DUAL ACCESS CONTROL FOR CLOUD-BASED DATA STORAGE AND SHARING

[1]K.Sadanandam, [2]B.Siddartha, [3]P.Vivaan Prakash,[4] D.Rithwik Reddy
[1]Assistant Professor, Dept. of CSE Anurag University
[1]sadanandam.cse@anurag.edu.in
[2,3,4]UG Scholars Dept. CSE Anurag University
[2]20eg105606@anurag.edu.in , [3] 20eg105638@anurag.edu.in ,[4] 20eg105645@anurag.edu.in

Abstract: Cloud-based information capacity administration has drawn expanding interests from both scholar and industry in the new years because of its proficient and minimal expense the board. Since it offers types of assistance in an open organization, it is critical for specialist co-ops to utilize secure information stockpiling and sharing system to guarantee information classification and administration client protection. To safeguard delicate information from being compromised, the most generally utilized strategy is encryption. Be that as it may, essentially encoding information (e.g., through AES) can't completely address the pragmatic need of information the executives. In addition, a compelling access command over download demand likewise should be thought about so Financial Forswearing of Manageability (EDoS) assaults can't be sent off to upset clients from appreciating administration. In this paper, we consider the double access control, with regards to cloud-based capacity, as in we plan a control component over the two information access and download demand without loss of safety and effectiveness. Two double access control frameworks are planned in this paper, where every one of them is for a particular planned setting. The security and exploratory investigation for the frameworks are likewise introduced.

I INTRODUCTION

In the new many years, cloud-based capacity administration has drawn in extensive consideration from both scholarly world and enterprises. It could be broadly utilized in numerous Web based business applications (e.g., Apple iCould) because of its extensive rundown benefits including access flexibility and liberated from neighborhood information the board. Expanding number of people and organizations these days like to re-appropriate their information to remote cloud so that they might diminish th cost of upgrading their local data management facilities/gadgets. However, the worry of security breach over out sourced data might be one of the principal hindrances impeding Web clients from broadly utilizing cloud-based capacity administration. In numerous functional applications, rethought information might should be additionally imparted to other people. For instance, a Drop box client Alice might share photographs with her companions. Without utilizing information encryption, before sharing the photographs, Alice needs to create a sharing connection and further offer the connection with companions. Despite the fact that promising some degree of access command over unapproved clients (e.g., those are not Alice's companions), the sharing connection might be apparent within th eDropbox organization level (e.g., executive could arrive at the connection). Since the cloud (which is sent in an open organization) isn't be completely

trusted, it is for the most part prescribed to scramble the information preceding being transferred to the cloud to guarantee information security and protection. One of the comparing solutions is to directly employ an encryption technique(e.g., AES) on the reevaluated information prior to transferring to cloud, so that just specified cloud client (with legitimate unscrambling key) can get to the information through substantial decoding. To forestall shared photographs being gotten to by the "insiders" of the framework, a clear way is to assign the gathering of approved information clients preceding encoding the information. At times, regardless, Alice might have no clue about who the photograph collectors/clients will be. It is conceivable that Alice just knows about ascribes w.r.t. photograph recipients. For this situation, customary public key encryption (e.g., Paillier Encryption), which requires the encrypt or to know who the information collector is ahead of time, can't be utilized. Giving strategy based encryption system over the rethought photographs is consequently alluring, so Alice utilizes the component to define access strategy over the scrambled photographs to ensure just a gathering of approved clients can get to the photographs. In a cloud-based capacity administration, there exists a typical assault that is notable as asset depletion assault. Since a (public) cloud might not have any command over download request(namely, a service user may send unlimited numbers of download solicitation to cloud server), a pernicious help client might send off the refusal of-administration (DoS)/disseminated disavowal of-administration (DDoS) assaults to consume the asset of distributed storage administration server with the goal that the cloud administration couldn't have the option to answer legitimate clients' administration demands. Thus, in the "pay-more only as costs arise" model, financial angles could be upset because of higher asset use. The expenses of cloud administration clients will rise decisively as the attacks scale up. This has been known as Monetary Refusal of Manageability (EDoS) assault [32], [33], which focuses to the cloud adopter's financial assets. Aside from financial misfortune, limitless download itself could open a window for network assailants to notice the encoded download information that might prompt some potential data spillage (e.g., file size). In this manner, a compelling command over download demand for reevaluated (encoded) information is additionally required. In this paper, we propose another component, named double access control, to handle the above previously mentioned two issues. To get information in cloud-based capacity administration, property based encryption (ABE) [9] is one of the promising candidates that enables the confidentiality of outsourced data as well as finegrained command over the rethought information. Specifically, Cipher text-Strategy ABE (CP-ABE) [5] gives an effective way of data encryption such that access policies, Defining the entrance honor of potential information recipients, can be specified over scrambled information. Note that we think about the utilization of CP-ABE in our component in this paper. Neverthe-less, essentially utilizing CP-ABE method isn't sufficient to plan a rich instrument ensuring the control of the two information access and download demand. A strawman answer for the control of download demand is to use sham cipher texts to check information beneficiary's decoding privileges. It, solidly, requires information proprietor, say Alice, to transfer various "testing" cipher texts alongside the "genuine" encryption of information to cloud, where the "testing" cipher texts are the encryptions of faker messages under the very access strategy as that of the "genuine" information. After receiving a download demand from a client, say Sway, cloud asks Weave to haphazardly unscramble one of the "testing" cipher texts. If a right outcome/unscrambling is returned (for example showing Weave is with substantial decoding freedoms), Sway is

approved by Alice to get to the "genuine" information, so the cloud permits Bounce to download the comparing cipher text. By the by, a few impediments of the above approach might be identified as follows. Most importantly, the information proprietor, Alice, is expected to scramble various sham cipher texts under a similar strategy as the "genuine" cipher text. This might yield an impressive computational above for Alice, which might get burden practice, for test ple, Alice simply needs to transfer one photograph to iCloud from her cell phone, however needs to get ready more than one code messages. Second, all cipher texts, including faker ones, are uploaded to cloud at the same time. This inevitably imposes additional expense on network transmission capacity (as well as delaying information transferring time), which may not be material to some service users whose cellular network is underpay-as-you-go arrangement or furnished with old age of broadband cell network innovation (e.g., 3G). Third, an information beneficiary/client, Bounce, needs to decode an irregular picked "testing" cipher text from cloud, as a trial of his legitimate download demand furthermore. Subsequently, Weave needs to "pay" twofold (unscrambling cost) for getting to the "genuine" information, which again may not be versatile in asset compelled setting. Hence, this paper brings up the accompanying issue.

II LITERATURE SURVEY

To apply ingrained policy-based control over encrypted data, ABE [9] has been introduced in the literature. Concretely, ABE has two main research branches: one is CP-ABE, and the other is KP-ABE which refers to as key-policy ABE. This paper mainly deals with the former. In a CP-ABE, decryption key is associated with attribute set and cipher text is embedded with access policy. This feature makes CP-ABE quite suitable for secure cloud data sharing(compared to KP-ABE). Note this is so because KP-ABE requires decryption key to be associated with access policy which yields heavy storage cost for cloud user. Since the introduction of seminal CP-ABE, many works have been proposed to employ CP-ABE in various applications, e.g., accountable and traceable CP-ABE , multi-authority],outsourced CP-ABE, and extendable variants . Although being able to support finegrained data access, CP-ABE, acting as a single solution, is far from practical and effective to hold against EDoS attack which is the case of DDoS in the cloud setting . Several counter- measures to the attack have been proposed in the literature. But Xue et al. stated that the previous works could not fully defend the EDoS attack in the algorithmic (or protocol) level, and they further proposed a solution to secure cloud data sharing from the attack. However, suffers from two disadvantages. First, the data owner is required to generate asset of challenge cipher texts in order to resist the attack, which enhances its computational burden. Second, a data user is required to decrypt one of the challenge cipher texts as a test, which costs a plenty of expensive operations (e.g., pairing). Here the computational complex-ity of both parties is inevitably increased and meanwhile, high network bandwidth is required for the delivery of cipher texts. The considerable computational power of cloud is not fully consider ding .In this paper, we will present a new solution that requires less computation and communication cost to stands till in front of the EDoS attack. Recently, Antonis Michalas proposed a data sharing protocol that combines symmetric searchable encryption and ABE, which allows users to directly search over encrypted data. To implement the functionality of key revocation in ABE, the protocol utilizes SGX to host a revocation authority. Bakas and Michalas later extended the protocol in and proposed a hybrid encryption scheme that reduces the problem of multi-user data sharing to that of a single-user.

In particular, the symmetric key used for data encryption is stored in an SGX enclave, which is encrypted with an ABE scheme. Similar to [20], it deals with the revocation problem in the context of ABE by employing the SGX enclave. In this work, we employ SGX to enable the control of the download request (such that the DDoS/EDoS attacks can be prevented). In this sense.

III EXISTING SYSTEM

A strawman solution to the control of download request is to leverage dummy ciphertexts to verify data receiver's decryption rights. It, concretely, requires data owner, say Alice, to upload multiple "testing" ciphertexts along with the "real" encryption of data to cloud, where the "testing" ciphertexts are the encryptions of dummy messages under the same access policy as that of the "real" data. After receiving a download request from a user, say Bob, cloud asks Bob to randomly decrypt one of the "testing" cipher text. If a correct result/decryption is returned (i.e. indicating Bob is with valid decryption rights), Bob is authorized by Alice to access the "real" data, so that the cloud allows Bob to download the corresponding cipher text .Nevertheless, several disadvantages of the above approach may be identified as follows.

First of all, the data owner, Alice, is required to encrypt a number of dummy cipher texts under the same policy as the "real" cipher text. This may yield a considerable computational overhead for Alice, which may bring inconvenience in practice, for example, Alice just wants to upload one photo to iCloud from her cell phone, but needs to prepare more than one cipher texts. Second, all cipher texts, including dummy ones, are uploaded to cloud at the same time. This inevitably imposes extra cost on network bandwidth (as well as prolonging data uploading time), which may not be applicable to some service users whose cellular network is under pay-as-you-go plan or equipped with old generation of broadband cellular network technology (e.g., 3G). Third, a data receiver/user, Bob, has to additionally decrypt a random-chosen "testing" cipher text from cloud, as a test of his valid download request. As a result, Bob has to "pay" double (decryption price) for accessing to the "real" data, which again may not be scalable in resource constrained setting.

IV PROPOSED SYSTEM

In this paper, we propose a new mechanism, dubbed dual access control, to tackle the above aforementioned two problems. To secure data in cloud-based storage service, attribute-based encryption (ABE) is one of the promising candidates that enable the confidentiality of outsourced data as well as fine-grained control over the outsourced data. In particular, Cipher text-Policy ABE (CP-ABE) [5] provides an effective way of data encryption such that access policies, defining the access privilege of potential data receivers, can be specified over encrypted data. Note that we consider the use of CP-ABE in our mechanism in this paper. Nevertheless, simply employing CP-ABE technique is not sufficient to design an elegant mechanism guaranteeing the control of both data access and download request.

The systems we propose are with the following distinct features:

(1) Confidentiality of outsourced data. In our proposed systems, the outsourced data is encrypted prior to being uploaded to cloud. No one can access them without valid access rights.

(2) Anonymity of data sharing. Given an outsourced data, cloud server cannot identify data owner, so that the anonymity of owner can be guaranteed in data storage and sharing.

(3) Fine-grained access control over outsourced (encrypted) data. Data owner keeps controlling his encrypted data via access policy after uploading the data to cloud. In particular, a data owner can encrypt his outsourced data under a specified access policy such that only a group of authorized data users, matching the access policy, can access the data.

(4) Control over anonymous download request and EDoS attacks resistance. A cloud server is able to control the download request issued by any system user, where the download request can set to be anonymous. With the control over download request, we state that our systems are resistant to EDoS attacks.

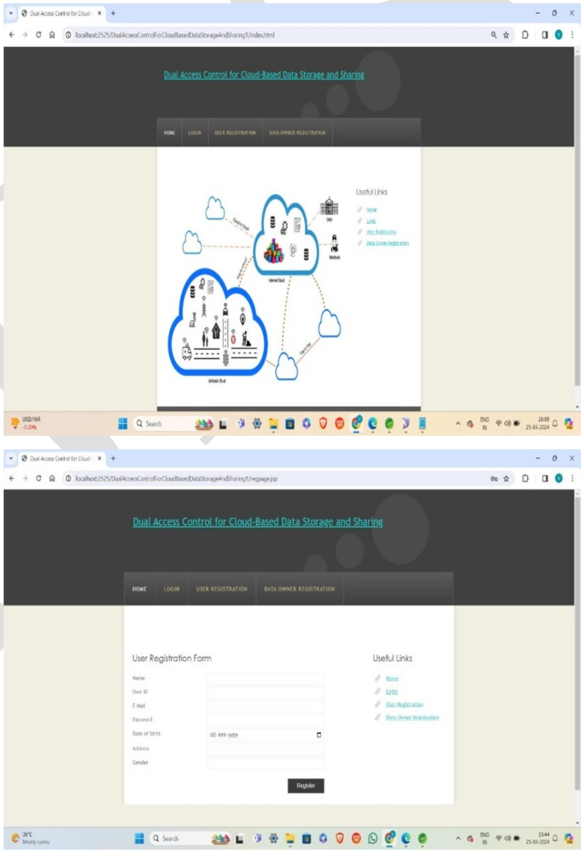
(5) High efficiency. Our proposed systems are built on the top of the CP-ABE system [36]. Compared with [36], they do not incur significant additional computation and communication overhead. This makes the systems feasible for real-world applications.

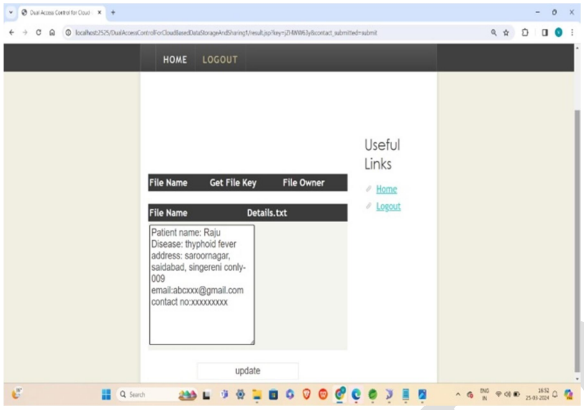
V IMPLEMENTATION

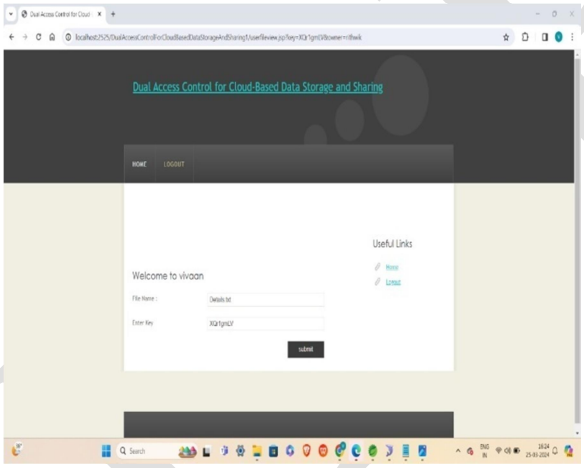
We employ the use of a hybrid system to protect the data, which combines the efficiency of a symmetric-key system with the convenience of a public-key system. In particular, the proposed dual access control systems are both in Key/Data Encapsulation Mechanism (KEM/DEM) setting The message is encrypted by an efficient symmetric-key encryption scheme, while the in efficient public-key scheme (i.e., the CP-ABE) is used only to encrypt/decrypt a short key value. To achieve the security requirements of anonymous data sharing, confidentiality of shared data and access control on shared data, we employ the CP-ABE technique as the basic building block. Specifically, we present the construction based on the CP-ABE scheme in due to its efficiency and elegant construction. To achieve the security requirements of anonymous download request and access control on download request, we design an effective mechanism that the cloud can judge whether a data user is authorized or not without revealing any sensitive information (including the identity of the data user, the plaintext of the outsourced data to it.In the first system, the cloud needs the help of the authority during the judgment on the download request (sent by a data user). As a result, the authority needs to be always online. However, in some other cases in practice the authority may not be always online. This leads to the second (enhanced) system where the authority can be offline after the parameter initialization procedure. In particular, we employ the SGX technique to replace the role of the authority during the access control on download request procedure. We now explain the rationale behind our proposed systems. In order to provide strong security and privacy guarantees for shared data on the cloud (that could defend the EDoS attack), a cloud-based data sharing system should support dual access control as described in Section 1. We start from the CP-ABE system proposed in [36], and adapt it to the KEM/DEM setting. However, simply employing the CP-ABE construction from [36] in the KEM/DEM setting is not sufficient to provide dual access control. New technique needs to be introduced such that the control of both data access and download request can be guaranteed. Different from the strawman solution described in Section1,we intro- duce a new approach to avoid using

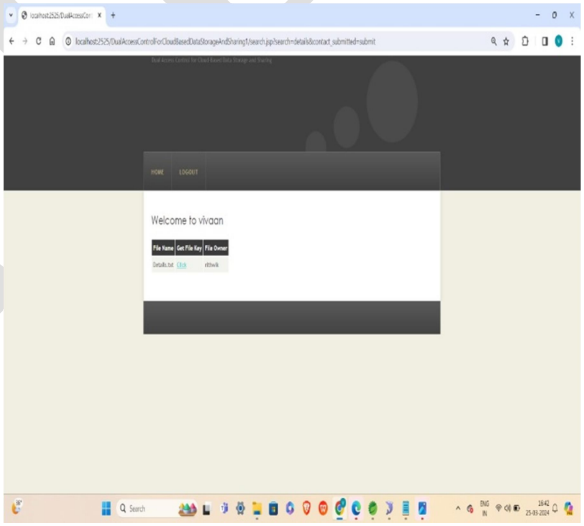
the“testing”ciphertext in the strawman solution. Specifically, we allow the data owner to generate a download request, which contains a randomized form of the secret key held by the data owner. The download request retains the “decryption capability” of the secret key such that it can be used to test whether the underlying data owner is capable to decrypt the shared cipher text(s). Since the above mentioned component contained in the download request is randomized, it cannot be utilized to infer the owner of the secret key. That is, the download request enables the cloud to check whether the data owner of the download request is authorized without leaking the identity of the underlying data owner (i.e., the download request is anonymous). To further prevent leaking secret information to the cloud, the verification of download request needs the help of the authority or the enclave of Intel SGX. Our first system is designed for the case where the verification of download request involves the help of the authority, while the second system is designed for the case where the enclave of Intel SGX is involved during the verification of download request procedure. We note that our technique described above is general in the sense that it can be applied to most of the current CP-ABE constructions based on bilinear maps.

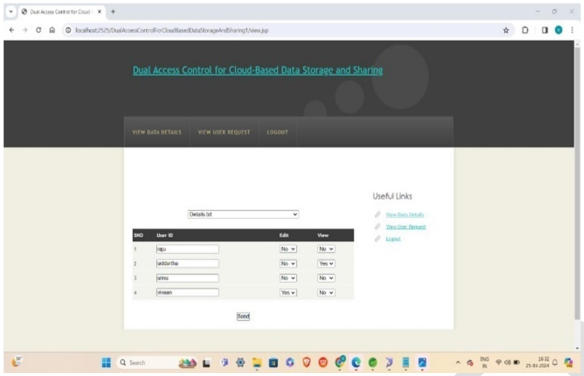
VI RESULTS

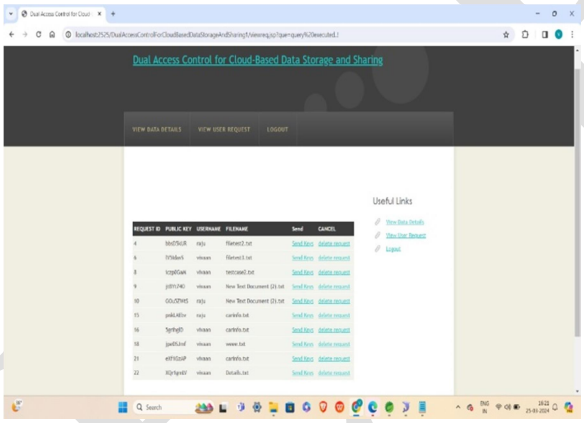



HOME
LOGOUT
Useful Links
Home
Logout
File Name
Get File Key
File Owner
File Name
Details.txt
Patient name: Raju
Disease: thyphoid fever
address: saroornagar,
saidabad, singereni conly-
009
email:abcxxx@gmail.com
contact no:xxxxxxxxxx
update


Dual Access Control for Cloud-Based Data Storage and Sharing
HOME
LOGOUT
Useful Links
Welcome to vivaan
submit


HOME
LOGOUT
Welcome to vivaan





VII CONCLUSION

We resolved a fascinating and dependable issue in cloud-based information sharing, and introduced two double access control frameworks. The proposed frameworks are impervious to DDoS/EDoS assaults. We express that the method used to achieve the feature of control on download request is"trans-plantable "to other CP-ABE constructions. Our experimental results show that the proposed frameworks don't force any significant computational and communication over head (contrasted with its fundamental CP-ABE building block). In our upgraded framework, we utilize the way that the restricted data stacked into the area can't be extracted. Notwithstanding, ongoing work shows that territory might spill some amounts of its secret(s)to a malicious host through the memory access designs]or other related side-divert attacks The model of transparent enclave execution is subsequently presented in Building a double access control framework for cloud information sharing from straightforward territory is an interesting problem.

REFERENCES

[1] Joseph A Akinyele, Christina Garman, Ian Miers, Matthew W Pagano, Michael Rushanan, Matthew Green, and Aviel D Rubin. Charm: a framework for rapidly prototyping cryptosystems. Jour- nal of Cryptographic Engineering, 3(2):111–128, 2013.

[2] IttaiAnati, Shay Gueron, Simon Johnson, and Vincent Scarlata. Innovative technology for cpu based attestation and sealing. In Workshop on hardware and architectural support for security and priva- cy (HASP), volume 13, page 7. ACM New York, NY, USA, 2013.

[3] AlexandrosBakas and AntonisMichalas. Modern family: A revo- cable hybrid encryption scheme based on attribute-based encryp- tion, symmetric searchable encryption and SGX. In SecureComm 2019, pages 472–486, 2019.

[4] Amos Beimel. Secure schemes for secret sharing and key distribution. PhD thesis, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

[5] johnBethencourt,AmitSahai,andBrentWaters. Ciphertext-policy attribute-based encryption. In S&P 2007, pages 321–334. IEEE, 2007.

[6] Victor Costan and SrinivasDevadas. Intel sgx explained. IACR Cryptology ePrint Archive, 2016(086):1–118, 2016.

[7] Ben Fisch, DhinakaranVinayagamurthy, Dan Boneh, and Sergey Gorbunov. IRON: functional encryption using intel SGX. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, pages 765–782, 2017. [8] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Advances in Cryptology-CRYPTO 1999, pages 537–554. Springer, 1999.

[9] VipulGoyal, OmkantPandey, AmitSahai, and Brent Waters. Attribute-based encryption for fine-grained access control of en- crypted data. In ACM CCS 2006, pages 89–98. ACM, 2006.

[10] Jinguang Han, Willy Susilo, Yi Mu, Jianying Zhou, and Man Ho Allen Au. Improving privacy and security in decentralized ciphertext-policy attribute-based encryption. IEEE transactions on information forensics and security, 10(3):665–678, 2015.

[11] Christofer Hoff. Cloud computing security: From ddos (distribut- ed denial of service) to edos (economic denial of sustainability). http://www. rationalsurvivability.com/blog/?p=66.

[12] Joseph Idziorek, Mark Tannian, and Doug Jacobson.Attribution of fraudulent resource consumption in the cloud. In IEEE CLOUD 2012, pages 99–106. IEEE, 2012.

[13] Simon Johnson, Vinnie Scarlata, Carlos Rozas, Ernie Brickell, and Frank Mckeen. Intel RSoftware guard extensions: Epid provision-ing and attestation services. White Paper, 1:1–10, 2016.

[14] Sangho Lee, Ming-Wei Shih, Prasun Gera, Taesoo Kim, Hyesoon Kim, and Marcus Peinado. Inferring fine-grained control flow inside sgx enclaves with branch shadowing. In 26th USENIX Security Symposium, USENIX Security, pages 16–18, 2017.

[15] Jiguo Li, Xiaonan Lin, Yichen Zhang, and Jinguang Han. Ksf- oabe: outsourced attribute-based encryption with keyword search functionforcloudstorage. IEEETransactionsonServicesComputing, 10(5):715–725, 2017.

[16] Jiguo Li, Yao Wang, Yichen Zhang, and Jinguang Han. Ful- l verifiability for outsourced decryption in attribute based encryption. IEEE Transactions on Services Computing, DOI: 10.1109/TSC.2017.2710190, 2017.

[17] Wei Li, KaipingXue, YingjieXue, and Jianan Hong. Tmacs: A robust and verifiable threshold multi-authority access control system in public cloud storage. IEEE Transactions on parallel and distributed systems, 27(5):1484–1496, 2016.

[18] Ben Lynn et al. The pairing-based cryptography library. Internet: crypto. stanford. edu/pbc/[Mar. 27, 2013], 2006.

[19] Frank McKeen, IlyaAlexandrovich, Alex Berenzon, Carlos V. Rozas, HishamShafi, VedvyasShanbhogue, and Uday R. Sava- gaonkar. Innovative instructions and software model for isolated execution. In HASP@ISCA 2013, page 10, 2013.

[20] AntonisMichalas. The lord of the shares: combining attribute- based encryption and searchable encryption for flexible data shar- ing. In SAC 2019, pages 146–155, 2019.