Cost-Effective Authentic and Anonymous Data Sharing with Forward Security

Miss Shweta S. Gulhane
Prof. A. L. Korde

Department of Computer Science & Engineering
K.S. Institute of Engineering and Technology, Hingoli (MS), India.

ABSTRACT

Data sharing has is not easier with the advances of cloud computing, and an accurate analysis on the shared data provides more benefits to both the society and individuals. Data sharing with a large number of participants must take into account several issues, including efficiency, data integrity and privacy of data owner. Ring signature is a promising candidate to construct an anonymous and authentic data sharing system. Ring signature showing possibility of achievement to construct an anonymous and authentic data sharing system. It allows a data owner to anonymously authenticate his data which can be put into the cloud for storage or analysis purpose. Yet the costly certificate verification in the traditional public key infrastructure (PKI setting becomes a waist for this solution to be scalable. Identity-based (ID-based) ring signature, which eliminates the process of certificate verification, can be used instead of traditional public key infrastructure. In this paper, we further enhance the security of ID-based ring signature by providing forward security: If a secret key of any user has been dedicated, all previous generated signatures that include this user still remain valid. This property is especially important to any large scale data sharing system, as it is impossible to ask all data owners to re authenticate their data even if a secret key of one single user has been dedicated. We provide a concrete and efficient instantiation of our scheme, prove its security and provide an implementation to show its practicality.

Keyword : - *Authentication, data sharing, cloud computing, forward security, smart grid.*

1. INTRODUCTION

1.1 Overview of the System

The popularity and widespread use of “CLOUD" have brought great convenience for data sharing and collection. Not only can individuals acquire useful data more easily, Sharing data with others can provide a number of beets to our society as well. As a representative example, consumers in Smart Grid can obtain their energy usage data in a fine-grained manner and are encouraged to share their personal energy usage data with others, e.g., by uploading the data to a third party platform such as Microsoft Hohm see figure 1.1. From the collected data a statistical report is created, and one can compare their energy consumption with others. This ability to access, analyze, and respond to much more precise and detailed data from all levels of the electric grid is critical to efficient energy usage.

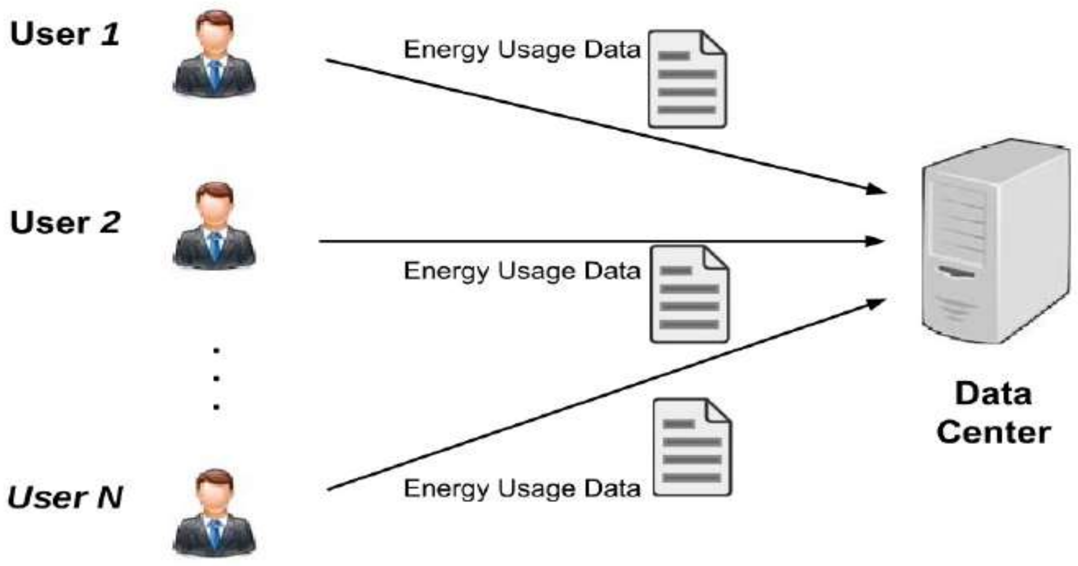


Fig -1: Usage Data Sharing in Smart Grid [1]

Due to its openness, data sharing is always deployed in a hostile environment and vulnerable to a number of security threats. Taking energy usage data sharing in Smart Grid as an example, there are several security goals a practical system must meet, including:

- Data Authenticity: In the situation of Smart Grid, the statistic energy usage data would be misleading if it is forged by adversaries. While this issue alone can be solved using well established cryptographic tools, one may encounter additional difficulties when other issues are taken into account, such as anonymity and efficiency;
- Anonymity: Energy usage data contains vast information of consumers, from which one can extract the number of persons in the home, the types of electric utilities used in a specific time period, etc. Thus, it is critical to protect the anonymity of consumers in such applications, and any failures to do so may lead to the reluctance from the consumers to share data with others; and
- Efficiency: The number of users in a data sharing system could be HUGE, and a practical system must reduce the computation and communication cost as much as possible. Otherwise it would lead to a waste of energy, which contradicts the goal of Smart Grid [1].

2. THEORIES AND APPROACHES

2.1 Mathematical Assumption

Definition 1 (RSA Problem): Let N = pq, where p and q are two k-bit prime numbers such thatp = 2p' +1 and q = 2q'+1 for some primes p', q'. Let e be a prime greater than 2l for some fixed parameter l, such that gcd(e,(N)) = 1. Let y be a random element in Z*N. We say that an algorithm S solves the RSA problem if it receives an input the tuple (N,e, y) and outputs an element z such that z^e = ymodN [3].

2.2 Security Model

A (1,n) ID-Based Forward Secure Ring Signature (IDFSRS) scheme is a tuple of probabilistic polynomial-time (PPT) algorithms:

- Setup. On input an unary string 1 where is a security parameter, the algorithm outputs a master secret key msk for the third party PKG (Private Key Generator) and a list of system parameters param that includes and the descriptions of a user secret key space D, a message space M as well as a signature space Ψ.
- Extract. On input a list param of system parameters, an identity IDiϵ{0,1}* for a user and the master secret key msk, the algorithm outputs the users secret key ski,0,ϵD such that the secret key is valid for time t=0. We

denote time as non-negative integers. When we say identity IDi corresponds to user secret key ski,0 or vice versa, we mean the pair (IDi,ski,0) is an input-output pair of Extract with respect to param and msk.

- Update. On input a user secret key skit, for a time period t, the algorithm outputs a new user secret key ski;t+1 for the time period t + 1.
- Sign. On input a list param of system parameters, a time period t, a group size n of length polynomial in, a set L ={IDi϶{0,1}i ϵ [1,n] of n user identities, a message m ϵ M, and a secret key sk_{II}t 2ϵ D II ϵ [1, n] for time period t, the algorithm outputs a signature δ ϵ Ψ. .
- Verify. On input a list param of system parameters, a time period t, a group size n of length polynomial in λ, a set set L ={IDi϶{0,1}i ϵ [1,n] of n user identities, a message m 2 M, a signature δ ϵ Ψ, it outputs either valid or invalid.
- Correctness. A (1, n) IDFSRS scheme should satisfy the verification correctness-signatures signed by honest signer are verified to be invalid with negligible probability.

2.2 Notions Of Security

The security of IDFSRS consists of two aspects: forward security and anonymity. Before giving their definition, we consider the following oracles which together model the ability of the adversaries in breaking the security of IDFSRS. Extration Oracle(EO): On input an identity IDi and a time period t, the corresponding secret key skit ϵ D for that time period is returned. Signing Oracle(SO): On input a time period t, a group size n, a set L of n user identities, a message m ϵ M, a valid signature δ is returned. Now we are ready to define the security of IDFSRS: 2.3.1. Forward Security: Forward security of IDFSRS scheme is defined in the following game between the simulator S and the adversary A in which A is given access to oracles EO and SO:

- S generates and gives A the system parameters param.
- A may query the oracles according to any adaptive strategy.
- A chooses a time t* , a group sizen* ϵ N, a set L* of n* identities and a message m* ϵ M.

A may continue to query the oracles according to any adaptive strategy.
A outputs a signature δ*t
A wins the game if:
Verify (t*; L*m*δ*t*) = valid.
None of the identities in L* has been queried to EO with time t < t* as the time input parameter.
(t*, L*,m*) are not queried to SO.
We denote Adv $f^s{}_A(\lambda)$ the probability of A winning the game. Definition 2 (Forward Secure): A(1,n) IDFSRS scheme is forward secure if for any PPT adversary Adv $f^s{}_A(\lambda)$ is a negligible function of

2.3.2. Anonymity: It should not be possible for an adversary to tell the identity of the signer with a probability larger than 1/n, where n is the cardinality of the ring, even assuming that the adversary has unlimited computing resources. We denote $Adv^{anon}{}_A$ (λ)= P [A guesses the identity A of the signer correctly] 1/n.
Definition 3 (Anonymity): A (1,n) IDFSRS scheme is unconditional anonymous if for any group of n users, any message m_M, any time t and any valid signature, any adversary A, even with unbounded computational power, cannot identify the actual signer with probability better than random guessing. In other words, A can only output the identity of the actual signer with probability no better than 1=n. That is, $Adv^{anon}{}_A$ (λ) = 0

2.3 Application of Forward Secure ID-Based Ring Signatures

In addition to energy data sharing in smart-grid, we sketch three other situations which may also need forward secure ID-based ring signatures.

2.4.1. Whistle Blowing: Suppose Bob is a member of the city council. One day he wishes to leak a secret news from the council meeting to a journalist. The news is supposed to be kept secret. Thus Bob wants to remain anonymous, yet such that the journalist is convinced that the leak was indeed from a council member. Bob cannot send to the journalist a standard digitally signed message, since such a message, although it convinces the journalist that it came from a council member, does so by directly revealing Bobs identity. Neither does it work for Bob to send the journalist a message through a standard anonymizer, since the anonymizer strips off all source identification and authentication in a way that the journalist would have no reason to believe that the message really came from a council member at all. Using another primitive called group signature does not solve the problem neither. A group signature allows a signer to sign a message on behalf of a group. The verifier only knows that one of the users of the group signs the message yet does not know who is the actual signer. It does not work in this case, because it requires prior cooperation of the other group members to set up, and leaves Bob vulnerable to later identification by the group manager, who may be controlled by the government. The correct approach for Bob is to send the secret information to the journalist through an anonymizer, signed with a ring signature that names each council member including himself as a ring member. The journalist can verify the ring signature on the message, and learn that it definitely came from a council member. However, neither he nor anyone (including those council members inside the ring) can determine the actual source of the leak. Forward security enhances the protection of all entities. Without forward security, if a secret key of a council member Alice is exposed, every ring signature containing Alice in the ring will become invalid. That means any previous ring signature given by Bob will be invalid (assuming Alice is included in the signature). This will greatly affect the accuracy of the report by the journalist who may rely on Bob for leaking important secret information.

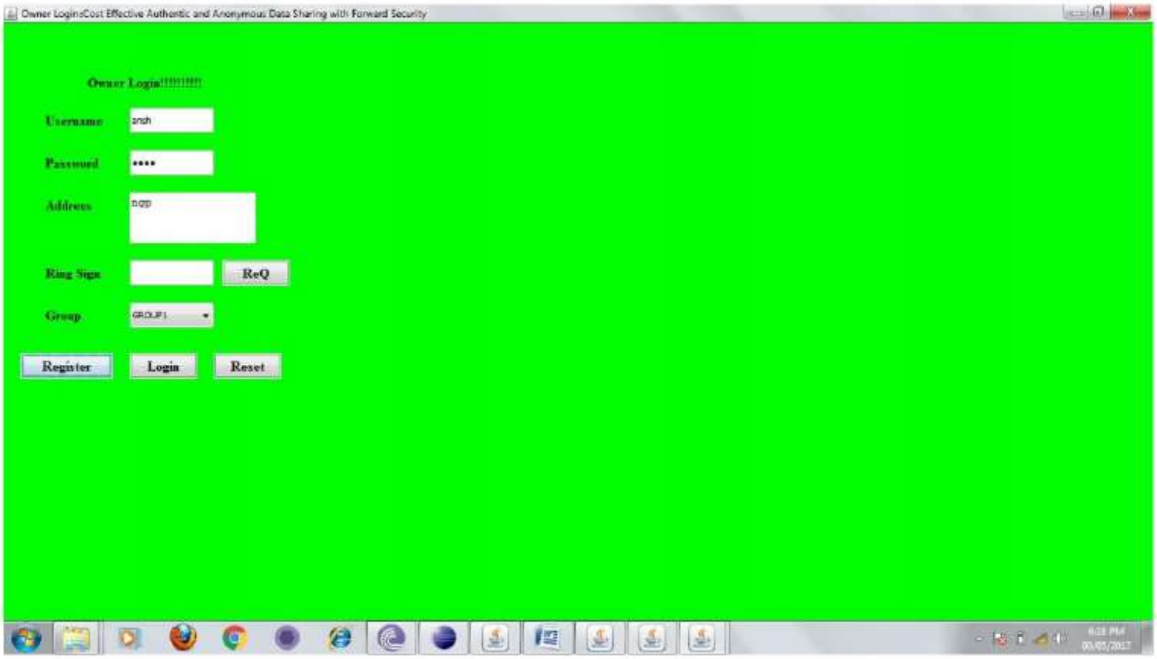
2.4.2. E-Contract Signing: A 1-out-of-2 ring signature (containing two users in the ring) can be used to construct concurrent signature. A concurrent signature allows two entities to produce two signatures in such a way that, from the point of view of any third party, both signatures are ambiguous with respect to the identity of the signing party until an extra piece of information (the keystone) is released by one of the parties. Upon release of the keystone, both signatures become binding to theirtrue signers concurrently.Concurrent signature is one of the essential tools for building e-contract signing and fair exchange protocol in the paradigm. It can protect both parties against a cheating party. Consider the following example of fair tendering of contracts. Suppose that A has a building construction contract that she wishes to put out to tender, and suppose companies B and C wish to put in proposals to win the contract. This process is sometimes open to abuse by A since she can privately show Bs signed proposal to C to enable C to better the proposal. Using concurrent signatures, B would sign his proposal to construct the building for an amount X, but keep the keystone private. If A wishes to accept the proposal, she returns a payment instruction to pay B amount X. She knows that if B attempts to collect the payment, then A will obtain the keystone through the banking system to allow the public to verify that the signature is really generated by B. But A may also wish to examine Cs proposal before deciding which to accept. However there is no advantage for A to show Bs signature to C since at this point Bs signature is ambiguous and so C will not be convinced of anything at all by seeing it. We see that the tendering process is immune to abuse by A. Adding forward security to it can further improve the security protection level. With forward security, the key exposure of either party does not affect the e-contracts previously signed. This provides a more fair, justice, safety and efficient environment for commercial users doing business in an e-commerce platform.

2.4.3. E-Auction: Similar to e-contract signing, ring signature schemes can be used to construct e-auction protocols. By using ring signature, a winner-identifiable anonymous auction protocol can be build efficiently. That is to say, the auctioneer can authenticate the real identity of the winner at the end of the protocol without additional interactions with the winning bidder even though all the bidders bid anonymously. Adding forward security further provides additional security to all entities involved in the auction activity. The loss of secret key by anybody does not affect the overall result. It is one of the best way to safeguard the robustness of the function.

3. FLOW OF SYSTEM

For any system or program it is important to define the flow of the program. A data flow diagram is a graphical representation of the flow of data through an information system, modelling its process aspects. Often they are a preliminary step used to create an overview of the system which can later be elaborated. A flow diagram shows what kind of information will be input to and output from the system, where the data will come from and go to, and where the data will be stored. It does not show information about the timing of processes, or information about whether processes will operate in sequence or in parallel.

3.1 Login Page



Owner Login:Cost Effective Authentic and Anonymous Data Sharing with Forward Security

Owner Login!!!!!!!!!

Username: ansh

Password: ••••

Address: ngp

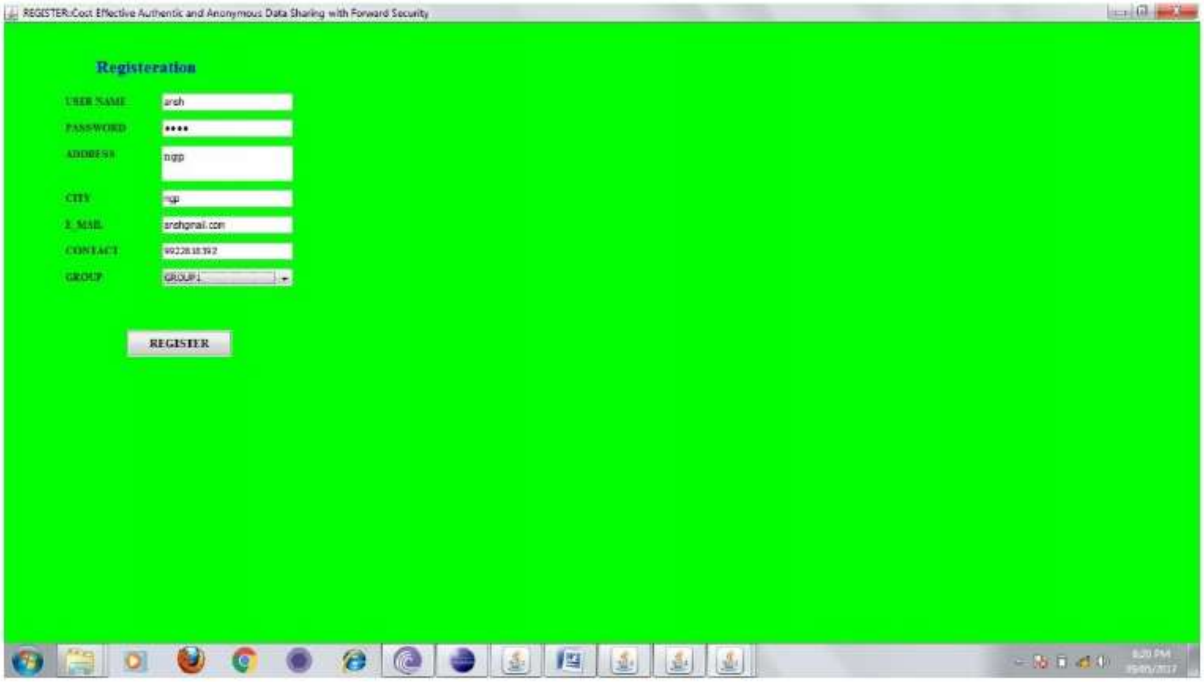
Ring Sign:

Group: GROUP1

Fig -2: Login Page

To login into system we have to enter the above fields correctly. For this figure 2 we must have to be a registered user if not there is a register button which will take you to the Registration Page to get registered yourself.

3.2 Registration Page



REGISTER:Cost Effective Authentic and Anonymous Data Sharing with Forward Security

Registeration

USER NAME: ansh

PASSWORD: ••••

ADDRESS: ngp

CITY: ngp

E_MAIL: anshgmail.com

CONTACT: 9922818392

GROUP: GROUP1

Fig -3: Registration Page

As to successfully login into system we must have to be registered user. In this figure 3 we have to enter user name, Password, Address, City, Email, Contact, Group in above form

3.3 Data Centre Verifier Page

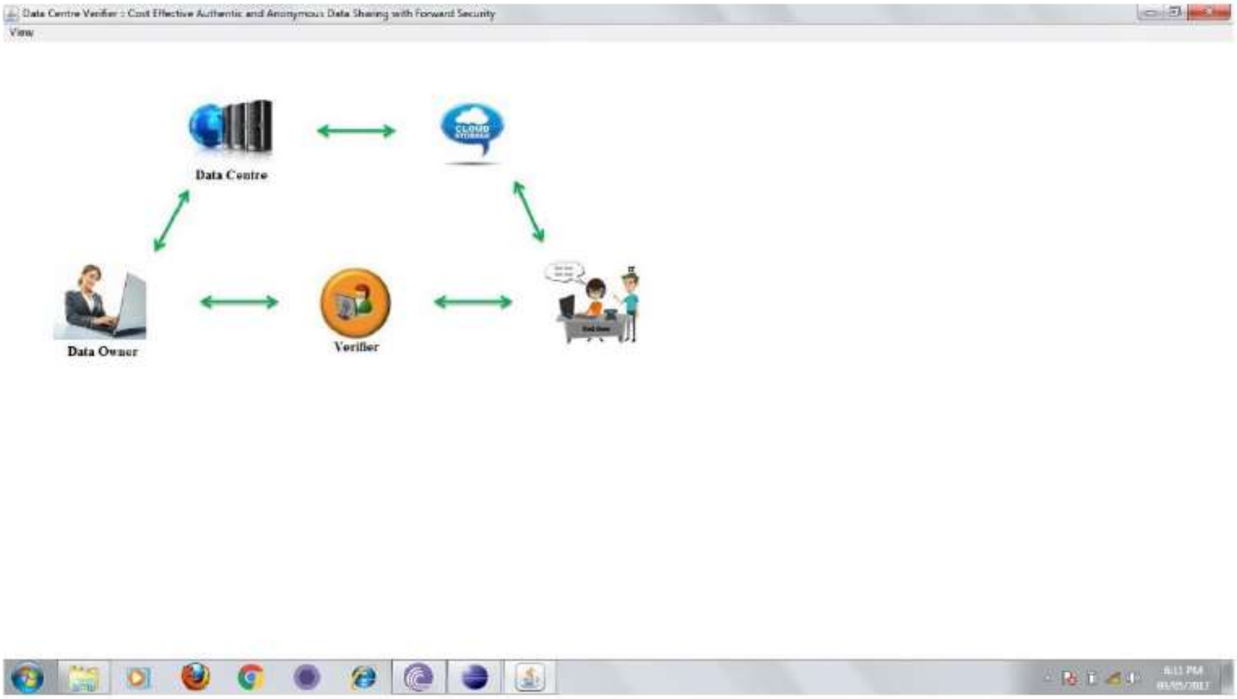
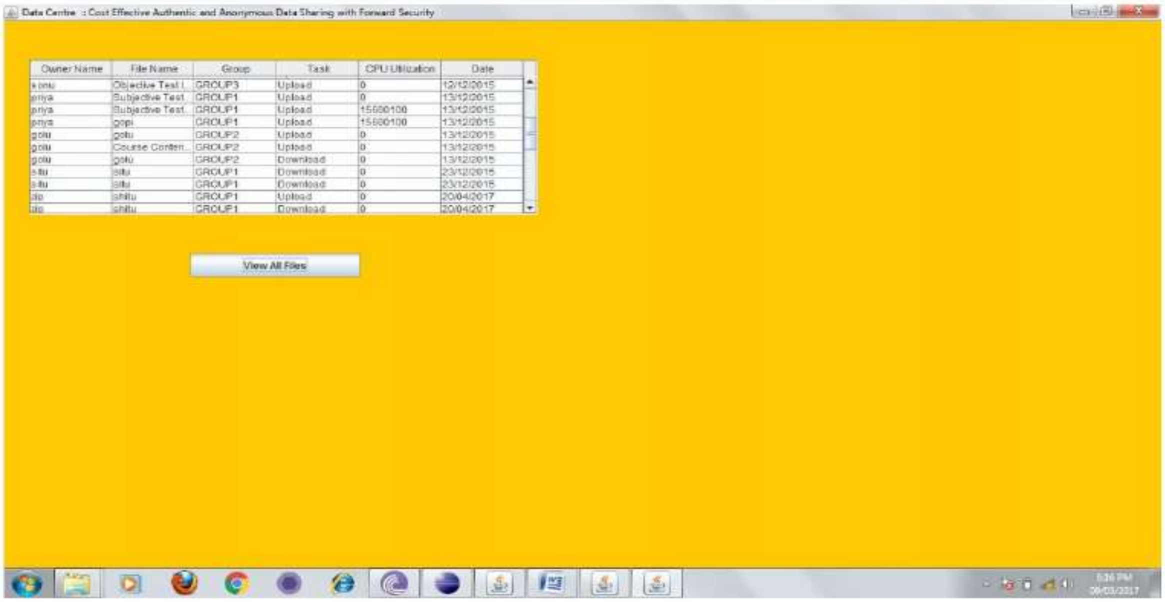

Data Centre Verifier : Cost Effective Authentic and Anonymous Data Sharing with Forward Security
View
Data Centre
CLOUD STORAGE
Data Owner
Verifier
End User

Fig -4: Data Center Verifier Page

As per figure 4 is of Data Center Verifier. It consists of five main module Cloud Server, Data Center, Verifier, Data Owner, End User. We can see all the background processes like Verification, Registration, Login etc. of system with this page. It shows the process by blinking the images and by displaying message. Also you can see details of registered user, group users, group sign.

3.4 Data Centre Page

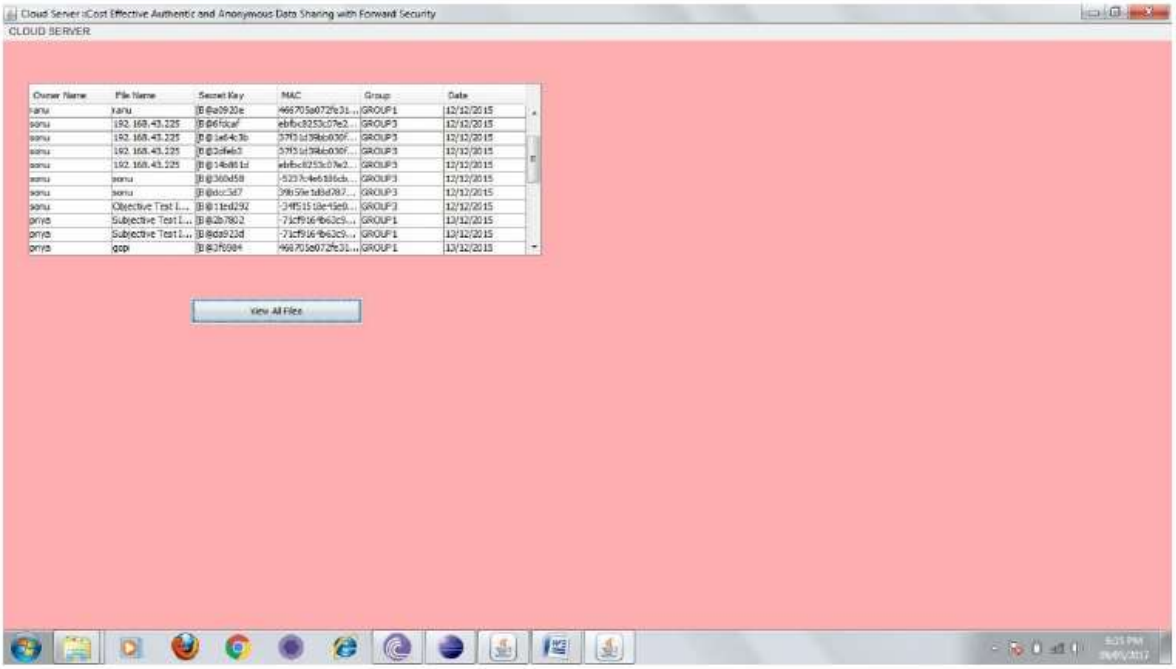

Data Centre : Cost Effective Authentic and Anonymous Data Sharing with Forward Security
View All Files

Owner Name	File Name	Group	Task	CPU Utilization	Date
konu	Objective Test I...	GROUP3	Upload	0	12/12/2015
priya	Subjective Test	GROUP1	Upload	0	13/12/2015
priya	Subjective Test...	GROUP1	Upload	15600100	13/12/2015
priya	gopi	GROUP1	Upload	15600100	13/12/2015
golu	golu	GROUP2	Upload	0	13/12/2015
golu	Course Conten...	GROUP2	Upload	0	13/12/2015
golu	golu	GROUP2	Download	0	13/12/2015
situ	situ	GROUP1	Download	0	23/12/2015
situ	situ	GROUP1	Download	0	23/12/2015
dip	shitu	GROUP1	Upload	0	20/04/2017
dip	shitu	GROUP1	Download	0	20/04/2017

Fig -5: Data Centre Page

Above figure 5 is of Data Center Page. It maintains all the transaction records of uploads and downloads, Calculate CPU Energy for each and every file uploads, Date and owner of transaction. And we can see the details of it here.

3.5 Cloud Server Page

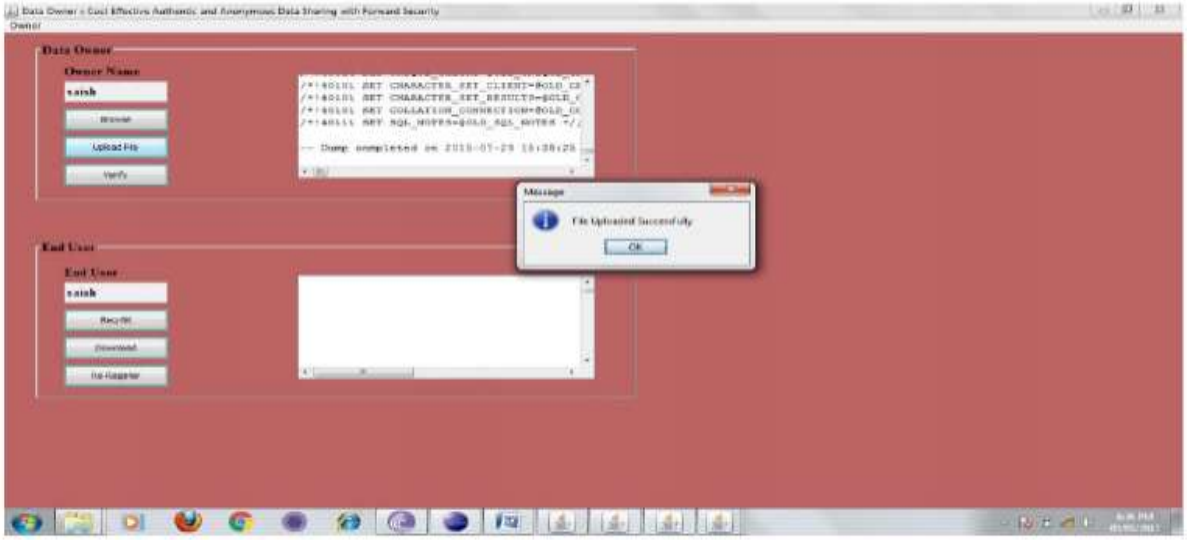

Cloud Server :Cost Effective Authentic and Anonymous Data Sharing with Forward Security
CLOUD SERVER
View All Files

Owner Name	File Name	Secret Key	MAC	Group	Date
kanu	kanu	[B@a0920e	466705a072fe31...	GROUP1	12/12/2015
sonu	192.168.43.225	[B@6fdcaf	ebfbc8253c07e2...	GROUP3	12/12/2015
sonu	192.168.43.225	[B@1e64c3b	57f51d38bb030f...	GROUP3	12/12/2015
sonu	192.168.43.225	[B@2dfeb3	57f51d38bb030f...	GROUP3	12/12/2015
sonu	192.168.43.225	[B@14b881d	ebfbc8253c07e2...	GROUP3	12/12/2015
sonu	sonu	[B@360d58	-5237c4e6186cb...	GROUP3	12/12/2015
sonu	sonu	[B@dcc3d7	39b59e1d8d787...	GROUP3	12/12/2015
sonu	Objective Test I...	[B@11ed292	-34f5151 8e45e0...	GROUP3	12/12/2015
priya	Subjective Test I...	[B@2b7802	-71cf9164b63c9...	GROUP1	13/12/2015
priya	Subjective Test I...	[B@da923d	-71cf9164b63c9...	GROUP1	13/12/2015
priya	gopi	[B@2f6984	466705a072fe31...	GROUP1	13/12/2015

Fig -6: Cloud Server Page

As per above figure 6 see maintain file transaction details, store all files, user details, group users. List all updated Secrete Key details based on the date and users and List all File attackers and File Receive Attackers. Also we can view all attackers information here.

3.6 Data Owner Page



Owner Name: saish

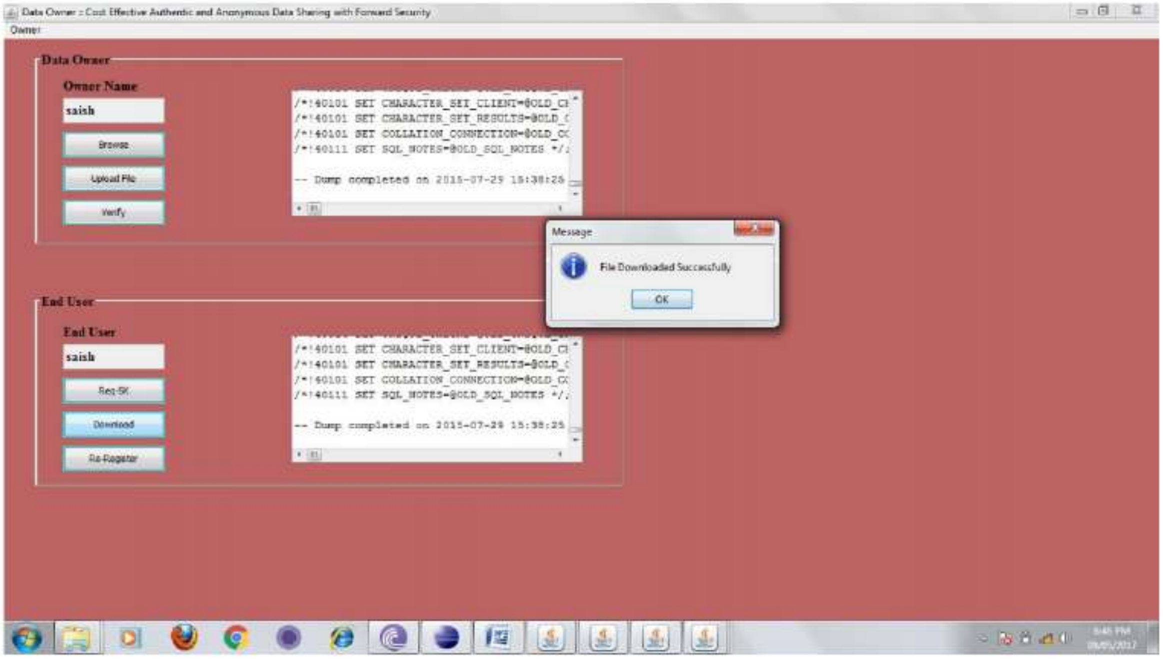
```
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CH
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_C
/*!40101 SET COLLATION_CONNECTION=@OLD_CO
/*!40111 SET SQL_NOTES=@OLD_SQL_NOTES */;

-- Dump completed on 2015-07-29 15:38:28
```

File Uploaded Successfully

End User: saish

Fig -7: Data Owner Page Uploading

As per figure 7 We can upload any file with the help of data owner page. It helps to request secret key and re-register. We can verify whether the file is safe to upload or not. If the file is attacked then it will show file is not safe message.



Owner Name: saish

```
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CH
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_C
/*!40101 SET COLLATION_CONNECTION=@OLD_CC
/*!40111 SET SQL_NOTES=@OLD_SQL_NOTES */;

-- Dump completed on 2015-07-29 15:38:25
```

File Downloaded Successfully

End User: saish

```
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CH
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_C
/*!40101 SET COLLATION_CONNECTION=@OLD_CC
/*!40111 SET SQL_NOTES=@OLD_SQL_NOTES */;

-- Dump completed on 2015-07-29 15:38:25
```

Fig -8: Data Owner Page Downloading

As per figure 8 We can download any file with the help of data owner page. It helps to request secret key and re-register. We can verify whether the file is safe to upload or not. If the file is attacked then it will show file is not safe message.

3.7 File Attacker Page

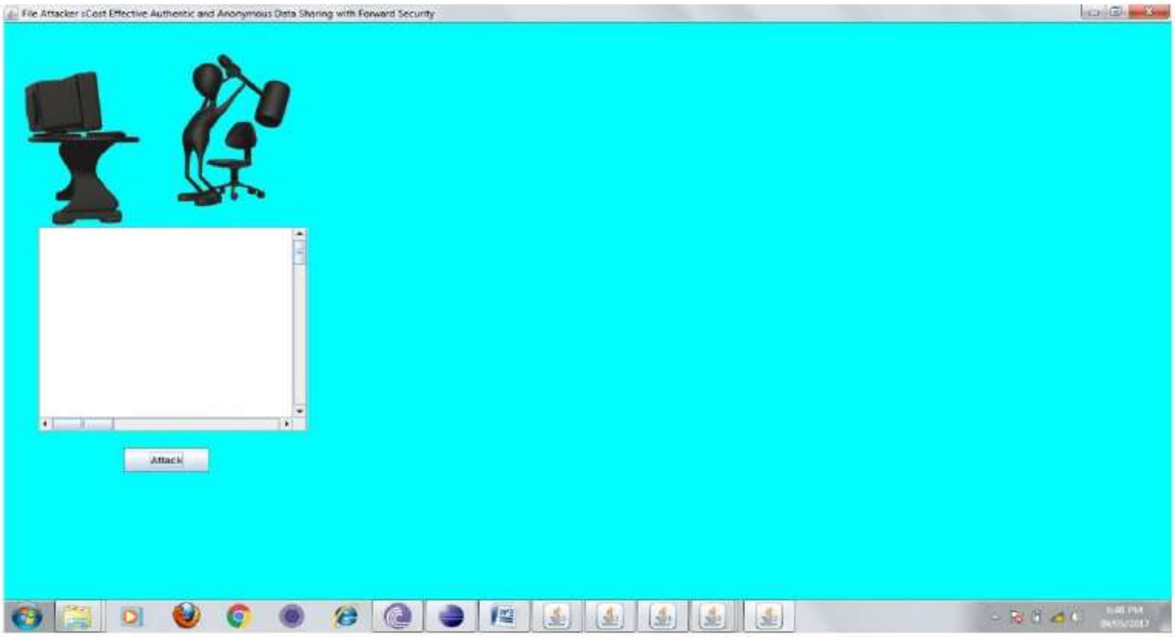

File Attacker :Cost Effective Authentic and Anonymous Data Sharing with Forward Security
Attack

Fig -9: Data Owner Page Downloading

As per figure 9 File attack can be done through this page. By providing File Name and Cloud Server IP we can attack on the Particular File which will make file unsafe.

3.8 Group Attacker Page

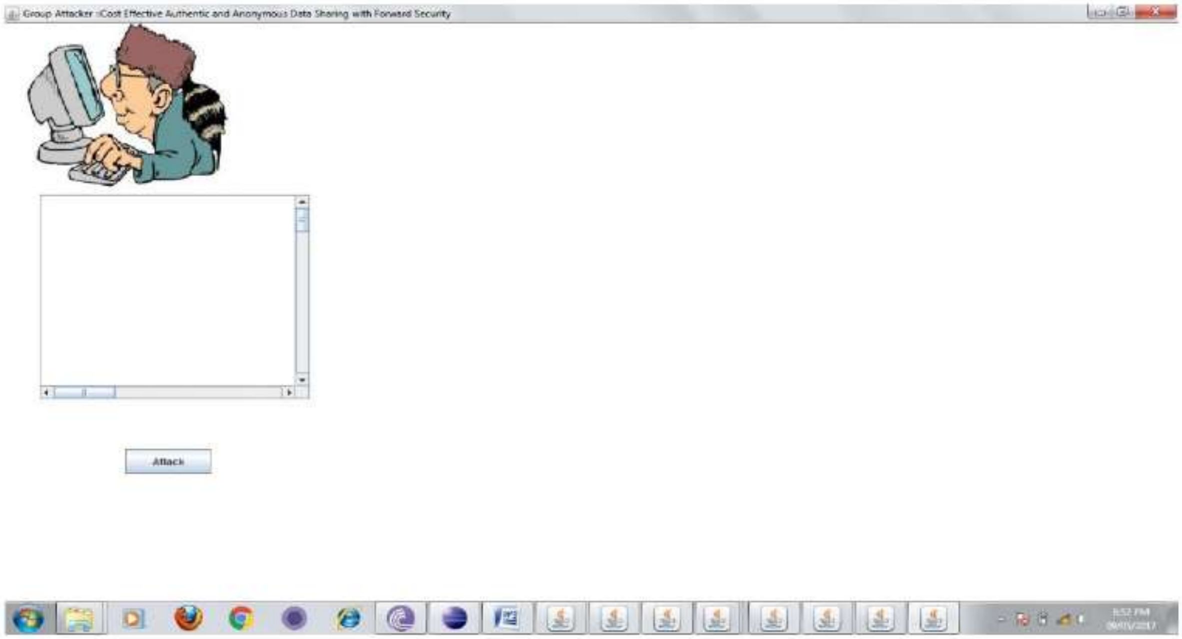

Group Attacker :Cost Effective Authentic and Anonymous Data Sharing with Forward Security
Attack

Fig -10: Group Attacker Page

As per figure 10 Through the Group Attack page we can attack on group. For this you need to select group on which you want to attack.

3.9 Ring Signature Attacker Page

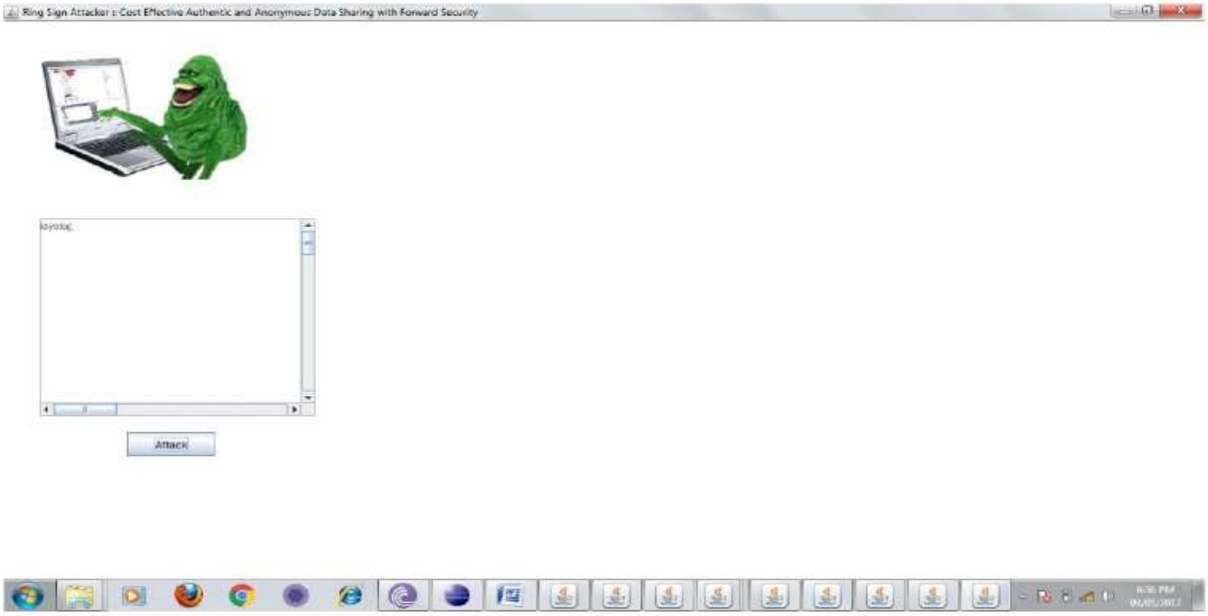

Ring Sign Attacker :: Cost Effective Authentic and Anonymous Data Sharing with Forward Security
loyolaj
Attack

Fig -11: Ring Signature Attacker Page

As per figure 11 Attacker can attack on ring signature by providing Username and IP Address. Later when User tries to login into system it shows invalid user in the system.

4. CONCLUSIONS

Motivated by the practical needs in data sharing, analyze a new notion called Forward Secure ID-Based Ring Signature. It allows an ID-based ring signature scheme to have forward security. It is the first in the literature to have this feature for ring signature in ID-based setting. Our scheme provides unconditional anonymity and can be proven forward-secure enforceable in the random oracle model, assuming RSA problem is hard. Our scheme is very efficient and does not require any pairing operations. The size of user secret key is just one integer, while the key update process only requires an exponentiation. We believe our scheme will be very useful in many other practical applications, especially to those require user privacy and authentication, such as ad-hoc network e-commerce activities and smart grid.

5. REFERENCES

[1]. Hasen Nicanfar, Peyman TalebiFard, Amr Alasaad, and Victor CM Leung. \Privacy-preserving scheme in smart grid communication using enhanced network coding". In Communications (ICC), 2013 IEEE International Conference on, pages 2022{2026. IEEE, 2013.

[2]. Shaohua Tang Yang Xiang Kaitai Liang Li Xu Jianying Zhou Xinyi Huang, Joseph K.Liu. \Cost-effective authentic and anonymous data sharing with forward security". volume 64. IEEE, 2014.

[3]. Masayuki Abe, Miyako Ohkubo, and Koutarou Suzuki. \1-out-of-n signatures from a variety of keys". Advances in CryptologyAsiacrypt 2002, pages 639{644, 20020)

[4]. Giuseppe Ateniese, Jan Camenisch, Marc Joye, and Gene Tsudik. \A practical and provably secure coalition-resistant group signature scheme". In Advances in CryptologyCRYPTO 2000, pages 244270. Springer, 2000.

[5]. Man Ho Au, Joseph K Liu, Tsz Hon Yuen, and Duncan S Wong. \ID-based ring signature scheme secure in the standard model". In International Workshop on Security, pages 1{16. Springer, 2006.

[6]. Amit K Awasthi and Sunder Lal. \ID-based ring signature and proxy ring signature schemes from bilinear pairings". arXiv preprint cs/0404097, 2004.

[7]. Joseph K Liu, Tsz Hon Yuen, and Jianying Zhou. \Forward secure ring signature without random oracles". In ICICS, volume 2011, pages 1{14. Springer, 2011. [9] Fangguo Zhang and Kwangjo Kim. \ID-based blind signature and ring signature from pairings". Advances in cryptology ASIACRYPT 2002, pages 629637, 2002.