IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⋇ Impact Factor 7.39 ⋇ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11699

LIGHTWEIGHT CLOUD STORAGE SECURITY

Dr. Shanthi Mahesh[1], Supritha Sharma[2]

Assistant Professor, Department of Information Science & Engineering,Atria Institute of Technology, Bengaluru, India[1]

Student, Department of Information Science & Engineering, Atria Institute of Technology, Bengaluru, India[2]

Abstract: In this paper, we introduce a new fine-grained two-factor authentication access control system for web-based cloud computing services. Specifically, in our proposed 2FA access control system, an attribute- based access control mechanism is implemented with the necessity of both a user secret key and a lightweight security device. As a user cannot access the system if they do not hold both, the mechanism can enhance the security of the system, especially in those scenarios where many users share the same computer for web-basedcloud services. In addition, attribute-based control in the system also enables the cloud server to restrict the access to those users with the same set of attributes while preserving user privacy, i.e., the cloud server only knows that the user fulfills the required predicate, but has no idea on the exact identity of the user.

Keywords: web-based cloud services, two-factor authentication, 2FA access control system, cloud storage

I. INTRODUCTION

Cloud computing is a virtual host computer system that enables enterprises to buy, lease, sell, or distribute software and other digital resources over the internet as an on-demand service. It no longer depends on a server or a number of machines that physically exist, as it is a virtual system. There are many applications of cloud computing, such as data sharing, data storage, big data management, medical information system etc. End usersaccess cloud-based applications through a web browser, thin client or mobile app while the business software and user's data are stored on servers at a remote location. The benefits of web-based cloud computing services are huge, which include the ease of accessibility, reduced costs and capital expenditures, increased operational efficiencies, scalability, flexibility and immediate time to market.

II. BACKGROUND AND SIGNIFICANCE

In this paper, we propose a fine-grained two-factor access control protocol for web-based cloud computing services, using a lightweight security device. The device has the following properties: (1) it can compute some lightweight algorithms, e.g. hashing and exponentiation; and (2) it is tamper resistant, i.e., it is assumed that noone can break into it to get the secret information stored inside. With this device, our protocol provides a 2FA security. First the user secret key (which is usually stored inside the computer) is required. In addition, the security device should be also connected to the computer (e.g. through USB) in order to authenticate the user for accessing the cloud. The user can be granted access only if he has both items. Furthermore, the user cannotuse his secret key with another device belonging to others for the access. Our protocol supports fine-grained attribute-based access which provides a great flexibility for the system to set different access policies accordingto different scenarios. At the same time, the privacy of the user is also preserved. The cloud system only knowsthat the user possesses some required attribute, but not the real identity of the user.
Our protocol provides a 2FA security. Our protocol supports fine-grained attribute-based access which providesa great flexibility for the system to set different access policies according to different scenarios. At the same time, the privacy of the user is also preserved.

DOI: 10.17148/IJARCCE.2022.11699

III. LITRATURE REVIEW

1) Title: "**Attribute-Based Encryption with Verifiable Outsourced Decryption"**

Attribute-based encryption (ABE) is a public-key-based one-to-many encryption that allows users to encrypt and decrypt data based on user attributes. A promising application of ABE isflexible access control of encrypted data stored in the cloud, using access polices and ascribed attributes associated with private keys and ciphertexts. One of the main efficiency drawbacks of the existing ABE schemes is that decryption involves expensive pairing operations and the number of such operations grows with the complexity of the access policy.

2) Title: "Fine-Grained Control of Security Capabilities"

We present a new approach for fine-grained control over users' security privileges (fast revocation of credentials) centered around the concept of an on-line semi-trusted mediator (SEM). The use of a SEM in conjunction with a simple threshold variant of the RSA cryptosystem (mediated RSA) offers a number of practical advantages over current revocation techniques. The benefits include simplified validation of digital signatures, efficient certificate revocation for legacy systems and fast revocation of signature and decryption capabilities. This paper discusses both the architecture and the implementation of our approach as well as its performance and compatibility with the existing infrastructure. Experimental results demonstrate its practicalaspects.

3) Title: "Improving Security and Efficiency in Attribute-Based Data Sharing"

With the recent adoption and diffusion of the data sharing paradigm in distributed systems such as online socialnetworks or cloud computing, there have been increasing demands and concerns for distributed data security.

One of the most challenging issues in data sharing systems is the enforcement of access policies and the support of policies updates. Ciphertext policy attribute-based encryption (CP-ABE) is becoming a promising cryptographic solution to this issue.

4) Title: Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption

Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine- grained, cryptographically enforced data access control. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability and efficiency of our proposed scheme.

5) Title: Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption

Cloud computing is a revolutionary computing paradigm, which enables flexible, on-demand, and low-cost usage of computing resources, but the data is outsourced to some cloud servers, and various privacy concerns emerge from it. Various schemes based on the attribute-based

encryption have been proposed to secure the cloud storage. However, most work focuses on the data contents privacy and the access control, while less attention is paid to the privilege control and the identity privacy. In this paper, we present a semi anonymous privilege control scheme Anony Control to address not only the data privacy, but also the user identity privacy in existing access control schemes. Anony Control decentralizes the central authority to limit the identity leakage and thus achieves semi anonymity. Besides, it also generalizes the file access control to the privilege control, by which privileges of all operations on the cloud data can be managed in a fine-grained manner. Subsequently, we present the Anony Control-F, which fully prevents the identity leakage and achieve the full anonymity. Our security analysis shows that both Anony Controland Anony Control-Fare secure under the decisional bilinear Diffie–Hellman assumption, and our performance evaluation exhibits the feasibility of our schemes.

DOI: 10.17148/IJARCCE.2022.11699

IV. RESEARCH DESIGN AND METHODS

IV.I ARCHITECTURE DIAGRAM

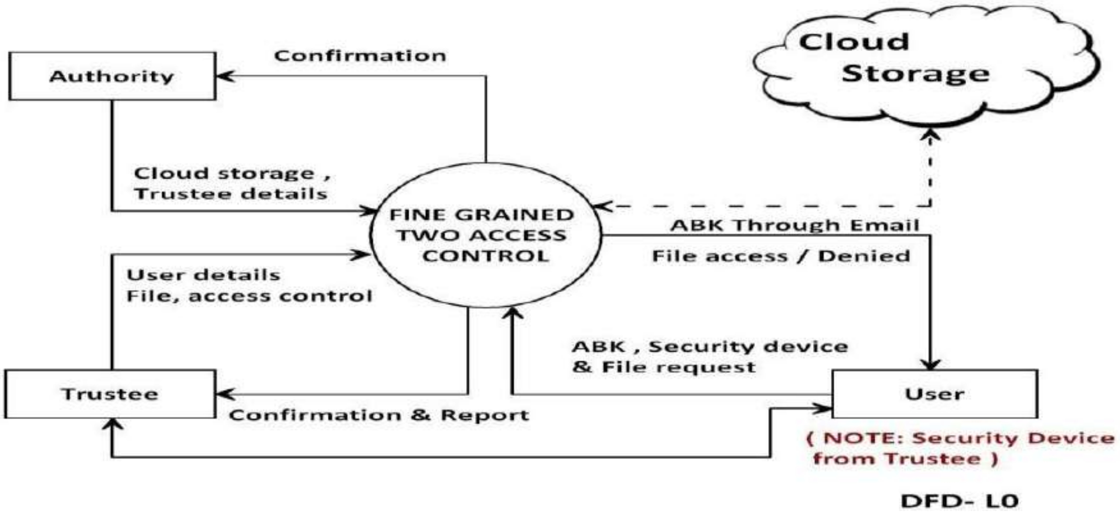


Fig. 1 General Architecture Diagram

Software Architecture of a software system typically involves modules like domain authority, data trustee, data consumer connected to each other via fine grained two-way access control and communicate using multiple clouds in cloud storagefor file access.

IV.II DATAFLOW DIAGRAM DOMAIN AUTHORITY MODULE

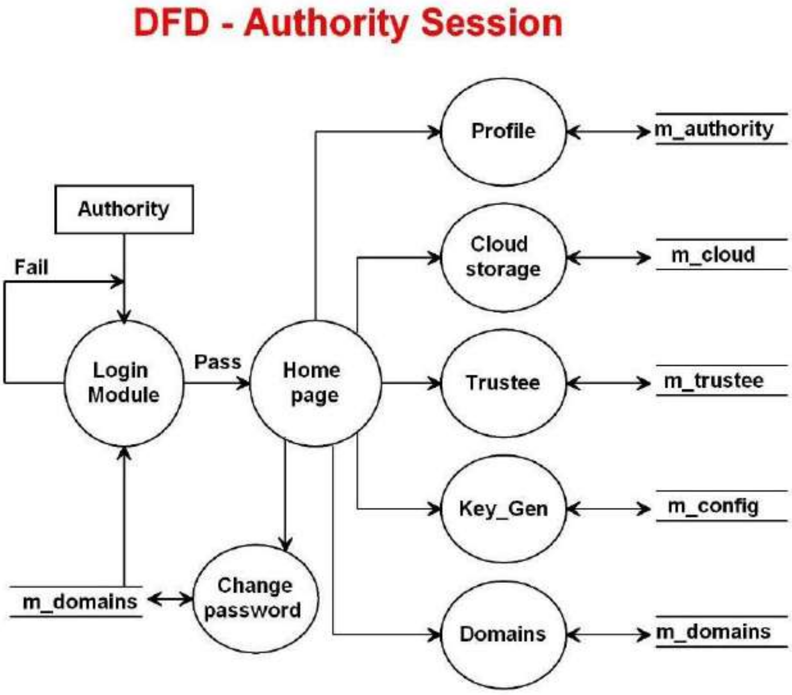


Fig. 2 Dataflow diagram of Domain Authority Module

The flowchart depicts that the Domain Authority is a super user who creates the Data Trustee user and maintains the cloud servers' configurations. He has the writes to Add, Edit or Delete any number of Trustee.

DOI: 10.17148/IJARCCE.2022.11699

Data Trustee Module

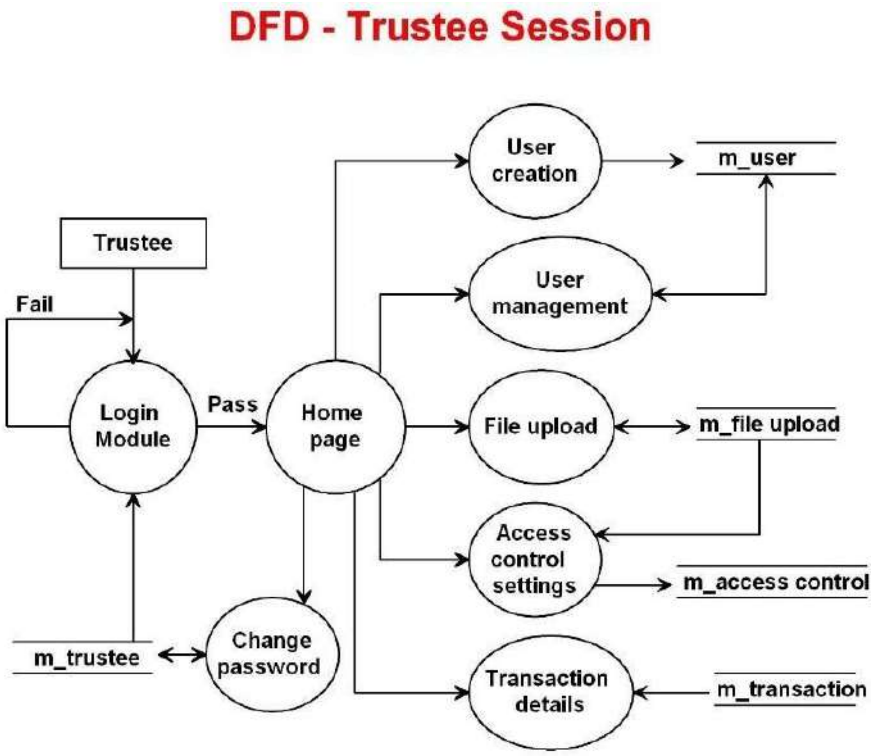


Fig. 3 Dataflow Diagram of Data Trustee Module

Trustee is a person who will store the files in cloud which in turn accessed by the authorized Data Consumers.Trustees are like Liberian who will upload all the files in the system. Whenever the file is uploaded it will be encrypted by the system using Trustee Encryption Key.

Trustee has to specify the Hierarchical Access Policy for each and every file. Access policies are set usingDepartment Attribute and Designation Attribute.

Data Consumer Module

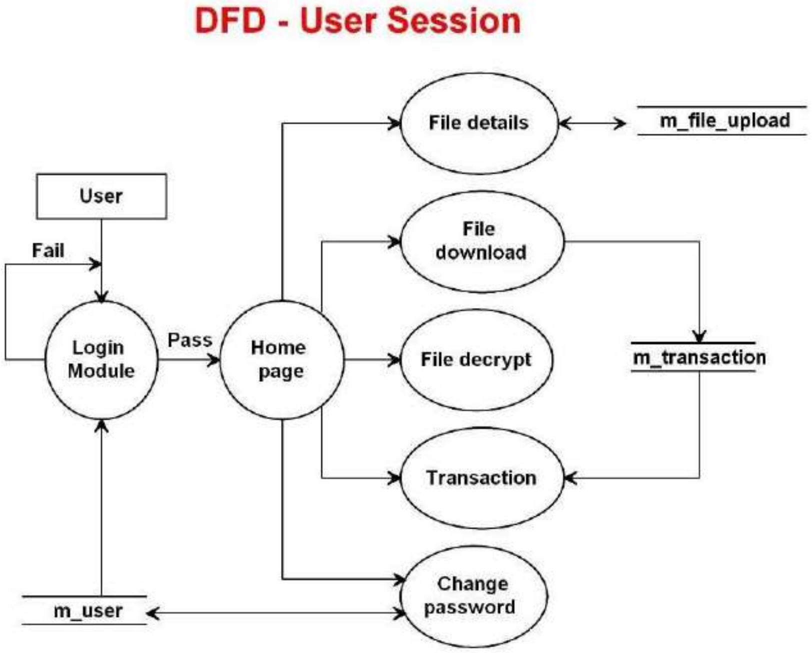


Fig. 3 Dataflow diagram of Data Consumer Module

Data Consumers are the data access users, suppose Trustee is a college Liberian then data consumers are likestudents, lectures and admin staff in a college.

Data Consumer will receive their access key (Attributed based Decryption Key) from respective Trusteethrough email and lightweight security device.

With the help of the access key they can able to download the files for which they have access, rememberaccess control is set by data owner.

IV.III SEQUENCE DIAGRAM

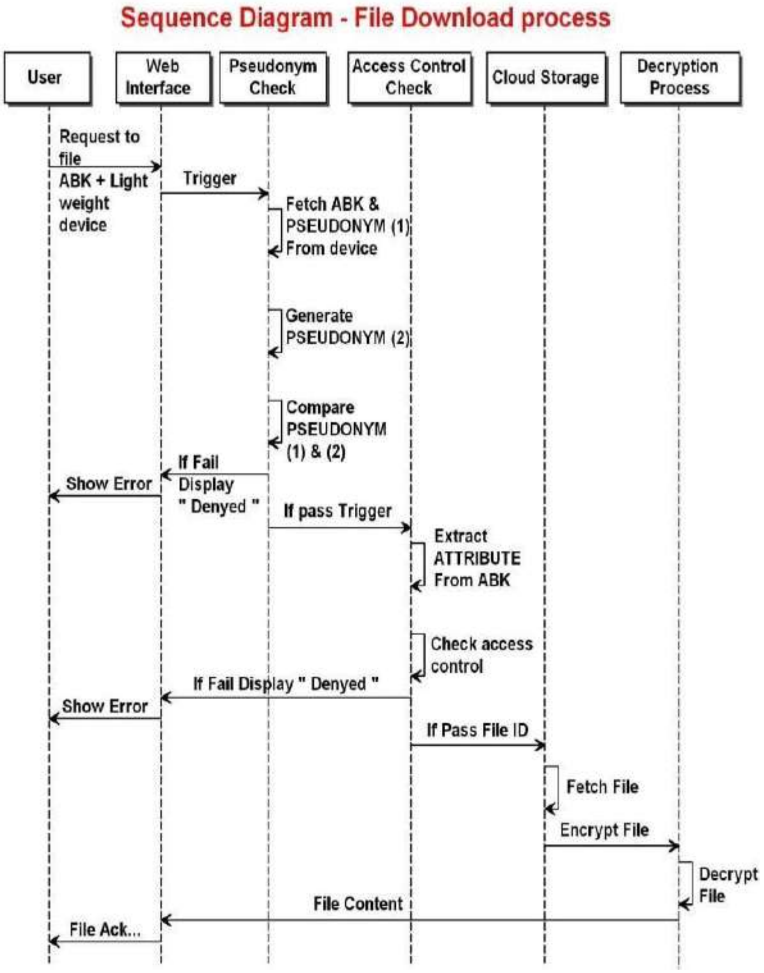


Fig. 3 Sequence Diagram of file download process

Above figure shows the sequence of operations performed to download a file. Suppose the data consumer wants to download any file, first he has to select the file from the list and the system ask for the access key,after system getting the access key it will separate the Attribute Set from the key and check for the access rights, if the user has the access he can download the encrypted file which in turn decrypted using the decryption key and download to the data consumer local system.

Once the Data Consumer logged in he has following functions.

File Details (View), File Download you should-Select the file from the list, Select the Attribute based Key (ABK) file from the local system and Pseudonym Key from lightweight security device, Decrypt the Attributebased Key using DNA Decryption, Generate the Pseudonym(1) Key from ABK , Fetch Pseudonym(2) from security device , Compare Pseudonym(1) & Pseudonym(2) if Fail deny the file access, Get the Attribute Values from decrypted ABK, Check the Access Control with Attribute, If Access Control pass download the file or deny the file access, Enter the transaction record in the table.

For File Decrypt one should- Select the file to be decrypted, Retrieve the Decryption Key from ABK, Decryptthe file, Download the file to user system.

DOI: 10.17148/IJARCCE.2022.11699

V. CONCLUSION

we have presented a new 2FA (including both user secret key and a lightweight security device) access control system for web-based cloud computing services. Based on the attribute-based access control mechanism, the proposed 2FA access control system has been identified to not only enable the cloud server to restrict the accessto those users with the same set of attributes but also preserve user privacy. Detailed security analysis shows that the proposed 2FA access control system achieves the desired security requirements. Through performance evaluation, we demonstrated that the construction is "feasible". We leave as future work to further improve theefficiency while keeping all nice features of the system.

VI. RESULTS

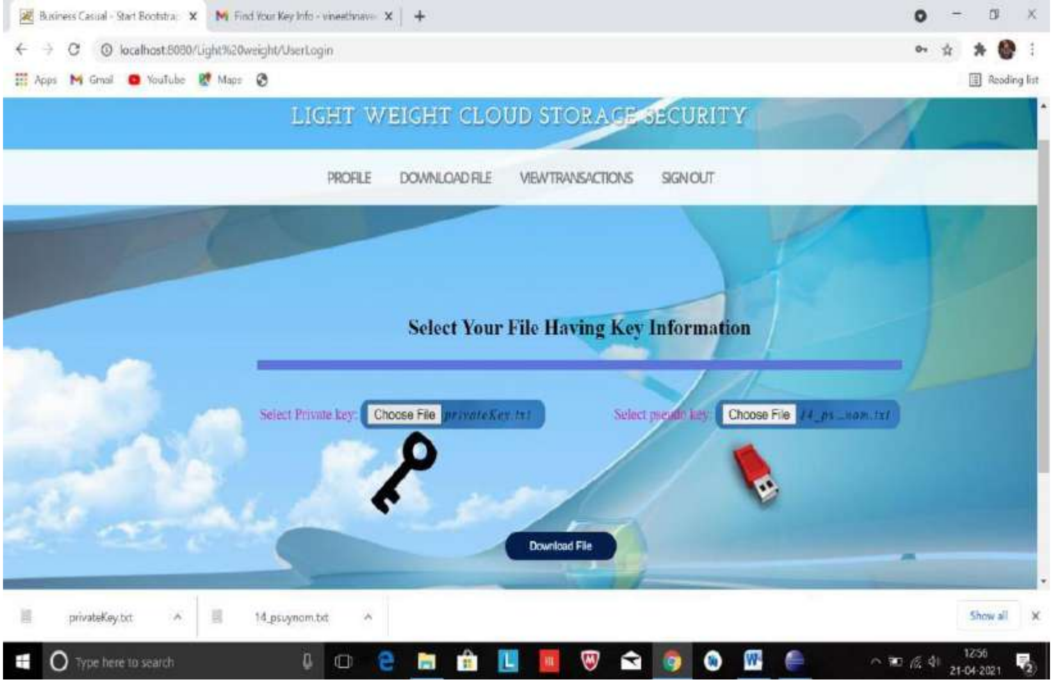
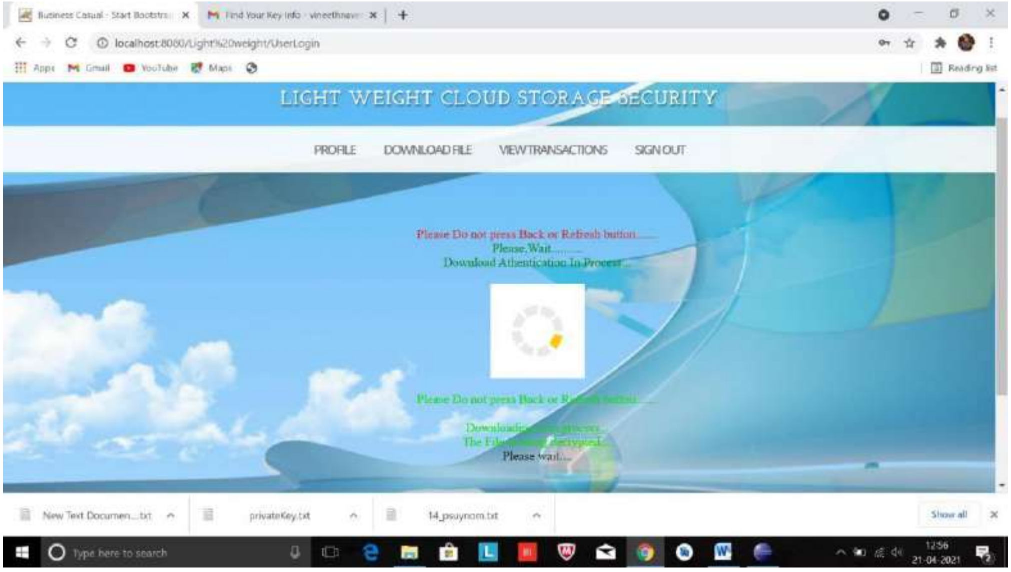


Figure A.1 – Screenshot of both the keys matching, thus the file will be decrypted and downloaded successfully.



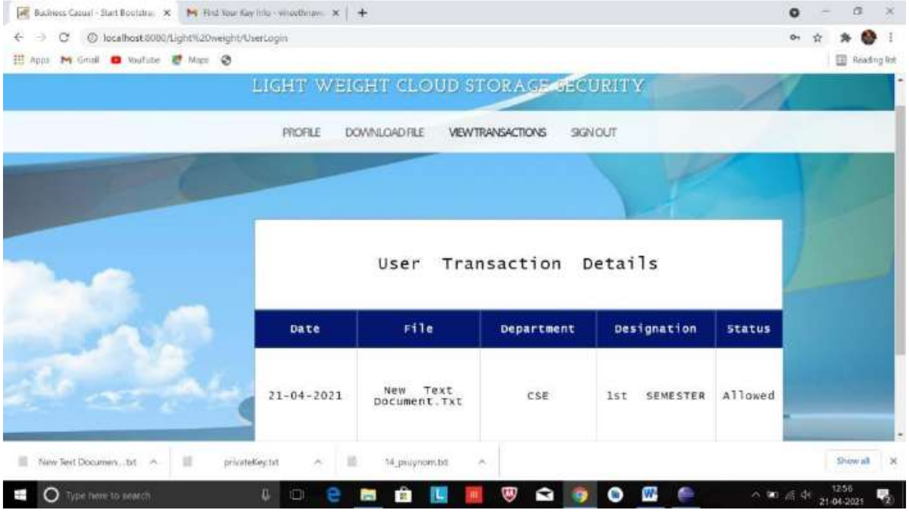
Please Do not press Back or Refresh button.....
Please Wait.........
Download Athentication In Process....

Please Do not press Back or Refresh button.....

Downloadin[illegible] process...
The File [illegible] decrypted...
Please wait....

Figure A.2 – Screenshot of file being downloaded successfully from cloud.

DOI: 10.17148/IJARCCE.2022.11699



User Transaction Details

Date	File	Department	Designation	Status
21-04-2021	New Text Document.Txt	CSE	1st SEMESTER	Allowed

Figure A.3 – Screenshot of user transaction.

REFERENCES

[1] M. H. Au and A. Kapadia, “PERM: Practical reputation-based blacklisting without TTPS,” in Proc. ACM Conf. Comput. Commun. Secur. (CCS), Raleigh, NC, USA, Oct. 2012, pp. 929–940. [2] M. H. Au, A. Kapadia, and W. Susilo, “BLACR: TTP-free blacklistable anonymous credentials with reputation,” in Proc. 19th NDSS, 2012, pp. 1–17.

[3] M. H. Au, W. Susilo, and Y. Mu, “Constant-size dynamic k-TAA,” in Proc. 5th Int. Conf. SCN, 2006, pp.111–125.

[4] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang, “A secure cloud computing based framework for big data information management of smart grid,” IEEE Trans. Cloud Comput., vol. 3, no. 2, pp. 233–244, Apr./Jun.2015.

[5] M. Bellare and O. Goldreich, “On defining proofs of knowledge,” in Proc. 12th Annu. Int. CRYPTO, 1992, pp. 390–420.

[6] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attributebased encryption,” in Proc. IEEESymp. Secur. Privacy, May 2007, pp. 321–334.

[7] D. Boneh, X. Boyen, and H. Shacham, “Short group signatures,” in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2004, pp. 41–55.

[8] D. Boneh, X. Ding, and G. Tsudik, “Fine-grained control of security capabilities,” ACM Trans. InternetTechnol., vol. 4, no. 1, pp. 60–82, 2004.

[9] J. Camenisch, “Group signature schemes and payment systems based on the discrete logarithm problem,” Ph.D. dissertation, ETH Zurich, Zürich, Switzerland, 1998.

[10]J. Camenisch, M. Dubovitskaya, and G. Neven, “Oblivious transfer with access control,” in Proc. 16thACM Conf. Comput. Commun. Secur. (CCS), Chicago, IL, USA, Nov. 2009, pp. 131–140.

[11]J. Camenisch and A. Lysyanskaya, “A signature scheme with efficient protocols,” in Proc. 3rd Int. Conf. Secur. Commun. Netw. (SCN), Amalfi, Italy, Sep. 2002, pp. 268–289.