

A Reliable and Equitable Attribute-Based Proxy Re-encryption System for Cloud Data Sharing

Rishi N¹ and S Anu Priya²

PG Student, Department of Computer Applications¹

Assistant Professor, Department of Computer Applications²

Vels Institute of Science Technology and Advanced Studies, Pallavaram, Chennai, India

22304347@vistas.ac.in and anupriya.scs@velsuniv.ac.in

Abstract: *The widespread acceptance and quick growth of cloud computing have made data sharing easier than ever before. What is preventing widespread adoption of cloud computing, however, is how to guarantee the security of the user's data in the cloud. Safe data sharing in cloud computing can be achieved through the use of proxy re-encryption. With the use of a semi trusted cloud server, a data owner can encrypt shared data in the cloud using their own public key, converting it into an encryption meant only for authorized recipients to control access. To help us grasp this fundamental better, this paper provides a thorough and motivating overview of re-encryption of proxy servers from a variety of angles. For granular access control of shared data, Ciphertext-Policy Attribute based Aes (CP-ABE) is a possible cryptographic primitive. Each user in CP-ABE has a set of attributes, and access structures based on attributes are used to encrypt data. If and only if a user's characteristics meet the requirements of the ciphertext access structure, the user can decrypt a ciphertext. Practical applications typically call for additional requirements in addition to this fundamental one. Our research centers on the significant problem of attribute revocation, which poses a challenge for CP-ABE methods*

Keywords: Proxy Re-Encryption, Data Sharing, Security, Cloud Computing

I. INTRODUCTION

Cloud computing's quick development and widespread use have made sharing and storing data easier [1]. For illustration purposes, let's say that a government organization permits its group employees to exchange and outsource files to the public cloud. Thanks to cloud computing, team members can view shared data produced by other group members without requiring significant financial investments for the establishment and upkeep of local storage. Furthermore, as long as a group member has Internet access, they can access the cloud-stored sharing data at any time and from any location. Big data and cloud computing are now popular study areas. The concept of cloud computing can be understood as a way to combine many different types of storage and computation resources into extremely potent computation grids. The efficient operation of cloud computing is supported by a variety of cutting-edge methods. Big data mostly refers to the instantaneous development of enormous data sets anywhere, anytime, and any time. It focuses on the effective organization and processing of data. People's worries regarding data security also surface when they take use of the benefits that these new technology and services offer. Naturally, consumers want only authorized persons to have access to their confidential information. Differentiated access services, where user roles and attributes are used to establish data access policies, are also beneficial in many circumstances. It's easy to predict that as cloud computing becomes more prevalent and people, organizations, and enterprises outsource all kinds of data—including extremely sensitive data—to the cloud, security requirements and concerns will only grow more pressing.

II. LITERATURE SURVEY

[1] Title: Security Challenges for the Public Cloud. Author: Cong Wang

The greatest revolutionary development in information technology today is represented by cloud computing. The main anticipated barriers to its widespread adoption, meanwhile, are security and privacy. Here, the writers list a number of important security issues and encourage more research into security fixes for a reliable public cloud infrastructure. Public cloud computing offers numerous benefits such as scalability, flexibility, and cost-effectiveness. However, along with these advantages come significant security challenges that must be addressed to ensure the confidentiality, integrity, and availability of data and services in the cloud environment. This paper by Cong Wang explores the key security challenges faced by organizations when adopting public cloud services and discusses strategies for mitigating these challenges effectively.

[2] Title: Fuzzy Identity-Based Encryption. Author: Brent Waters

We provide Fuzzy Identity-Based Encryption, a novel form of Identity-Based Encrypting (IBE) technique. An identity is seen as a collection of descriptive features in Fuzzy IBE. If the identities ω and ω' are close to one another as determined by the "set overlap" distance metric, a fuzzy IBE method permits a private key for identity ω to decrypt the cipher text encrypted with identity ω' . Biometric identities can be encrypted using a fuzzy IBE scheme because of its error-tolerance feature, which makes it possible to use biometric identities despite the fact that they will always contain some noise when they are sampled. Fuzzy Identity-Based Encryption, or fuzzy IBE, is a cryptographic system that goes beyond identity-based encryption to address scenarios in which the recipient's identity may not be known with precision. Fuzzy identities that coincide with these attribute sets are linked to decryption keys in fuzzy identity-based encryption (Fuzzy IBE). Encrypted text is password-protected under sets of attributes. In this work, Brent Waters examines the idea of fuzzy IBE and looks at its uses, security features, and real-world applications.

[3] Title: Attribute-based encryption with verifiable outsourced decryption. Author: C Guan

Users can encrypt and decode data depending on their attributes using attribute-based encryption (ABE), a public-key based one-to-many encryption. Flexible management of encrypted data kept in the cloud via the use of access policies and assigned attributes linked to encryption keys and ciphertexts is a promising use case for ABE. The fact that decryption necessitates costly pairing operations—the quantity of which increases with access complexity—is one of the primary efficiency issues with the current ABE systems. Access control is made possible by a cryptographic approach called Attribute-Based Encryption (ABE), which takes into account user and data attributes. Hiring outside service providers to handle decryption can increase efficiency in situations where decryption processes are computationally costly, but it also creates privacy and integrity issues. The innovative method presented in this study by C. Guan combines verifiable outsourced decryption with ABE, enabling data owners to assign decryption duties while guaranteeing the integrity and confidentiality of the decrypted data. The plan, security evaluation, and actual execution of this system are presented in this work.

[4] Title: Attribute-based encryption for cloud computing access control that is verifiable and exculpable via outsourcing. Author: R Zhang

In order to accomplish both dedicated encryption and outsourced decryption in two system storage models, we present two ciphertext-policy attribute-based essential packaging mechanism (CP-AB-KEM) techniques. We also provide associated security analysis. With our schemes, the sender or the recipient only needs to do one flexible exponentiation computation because the bulk of the work is outsourced to encryption services suppliers (ESPs) or decryption service providers (DSPs). A strong cryptographic method for controlling entry in cloud computing settings is called attribute-based encryption, or ABE. However, it might be difficult to guarantee the accountability and integrity of the method for decryption when decryption processes are contracted out to outside service providers. In order to facilitate safe and responsible outsourcing of decryption, this study by R. Zhang presents a novel approach to ABE and enhances it with qualities of verifiability and exculpability. The suggested system enables data owners to assign decryption responsibilities to outside parties while guaranteeing the

accuracy of the encrypted data and offering tools for confirming the accuracy of the decryption procedure and holding violators liable.

[4] Title: attribute-based ciphertext-policy encryption: Author: J Bethencourts

It is necessary for a user to possess specific credentials or qualities in order to access data in several distributed systems. Applying trustworthy servers to handle access control and store data is currently the only way to enforce these kinds of regulations. The data's confidentiality will be jeopardized, though, if any of the servers holding the data are compromised. AB-CP-ABE, or attribute-based ciphertext-policy encryption, is a cryptographic technique that allows for fine-grained restriction of access over encrypted data by taking into account both user attributes and data owner regulations.

The idea of AB-CP-ABE is presented in this work by J. Bethencourt, along with its design concepts, security features, and real-world apps. It investigates and evaluates the benefits and drawbacks of AB-CP-ABE applications across a range of fields.

III. METHODOLOGY

To facilitate safe and adaptable data exchange in cloud contexts, AB-PRE combines Proxy Re-encryption (PRE) with Attribute-Based Encryption (ABE). Key generation is the process of creating user-specific private keys and master keys depending on attributes. In order to encrypt data in accordance with attribute-defined access regulations, encryption uses ABE. By enabling the data administrator to restore the ciphertexts for particular users, proxy re-encryption makes it easier to provide access permissions. Through the use of their private keys, authorized users can decrypt re-encrypted ciphertexts, maintaining data access control and guaranteeing secrecy. In cloud contexts, this methodology offers a strong framework for equitable and verifiable data sharing. This methodology ensures verifiable and equitable access to information in cloud environments by offering a methodical approach to AB-PRE scheme implementation. Key creation, encryption, proxy re-encryption, fairness and verifiability checks, decryption, security analysis, and real-world implementation issues are all included. Practitioners and scholars can create and implement AB-PRE schemes in practical cloud environments by using this methodology.

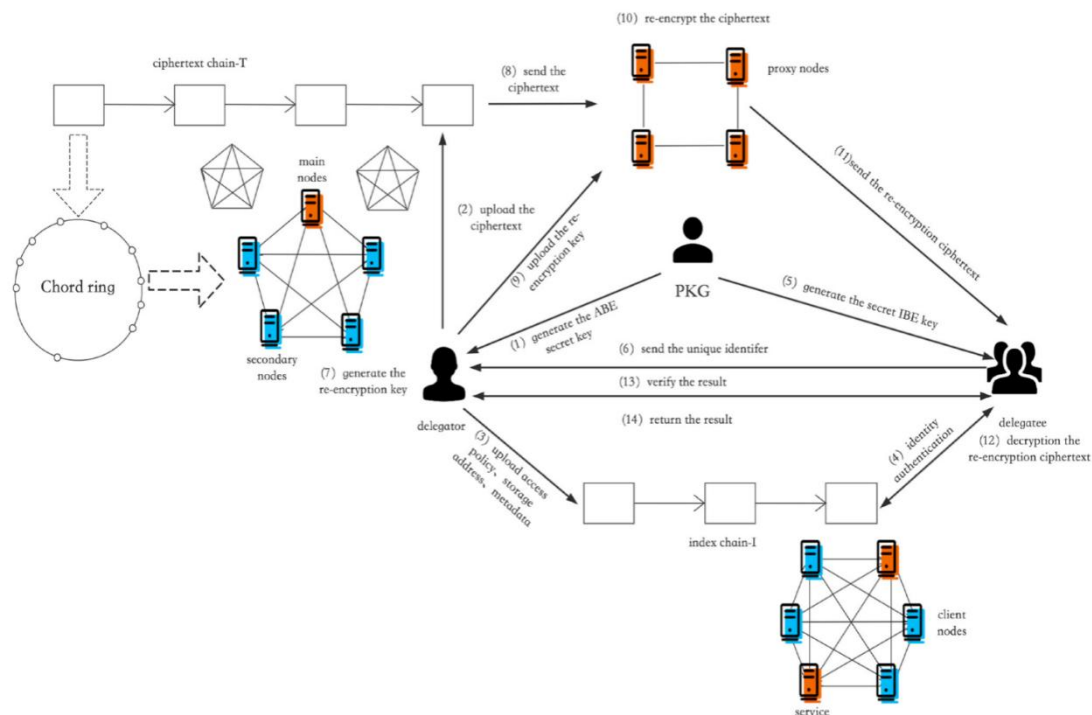


Fig.1 Proposed Approach for Proxy Re-encryption

Only when a user's credential matches the access policy can they, in a typical ABE [2] arrangement, obtain the plaintext from a ciphertext. ABE is divided into two groups: key-policy ABE (the key pair KP) [6] and ciphertext-policy ABE (CP-ABE) [5], based on how a secret key or ciphertext is created. On the other hand, KP-ABE generates a secret key with an attribute set and a ciphertext with an access policy, unlike CP123 ABE. Since the authority determines who is an authorized user, KP-ABE is appropriate in situations like those shown in the pay-tv setup. CP-ABE, on the other hand, works well with cloud sharing systems because the user may designate who has access. After their work, questions about the effectiveness, security, and anonymity of ABE have been addressed.

Security and functionality comparison:

We compared the suggested scheme with other schemes with regard to fairness, security, verifiability, and access structure. The work in a key policy environment and our construction work at the ciphertext of the policy setting are summarized in Table I. Additionally, and accomplish the semantic security, and our construction accomplishes the CCA security. But only our construction satisfies the fairness and verifiability requirements. Verifiable and equitable data sharing capabilities are provided in cloud environments via the AB-PRE scheme, which offers a special blend of security and usefulness. In contrast to conventional encryption methods and access control techniques, AB-PRE provides versatility and specific control of access based on user attributes while addressing concerns related to secrecy, integrity, verifiability, and fairness. However, based on implementation-related aspects, its performance might change. Selecting the right data sharing method for a given cloud application requires careful consideration of the negotiations regarding security, efficiency and performance.

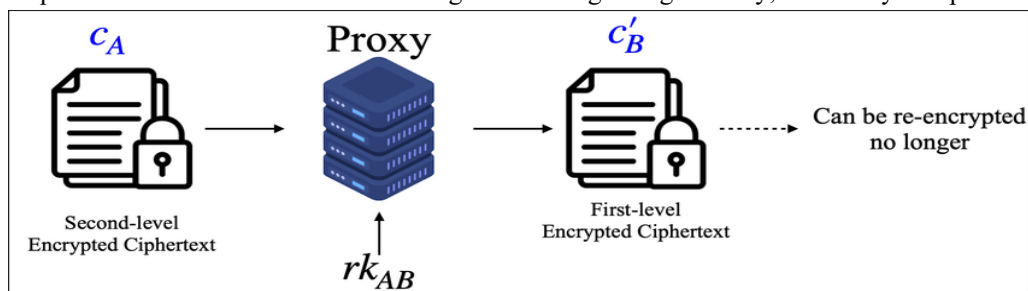


Fig. 2 Encryption level cloud server

Performance evaluation / Algorithm

(i) Log encryption can be accomplished by attribute-based encryption, or ABE. Rather than encrypting every section of a log using all of the recipients' keys, the log can only be encrypted using attributes that correspond to the attributes of the receivers.

(ii) We implemented the suggested VF-CP-ABPRE scheme in order to assess its computational cost, and we contrasted it with the attribute-based data sharing schemes based on ciphertext policy and key policy. For pairing calculation, we employ a Java cryptography pack in our implementation, which is built using a C library for pairing-based cryptography. The combined order is 160 bits, and we employ the $Y^2 = X^3 + X$ oval curve (type A). The hash functions H 1 and H 2 in our method are SHA-256. For this experiment, we used a laptop with the following specifications: CPU: Intel i5-8520U @1.60GHZ 1.80GHZ, RAM: 8G. Additionally, the laptop operates.

IV. EXPERIMENTAL RESULTS

Various Our plan takes into account data sharing application scenarios where data is password-protected and kept on servers that are only partially trustworthy. In this system, upon the occurrence of an attribute revocation event, the authority creates a proxy re-key. Following transmission of the proxy re-keys, the proxy servers re-encrypt the ciphertexts that are already stored on them and, if needed, update the user secret key components. Our method considers only one revocation event for ease of description. It is anticipated that carrying out these actions repeatedly will handle multiple revocation occurrences. Proxy servers will experience issues with efficiency in

practice as a result of having to re-encrypt ciphertexts saved upon each revocation event, even though this assumption is handy for theoretical study of the scheme. In real-world situations, users might not have noticed all of the revocation events before returning to the servers. We suggest allowing proxy servers to respond to revocation occurrences in an aggregative manner in order to effectively handle attribute revocation, which further facilitates lazy re-encryption. Proxy servers maintain a duplicate of a table with proxy re-keys of past events for this reason. As the size of the access policy increases, the time comparison in shows that our scheme's Claim verification time remains substantially lower than that of competing schemes. While the re-encryption operation's execution time increases linearly with the access policy, it is still significantly longer than it is in our method. This is because our technique only requires three computations of the hash function and three exponents in group G for the Claim process to function. With an increasing scope of the access policy, computing cost remains constant.

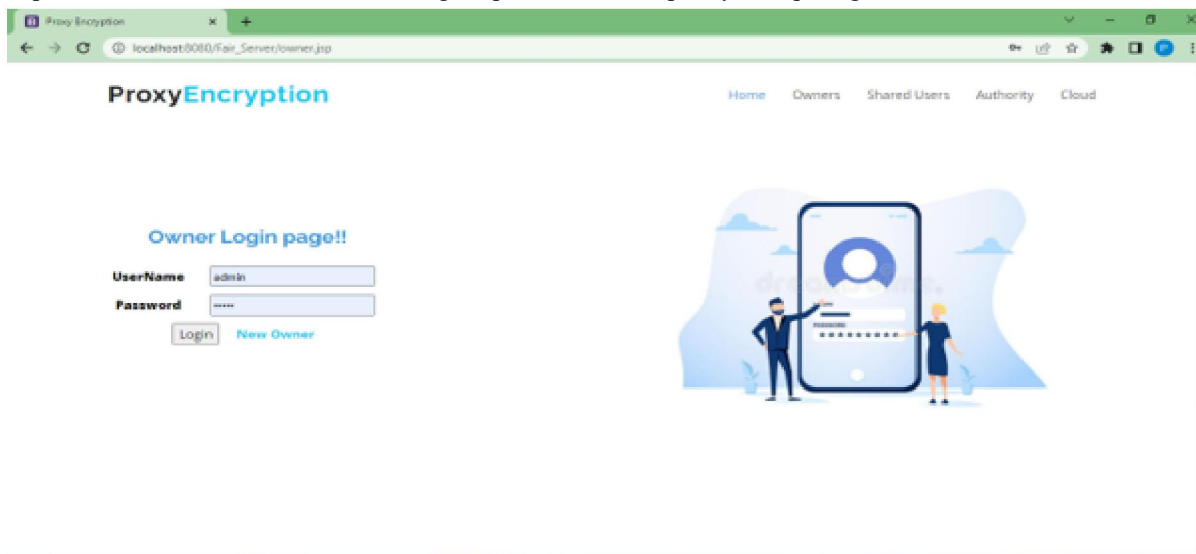


Fig. 3 Homepage

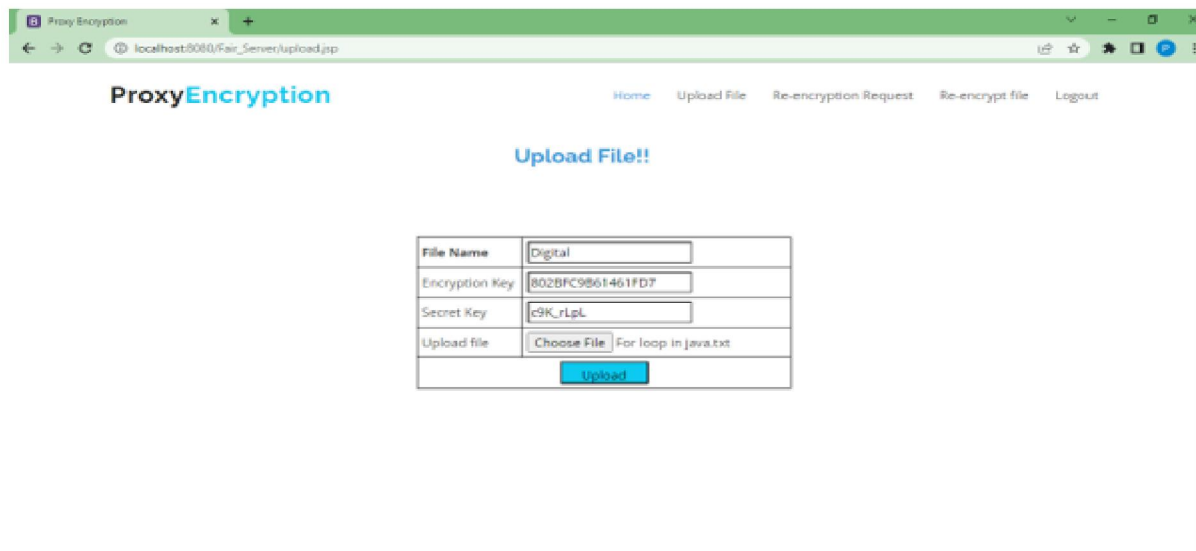
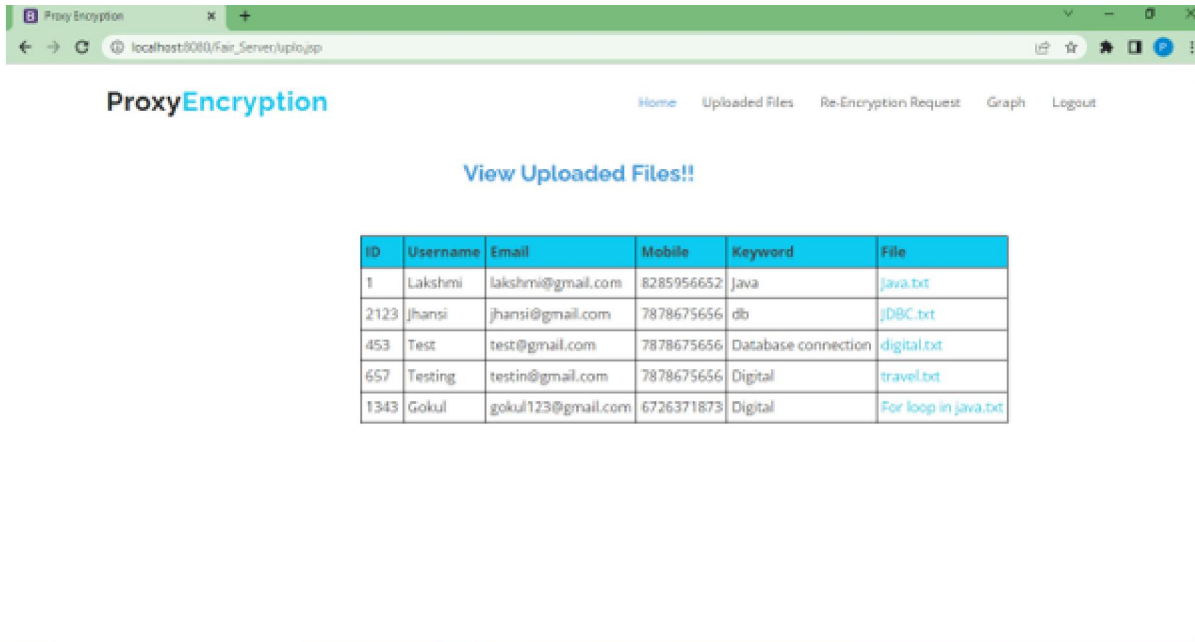


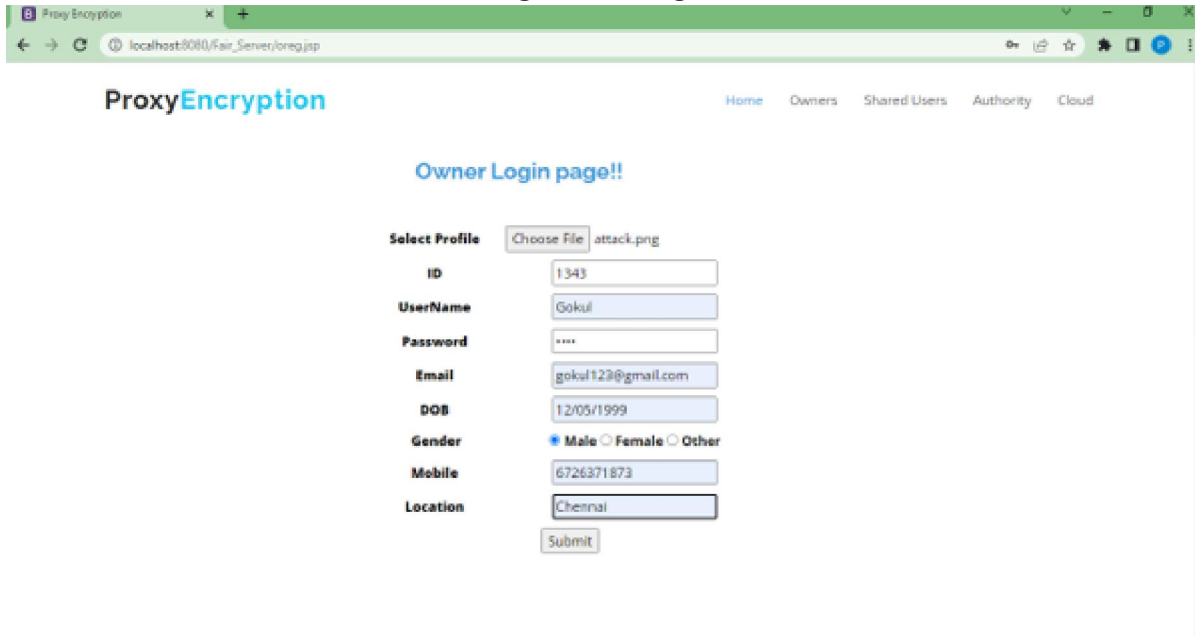
Fig.4 Uploading Data's



The screenshot shows a web browser window with the URL `localhost:8080/Fair_Server/upto.jsp`. The page title is "ProxyEncryption". The navigation bar includes links for Home, Uploaded Files, Re-Encryption Request, Graph, and Logout. The main heading is "View Uploaded Files!!". Below it is a table with the following data:

ID	Username	Email	Mobile	Keyword	File
1	Lakshmi	lakshmi@gmail.com	8285956652	Java	java.txt
2123	Jhansi	jhansi@gmail.com	7878675656	db	jDBC.txt
453	Test	test@gmail.com	7878675656	Database connection	digital.txt
657	Testing	testin@gmail.com	7878675656	Digital	travel.txt
1343	Gokul	gokul123@gmail.com	6726371873	Digital	For loop in java.txt

Fig.5 Cloud Login



The screenshot shows a web browser window with the URL `localhost:8080/Fair_Server/oreg.jsp`. The page title is "ProxyEncryption". The navigation bar includes links for Home, Owners, Shared Users, Authority, and Cloud. The main heading is "Owner Login page!!". Below it is a form with the following fields:

Select Profile: attack.png

ID:

UserName:

Password:

Email:

DOB:

Gender: ☒ Male ☐ Female ☐ Other

Mobile:

Location:

Fig.6 Owner Register page

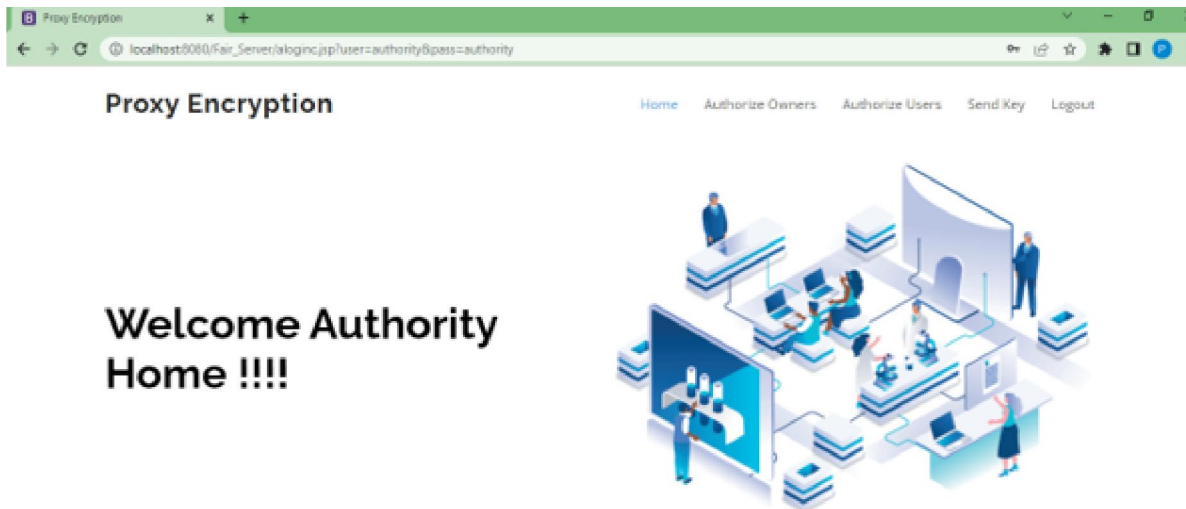


Fig. 7 Authority Login

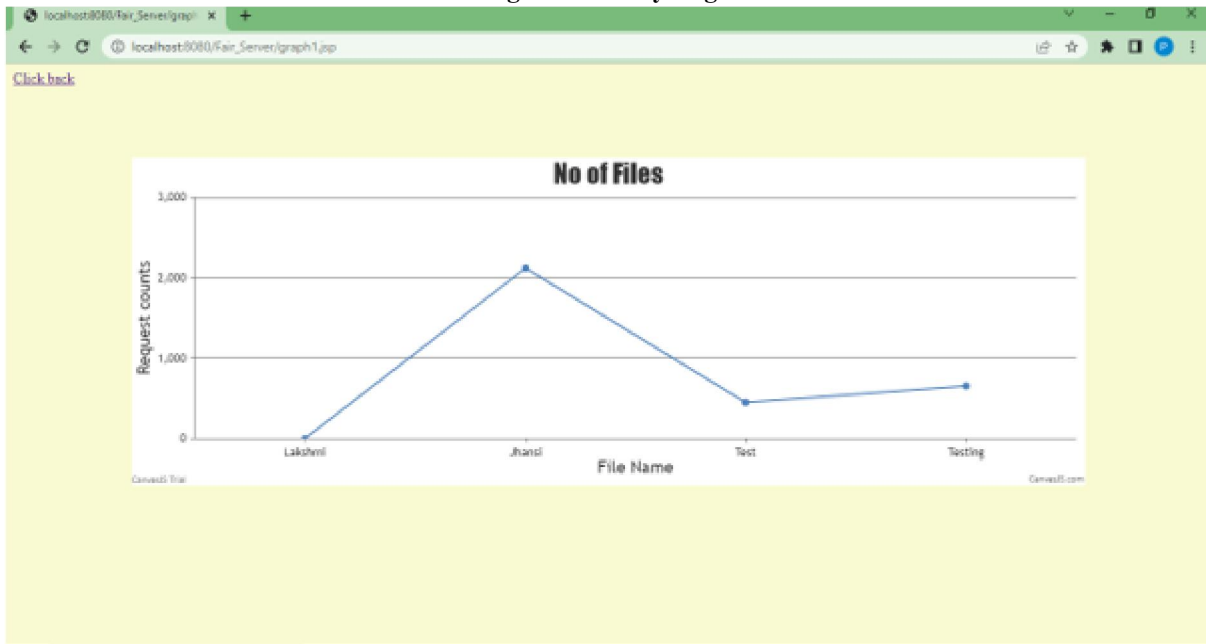


Fig.8 Graph

V. CONCLUSION

In addition to introducing the notion of viable and fair ciphertext-policy attribute-based proxy re-encryption (VF-CP-ABPRE), this work develops the verifiability and fairness safety needs for attribute-based exchange of information in clouds. An additional user can confirm that the re-encrypted ciphertext is legitimate thanks to the approach. Additionally, if the cloud has really supplied an accurate re-encrypted ciphertext, a shared user is unable to maliciously accuse the cloud provider. The semantic security, verifiability, and fairness of our VF-CP-ABPRE scheme have also been demonstrated in our security model. We also carried out an evaluation of our suggested We tackled the crucial problem of attribute revocation in systems that rely on attributes. Specifically, we examined real-world application

scenarios with semi trustable proxy servers available and suggested an attribute revocation-supporting approach. Our suggested system has the desirable feature of minimally taxing authority at attribute revocation situations. We were able to accomplish this by integrating the proxy re-encryption method with CP-ABE in a novel way, which gave the authority the ability to assign the majority of onerous work to proxy servers. We demonstrate the provability of our proposed approach against selected ciphertext attacks. Furthermore, we demonstrated how our approach may be applied to the KP- A BE scheme. Integrating our architecture with a secure computation method to ensure the integrity of proxy servers is an intriguing area for future research.

REFERENCES

- [1] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2018.
- [2] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in International Conference on Theory and Applications of Cryptographic Techniques, 2005, pp. 457–473.
- [3] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Transactions on information forensics and security, vol. 8, no. 8, pp. 1343–1354, 2017.
- [4] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-Policy Attribute-Based Encryption. In Proc. of SP'07, Washington, DC, USA, 2017.
- [5] M. Blaze, G. Bleumer, and M. Strauss. Divertible Protocols and Atomic Proxy Cryptography. In Proc. of EUROCRYPT '98, Espoo, Finland, 2018.
- [6] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, et al., "A view of cloud computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010.
- [7] K. Popovic and Z. Hocenski, "Cloud computing security issues and challenges," in 33rd International Convention on Information and Communication Technology, Electronics and Microelectronics. IEEE, 2010, pp. 344–349.
- [8] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, no. 1, pp. 69–73, 2012.
- [9] J. Herranz, F. Laguillaumie, and C. Rafols, "Constant size ciphertexts in threshold attribute-based encryption," in International Workshop on Public Key Cryptography. Springer, 2010, pp. 19–34.
- [10] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. De Panafieu, and C. Rafols, "Attribute-based encryption schemes with constant-size.