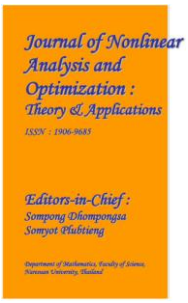
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1, No.15 : 2024
ISSN : **1906-9685**



COMBINING DATA OWNER SIDE AND CLOUD SIDE ACCESS CONTROL FOR ENCRYPTED CLOUD STORAGE

A. DURGA DEVI [1], K. Venkata Parvathi,

[1]**Assistant professor , PG DEPT,** Dantuluri Narayana Raju College**, Bhimavaram, Andharapradesh**
Email: - adurgadevi760@gmail.com
[2]**PG Student of PG, Dantuluri** Narayana Raju College**, Bhimavaram, Andharapradesh**
Email: - venkataparvathik@gmail.com

ABSTRACT

People endorse the great power of cloud computing, but cannot fully trust the cloud providers to host privacy-sensitive data, due to the absence of user-to-cloud controllability. To ensure confidentiality, data owners outsource encrypted data instead of plaintexts. To share the encrypted files with other users, Ciphertext-Policy Attribute-based Encryption (CP-ABE) can be utilized to conduct fine-grained and owner-centric access control. But this does not sufficiently become secure against other attacks. Many previous schemes did not grant the cloud provider the capability to verify whether a downloader can decrypt. Therefore, these files should be available to everyone accessible to the cloud storage. A malicious attacker can download thousands of files to launch Economic Denial of Sustainability (EDoS) attacks, which will largely consume the cloud resource. we propose a solution to secure encrypted cloud storages from EDoS attacks and provide resource consumption accountability. It uses CP-ABE schemes in a black-box manner and complies with arbitrary access policy of CP-ABE.

1 INTRODUCTION

Cloud storage has many benefits, such as always-online, pay-as-you-go, and cheap [1]. During these years, more data are outsourced to public cloud for persistent storage, including personal and business documents. It brings a security concern to data owners [2]– [4]: the public cloud is not trusted, and the outsourced data should not be leaked to the cloud provider without the permission from data owners.

Many storage systems use server-dominated access control, like password-based [5] and certificate-based authentication [6]. They overly trust the cloud provider to protect their sensitive data. The cloud providers and their employees can read any document regardless of data owners'

access policy. Besides, the cloud provider can exaggerate the resource consumption of the file storage and charge the payers more without providing verifiable records [2], [7], [8], since we lack a system for verifiable computation of the resource usage.

Literature Survey

Generalized digital certificate for user authentication and key establishment for secure communications

L. Harn and J. Ren

Public-key digital certificate has been widely used in public-key infrastructure (PKI) to provide user public key authentication. However, the public-key digital certificate itself cannot be used as a security factor to authenticate user. In this paper, we propose the concept of generalized digital certificate (GDC) that can be used to provide user authentication and key agreement. A GDC contains user's public information, such as the information of user's digital driver's license, the information of a digital birth certificate, etc., and a digital signature of the public information signed by a trusted certificate authority (CA). However, the GDC does not contain any user's public key. Since the user does not have any private and public key pair, key management in using GDC is much simpler than using public-key digital certificate. The digital signature of the GDC is used as a secret token of each user that will never be revealed to any verifier. Instead, the owner proves to the verifier that he has the knowledge of the signature by responding to the verifier's challenge. Based on this concept, we propose both discrete logarithm (DL)-based and integer factoring (IF)-based protocols that can achieve user authentication and secret key establishment.

3 IMPLEMENTATION STUDY

EXISTING SYSTEM:

Cloud Computing allow users to store or access data from anywhere and anytime with cheap cost. All data storage at cloud side will be at security risk due to unavailable control of data owner on store data. To provide security to data many data security algorithms are introduce and the most famous one is CP-ABE (Cipher Policy Attribute Based Encryption). In this data owner can encrypt data by specifying attributes of those users who can access data and the CP-ABE will generate encryption public and private keys by using those attributes and then encrypt and upload data to cloud. Any user with access control can request file from the cloud and then download that file and if user has permission in his attributes then file will be decrypted otherwise file will not be decrypted.

Disadvantages:

- Public Cloud is not trusted
- Data leakage
- Encryption is not sufficient

Proposed System & alogirtham

To avoid author has introduce concept called Combining Data Owner & Cloud Side Access Control. In this technique while uploading file user will generate secret data and encrypt that secret data with bloom filter algorithm and then encrypt file data with CP-ABE and then upload encrypted file with secret data and bloom filter data to cloud for storage. If any user wants to download file then cloud will ask secret data from user and then encrypt that data with bloom filter and check existing data owner bloom filter with user bloom filter and if match found then only cloud send download file to user. By applying secret data bloom filter match author has prevented EDoS attack.

4.1 Advantages:

- Owner-side access control in encrypted
- Secure against malicious data users
- More Secure

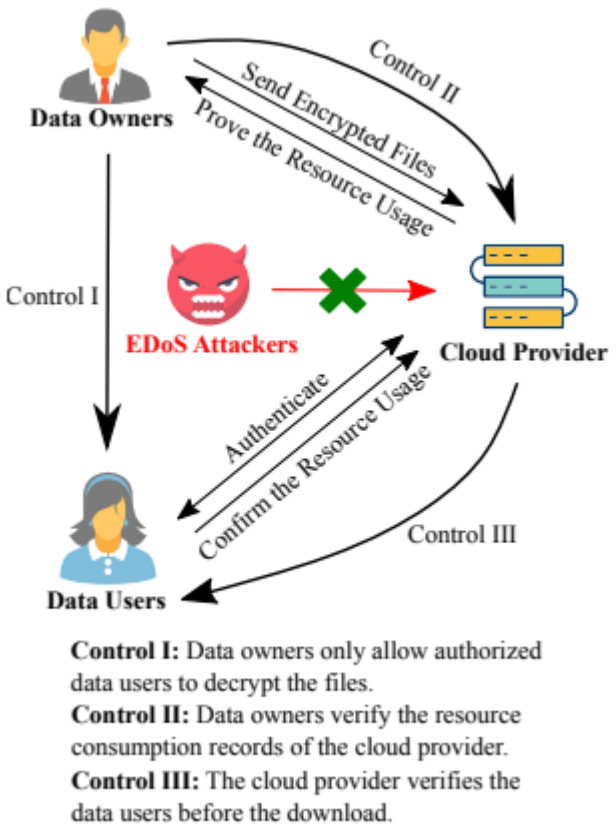


Fig:3.1 System Architecture

IMPLEMENTATION

Modules

MODULE DESCRIPTION

MODULES

Data Owner:

Data User:

Cloud Provider:

DESCSRIPTION:

Data Owner: data owner will upload file and then using CP-ABE define access control and then encrypt data and then outsource encrypted data with secret key data for user verification. Sometime cloud may cheat customers by saying customer has consume this many resource and the author is saying big companies may not do that but still to prevent cloud from fraud usage cost author has provided customer an option to verify resource consumption. By using this option data owner can request cloud to provide details about his data usage or download.

Data User: this is the user of data which request cloud for file download and before download cloud will ask user for verification by entering secret data obtained from data owner. All data owner shares their secret data with their data users.

Cloud Provider: This is a cloud server which store user data and perform user verification and provide resource consumption details to data owners.

5 RESULTS AND DISCUSSION

Home Page:

Fig: 5.1

Data User Login:

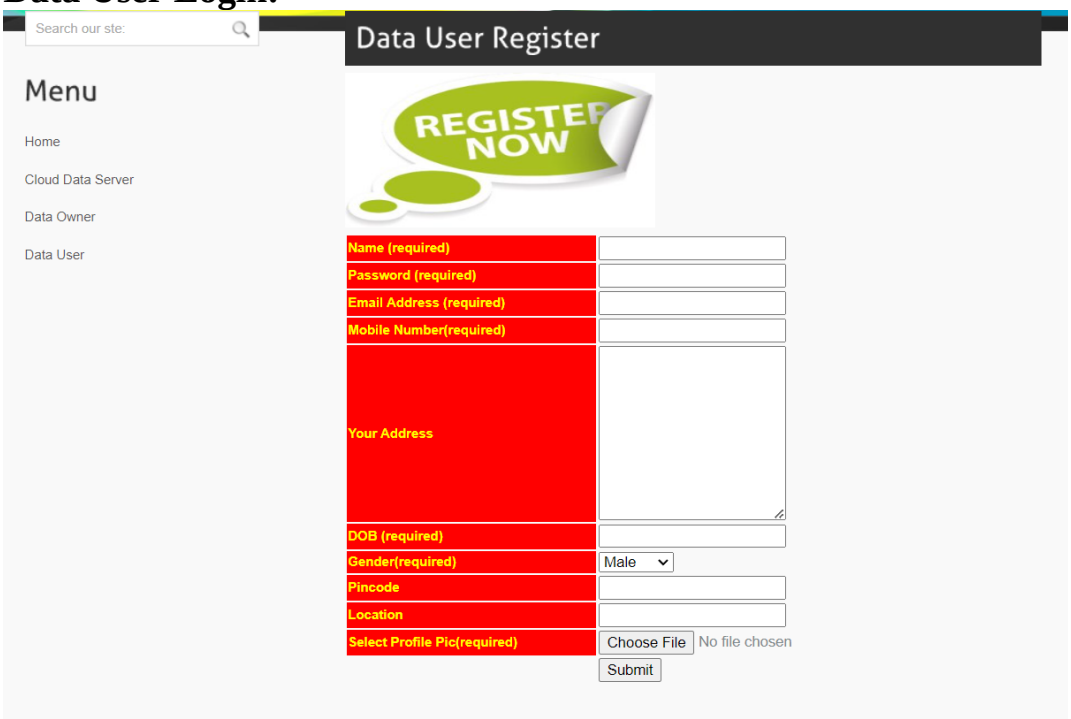


Fig: 5.2

Data owner Login:

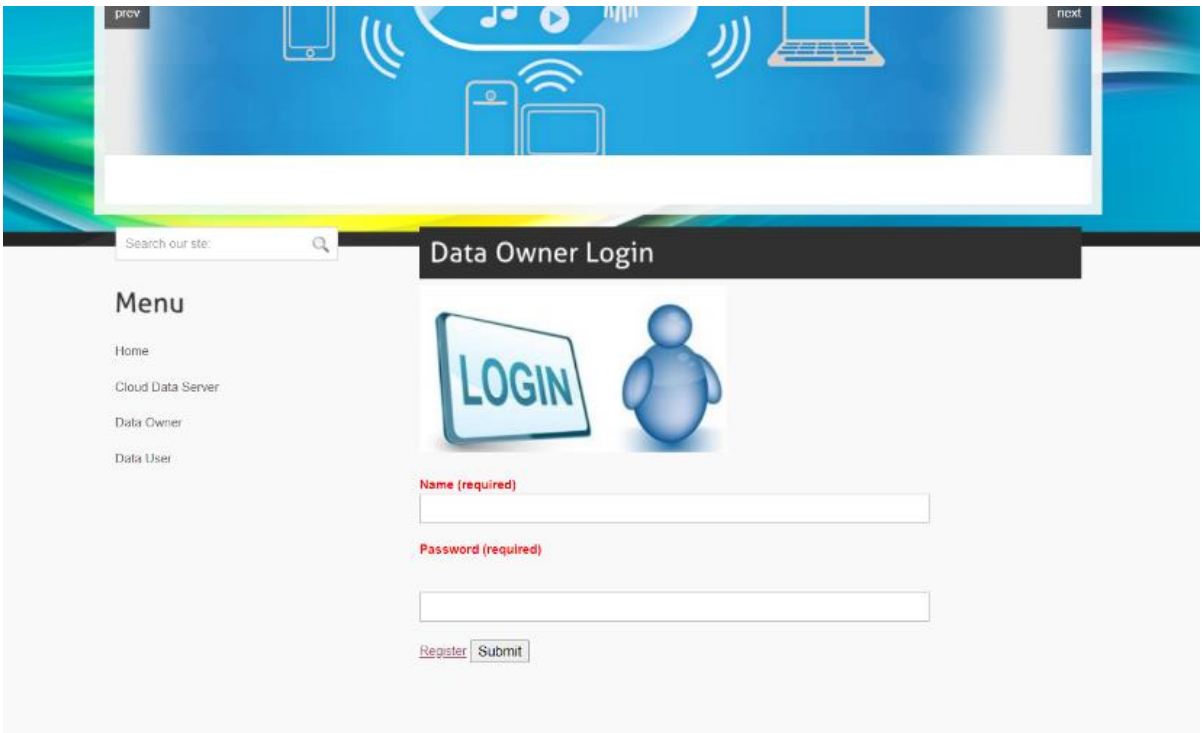


Fig: 5.3

Cloud Server Main:

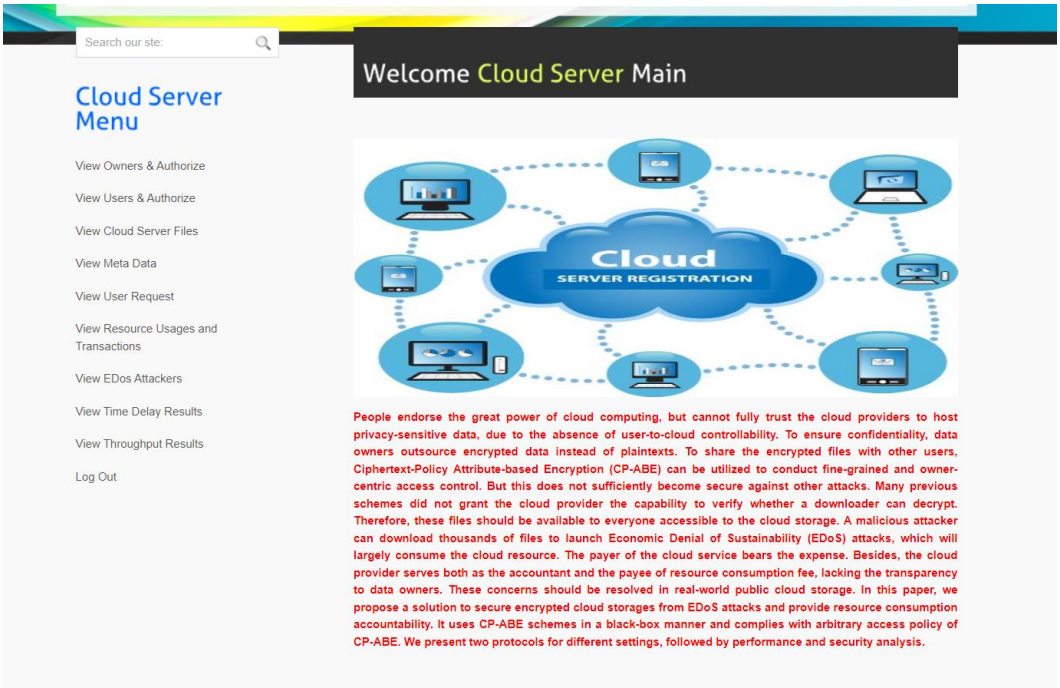


Fig: 5.4

Upload File:

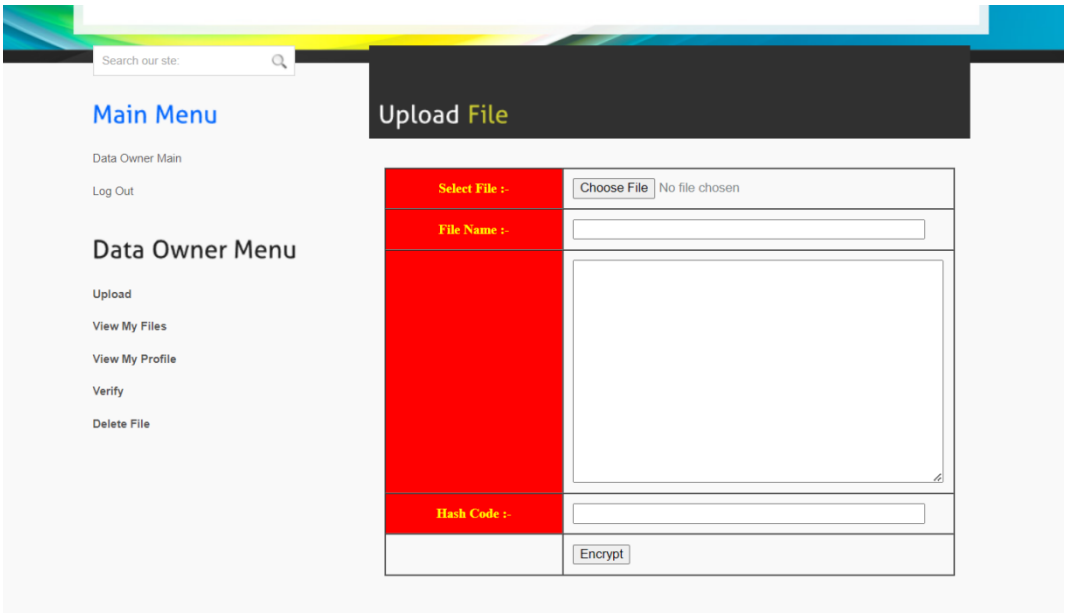


Fig: 5.5

Upload file and providing hash code:

Fig: 5.6

View data time delay result:

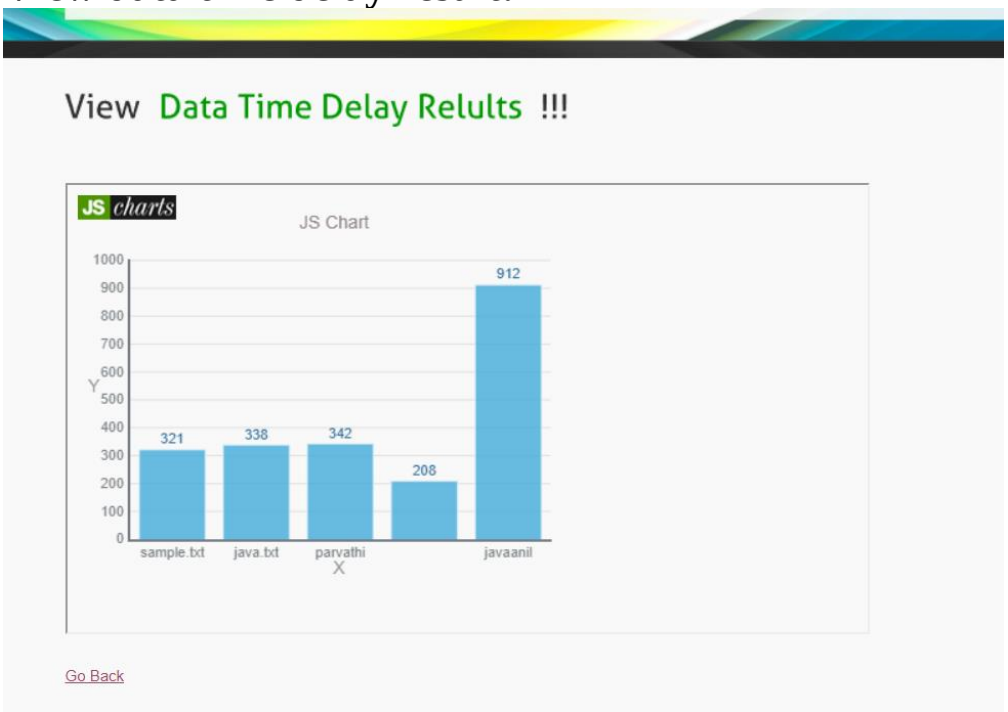


Fig: 5.7

View data throughput results:

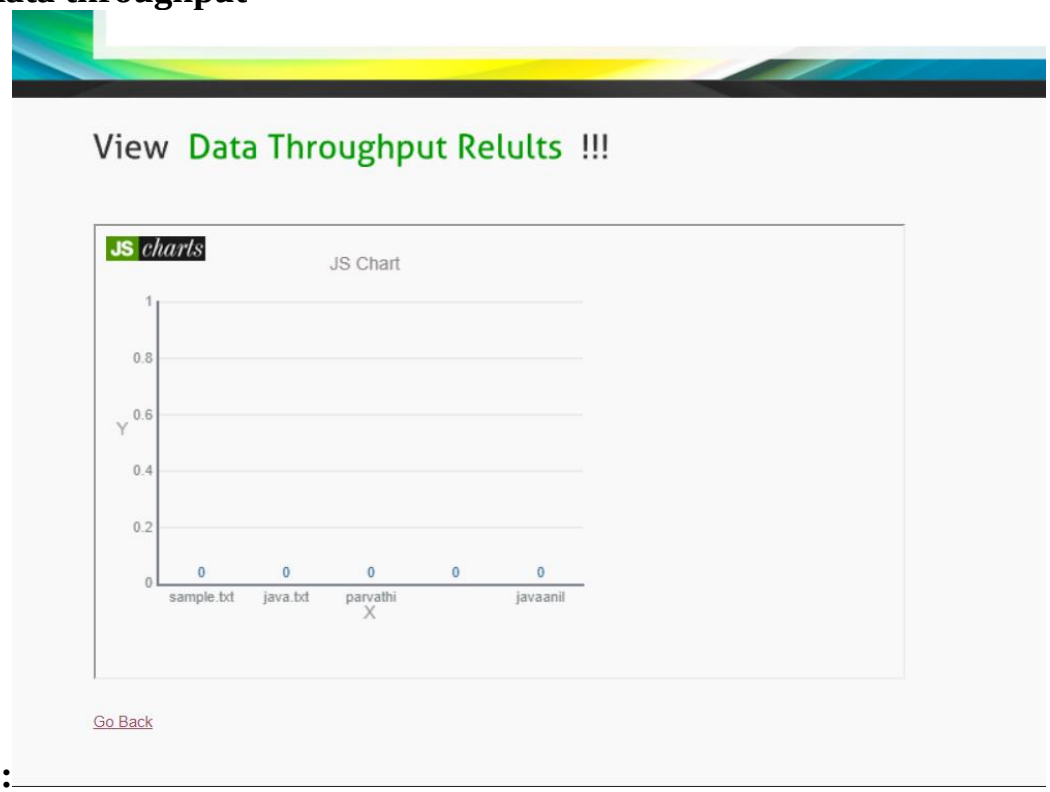


Fig: 5.8

Verify file:

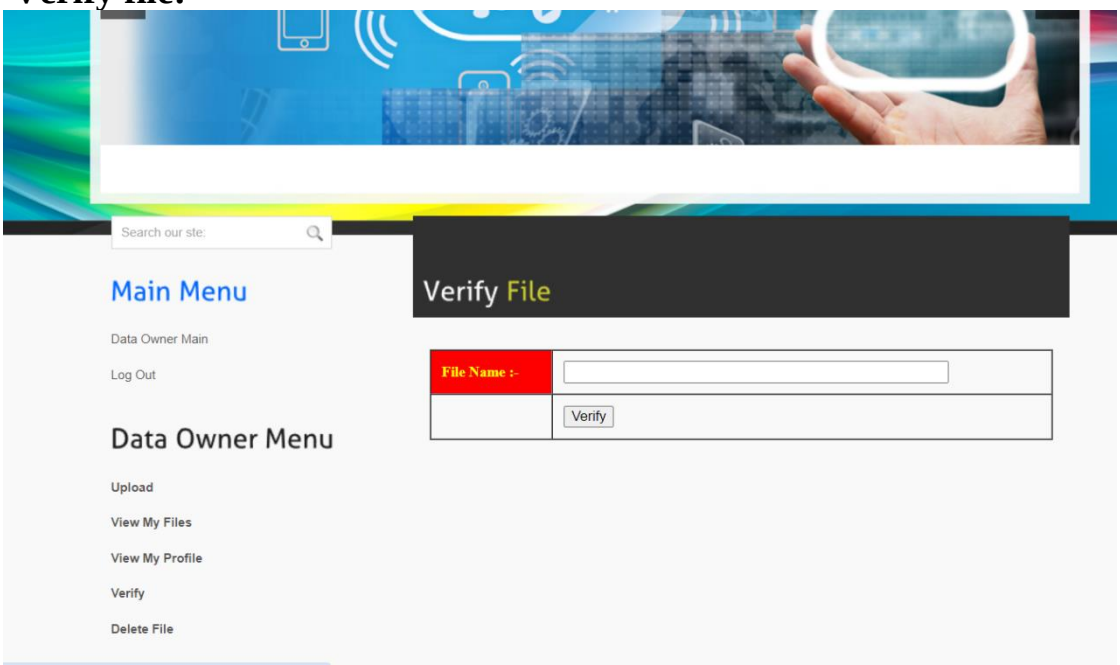


Fig: 5.9

View myfiles:

View My File !!!

Owner Name	FileName	Hash Code	Secret Key	Date
anil	sample.txt	2fcded1c7bef8b7e35a144801753b1c1c540f079	[B@1140db	16/05/2024 16:05:09
anil	java.txt	-29de6fa64a17532bec490d1cf723e7a3996793c9	[B@118317f	16/05/2024 16:10:50
anil	parvathi	2015f82662712d3ab04d5c7148eac96cce103f6c	[B@1931579	10/06/2024 12:06:00
anil		4c7f1b0a072fee669cfff1f1b59881726df405a6	[B@ca6cea	10/06/2024 14:36:36

Go Back

Fig: 5.10

View my details:

View My Details

Owner Image	Owner Name	E-Mail	Mobile	Address	DOB	Location	Status
	anil	info.hmies@gmail.com	9347225321	vskp	11-may-1999	vskp	Authorized

Go Back

Fig: 5.11

Delete files:

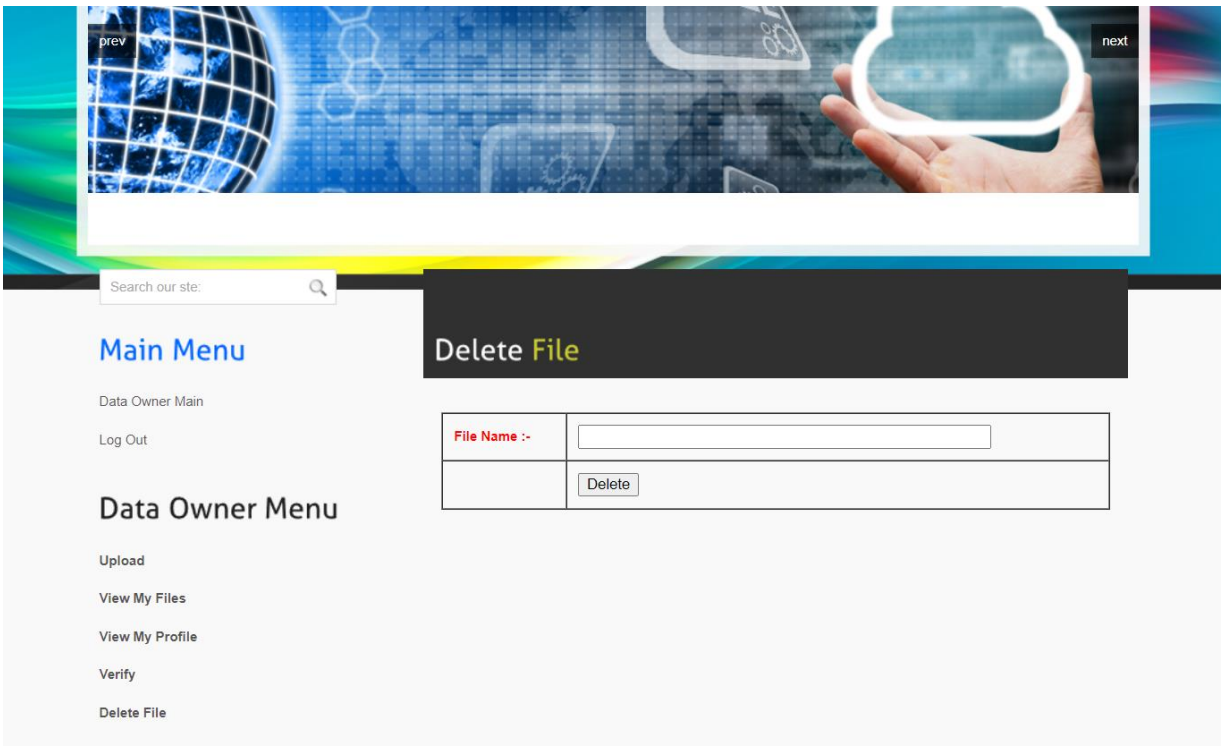


Fig: 5.12

View data user & set policy:

Fig: 5.13

Data user login:

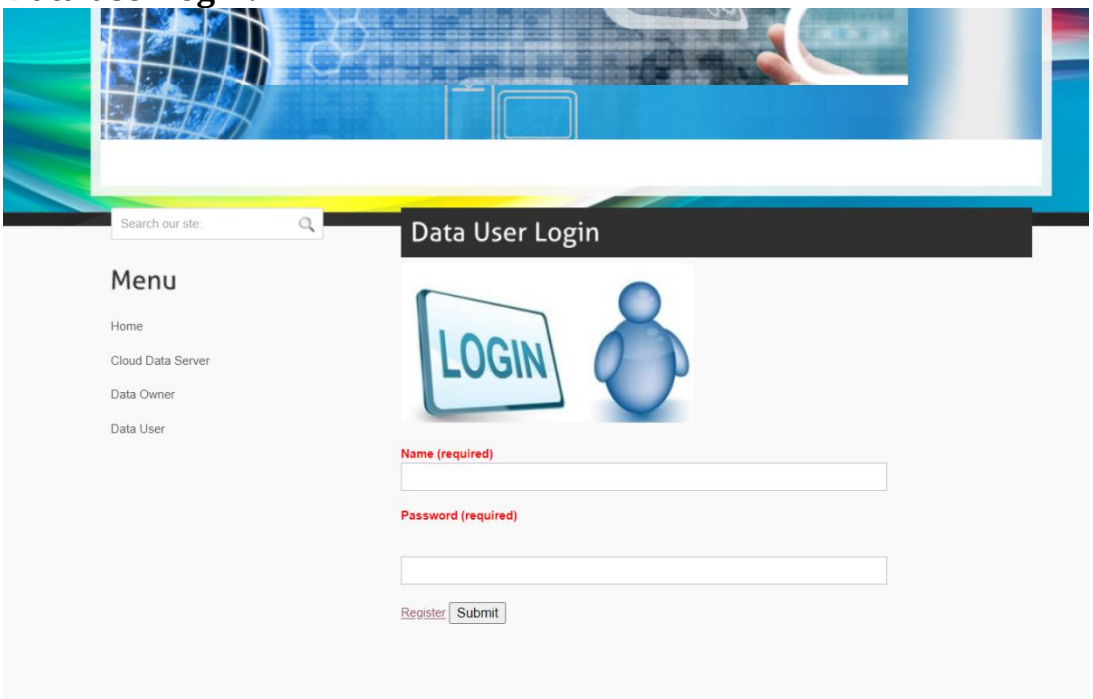


Fig: 5.14

Data user main:

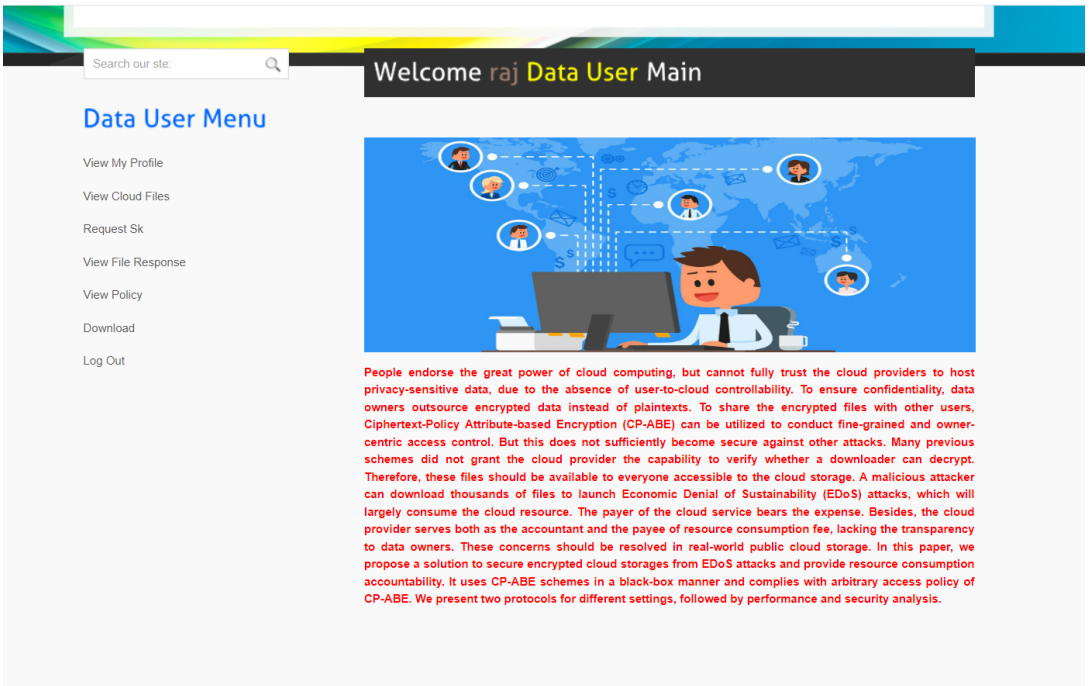


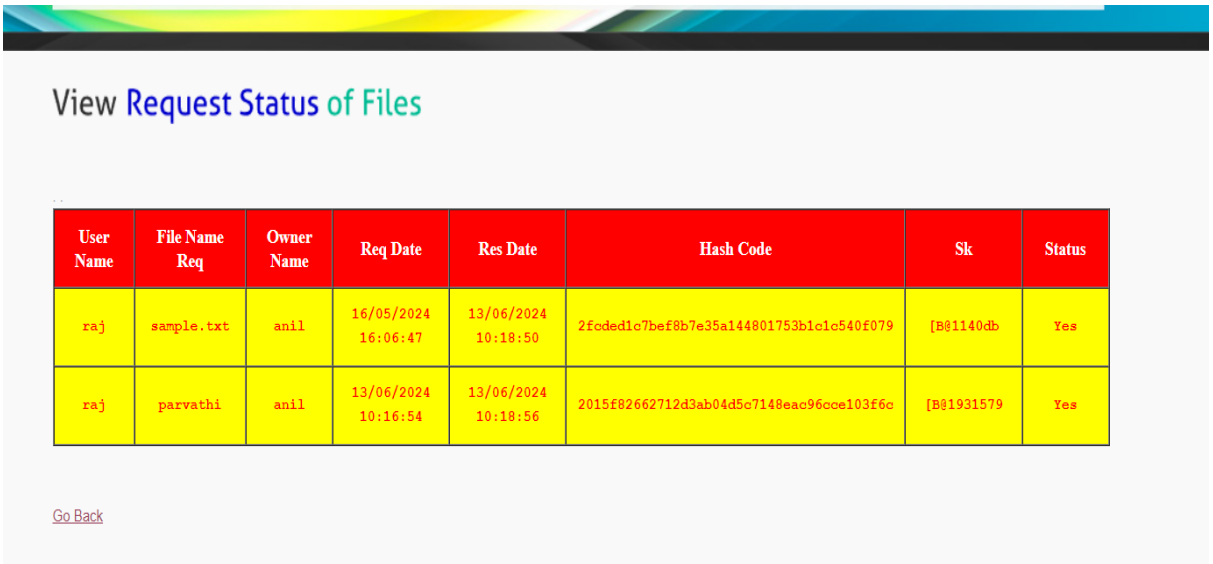
Fig: 5.15

Data owner view my file:

Owner Name	FileName	Hash Code	Secret Key	Date
anil	sample.txt	2fcded1c7bef8b7e35a144801753b1c1c540f079	[B@1140db	16/05/2024 16:05:09
anil	java.txt	-29de6fa64a17532bec490d1cf723e7a3996793c9	[B@118317f	16/05/2024 16:10:50
anil	parvathi	2015f82662712d3ab04d5c7148eac96cce103f6c	[B@1931579	10/06/2024 12:06:00
anil		4c7f1b0a072fee669cfff1f1b59881726df405a6	[B@ca6cea	10/06/2024 14:36:36

Fig: 5.16

View request status of files:



User Name	File Name Req	Owner Name	Req Date	Res Date	Hash Code	Sk	Status
raj	sample.txt	anil	16/05/2024 16:06:47	13/06/2024 10:18:50	2fcded1c7bef8b7e35a144801753b1c1c540f079	[B@1140db	Yes
raj	parvathi	anil	13/06/2024 10:16:54	13/06/2024 10:18:56	2015f82662712d3ab04d5c7148eac96cce103f6c	[B@1931579	Yes

Fig: 5.17

Download files:

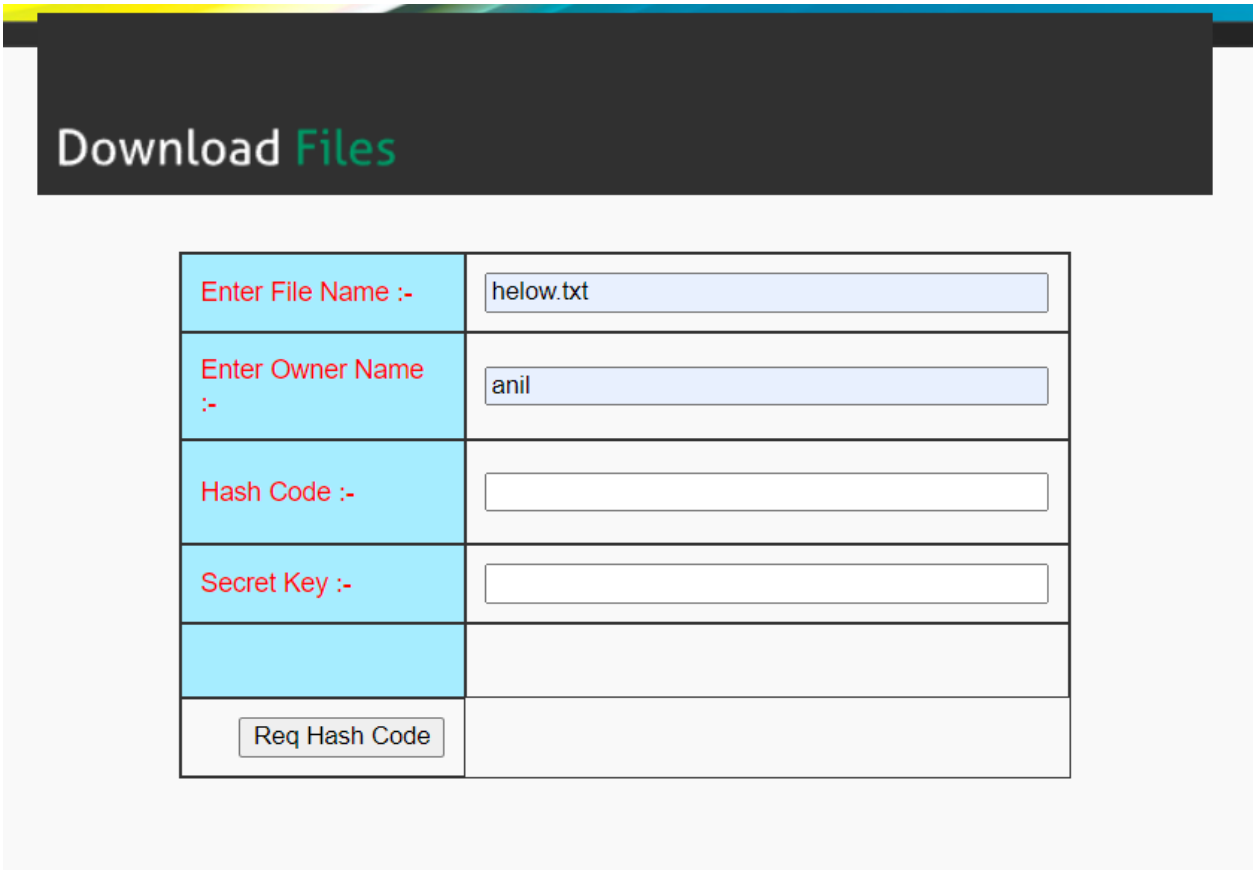


Fig: 5.18

View data owner & authorize:

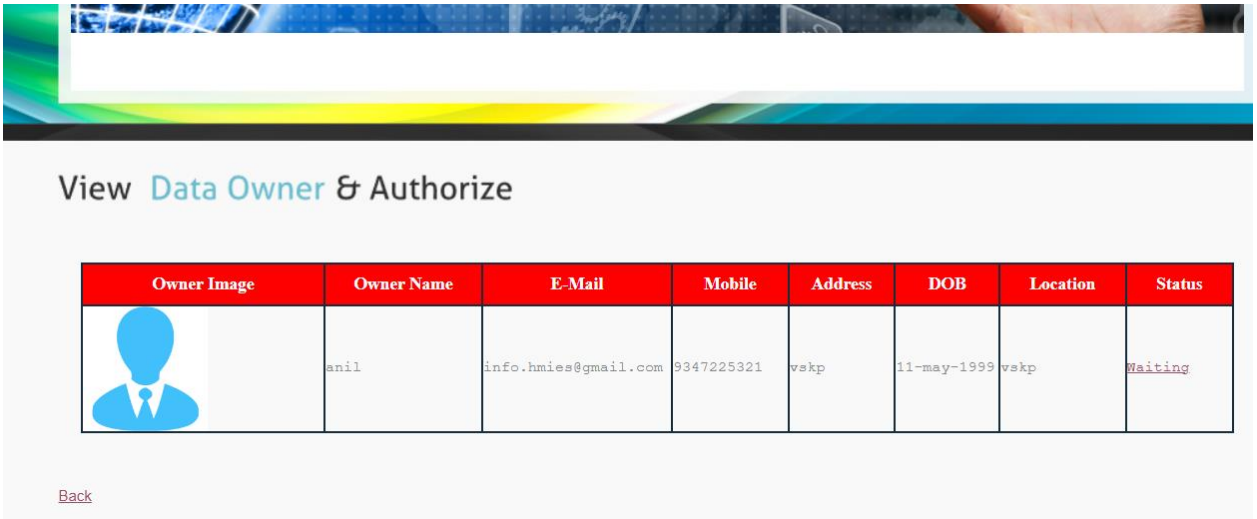


Fig: 5.19

Download files:

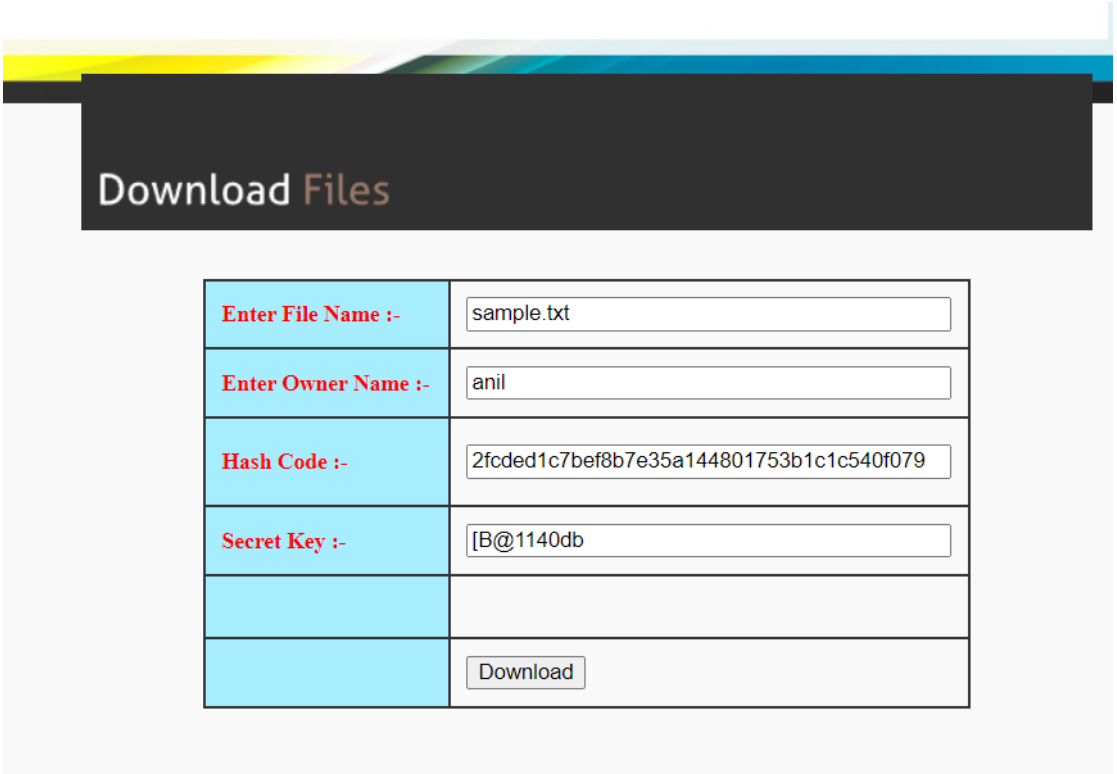


Fig: 5.19

Download files:

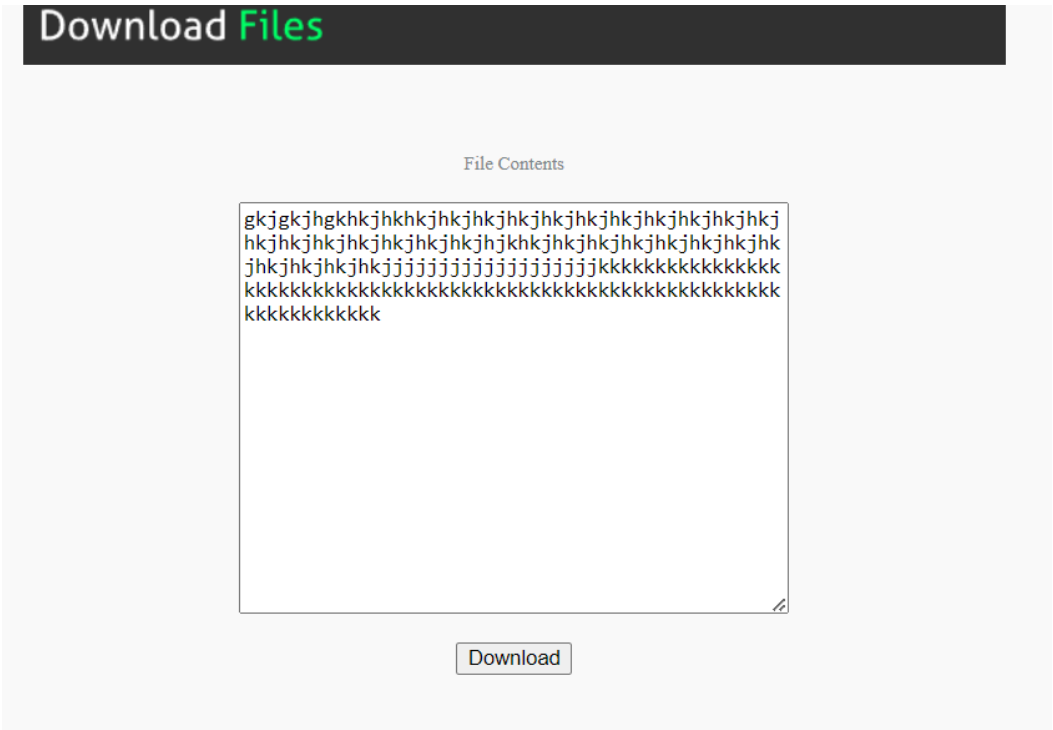


Fig: 5.20

6. CONCLUSION AND FUTURE WORK

CONCLUSION

In this paper, we propose a combined the cloud-side and data owner-side access control in encrypted cloud storage, which is resistant to DDoS/EDoS attacks and provides resource consumption accounting. Our system supports arbitrary CP-ABE constructions. The construction is secure against malicious data users and a covert cloud provider. We relax the security requirement of the cloud provider to covert adversaries, which is a more practical and relaxed notion than that with semi-honest adversaries. To make use of the covert security, we use bloom filter and probabilistic check in the resource consumption accounting to reduce the overhead. Performance analysis shows that the overhead of our construction is small over existing systems.

7. REFRENCES

[1] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," Journal of Internet Services and Applications, vol. 1, no. 1, pp. 7–18, 2010.

[2] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, no. 1, pp. 69–73, 2012.

[3] L. Zhou, Y. Zhu, and A. Castiglione, "Efficient k-NN query over encrypted data in cloud with limited key-disclosure and offline data owner," Computers & Security, vol. 69, pp. 84–96, 2017.

[4] S. Hu, Q. Wang, J. Wang, Z. Qin, and K. Ren, "Securing SIFT: Privacy-preserving outsourcing computation of feature extractions over encrypted image data," IEEE Transactions on Image Processing, vol. 25, no. 7, pp. 3411–3425, 2016.

[5] H.-M. Sun, Y.-H. Chen, and Y.-H. Lin, "oPass: A user authentication protocol resistant to password stealing and password reuse attacks," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 651–663, 2012.

[6] L. Harn and J. Ren, "Generalized digital certificate for user authentication and key establishment for secure communications," IEEE Transactions on Wireless Communications, vol. 10, no. 7, pp. 2372–2379, 2011.

[7] V. Sekar and P. Maniatis, "Verifiable resource accounting for cloud computing services," in Proceedings of the 3rd ACM workshop on Cloud computing security workshop. ACM, 2011, pp. 21–26.

[8] C. Chen, P. Maniatis, A. Perrig, A. Vasudevan, and V. Sekar, "Towards verifiable resource accounting for outsourced computation," in ACM SIGPLAN Notices, vol. 48, no. 7. ACM, 2013, pp. 167–178.

[9] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in 2007 IEEE Symposium on Security and Privacy (SP'07). IEEE, 2007, pp. 321–334.

[10] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in Public Key Cryptography– PKC 2011. Springer, 2011, pp. 53–70.