IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

DESIGN OF MODIFIED AES ALGORITHM FOR END-TO-END DATA SECURITY

Rubhashree M

Assistant Professor
Department of computer science and Engineering
Jansons Institute of Technology,Coimbatore

Ragul P,Ramana G K,Sharmila C,Susmitha Sri M

Final Year
Department of computer science and Engineering
Jansons Institute of Technology,Coimbatore

ABSTRACT:

Cryptography is a process by which information or messages can be sent from one user to another user which provides several security services such as confidentiality, data integrity or authentication to the wireless communication system. As there is need for secure communication, efficient cryptographic processing is required for good system performance. An effective access control over download request also needs to be considered so that Economic Denial of Sustainability (EDoS) attacks cannot be launched to hinder users from enjoying service. In this paper, we consider the dual access control, in the context of cloud-based storage, in the sense that we design a control mechanism over both data access and download request without loss of security and efficiency. Two dual access control systems are designed in this paper, where each of them is for a distinct designed setting.

1.INTRODUCTION:

In a cloud-based storage service, there exists a common attack that is well-known as resource-exhaustion attack. Since a (public) cloud may not have any control over download request namely, a service user may send unlimited numbers of download request to cloud server, a malicious service user may launch the denial-of-service (DoS)/distributed denial-of-service (DDoS) attacks to consume the resource of cloud storage service server so that the cloud service could not be able to respond honest users' service requests. Asa result, in the "pay-as-you-go" model, economic aspects could be disrupted due to higher resource usage. The costs of cloud service users will rise dramatically as the attacks scale up. This has been known as Economic Denial of Sustainability (EDoS) attack, which targets to the cloud adopter's economic resources. Apart from economic loss, unlimited download itself could open a window for network attackers to observe the encrypted download data that may lead to some potential information leakage (e.g,file size). In this project, we propose a new mechanism, Digital Signature based Trio Access Control with Key Shares, to tackle the above aforementioned two problems and also Key stealing attacks and network URL attacks.

2.EXISTING SYSTEM AND ITS DRAWBACKS

Existing system is a Charm, an extensible framework for rapidly prototyping cryptographic systems. Charm provides a number of features that explicitly support the development of new protocols, including support for modular composition of cryptographic building blocks, infrastructure for developing interactive protocols, and an extensive library of re-usable code.

Our framework also provides a series of specialized tools that enable different cryptosystems to interoperate. We implemented over 40 cryptographic schemes using Charm, including some new ones that, to our knowledge, have never been built in practice.

First, the data owner is required to generate a set of challenge ciphertexts in order to resist the attack, which enhances its computational burden.

Second, a data user is required to decrypt one of the challenge ciphertexts as a test, which costs a plenty of expensive operations (e.g., pairing). Here the computational complexity of both parties is inevitably increased and meanwhile, high network bandwidth is required for the delivery of ciphertexts.

PROPOSED WORK:

Proposed system is 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 enables the confidentiality of outsourced data as well as fine- grained control over the outsourced data. Digital Signature generation using ECC is used to generate digital signature to the users, that will avoids network and URL based attacks. Key Shares are added in this account to avoid cloud insiders key stealing attacks. Overall “Digital Signature based Trio Access Control with Key Shares” will provide high secure to the cloud systems.

4. MODULES:

1. User Interface Administration: The main idea of this module is to design the user interface for users in the project. The login page is to design for data owner and data user. After the data owner logins into the system, the page displayed which allows the data owner to achieve the encrypted file upload to the system. When the user logins to the system, the system allows the user to input the decryption key and attributes for retrieval of specified file. Before accessing the file from system, the user must register into the system.

2. File Encryption and Uploading: Each file which is to be uploaded is encrypted with encryption key. Once file is encrypted, next step is to upload it to the storage system along with data decryption key. Owner specifies the set of attributes for access structure, it then encrypts the file. Finally, owner uploads encrypted file and encryption key and set of attributes to the storage system.

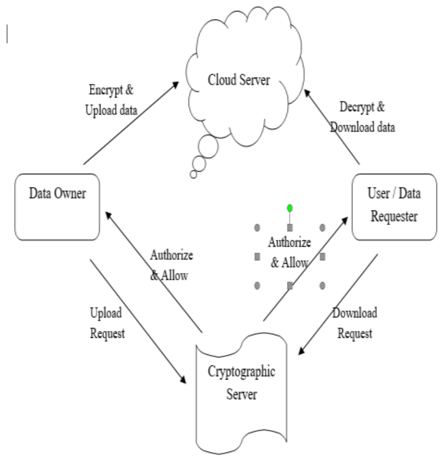
3. Access Control on Download Request: This module provides the access control over download request in the sense that only authorized users can download and the shared data. For a download request DReq for a shared encrypted file, the access control on download request procedure consists of the following steps:
The user gives a call request and sends the request to the cloud server.
Upon receiving the call request from the user, the cloud server authority takes DReq as input. It then checks and sends approval to the user. Then the data gets downloaded to the corresponding user.
If does not satisfy, the data will not get decrypted and downloaded.

4. Key Share Generation: K is a random secret generated by the CS for each of the data files. The length of K in SeDaSC is 256 bits, as is recommended by most of the standards regarding key length for symmetric key algorithms (SKAs). However, the length of the key can be altered according to the requirements of the underlying SKA. K is obtained in a two-step process. In the first step, a random number R of length 256 bits is generated such that R = {0, 1}256. In the next step, R is passed through a hash function that could be any hash function with a 256-bit output. In our case, we used secure hash algorithm 256 (SHA-256). The second step completely randomizes the initial user-derived random number R. The output of the hash function is termed as K and is used in symmetric key encryption [e.g., the Elliptic Curve Cryptography (ECC)] for securing the data.
CS Key Share Ki: For each of the users in the group, the CS generates Ki, such that Ki = {0, 1}256. Ki serves as the CS portion of the key and is used to compute K whenever an encryption/decryption request is received by the CS. Moreover, it is ensured by comparison that the distinct Ki is generated for every file user.
User Key Share Ki: Kis computed for each of the users in the group as follows:
K1i= K $\oplus$ Ki., Ki serves as the user portion of the key and is used to compute K when needed.

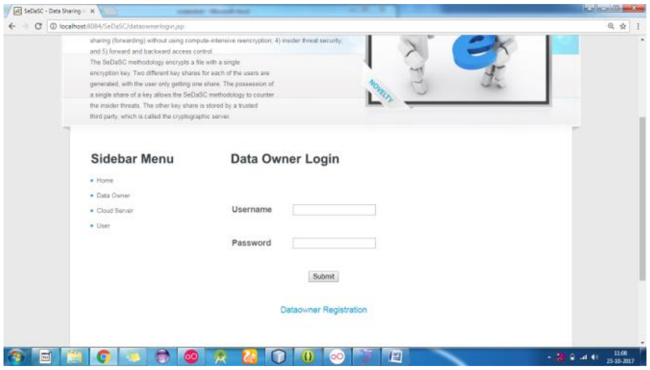
5. Access Control on Download Request: This module provides the access control over download request in the sense that only authorized users can download and the shared data. For a download request DReq for a shared encrypted file, the access control on download request procedure consists of the following steps:
– The user gives a call request and sends the request to the cloud server.
– Upon receiving the call request from the user, the cloud server authority takes DReq as input. It then checks and sends approval to the user. Then the data gets downloaded to the corresponding user.
– If does not satisfy, the data will not get decrypted and downloaded.

6.File Decryption and Download: User requests the file by providing details and in response system replies with encrypted file. Before that the system will check the role and signature of the users whether the receiver have the same role as the sender mentioned. It will avoid the unauthorized users or hackers. The receiver receives the encrypted file, and he has correct role and signature, if it’s correct, the original file gets decrypted for the receiver. This allows them to access information without authorization and thus poses a risk to information privacy.

5. ARCHITECTURE DIAGRAM



6. OUTCOMES:


SeDaSC - Data Sharing

localhost:8084/SeDaSC/dataownerlogin.jsp

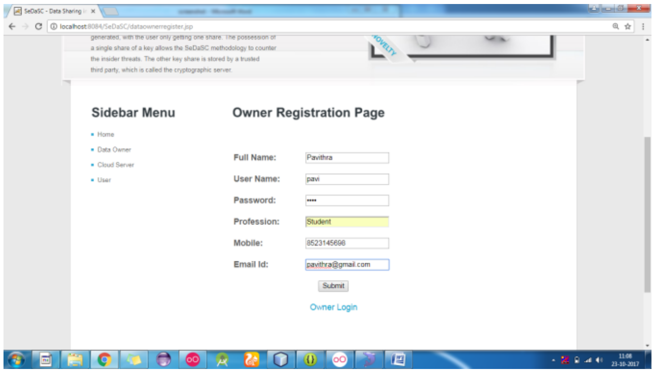
sharing (forwarding) without using compute-intensive reencryption; 4) insider threat security; and 5) forward and backward access control.
The SeDaSC methodology encrypts a file with a single encryption key. Two different key shares for each of the users are generated, with the user only getting one share. The possession of a single share of a key allows the SeDaSC methodology to counter the insider threats. The other key share is stored by a trusted third party, which is called the cryptographic server.

Sidebar Menu

Data Owner Login

Username

Password


SeDaSC - Data Sharing

localhost:8084/SeDaSC/dataownerregister.jsp

generated, with the user only getting one share. The possession of a single share of a key allows the SeDaSC methodology to counter the insider threats. The other key share is stored by a trusted third party, which is called the cryptographic server.

Sidebar Menu

Owner Registration Page

Full Name: Pavithra

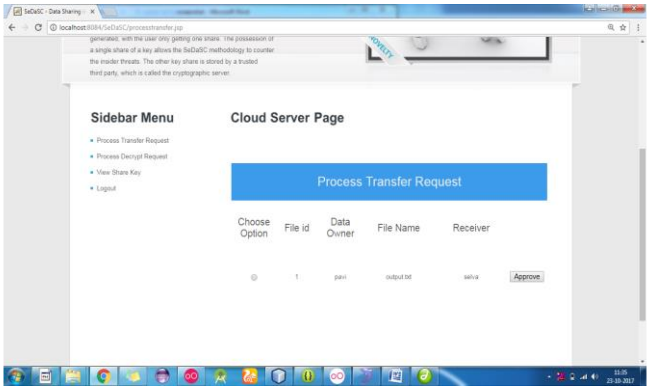
User Name: pavi

Password: ••••

Profession: Student

Mobile: 8523145698

Email Id: pavithra@gmail.com


SeDaSC - Data Sharing

localhost:8084/SeDaSC/processtransfer.jsp

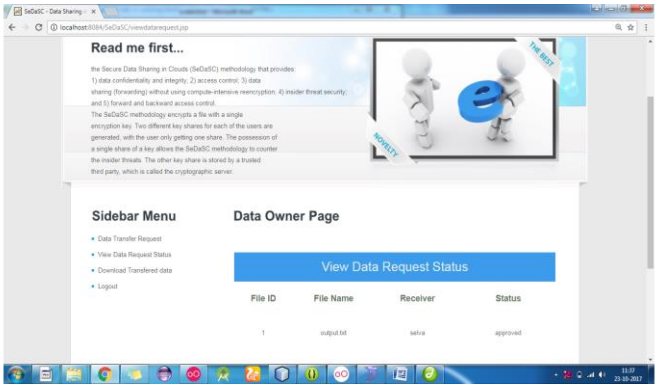
generated, with the user only getting one share. The possession of a single share of a key allows the SeDaSC methodology to counter the insider threats. The other key share is stored by a trusted third party, which is called the cryptographic server.

Sidebar Menu

Cloud Server Page

Process Transfer Request

Choose Option	File id	Data Owner	File Name	Receiver	
○	1	pavi	output.txt	selva	Approve


SeDaSC - Data Sharing

localhost:8084/SeDaSC/viewdatarequest.jsp

Read me first...

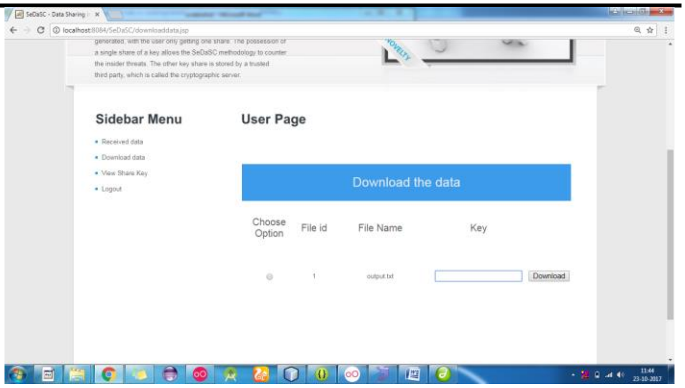
the Secure Data Sharing in Clouds (SeDaSC) methodology that provides: 1) data confidentiality and integrity; 2) access control; 3) data sharing (forwarding) without using compute-intensive reencryption; 4) insider threat security; and 5) forward and backward access control.
The SeDaSC methodology encrypts a file with a single encryption key. Two different key shares for each of the users are generated, with the user only getting one share. The possession of a single share of a key allows the SeDaSC methodology to counter the insider threats. The other key share is stored by a trusted third party, which is called the cryptographic server.

Sidebar Menu

Data Owner Page

View Data Request Status

File ID	File Name	Receiver	Status
1	output.txt	selva	approved


SeDaSC - Data Sharing

localhost:8084/SeDaSC/downloaddata.jsp

generated, with the user only getting one share. The possession of a single share of a key allows the SeDaSC methodology to counter the insider threats. The other key share is stored by a trusted third party, which is called the cryptographic server.

Sidebar Menu

User Page

Download the data

Choose Option	File id	File Name	Key	
○	1	output.txt		Download

7. CONCLUSION:

Secure Cloud Data Sharing using Digital Signature based Trio Access Control with Key Shares is implemented to secure the data transfer by verifying the data owner, user and the cloud server. The user also have to be verified before getting the file, this verification is done by cloud server. The key shares are generated and shared with user and the cloud server. To secure data in cloud-based storage service, key share is one of the promising candidates that enables the confidentiality of outsourced data as well as fine-grained control over the outsourced data. Digital Signature generation using ECC is used to generate digital signature to the users, that will avoids network and URL based attacks. Key Shares are added in this account to avoid cloud insiders key stealing attacks. Overall "Digital Signature based Trio Access Control with Key Shares" will provide high secure to the cloud systems. In the future, it would be interesting to consider Digital Signature based Trio Access Control with different types of expressibility. While, Digital Signature based Trio Access Control and Key shares capture two interesting and complimentary types of systems there certainly exist other types of systems. The primary challenge in this line of work is to find a new systems with elegant forms of expression that produce more than an arbitrary combination of techniques.

REFERENCES

1. Joseph A Akinyele, Christina Garman, Rubin. Charm: a framework for rapidly prototyping cryptosystems. Journal of Cryptographic Engineering, 3(2):111–128, 2013.

2. Ittai Anati, Shay Gueron, Simon Johnson, and Vincent Scarlata. Innovative technology for cpu based attestation and Ian Miers, Matthew W Pagano, Michael Rushanan, Matthew Green, and Aviel D sealing. In Workshop on hardware and architectural support for security and privacy (HASP), volume 13, page 7. ACM New York, NY, USA, 2013.

3. Alexandros Bakas and Antonis Michalas. Modern family: A revocable hybrid encryption scheme based on attribute-based encryption, 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. John Bethencourt, Amit Sahai, and BrentWaters. Ciphertext-policy attribute-based encryption. In S&P 2007, pages 321–334. IEEE, 2007.

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

7. Ben Fisch, Dhinakaran Vinayagamurthy, 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.