International Journal of Scientific Research in Computer Science, Engineering and Information Technology

© 2018 IJSRCSEIT | Volume 3 | Issue 7 | ISSN : 2456-3307

An Efficient Certificate Less Encryption for Secure Data Sharing In Public Clouds

D. Sudha[1], D. Nandhini[2*]

[1]Assistant Professor, Department of Computer Science A.V.C College, Mayiladuthurai, Tamil Nadu, India

[*2]Research Scholar, Department of Computer Science A.V.C College, Mayiladuthurai, Tamil Nadu, India

ABSTRACT

Mediated certificateless encryption scheme is proposed without pairing operations for securely sharing sensitive statistics in public clouds. Mediated certificateless public key encryption (mCL-PKE) solves the key escrow problem in identification based totally encryption and certificate revocation problem in public key cryptography. However, existing mCL-PKE schemes are both inefficient because of the usage of pricey pairing operations or inclined against partial decryption assaults. In order to deal with the overall performance and protection troubles, in this proposed work, first propose a mCL-PKE scheme without the usage of pairing operations. Apply mCL-PKE scheme to assemble a sensible solution to the trouble of sharing touchy facts in public clouds. The cloud is employed as a secure garage as well as a key generation middle. In this gadget, the statistics owner encrypts the sensitive records the use of the cloud generated users' public keys based totally on its get entry to manage rules and uploads the encrypted records to the cloud. Keys are generated using KP-ABE encryption scheme. Upon a success authorization, the cloud partially decrypts the encrypted data for the users. The users finally fully decrypt the partly decrypted records the usage of their personal keys. The confidentiality of the content and the keys is preserved with admire to the cloud, due to the fact the cloud cannot completely decrypt the facts. Additionally recommend an extension to the above technique to enhance the efficiency of encryption at the data proprietor. Here implement mCL-PKE scheme and the overall cloud based device, and compare its protection and performance. This effects show that proposed schemes are efficient and realistic.

Keywords : Secure Data Sharing, Public Key Encryption, mCL-PKE scheme, Access Control Policy, Secure Decryption

I. INTRODUCTION

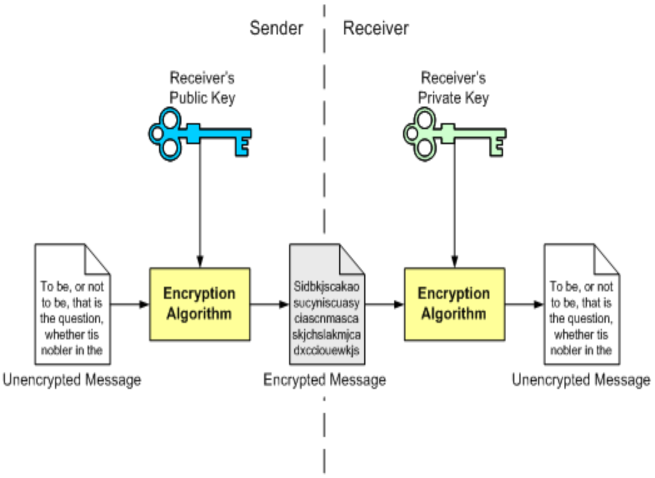
Data security over cloud is extra burden to carrier providers and users. The use of public keys in conventional public key schemes calls for certain information systems called digital certificate to bind the position identifiers with public keys, which makes most ever proposed certificate-primarily based public-key encryption schemes inherently be afflicted by the troubles of keys generation, garage and management of revoked and non-revoked virtual certificates. In current years, how fine to installation and control the Public-Key Infrastructures to aid the authentication of cryptographic keys in current cryptosystems has become a habitual catch 22 situation. Many Identity based public key encryption schemes were proposed to simplify the keys management and do away with the need of virtual certificate in view that Shamir introduced the idea of identity-primarily based cryptography (IBC) in 1984 to deal with the demanding situations triggered by virtual certificate. But the inherent non-public key escrow of ID-based totally cryptography continues to be a key difficulty to be solved as all personal keys of the customers are generated by a relied on trusted third party (TTP) who may want to decrypt any message or join up behalf of any entity.

Public-key cryptography, or asymmetric cryptography, is an encryption scheme that uses two mathematically associated, however not identical, keys - a public key and a non-public key. Unlike symmetric key algorithms that depend on one key to each encrypt and decrypt, every key performs a unique feature. The public key is used to encrypt and the private secret's used to decrypt. It is computationally infeasible to compute the personal key based on the general public key. Because of this, public keys may be freely shared, permitting users an easy and convenient technique for encrypting content material and verifying digital signatures, and private keys can be stored secret, making sure best the proprietors of the personal keys can decrypt content material and create virtual signatures.

Since public keys want to be shared but are too big to be easily remembered, they're stored on virtual certificates for secure shipping and sharing. Since private keys aren't shared, they're absolutely stored within the software program or working gadget you operate, or on hardware (e.G., USB token, hardware protection module) containing drivers that allow it to be used with present software program or working system.

In the certificateless machine, KGC only knows the partial private key of a person who also uses a secret value to obtain his full private key. The CL-PKC is a model of public key cryptography that is intermediate among the identification-based and traditional PKI strategies and is designed to conquer the key escrow problem of identification-based cryptography. Many certificateless public key encryption schemes and corresponding certificateless signature schemes the usage of bilinear pairings had been proposed. However, most ever proposals centered on developing public key structures to avoid using certificate and they didn't suitable an surroundings in which immediately revocation may be required.

Multiple encryption and decryption, certificates and other protection troubles make more highly-valued for facts protection inside the cloud. To cope with these barriers, The Mediated Certificate-much less public key encryption scheme is proposed. In this approach, the data security is as identical to the certificated encryption techniques. This scheme does not considered on the pairing based operation. It reduces the computational overhead and to efficiently encrypt for more than one users. The novel approach of mclPKE scheme is to percentage cozy records in public clouds. It does now not be afflicted by the key escrow problem. The KP-ABE Asymmetric key technique used for performing encryption for multiple customers. The KP-ABE algorithm is successfully encrypt and decrypt the record using record key. It also be used for appearing virtual signature and it will be helpful for improving the safety.


Sender
Receiver
Receiver's Public Key
Receiver's Private Key
To be, or not to be, that is the question, whether tis nobler in the
Encryption Algorithm
Sidbkjscakao sucyniscuasy ciascnmasca skjchslakmjca dxccioueukjs
Encryption Algorithm
To be, or not to be, that is the question, whether tis nobler in the
Unencrypted Message
Encrypted Message
Unencrypted Message

Process of Public Key Encryption

Purpose of Encryption

Confidentiality - Due to the fact the content is encrypted with an character's public key, it can only be decrypted with the person's personal key, making sure best the intended recipient can decrypt and view the contents.

Integrity - Part of the decryption process includes verifying that the contents of the original encrypted message and the brand new decrypted fit, so even the slightest change to the unique content material might purpose the decryption procedure to fail.Comparison between Public and Private Key Encryption

Comparison among Public and Private Key Encryption

Public key cryptography is not supposed to take the region of private key cryptography; it's miles for use as a complement to the secret key structures. That being stated, there are some times when private key cryptography is not perfect and public key cryptography will become critical, in particular in conditions with massive numbers of users. Typically, public key encryption is the cryptography method of choice when there is a multi-consumer environment and it is necessary to make certain confidentiality through key distribution and digital signatures for verifying user identities.

Public key cryptology has a bonus over symmetric personal key encryption structures as it circumvents the logistics and dangers inherent to secretly swapping keys. Due to its scalability and heightened security when compared to non-public key cryptography, public key cryptography stays incredibly famous and is broadly utilized in business enterprise environments these days.

II. RELATED WORK

Reza Curtmola, et.al,.[1] proposed alternative method to security definitions is the so referred to as semantic security or "simulation-primarily based" technique. At a excessive stage, in such an method the safety guarantee is provided via the lifestyles, for all adversaries, of a polynomial-time set of rules which, being given very little facts, is able to compute whatever the adversary is capable of compute from the given information, also gift simulation-based definitions for SSE, each for the non-adaptive and adaptive setting. Searchable symmetric encryption (SSE) lets in a celebration to outsource the storage of its information to any other birthday party (a server) in a non-public way, even as retaining the capacity to selectively seek over it. This trouble has been the focal point of active research in latest years. The first production is the most efficient non-adaptive SSE scheme up to now in phrases of computation on the server, and incurs a minimal (i.e., regular) price for the person. Proposed 2d creation achieves adaptive security, which was not formerly done with the aid of any consistent-round solution. Proposed multi-person construction is very green at the server side: whilst given a trapdoor, the server best desires to assess a pseudo-random permutation as a way to determine if the user is revoked. If access control mechanisms have been used alternatively for this step, a "heavier" authentication protocol might be required.

David Cash, et.al,.[2] proposed work consist the layout, evaluation and implementation of the primary searchable symmetric encryption (SSE) protocol that supports conjunctive search and trendy Boolean queries on outsourced symmetrically-encrypted records and that scales to very huge databases and arbitrarily structured records together with loose textual content seek. To date, paintings on this vicinity has focused specially on unmarried-keyword seek. For the case of conjunctive seek, prior dedicated SSE buildings required work linear within the general wide variety of documents in the database and furnished exact privateness most effective for based characteristic-price records, rendering those solutions too gradual and rigid for huge realistic databases. The premise of this paintings is that in order to provide absolutely practical SSE answers one needs to just accept a sure degree of leakage; therefore, the intention is to gain an acceptable stability among leakage and overall performance, with formal evaluation making sure higher bounds on such leakage. Answers strike such a practical stability by offering performance that scales to very big facts bases; helping search in both dependent and textual information with well known Boolean queries; and confining leakage to get entry to (to encrypted information) styles and some query-time period repetition handiest, with formal evaluation defining and proving the exact limitations of leakage. Stress that at the same time as in proposed solutions leakage by no means happens within the shape of direct publicity of undeniable statistics or searched values, whilst combined with facet-statistics that the server might also have (e.G., what are the most commonplace searched words), such leakage can permit for statistical inference on plaintext data.

Chang Liuy, et.al,.[3] proposed the perception of Multi-Data-Source SSE (MDS-SSE), which allows each data supply to build a neighborhood index in my opinion and allows the storage company to merge all local indexes into a international index afterwards. Here advocate a unique MDS-SSE scheme, wherein an adversary simplest learns the variety of statistics sources, the quantity of complete statistics files, the get right of entry to sample and the quest pattern, but no longer some other distribution records inclusive of how information files or search outcomes are allotted over information resources. This will provide rigorous security proof of proposed scheme, and report experimental outcomes to illustrate the efficiency of proposed scheme. There are 3 roles in a MDS-SSE device: (1) okay data assets, denoted as DS = DS1, ...,DSk, who very own okay collections of statistics documents. (2) Data users, denoted as DU, who trouble search queries for fascinated keywords. (3) Storage issuer, denoted as SP, who stores encrypted person facts documents and responses DU’s seek queries. Note that DU may be DS themselves, or any authorized users who proportion the name of the game key with DS. DS encrypt facts documents and construct searchable indexes before statistics outsourcing. DU use secret key to problem seek tokens and afterwards SP searches the index and returns the identifiers of information files containing searched keywords.

Peng Xu, et.al,.[4] proposed a customary differences from identity-based encryption (IBE) to PEFKS respectively underneath special conditions, and show their SS-CKA and IK-NCK-KGA securities. Specifically, first gift a established transformation for the key-word space with the uniform distribution (known as PEFKS-UD). Also advise an instance of PEFKS-UD primarily based at the anonymous IBE scheme. Secondly, endorse every other regular transformation for the keyword area with the non-uniform distribution (referred to as PEFKS-ND). In addition, cite two strategies to kind keywords, that's the key to recognize PEFKS-ND. Beyond the attitude of cryptosystem, discuss the biased benefit of KGA on PEFKSND, which is as a result of the non-uniform distribution of the keyword space, and remove darkness from that have reduced the biased gain as a lot as feasible. When receiving a query, FuzzTest is used to filter maximum of ineffective key-word searchable ciphertexts. But the remainders still include the keyword searchable ciphertexts which do not fulfill the question. ExactT est is used to discover the suitable keyword searchable ciphertexts from those remainders. In exercise, a proxy server implements FuzzTest to reply the question of a receiver. The receiver implements ExactT est to discover the appropriate searchable ciphertexts from the responses.

Rouzbeh Behnia, et.al,.[5] proposed a Public key Encryption with Keyword Search (PEKS) targets in mitigating the influences of data privacy as opposed to utilization dilemma by means of allowing any consumer within the machine to ship encrypted files to the server to be searched with the aid of a receiver.

The receiver can retrieve the encrypted documents containing unique keywords by way of supplying the corresponding trapdoors of these key phrases to the server. Despite their merits, the existing PEKS schemes introduce a excessive give up-to-give up delay which can preclude their adoption in exercise. Moreover, here do now not scale nicely for big security parameters and provide no put up-quantum safety promise. In this work, advise novel lattice-based totally PEKS schemes that provide a excessive computational efficiency along side higher protection assurances than that of present options. Specifically, NTRUPEKS scheme achieves 18 instances decrease stop-to-cease delay than the maximum efficient pairing-based options. Proposed LWE-PEKS gives provable safety inside the trendy version with a reduction to the worst-case lattice troubles. This absolutely carried out NTRU-PEKS on embedded devices with a deployment on real cloud infrastructures to illustrate its effectiveness.

III. IMPLEMENTATION

Implementation is the process of executing the security concerns in cloud environment. In proposed work certificateless access control with secure encryption mechanism was implemented. In below existing and proposed work of the secure file sharing mechanism was explained.

Attribute-based Encryption Scheme with Non-Monotonic Access Structures

Preceding ABE schemes had been reserved to expressing satisfactory monotonic get right of entry to structures and there may be no remarkable technique to correspond to horrible constraints in a keys receives right of access to additives. Non-monotonic right of entry shape can use the awful word to explain each attribute in the message, but the monotonic get admission to the structure can't. This scheme includes 4 algorithms:

Setup(d): In the easy production, a factor d specifies what number of attributes each cipher text has.

Encryption (M, γ,PK): To encrypt a spatial statistics M ε GT under a fixed of d attributes γ C Zp, pick out a random costs ε Zp and output the cipher textual content E.

Key Generation (˜A, MK, PK): This set of regulations outputs a key D that lets in the purchaser to decrypt an encrypted message tremendous if the attributes of that cipher text fulfill the accessed shape ˜A

Decrypt(CT;D): Input the encrypted statistics CT and personal key D, if they get entry to structure is happy it generate the proper spatial information M.

It permits Non-monotonic insurance, i.e. Coverage with awful attributes. The trouble with Attribute-based totally absolutely Encryption method with Non- Monotonic Access Structures is that there are numerous bad attributes in the encrypted records, however, they do no longer narrate to the encrypted data. It way that every function presents a terrible phrase to give an explanation for it, but those are vain for decrypting the encrypted data. It can reason the encrypted records overhead becoming huge. It is incompetent and compounds every cipher textual content needs to be encrypted with d attributes, in which d is a device smart ordinary.

mCL-PKE Scheme:

The proposed mCL-PKE methodology solves the key escrow problem of traditional identity-based cryptosystems and provides instantaneous revocation property simultaneously. A model for the use of public key cryptography which avoids the inherent escrow of identity-based cryptography and yet which does not require certificates to guarantee the authenticity of public keys. The non-availability of certificates and the presence of an adversary who has access to a master key necessitates the careful development of a new security model. Here focus on mediated certificateless public key encryption (mCL-PKE), showing that a concrete pairing-based mCL-PKE scheme is secure provided that an underlying problem closely related to the bilinear Diffie-Hellman problem is hard.

mCL-PKE Processing Steps:

A mCL-PKE scheme is specified by seven randomized algorithms: Setup, Partial-Private-Key-Extract, Set-Secret-Value, Set-Private-Key, Set-Public-Key, Encrypt and Decrypt:

Setup: This set of rules takes security parameter k and returns the gadget parameters params and master-key. The system parameters includes an outline of the message area M and ciphertext area C. Usually, this set of rules is administered with the aid of the KGC. Count on during that params are publicly and authentically to be had, however that simplest the KGC is aware of master-key.

Partial-Private-Key-Extract: This algorithm takes params, master-key and an identifier for entity A, IDA ∈ zero, 1 ∗ , as enter. It returns a partial private key DA. Usually this set of rules is run by means of the KGC and its output is transported to entity A over a private and true channel.

Set-Secret-Value: This algorithm takes as inputs parameters and an identity IDA of entity A as inputs and outputs A's secret value xA.

Set-Private-Key: This set of rules takes params, an entity A's partial non-public key DA and A's secret value xA as input. The value xA is used to transform DA into the (complete) secret key SA. The set of rules returns SA.

Set-Public-Key: This set of rules takes params and entity A's secret value xA as enter and from those constructs the general public key PA for entity A. Normally both Set-Private-Key and Set-Public-Key are run by an entity A for itself, after jogging Set-Secret-Value. The same secret value xA is used in every. Separating them makes it clear that there may be no want for a temporal ordering at the technology of public and personal keys in proposed mCL-PKE scheme. Usually, A is the only entity in possession of SA and xA, and xA will be selected at random from a suitable and huge set.

Encrypt: This algorithm takes as inputs parameters such as, a message M ∈ M, and the public key PA and identifier IDA of an entity A. It returns both a ciphertext C ∈ C or the null image ⊥ indicating an encryption failure. This will constantly occur in the occasion that PA does not have the best form. In proposed scheme, that is the only manner an encryption failure will arise.

Decrypt: This set of rules takes as inputs params, C ∈ C, and a private key SA. It finally returns a message M ∈ M or a message ⊥ indicating a decryption failure.

Key Policy Attribute Based Encryption (KP-ABE):

It is the modified form of the traditional version of ABE. Users are assigned with a get right of access to tree shape over the information attributes. Doorstep gates are the nodes of the get right of entry to the tree. The attributes are connected thru leaf nodes. To replicate the get right of entry to tree configuration the decision of the game key of the man or woman is defined. Cipher texts are categorized with gadgets of attributes and personal keys are connected with monotonic way in systems that manage which cipher texts a client is capable to decrypt. Key Policy characteristic Based Encryption (KP-ABE) method is considered for one-to-many communications. KP-ABE scheme includes the subsequent four algorithms:

Setup: Algorithm takes input as K safety factor and returns PK as a public key and a device draw near mystery key MK.PK is used by spatial records senders for encryption. MK is used to produce customer mystery keys and is notion handiest to the power.

Encryption: Algorithm takes a spatial facts M, the general public key PK, and a set of attributes as coming into. It outputs the cipher text E.

Key Generation: Algorithm takes as to go into get right of entry to form T and the draw close thriller key MK. It outputs a thriller key SK that allows the patron to decrypt spatial facts encrypted under a hard and speedy of attributes if and amazing if fits T.

Decryption: It takes as to enter the customer's thriller key SK for buying right of entry to shape T and the cipher text E, which modified into encrypted below the characteristic set.

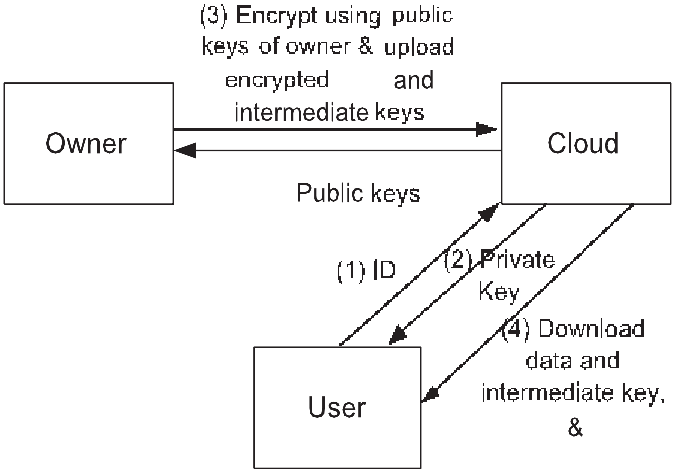

(3) Encrypt using public keys of owner & upload encrypted and intermediate keys
Owner
Cloud
Public keys
(1) ID
(2) Private Key
(4) Download data and intermediate key, &
User

Fig 3.1: Process of Data Encryption and Key Generation

This set of guidelines outputs the spatial information M if and best if the feature set satisfy the purchaser's get proper of entry to configuration T. The KP-ABE method can accumulate top notch-grained get proper of rights to use to manipulate and additional elasticity to manipulate users than ABE method. The trouble with the KP-ABE method is the encryptor cannot choose who can decrypt the encrypted data. It can exceptional choose descriptive attributes for the facts; it is wrong in a few utility due to the fact a facts proprietor has to remember the critical component issue.

The proposed system is to have the following modules together with useful requirements.

1. Identity token issuance
2. Identity token registration
3. Data encryption and importing
4. Data view and decryption
5. Encryption evolution management

Identity token issuance

IdPs are relied on third parties that issues identity tokens to Users based on their identification attributes. It must be mentioned that IdPs need not be online after distribution of identity tokens.

Identity token registration

Users check in their token to acquire secrets in order to later decrypt the statistics they may be allowed to access. Users sign up their tokens associated with the attribute conditions in ACC with the Owner, and the relaxation of the identity tokens related to the attribute conditions in ACB/ACC with the Cloud. When Users register with the Owner, the Owner problems them units of secrets and techniques for the characteristic situations in ACC which are also present in the sub ACPs in ACPB Cloud. The Owner maintains one set and offers the alternative set to the Cloud. Two distinct sets are used with a view to save you the Cloud from decrypting the Owner encrypted facts.

Data encryption and uploading

The Owner first encrypts the records based at the Owner's sub ACPs so one can hide the content from the Cloud and then uploads them at the side of the public facts generated by using the AB-GKM::KeyGen set of rules and the remaining sub ACPs to the Cloud. The Cloud in turn encrypts the statistics based on the keys generated the use of its own AB-GKM::KeyGen set of rules. Note that the AB-GKM::KeyGen on the Cloud takes the secrets issued to Users and the sub ACPs given with the aid of the Owner into consideration to generate keys.

Data View and Decryption

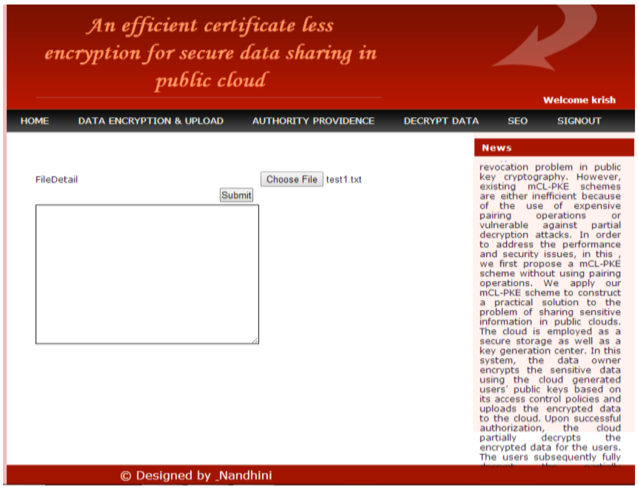
Users down load encrypted records from the Cloud and decrypt twice to get original information. First, the Cloud generated public data tuple is used to derive the OLE key and then the Owner generated public information tuple is used to derive the ILE key the usage of the AB-GKM::KeyDer algorithm. These keys allow a User to decrypt a statistics item best if the User satisfies the original ACP applied to the facts item.

Encryption Evolution Management

Over time, either ACPs or consumer credentials may also alternate. Further, already encrypted information may go through common updates. In such situations, information already encrypted need to be re-encrypted with a new key. As the Cloud imports access control enforcing encryption, it surely re-encrypts the affected statistics without the intervention of the Owner.

IV. Experimental Results

Experimental results explain the overall implementation process. This certificateless access control mechanism was developed with the combination of ASP.NET with SQL Database system. Proposed implementation provides efficient file storage and file sharing process in cloud.

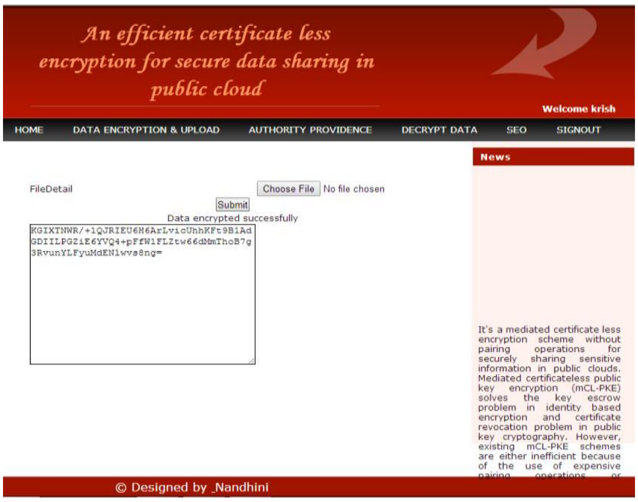


FileDetail test1.txt

revocation problem in public key cryptography. However, existing mCL-PKE schemes are either inefficient because of the use of expensive pairing operations or vulnerable against partial decryption attacks. In order to address the performance and security issues, in this , we first propose a mCL-PKE scheme without using pairing operations. We apply our mCL-PKE scheme to construct a practical solution to the problem of sharing sensitive information in public clouds. The cloud is employed as a secure storage as well as a key generation center. In this system, the data owner encrypts the sensitive data using the cloud generated users' public keys based on its access control policies and uploads the encrypted data to the cloud. Upon successful authorization, the cloud partially decrypts the encrypted data for the users. The users subsequently fully

Fig 1: Data Owner Upload File on Cloud Server

Data owner need to get access permission from cloud service provider. Then upload the file on cloud server.



FileDetail No file chosen

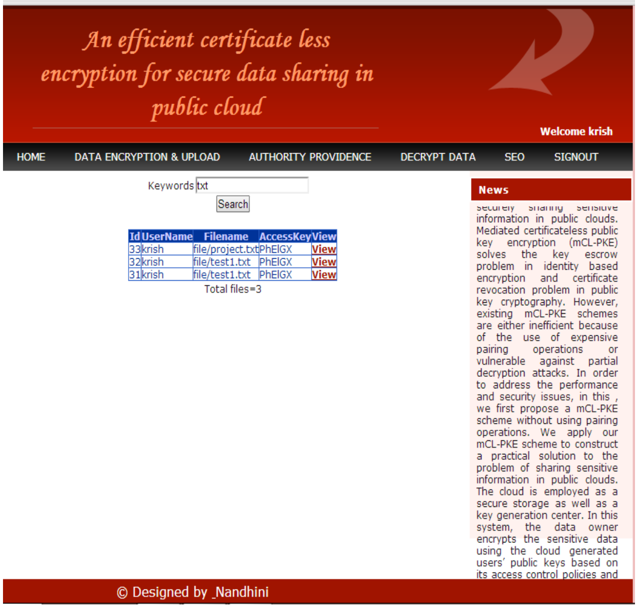
Data encrypted successfully

```
KGIXTNWR/+1QJRIEU6H6ArLvicUhhKFt9B1Ad
GDIILPGZiE6YVQ4+pFfW1FLZtw66dMmThoB7g
3RvunYLFyuMdEN1wvs8ng=
```

It's a mediated certificate less encryption scheme without pairing operations for securely sharing sensitive information in public clouds. Mediated certificateless public key encryption (mCL-PKE) solves the key escrow problem in identity based encryption and certificate revocation problem in public key cryptography. However, existing mCL-PKE schemes are either inefficient because of the use of expensive pairing operations or

Fig 2: File Encryption

This figure shows the file encryption process. During file upload, that is encrypted for secure cloud processing. Encryption ensures the data confidentiality in cloud storage.



Keywords txt

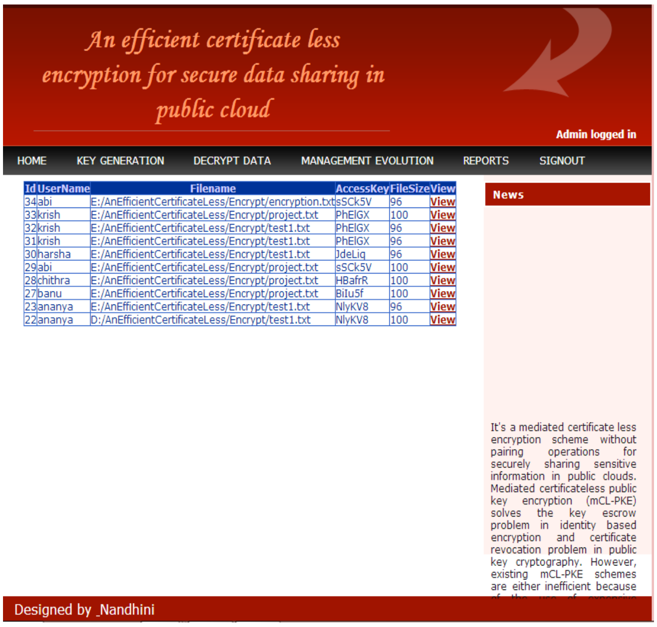
Id	UserName	Filename	AccessKey	View
33	krish	file/project.txt	PhEIGX	View
32	krish	file/test1.txt	PhEIGX	View
31	krish	file/test1.txt	PhEIGX	View

Total files=3

securely sharing sensitive information in public clouds. Mediated certificateless public key encryption (mCL-PKE) solves the key escrow problem in identity based encryption and certificate revocation problem in public key cryptography. However, existing mCL-PKE schemes are either inefficient because of the use of expensive pairing operations or vulnerable against partial decryption attacks. In order to address the performance and security issues, in this , we first propose a mCL-PKE scheme without using pairing operations. We apply our mCL-PKE scheme to construct a practical solution to the problem of sharing sensitive information in public clouds. The cloud is employed as a secure storage as well as a key generation center. In this system, the data owner encrypts the sensitive data using the cloud generated users' public keys based on its access control policies and

Fig 3: Key Generation

Above figure shows the key generation process. Unique keys are generated for each file that are stored in cloud.



An efficient certificate less encryption for secure data sharing in public cloud

Admin logged in

Id	UserName	Filename	AccessKey	FileSize	View
34	abi	E:/AnEfficientCertificateLess/Encrypt/encryption.txt	sSCk5V	96	View
33	krish	E:/AnEfficientCertificateLess/Encrypt/project.txt	PhElGX	100	View
32	krish	E:/AnEfficientCertificateLess/Encrypt/test1.txt	PhElGX	96	View
31	krish	E:/AnEfficientCertificateLess/Encrypt/test1.txt	PhElGX	96	View
30	harsha	E:/AnEfficientCertificateLess/Encrypt/test1.txt	JdeLiq	96	View
29	abi	E:/AnEfficientCertificateLess/Encrypt/project.txt	sSCk5V	100	View
28	chithra	E:/AnEfficientCertificateLess/Encrypt/project.txt	HBafrR	100	View
27	banu	E:/AnEfficientCertificateLess/Encrypt/project.txt	BiIu5f	100	View
23	ananya	E:/AnEfficientCertificateLess/Encrypt/test1.txt	NlyKV8	96	View
22	ananya	D:/AnEfficientCertificateLess/Encrypt/test1.txt	NlyKV8	100	View

It's a mediated certificate less encryption scheme without pairing operations for securely sharing sensitive information in public clouds. Mediated certificateless public key encryption (mCL-PKE) solves the key escrow problem in identity based encryption and certificate revocation problem in public key cryptography. However, existing mCL-PKE schemes are either inefficient because

Designed by .Nandhini

Fig 4: File Details

Above figure shows the file details. Here user can view user name, file name, access key and file details. User can also download and decrypt the file using secret key.

V. CONCLUSION

In this work an efficient mediated certificateless public key encryption scheme was proposed with instantaneous revocation property. Proposed the notion of security-mediated certificateless (SMC) cryptography, which has instantiated one more of the set of compromises within the various desirable properties for solving the certification problem in public key cryptography. The proposed scheme provided a generic construction and also a concrete encryption scheme. An attractive feature of proposed proposal is that it can use the same parameters used for most other identity-based and share the same key generation centre (KGC). Proposed scheme also supports distributed security mediators (SEMs). The proposed MCL-PKE scheme can eliminate the inherent private escrow drawback of traditional ID-based cryptosystem, and it is secure against Type-I and Type-II adversary in the random oracle model under the computational infeasibility of CDH assumption.

VI. REFERENCES

[1]. A. Shamir. Identity Based Cryptosystems and Signature Scheme. In Proc. of CRYPTO 1984, LNCS 196, Berlin: Springer-Verlag, 1984. pp. 47-53.

[2]. S.S. Al-Riyami and K.G. Paterson. Certificateless Public Key Cryptography. In proc. of ASIACRYPTO 2003, LNCS 2894, Berlin: Springer-Verlag, 2003. pp. 452-473.

[3]. B.Libert and J. Quisquater. Efficient revocation and threshold pairing based cryptosystems. PODC 2003. Boston, Massachusetts. 2003. pp.163-171.

[4]. S.S. Al-Riyami and K.G. Paterson. CBE from CLPKE: A Generic Construction and Efficient Schemes. In Proc. of PKC 2005, LNCS 3386, Berlin: Springer- Verlag, 2005. pp. 398-415.

[5]. J. Baek, R, Safavi-Nani and W. Susilo. Certificateless Public Key Encryption without Pairing. In Proc. ISC 2005, LNCS 3650, Berlin: Springer-Verlag, 2005. pp. 134-148.

[6]. Y. Shi and J. Li. Provable Efficient Certificateless Public Key Encryption. Cryptology eprint Archive, Report.http://eprint.iacr.org/2005/287.

[7]. H. S. Ju, D. Y. Kim, and D. H. Lee et al. Efficient Revocation of Security Capability in Certificateless Public Key Cryptography. In Proc. of KES 2005, LNAI 3682, Berlin: Springer-Verlag, 2005. pp. 453-459.

[8]. X. Huang, W. Susilo and Y. Mu et al. On the Security of Certificateless Signature Schemes from Asiacrypto 2003. In Proc. of CANS 2005, LNCS 3810, Berlin: Springer-Verlag, 2005. pp. 13-25.

[9]. X. Li, K. Chen and L. Sun. Certificateless Signature and Proxy Signature Schemes from

Bilinear Pairings. Lithuanian Mathematical Journal, vol 45, pp. 76-83, Springer-Verlag, 2005.

[10]. D. Boneh, X. Ding, G. Tsudik, and C. Wong. A Method for Fast Revocation of Public Key Certificates and Security Capabilities. In Proc. of the 10th USENIX Security Symposium, Washington D. C., 2001. pp. 297-308.