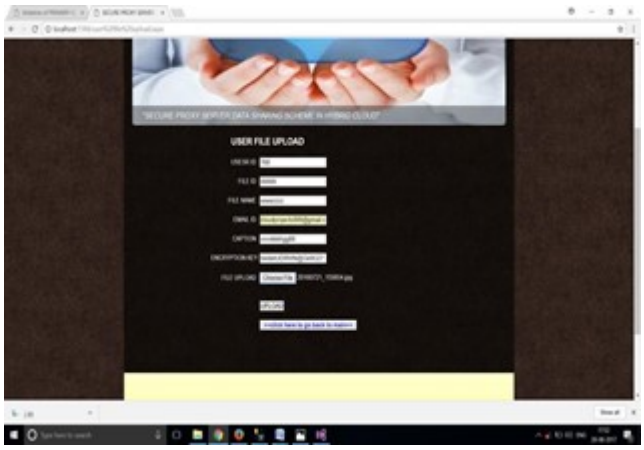
Below are some of the screen shots of our process

Output Screenshot1: User Registration page

User need to authorize himself by entering the correct details in the form given to him, in order to use the cloud service

Output Screenshot 2: User Login page

Once the registration process completes user need to login by simply entering user id and password

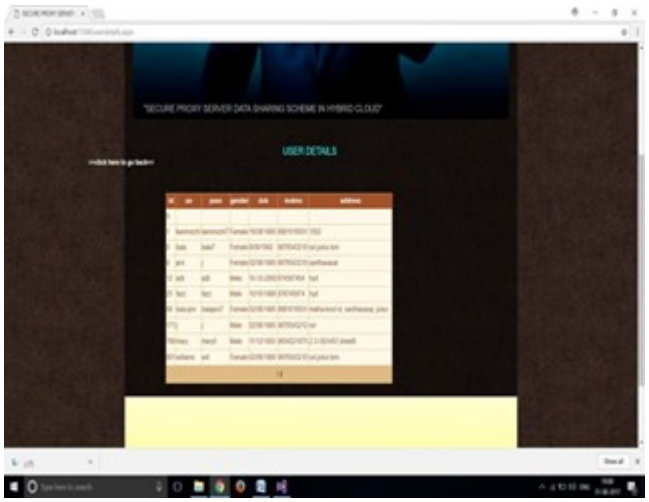


Output Screenshot 3: User File Upload page

If the user need to upload his personal file which he wants to preserve from hacking or any other security issues ,then he needs to enter some of the information related to file such as file id ,filename, size caption along with user id and email address .So that encryption key generates

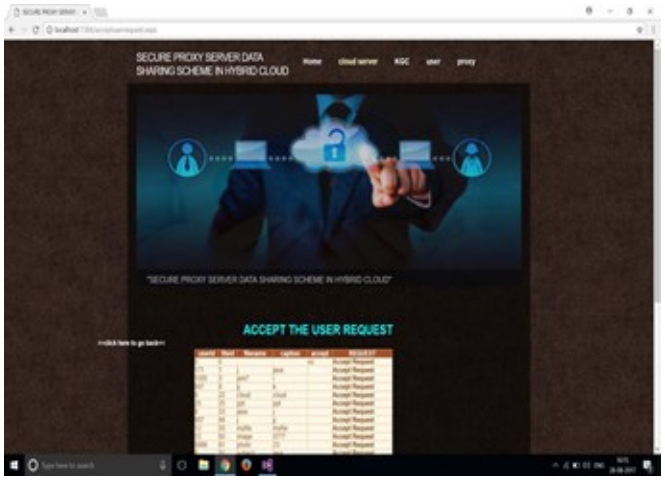
Output Screenshot 4: User file download request page

When user wants to download his own file from cloud, he need to send request to his respected file by clicking send option.



Output Screenshot 5: Proxy verifying user page

Proxy check all the details of user whether the user is authorize or not

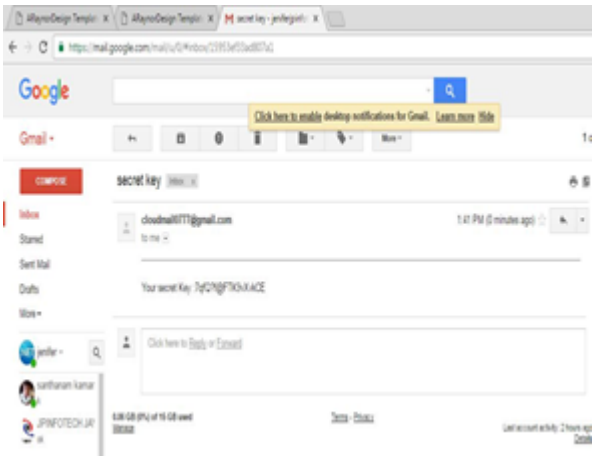


Output Screenshot 6: Accepting request page

If the user is authorize and the true owner of the file proxy accepts request

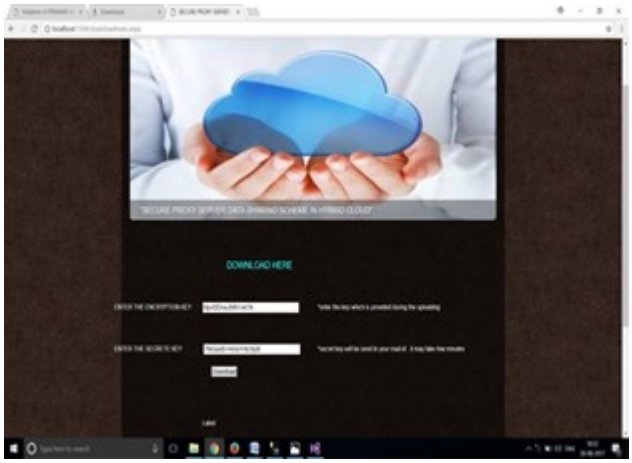
Output Screenshot 7: Generating secret key page

Key generation center(KGC) generates secrete key, which will be sent to user's mail id



Output Screenshot 8: Secret key receive page

User receive file's secret key through mail



Output Screenshot 9: keys submission page

When user request for downloading his own file, then user needs to enter file's encryption key, which was generated at upload time and a secret key which was sent to his mail

Output Screenshot 10: User file download page

If the encryption key and secret key is correctly entered, user can have his file by just clicking download option

IV. CONCLUSION

This Paper aims to provide high data security and fast performance by introducing a proxy cryptography technique. In this technique is useful for data owners at client side. It encrypts the data before outsourcing it to the cloud server and forwards information to auditor for further processing like integrity key generation dynamically. Sending integrity key to respective data owners through proxy servers. The script place CPIDP technique represent and insurance create. In clear no prosecution, the info partner mayhap study intensively relate to anybody distort waiter, the message heritor will assign the job of message processing and uploading pointing to the 3rd team, as an illustration the executor. On the alternative hand, the farfetched data soundness checking custom enjoy be active to complete misappropriate for power-limited end devices.

V. REFERENCES

[1]. J. Zhang, W. Tang, and J. Mao, "Efficient public verification proof of retrievability scheme in cloud," Cluster Comput., vol. 17, no. 4, pp. 1401-1411, 2014.

[2]. Huaqun Wang, Debiao He, and Shaohua, "Identity-Based Proxy-Oriented Data Uploading andRemote Data Integrity Checking in Public Cloud", ieee transactions on information forensics and security, vol. 11, no. 6, june 2016.3E. Zhou and Z. Li, "An improved remote data possession checking protocol in cloud storage," in Algorithms and Architectures for Parallel Processing (Lecture Notes in Computer Science), vol. 8631. Berlin, Germany: Springer-Verlag, 2014, pp. 611-617.

[3]. C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," IEEE Trans. Services Comput., vol. 5, no. 2, pp. 220-232, Apr./Jun. 2012.

[4]. P. Xu, H. Chen, D. Zou, and H. Jin, "Fine-grained and heterogeneous proxy re-encryption for secure cloud storage," Chin. Sci. Bull., vol. 59, no. 32, pp. 4201-4209, 2014.

[5]. B. Lynn, "On the implementation of pairing-based cryptosystems," Ph.D. dissertation, Dept. Comput. Sci., Stanford Univ., Stanford, CA, USA, 2008.