International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 369-379 www.ijaem.net ISSN: 2395-5252

Coarse Grained Security in Cloud with Cryptographic Access Control

Dr.D.J.Samatha Naidu [#1], D.Sudhakar [*2], T.Amrutha [#3]
[1]*Professor & Principal, APGCCS, Rajampet, YSR Kadapa, India*
[2]*Assistant Professor, MCA Department, APGCCS, Rajampet, YSR Kadapa, India*
[3]*MCA Department, APGCCS, Rajampet, YSR Kadapa, India*

Date of Submission: 01-10-2022 Date of Acceptance: 12-10-2022

ABSTRACT— Cloud computing provides a flexible and convenient way for data sharing, which brings various benefits for both the society and individuals. Though the architecture of cloud is robust and flexible towards new data sets, but it lags in handling the issues related to security.Especiallywhenappliedinapplicationsrelate dtosocialnetworks, financial transactions. The data storage in virtual machine may rise to problems such as authentication, collusion resilience and service hijacking in cloud environment. Cloud stores a lot of information persistently over its life time. To overcome such issues, we tried to tailor the existing KP-ABE by introducing sessions and named it as KPAC to fulfil the requirement which can be adaptable to cloud environment with concerning to the needs of security. Further, I tried to prove our approach is resilient to the attacks mentioned. In short I proposed coarse gained security in cloud with cryptographic access control. The data is directly conveyed to the central location for storage and access. For access-control to cloud data, every virtual machine is equipped with an ACL. Upon every information access demand, the virtual machine is request is approved if the client's identity is present in the ACL. Hence, each attribute of my VM is associated with predefined key-in material. Further, the users privileges are associated with a key that specifies the data field that the user is authorized. Cloud computing have discovered their wide applications in IT are, social organizations and money related exchanges. To achieve the focused-on applications and satisfy its functionalities, a cloud generally stores a lot information over its life time. Information storing and access in cloud network essentially follows two methodologies, to be specific, distributed and centralized approaches. Distributed data storage avoids single point of failure, consume less bandwidth etc., as compared to centralized one.

Keywords— Bandwidth, Encryption, Computational Intelligence, Hash-Solomon, Distribution Proportion.

I. INTRODUCTION

Cloud computing have discovered their wide applications in IT area, Social organizations and money related exchanges. To achieve the focused-on application and satisfy its functionalities, a Cloud generally stores a lot of information persistently over its lifetime. Informations to ring and access in Cloud networks essentially follows two methodologies, to be specific, distributed and centralized approaches. Distributed data storage avoids single point of failure, consumelessb and width etc., as compared to centralized one.

Cloud computing is a paradigm that provides massive computation capacity and huge memory space at a low cost. It enables users to get intended services irrespective of time and location across multiple platforms (e.g., mobile devices, personal computers), and thus brings great convenience to cloud users. Among numerous services provided by cloud computing, cloud storage service, such as Apple's I Cloud, Microsoft's Azure and Amazon's S3 However, it also suffers from several security threats, which are the primary concerns of cloud users. Therefore, while outsourcing data to cloud server, users also want to control access to these data such that only those currently authorized users can share the outsourced data. a data sharing system can provide confidentiality and backward secrecy. Furthermore, the method of decrypting and re-encrypting all the shared data can ensure forward secrecy. However, this brings new challenges. In general, the use of secret key should be limited to only usual decryption, and it is inadvisable to update the cipher text periodically by using secret key. To update the cipher text of the shared data, the data

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 369-379 www.ijaem.net ISSN: 2395-5252

provider has to frequently carry out the procedure of download-decrypt-re encrypt-upload. This process brings great communication and computation cost, and undesirable for cloud users with low capacity of computation and storage

Purpose

Coarse-grained access control is important because it changes the rules of static authorization and enables secure sharing of many more sensitive information assets. However, this does require an effective and proven fine-grained authorization tool such as Axiomatics dynamic data masking solution.

Scope

In this work I propose a new and more efficient algorithm that produces solutions which are very close to the optimal ones. Our contribution is efficient not only for the bursting of behavior-based compositions but also for architecture-based compositions of services

II.RELATED WORK

Existing System

A Cloud network normally comprises of an enormous number of assets that can be handily served to different areas important to limit the costs of Consumers towards computing infrastructure the data is stored in some local virtual machine before upgrading it to the central location of the cloud. Whereas inlater case, the data is directly conveyed to the central location for storage and access the data is stored in some local virtual machine before upgrading it to the central location of the cloud. Whereas in later case, the data is directly conveyed to the central location for storage and access. For access-control to cloud data, every virtual machine is equipped with an ACL. Upon every information access demand, the virtual machine the request is approved if the client's identity is present in the ACL. Hence, each attribute of our VM is associated with predefined key-in material. Further, the user's privileges are associated with a tree that specifies the data fields that the user is authorized.

Disadvantages

- Achieving a coarse-grained security is always a challenge in cloud networks because of the issues such as authentication, hijacking and user colluding.
- The colluding users need necessary information such a secret key for targeting data.
- Secure channel is essential for the key authority and non-revoked users to transmit new keys, however, existing scheme only achieves selective security.
- Every information access demand, the virtual machine the request is approved if the client's identity is present in the ACL.

III. PROPOSED WORK

Proposed System

In this we introduced KPAC Key Policy-Based access control scheme which is more like KP-ABE, and is specially tailored for Cloud networks. The idea behind our framework on the intrinsic data of virtual machine. The explicit nature of cloud services allows us to dedicate each virtual machine with a specific set of pre-defined attributes such as time, type, place and owner of the data. This convenience allows us to tuning of attribute towards access control. Hence, each attribute of our VM is associated with predefined key-in material. Further, the user's privileges are associated with a tree that specifies the data fields that the user is authorized. The cloud data is encrypted with the attributes whose ever access structure satisfies the encryption key can able to decrypt the message.

Advantages

- The opponent cannot derive the data, as the Master key gets encrypted with one-way hash function at each stage with a set of preloaded fields of the virtual machine.
- The private key of an unauthorized user cannot reveal any use ful information to the other user in terms of computing as in every session.
- Service Hijacking one-wayness keychain enable VM to keep the updates encryption key

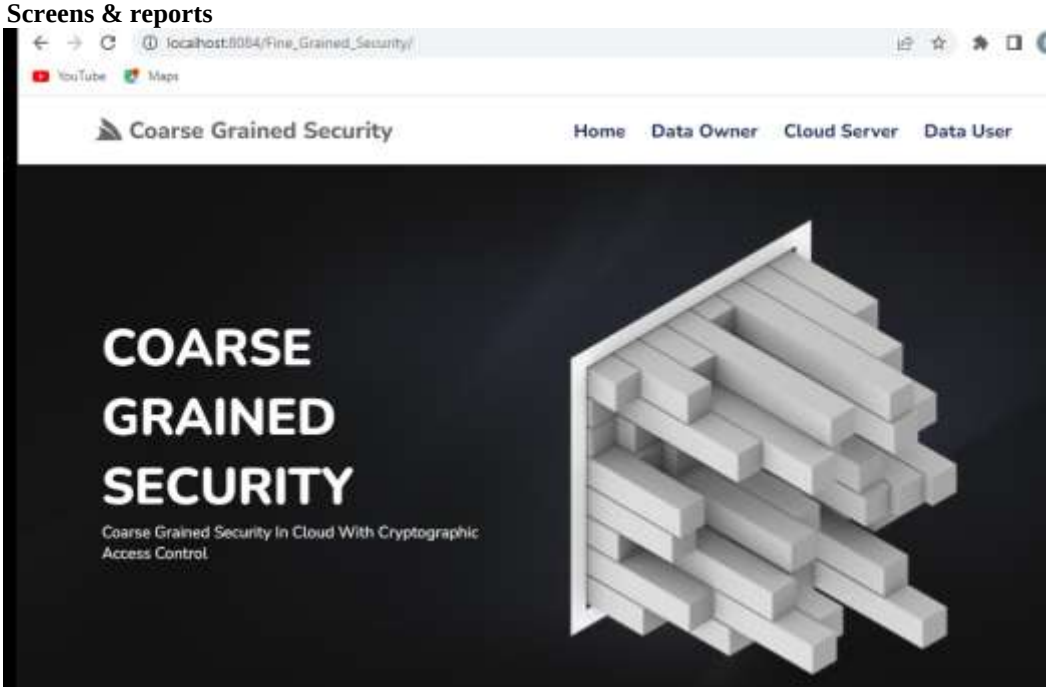
IV. COMPARATIVE RESULTS

Implementation is the process of ensuring that the information system is operational and therefore allowing the user to perform his operations for his use and evaluation operations. The implementation includes the following activities.

a. Obtain and install system hardware.
b. Install the system and run it on the intended hardware.
c. Provide users with access to the system.
d. Database creation and updating.
e. Train users on the new system.
f. Document the system for its users and for those who will be responsible for its maintenance in the future.
g. Make arrangements to support the user while using the system.
h. Transfer of responsibilities underway for the developer's system in operation or maintenance.

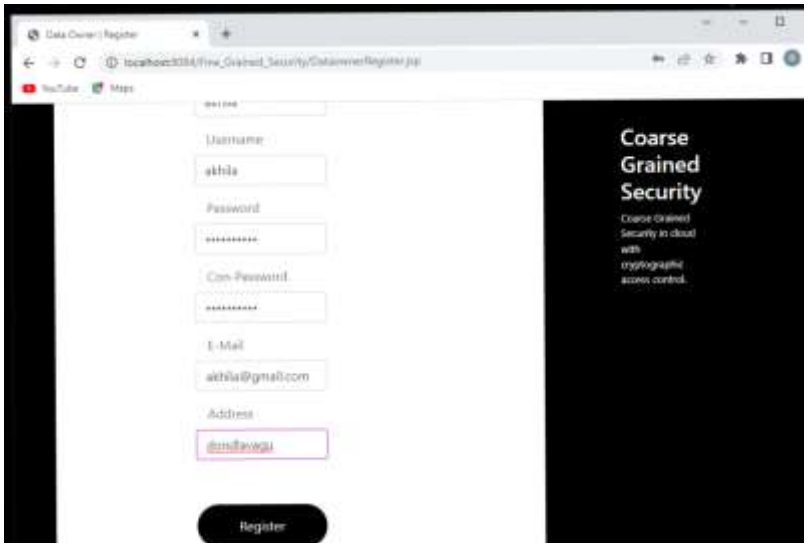
International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 369-379 www.ijaem.net ISSN: 2395-5252

Sample Screens & reports



Screen 1: Home Page

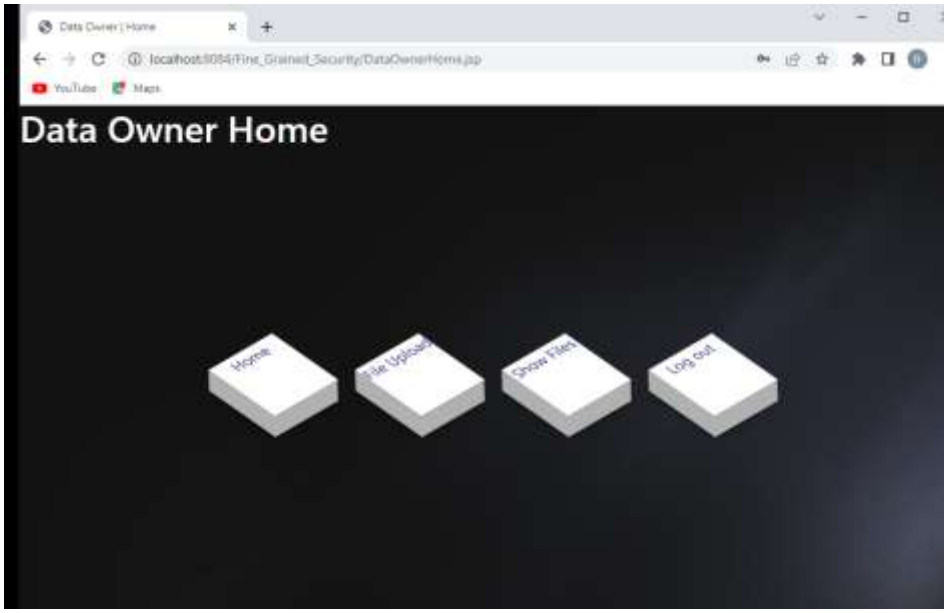
Description: This screen displays homepage. It shows different modules available are like home, data owner, data user, cloud server.



Screen 2: Registration Module

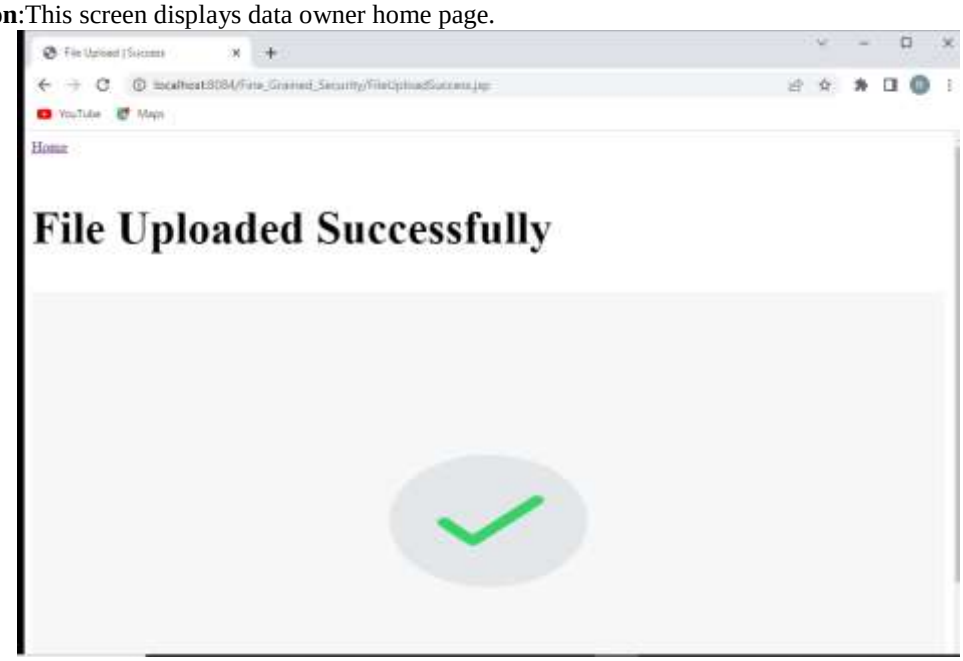
Description: This screen displays Data owner Registration which contains the fields like name, password, mail address, and other fields.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 369-379 www.ijaem.net ISSN: 2395-5252



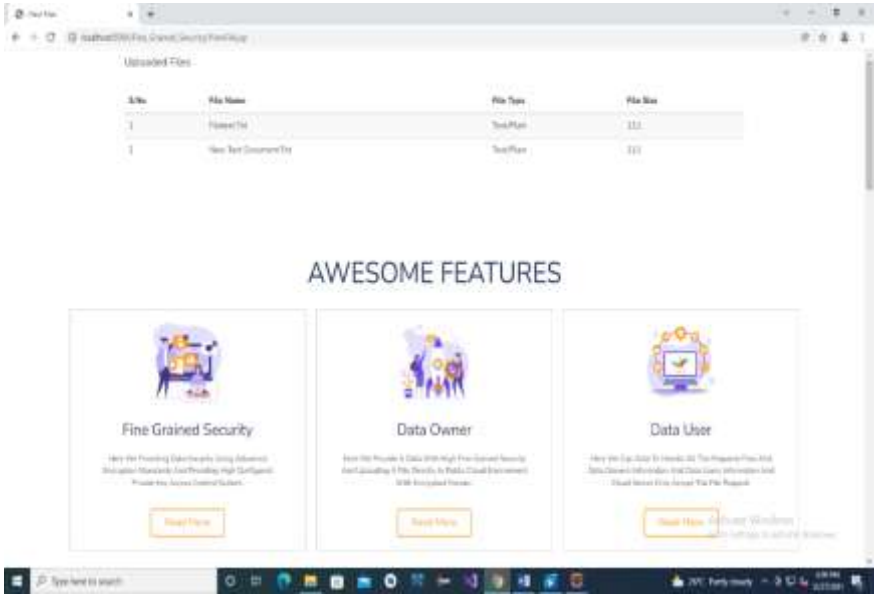
Screen 5.1.3:Data Owner Home

Description:This screen displays data owner home page.



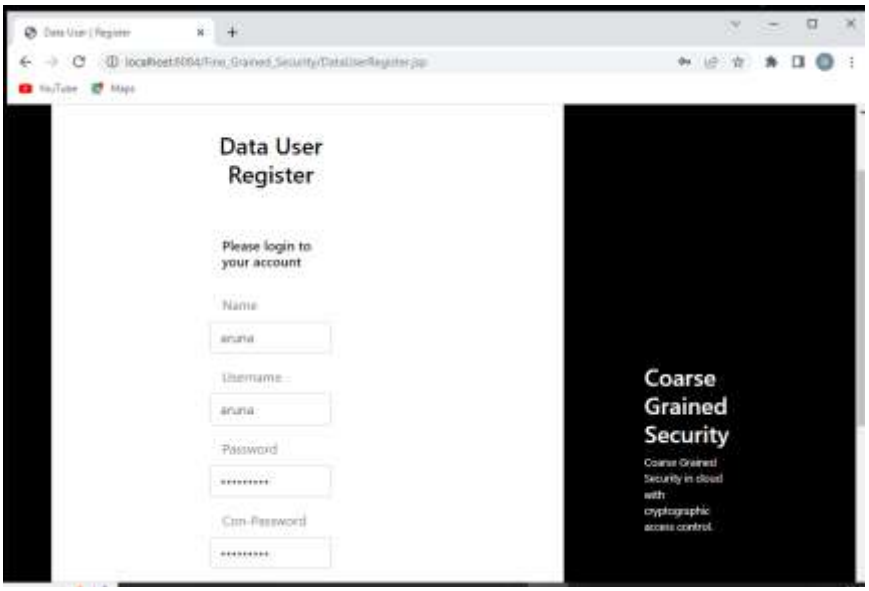
Description: The above screen display the data owner is uploading a file in to cloud server in successfully.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 369-379 www.ijaem.net ISSN: 2395-5252



Screen 5: File Upload Details

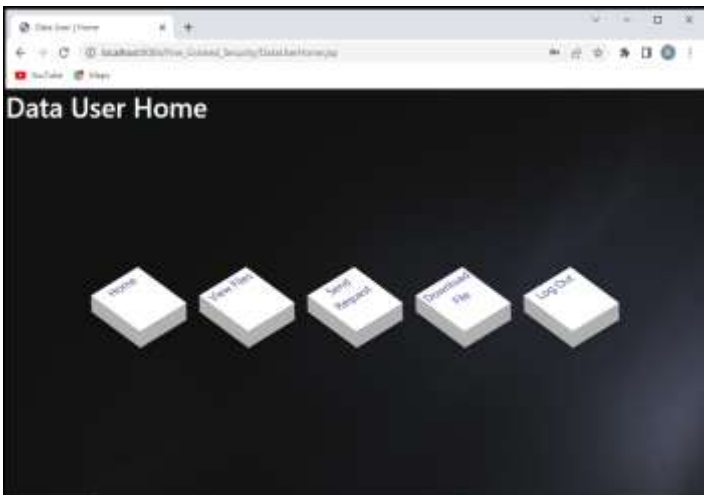
Description: The above screen display the details of the upload files.



Screen 6: Data User Register

Description: The above screen displays to register page the data user

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 369-379 www.ijaem.net ISSN: 2395-5252

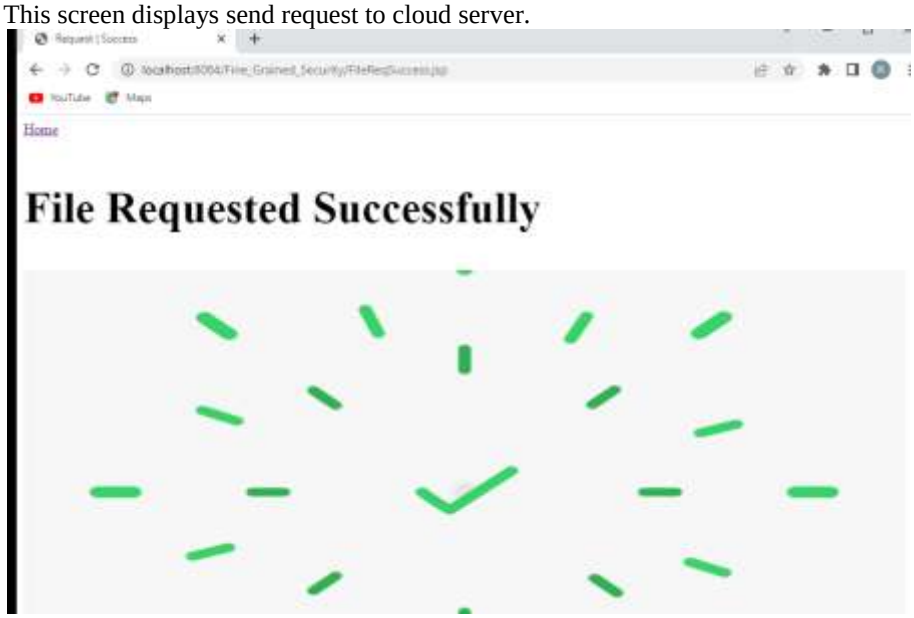


Screen 7: Data User Home

Description: This screen displays data user home.

Screen 8:Send Request

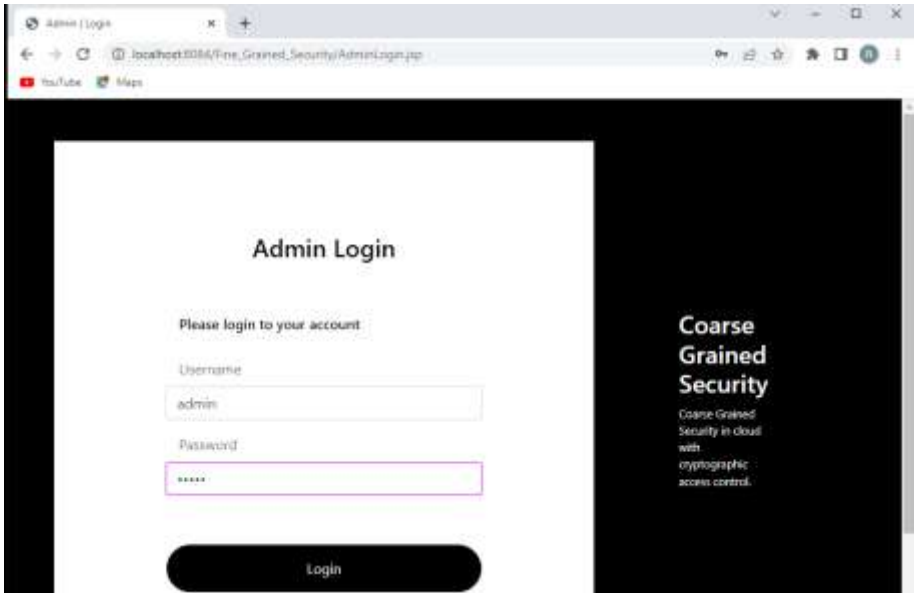
Description: This screen displays send request to cloud server.



Screen 9: User Request Successfully.

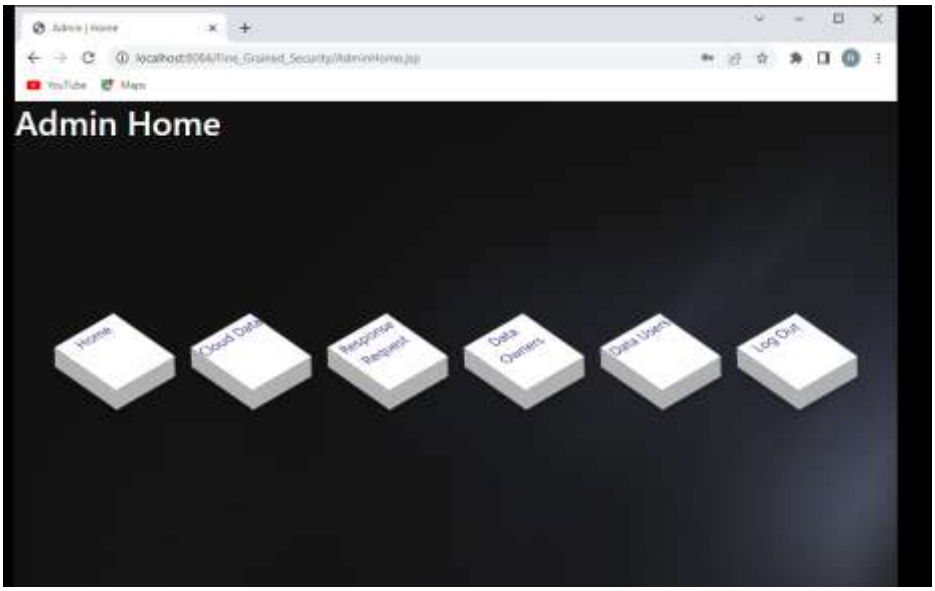
Description: This screen displays users request successfully.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 369-379 www.ijaem.net ISSN: 2395-5252



Screen 10: Cloud Server Login

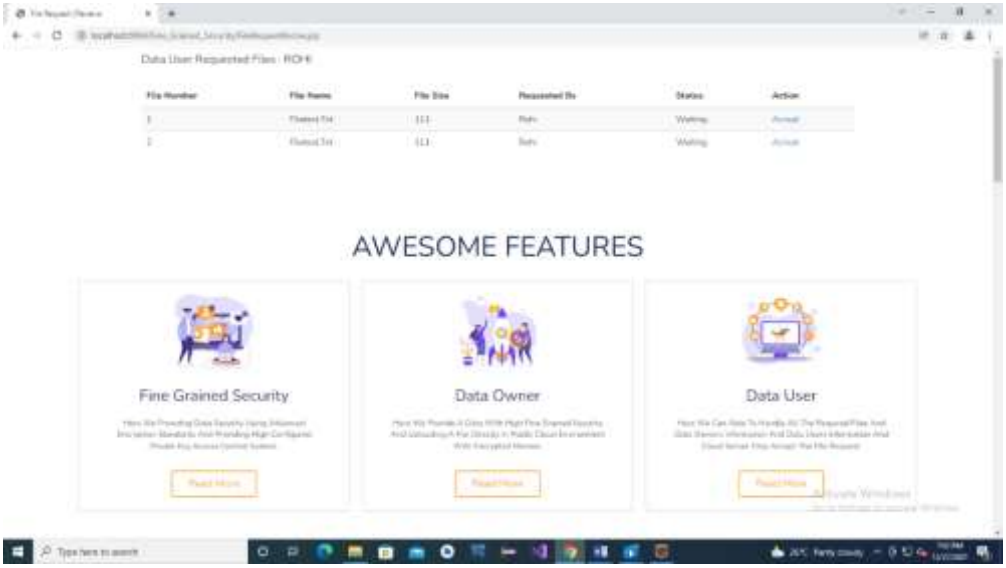
Descripton:i This screen displays Cloud Server Login.



Screen 11: Cloud Server Home

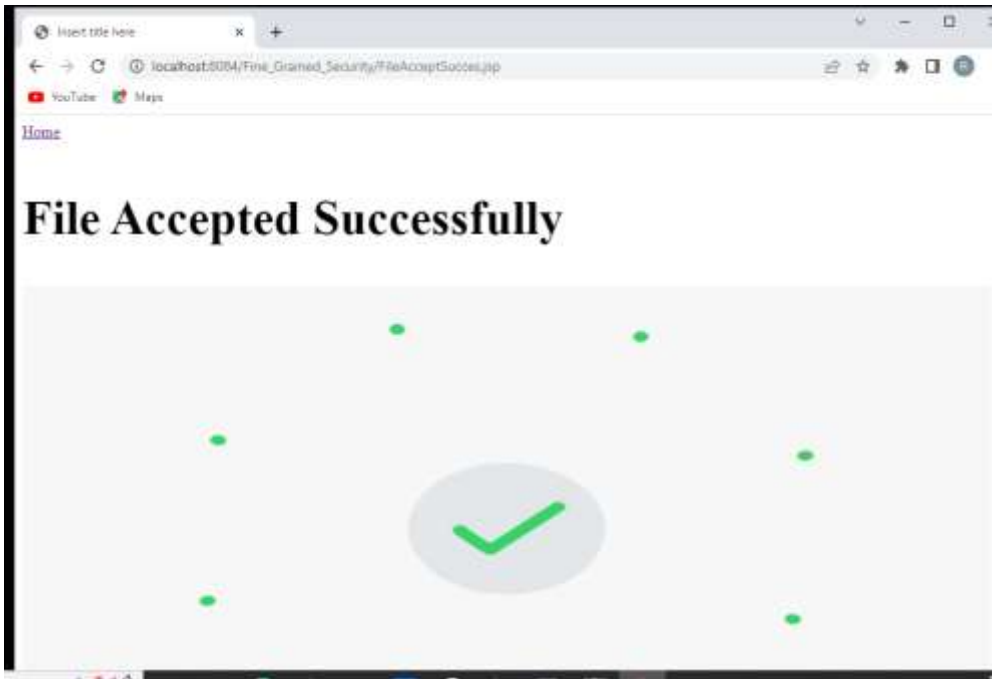
Description: This screen displays cloud server home page.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 369-379 www.ijaem.net ISSN: 2395-5252



Screen 12: Accept File

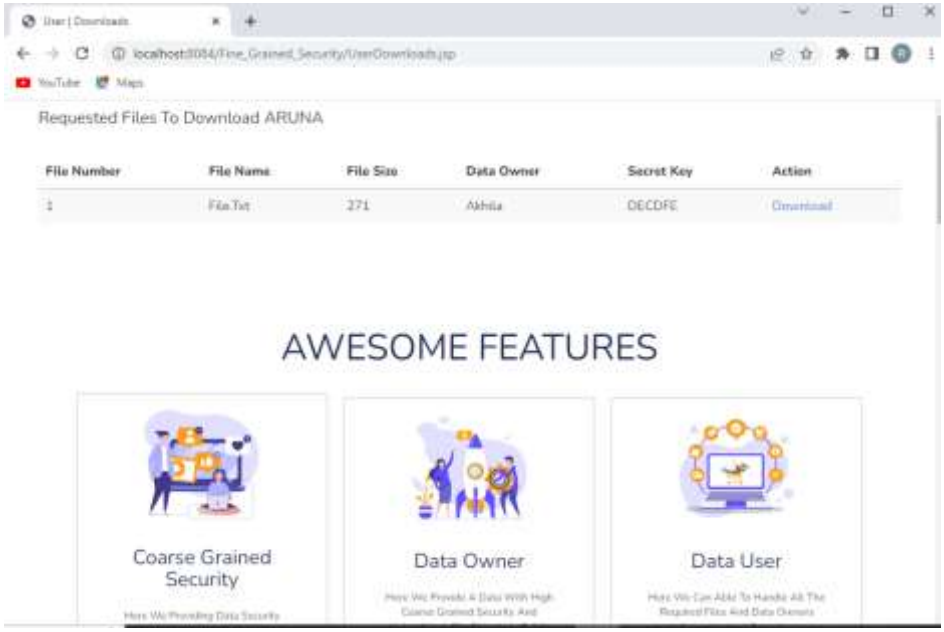
Description: This screen displays cloud server accept file.



Screen 13: File Accepted Successfully

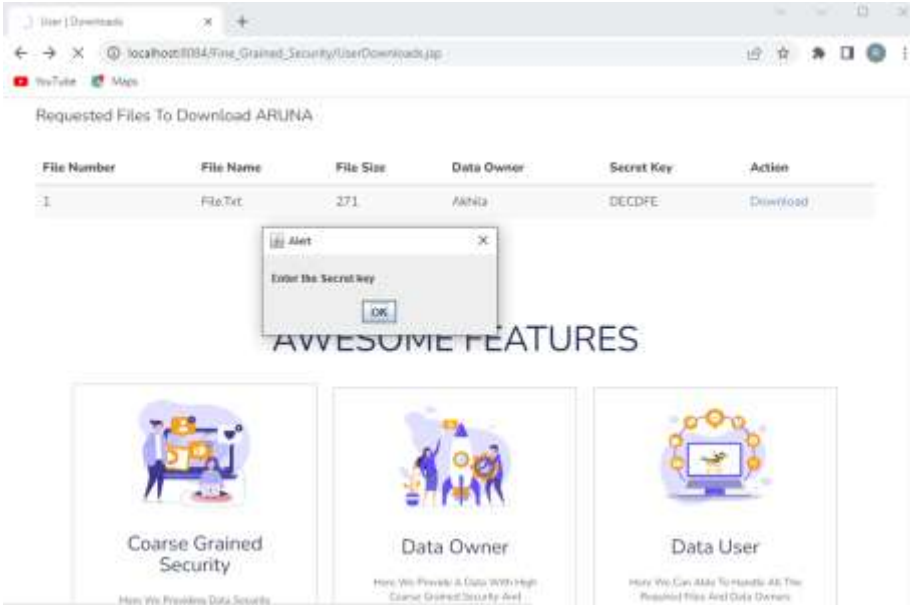
Description: This screen displays cloud server accept successfully.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 369-379 www.ijaem.net ISSN: 2395-5252



Screen 14: Download File

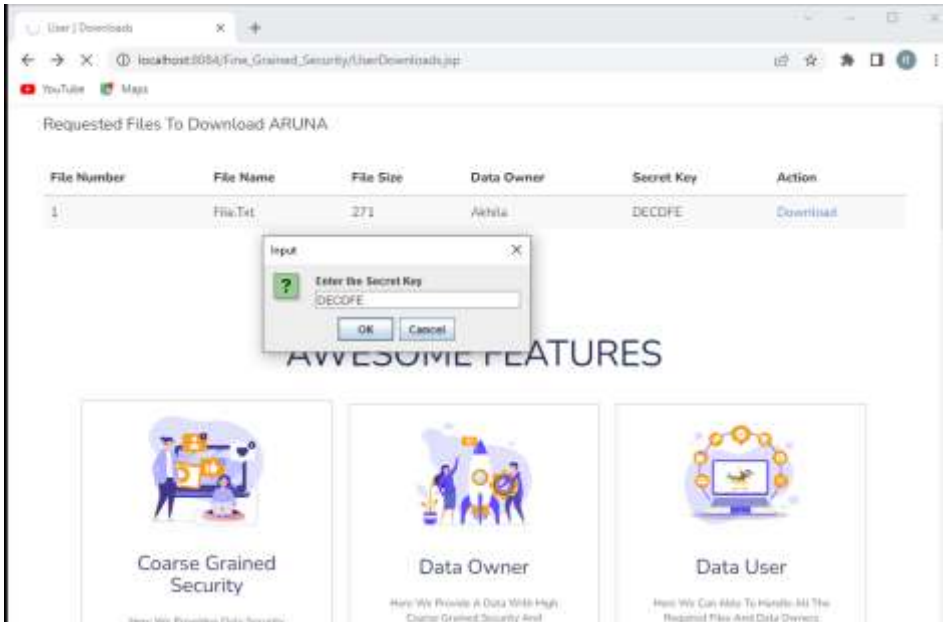
Description: This screen displays download file.



Screen 15: Enter Key

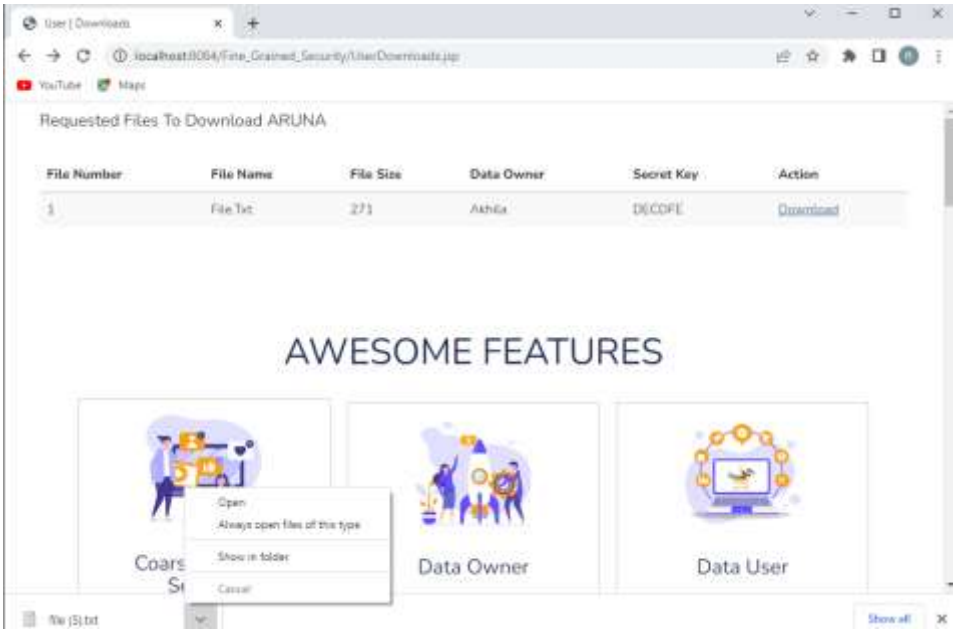
Description: This screen displays enter key to download file.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 369-379 www.ijaem.net ISSN: 2395-5252



Screen 16: Verify Keys

Description: This screen displays verify keys.



Screen 17: Download File

Description: These screens displays download file.

V. CONCLUSION

Finally, I conclude that, as per the literature and study can say that there are certain limitations of centralized storage.Soto enhance the security of data use decentralized cloud storage. This paper suggests a secure and efficient way to store data on cloud. Block chain-based cloud storage with data encryption gives data security in decentralized structure. The proposed model is suitable to implement the block chain structure. The algorithms used to implement the system model is efficient and required less time and give high security for the data which is being stored on cloud. This kind of architecture makes the system

more robust and resistant to different security attacks which are performed by unauthorized users who try to steal and disclose the information in data files of user for their benefits. In the future, i plan to research on applying the principles of coarse grained security to implement and enhance future based security

ACKNOWLEDGMENT
We thank all theauthors and their value Contribution Work helped me to complete my final year project.

REFERENCES

[1]. M.Armbrust,A.Fox,R.Griffith,A.D.Joseph, R.Katz,A.Konwinski,G.Lee,D.Patterson,A .Rabkin,I.Stoica,andM.Zaharia,‘‘AViewof Cloud Computing," Commun. ACM, vol. 53, no. 4, pp. 50-58, Apr.2010.

[2]. Modi, C., Patel, D., Borisaniya, B., Patel, A. &Rajarajan, M. (2013).“A survey on security issues and solutions at different layers of Cloudcomputing”. The Journal of supercomputing, 63(2), pp. 561-592. doi:10.1007/s11227-012-0831-5J.

[3]. Yao,S.Chen,S.Nepal,D.Levy,andJ.Zic,‘‘Tr ustStore:MakingAmazon S3 Trustworthy With Services Composition," in Proc.10thIEEE/ACMInt'lSymposiumonCl uster,CloudandGridComputing(CCGRID), 2010,pp.600-605.

[4]. D. Zissis and D. Lekkas, ‘‘Addressing Cloud Computing SecurityIssues," Future Gen. Comput. Syst., vol. 28, no. 3, pp. 583-592, Mar.2011

[5]. C. Wang, Q. Wang, K. Ren, and W. Lou, ‘‘Privacy-Preserving PublicAuditingforDataStorageSecurityinC loudComputing,"inProc.30stIEEEConf.on Comput.andCommun.(INFOCOM),2010, pp.1-9.

[6]. G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, ‘‘Scalable andEfficient Provable Data Possession," in Proc. 4th Int'l Conf. Securityand PrivacyinCommun.Netw.(SecureComm),2 008,pp.1-10.

[7]. G.Ateniese,R.Burns,R.Curtmola,J.Herring ,O.Khan,L.Kissner,Z. Peterson, and D. Song, ‘‘Remote Data Checking Using ProvableData Possession," ACM Trans. Inf. Syst. Security, vol. 14, no. 1, May2011, Article12.

[8]. G.Ateniese,R.B.Johns,R.Curtmola,J.Herrin g,L.Kissner,Z.Peterson,andD.Song,‘‘Prov ableDataPossessionatUntrustedStores,"inP roc.14thACMConf.onComput.andCommu n.Security(CCS),2007,pp.598-609.

[9]. R.Curtmola,O. Khan,R.C. Burns, andG.Ateniese,‘‘MR-PDP:Multiple-ReplicaProvableDataPossession,"inProc.2 8thIEEEConf.onDistrib.Comput. Syst.(ICDCS), 2008,pp.411-420.

[10]. C.Erway,A.Ku¨pc¸u¨,C.Papamanthou,and R.Tamassia,‘‘DynamicProvable Data Possession," in Proc. 16th ACM Conf. on Comput. andCommun.Security(CCS),2009,pp.213-222.