Securing Land Document in Bank by using Identity based MRSA Technique

S. Sravani[1] Dr. K. Venkataramana[2]
[1]Student [2]Professor
[1,2]Department of Computer Applications
[1,2]KMM Institute of PG Studies, Tirupati, India

Abstract— Identity-based public key encryption provides easy introduction of public key cryptography by allowing an entity's public key to be extract from an arbitrary identification value, such as name or email address. The main practical benefit of identity-based cryptography is in greatly decreased the need for, and reliance on, public key certificates. Although some interesting identity-based techniques are developed in the past, none are compatible with favored public key encryption algorithms (such as El Gamal and RSA). This limits the advantage of identity-based cryptography as a shift step to full-blown public key cryptography. Furthermore, it is fundamentally difficult to reconcile one grained revocation with identity-based cryptography. Mediate RSA . Neither the user nor the SEM will cheat each other since every cryptographic operation (signature or decryption) need both parties. MRSA permits quick and new-grained manage of users' security privileges. However, MRSA still relies on conventional public key certificates to store and transmit public keys. During this, we tend to present IB-MRSA, an easy variant of MRSA that combines identity-based and mediated cryptography Infrastructures.

Keywords: Identity Based Encryption, Mediated RSA, Mediated RSA

I. INTRODUCTION

Data mining is the process of discovering patterns in large data sets involving methods at the intersection of machine learning, statistics, and database systems. Data mining is an interdisciplinary subfield of computer science and statistics with an overall goal to extract information (with intelligent methods) from a data set and transform the information into a comprehensible structure for further use. Data mining is the analysis step of the "knowledge discovery in databases" process, or KDD. Aside from the raw analysis step, it also involves database and data management aspects, data pre-processing, model and inference considerations, interestingness metrics, complexity considerations, post-processing of discovered structures, visualization, and online updating. The difference between data analysis and data mining is that data analysis is to summarize the history such as analyzing the effectiveness of a marketing campaign, in contrast, data mining focuses on using specific machine learning and statistical models to predict the future and discover the patterns among data. The term "data mining" is in fact a misnomer, because the goal is the extraction of patterns and knowledge from large amounts of data, not the extraction (mining) of data itself. It also is a buzzword and is frequently applied to any form of large-scale data or information processing (collection, extraction, warehousing, analysis, and statistics) as well as any application of computer decision support system, including artificial intelligence (e.g., machine learning) and business intelligence. The book Data mining: Practical machine learning tools and techniques with Java (which covers mostly machine learning material) was originally to be named just Practical machine learning, and the term data mining was only added for marketing reasons. Often the more general terms (large scale) data analysis and analytics – or, when referring to actual methods, artificial intelligence and machine learning – are more appropriate. The One important impediment to the widespread adoption of public key cryptography is its weakness on a public key infrastructure that is shared among its users. Before secured communications can take place, both sender and receiver must create encryption and signature key pairs, submit certificate invocation along with proof of identity to a Certificate Authority(CA), and receive CA-signed certificates, which they can then use to authenticate one another and exchange encrypted messages. In a typical public key infrastructure (PKI) setting, a user's public key is specific steganography in a public key corticated which is, critical, a binding between the corticated holder's identity and the claimed public key. This common model requires universal trust in corticated issuers. It has some well-known and bothersome side-effects such as the require for cross-domain trust and certificates revocation. The main issue, however, is the basic premise that all certificate are public, ubiquitous and, hence, readily available to anyone. We notice that this belief is not always realistic, especially, in wireless (or any fault-prone) networks where connectivity is sporadic.

II. RELATIVE STUDY

In a typical public key infrastructure setting, a user's public key is explicitly encoded in a public key certificate. It has some well-known and bothersome side-effects such as the need for cross domain trust and certificate revocation. Under the random oracle model, IB-MRSA with OAEP is shown as secure as standard RSA with OAEP. it can be shown that, in the random oracle model, IB-mRSA with OAEP is as secure against adaptive chosen cipher text attacks.

A. Concrete Security Treatment of Symmetric Encryption: Analysis of the DES Modes Of Operation,

We study notions of security and schemes for symmetric (ie: private key) encryption in a concrete security framework. We give several different notions of security and analyze the concrete complexity of reductions among them. Next we provide concrete security analyses of various methods of encrypting using a block cipher, including two of the most popular methods, Cipher Block Chaining and Counter Mode. We establish tight bounds (meaning matching upper bounds and attacks) on the success of adversaries as a function of their resources.

B. Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Cipher Text Attack

The zero-knowledge proof of knowledge, first denned by Fiat, Fiege and Shamir, was used by Galil, Haber and Yung as a means of constructing (out of a trapdoor function) an interactive public-key cryptosystem provably secure against chosen cipher text attack. We introduce a revised setting which permits the definition of a non-interactive analogue, the non-interactive zero-knowledge proof of knowledge, and show how it may be constructed in that setting from a non-interactive zero-knowledge proof system for NP . We give a formalization of chosen cipher text attack in our model which is stronger than the "lunchtime attack" considered by Naor and Yung, and prove a non-interactive public-key cryptosystem based on non-interactive zero-knowledge proof of knowledge to be secure against it.

III. PROPOSED ALGORITHM

We propose a simple identity-based cryptosystem grow atop some Mediated RSA (mRSA) by Boneh, et al. mRSA is an experimental and RSA-compatible procedure of break an RSA private key between the user and the security mediator, called a SEM. Neither the user nor the SEM knows the factorization of the RSA modulus and neither can decrypt/sign message without the other's help. By virtue of need the user to touch its SEM for each decryption and/or signature action, mRSA supply quick and one-grained revocation of users' security privileges.

A. Algorithm Analysis:

1) IB-mRSA Encryption Algorithm

To encrypt a message, the sender requires only the receiver email address and the domain certificate. The encryption algorithm is shown in below.

1) Step 1. Retrieve n,k and KG algorithm identifier from the domain certificate;
2) Step 2. s ← k − |KG()| − 1
3) Step 3. e ← 0s||KG(IDA)||1
4) Step 4. Encrypt input message m with (e,n) using standard RSA/OAEP, as specified in PKCS#1v2.1

Since the receiver public key is obtain from the receiver's individual identifier, the sender does not need a public key certificate to protect that the intended receiver is the correct public key holder. Furthermore, fast revocation provide a by mRSA obviates the need for the sender to perform any revocation checks.

2) IB-mRSA Decryption Algorithm

IB-mRSA decryption is similar to that of mRSA. To make this paper self-contained, we borrow the protocol explanation in For a detailed explanation and security analysis of additive mRSA, we refer the reader.

Protocol IB-mRSA.decr (executed by User and SEM)

1) Step1. USER: m' ← encrypted message
2) Step2. USER: send m' to SEM
3) Step 3. In parallel

3) SEM:

1) If USER revoked return (ERROR)
2) PDsem ← m0dsem mod n
3) Send PDsem to USER

4) USER: (a) PDu ← m0du mod n

4) Step4.USER: M ← (PDsem∗PDu) mod n
5) Step 5. USER: m ← OAEP Decoding of M
6) Step6. USER: If succeed, return (m)

B. Security of Identity-BASEDmRSA

We now examine the security of IB-mRSA OAEP in a setting with n users. All users share a common RSA modules N and each user (Ui) is associated with a unique identity IDi,which is mapped into an RSA public advocated via a mapping function KG .

1) Security Analysis

In the following, we argue that if KG is an suitable hash function, IB-mRSA/OAEP is semantically secure against adaptive chosen cipher text attacks (CCA-2) in the random oracle model. We use the term invisible which is a notion identical to semantic security.

2) The Public Key Mapping Function

The key generation function KG in IB-mRSA is a hash function H. to protect the security of the scheme must satisfy the following requirements.

C. Availability of Public Keys

The output of H should have an inordinate probability of being relatively prime to φ(n).obviously, for the inverse (private key) to exist, a public exponent cannot have common factor with φ(n).

1) Collision Resistances:

H Should is a collision-resistant function. i.e., given any two distinct inputs ID1, ID2, the probability of H (ID1) =H (ID2) should be trifling. In other words, no two users in the domain can share public exponent.

2) Division Resistances:

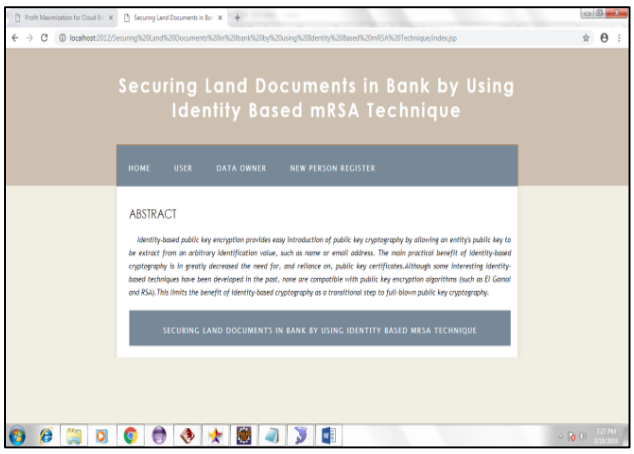
As discussed in division intractability pf H is vital to the securities of IB-mRSA generate a1.survey the probability of division for hash function.

3) Security of Common Modulus

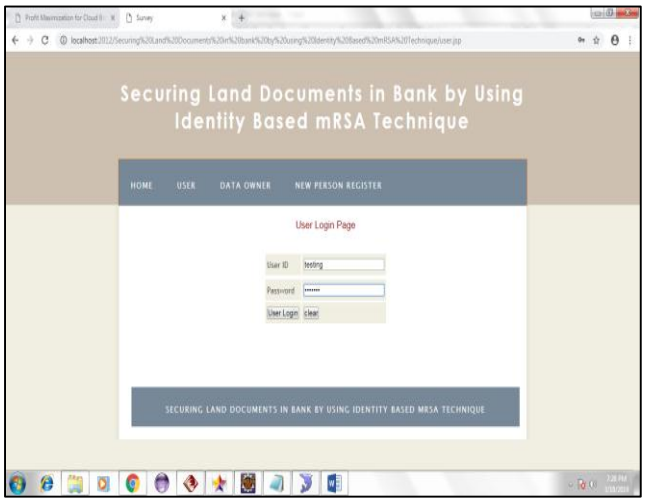
As mentioned earlier, using common RSA modules is clearly inappropriate in plain RSA setting. In the mediated RSA architecture, sharing a modulus is practical since no party knows a complete private/public key-pair.

IV. RESULTS

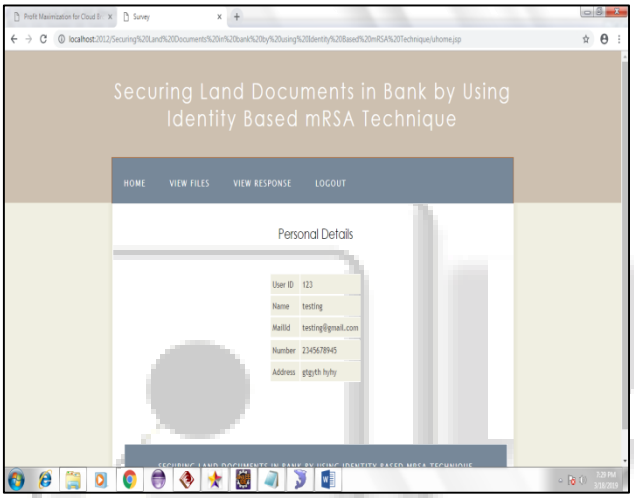
A. Homepage



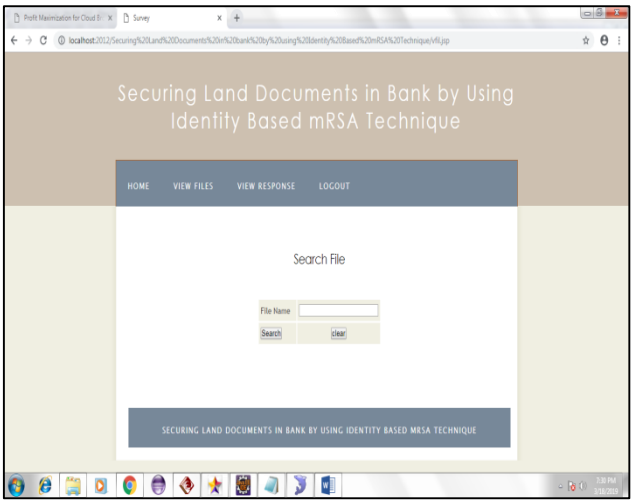
B. User Login



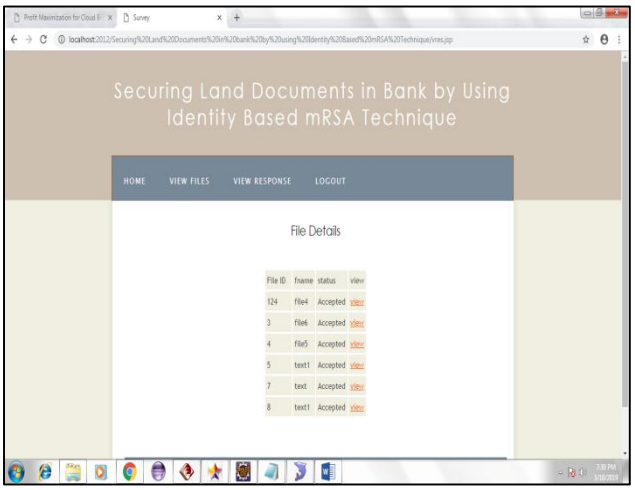
C. User Home



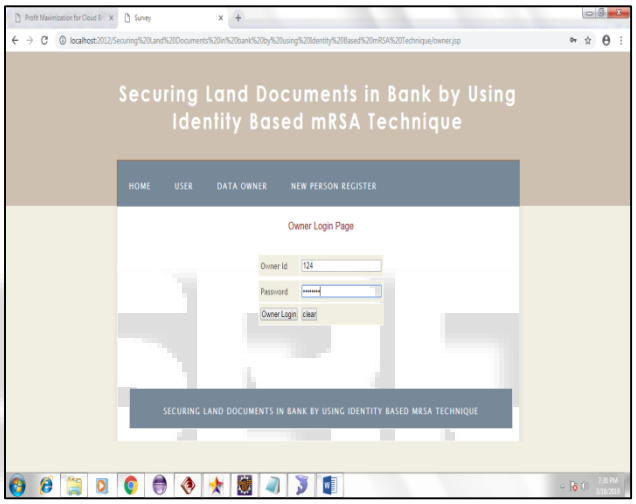
D. View Files



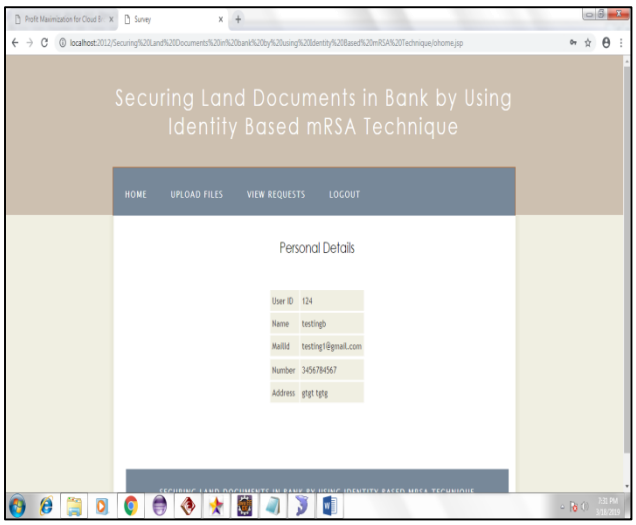
E. View Response



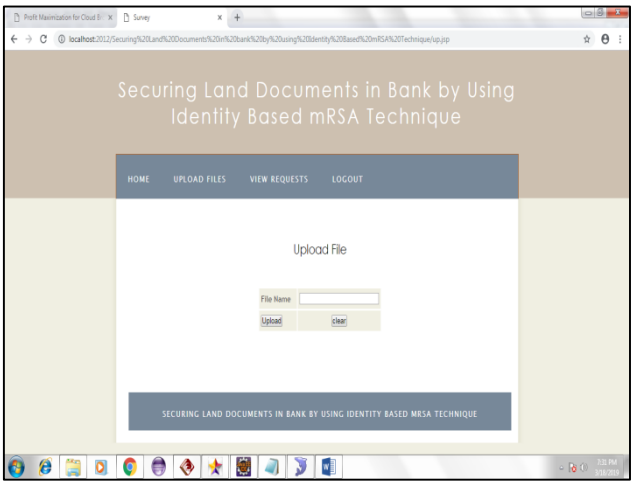
F. Data Owner Login



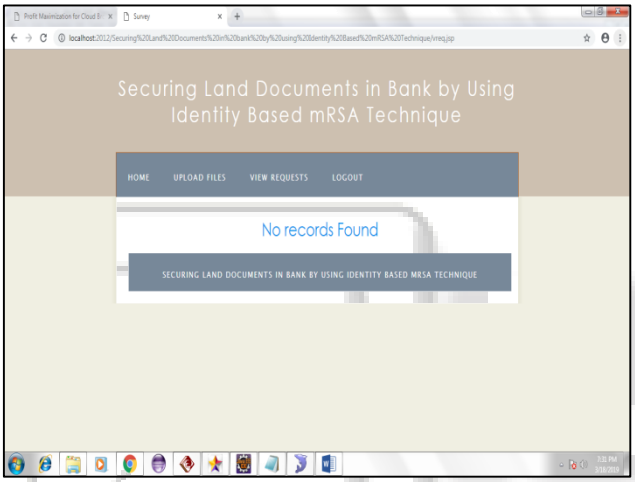
G. Data Owner Home



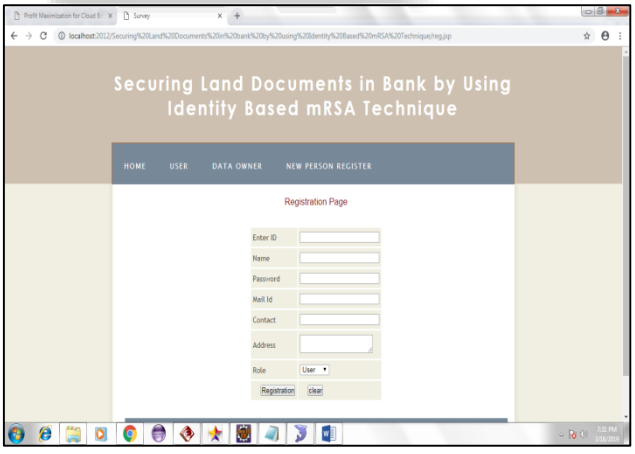
H. Upload Files



I. View Requests



J. New Person Register



V. CONCLUSION

We described Identity-based systems offer some significant advantages over PKI, especially in their increased user-friendliness, although they do not come back without some drawbacks. For its advocates, IBC provides a better compromise between security and complexity than previous systems. IB-mRSA, a sensible and secure identity-based encryption scheme. it's compatible with standard RSA encryption and offers one-grained control (revocation) of users security privileges.

REFERENCES

[1] M. Bellare, A. Boldyreva, and S. Micali. Public-Key Encryption in a Multi-user Setting : Security Proofs and Improvements. In Eurocrypt '00, LNCS. Springer-Verlag, 2000.
[2] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations Among Notions of Security for Public-Key Encryption Schemes. In Crypto '98, LNCS 1462, pages 26–45. Springer-Verlag, 1998.
[3] M. Bellare and P. Rogaway. Optimal Asymmetric Encryption – How to Encrypt with RSA. In Eurocrypt '94, LNCS 950, pages 92–111. Springer-Verlag, 1995.
[4] M. Bellare and A. Sahai. Non-Malleable Encryption : Equivalence between Two Notions and an Indistinguishability-Based Characterization. In Crypto '99, LNCS 1666, pages 519–536. SpringerVerlag, 1998.
[5] D. Bleichenbacher. A Chosen Ciphertext Attack against Protocols based on the RSA Encryption Standard PKCS = 1. In Crypto '98, LNCS 1462, pages 1–12. Springer-Verlag, 1998.
[6] D. Coppersmith. Finding a Small Root of a Univariate Modular Equation. In Eurocrypt '96, LNCS 1070, pages 155–165. Springer-Verlag, 1996.
[7] D. Coppersmith. Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities. Journal of Cryptology, 10:233–260, 1997.
[8] D. Coppersmith, M. Franklin, J. Patarin, and M. Reiter. Low-Exponent RSA with Related Messages. In Eurocrypt '96, LNCS 1070, pages 1–9. Springer-Verlag, 1996.
[9] R. Cramer and V. Shoup. A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack. In Crypto '98, LNCS 1462, pages 13–25. Springer-Verlag, 1998.
[10] W. Diffie and M. E. Hellman. New Directions in Cryptography. In IEEE Transactions on Information Theory, volume IT–22, no. 6, pages 644–654, November 1976

