International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 20 Issue 3 – MARCH 2016.

# FORWARD SECURE SMART GRID WITH ID BASED RING SIGNATURE

[1]Swathika B S, [2]Rajesh R

[1]*BE Student, Department of Computer Science and Engineering, IFET College of Engineering, Villupuram, bsswathika@gmail.com.*
[2]*Assistant Professor, Department of Computer Science and Engineering, IFET College of Engineering, Villupuram.*

***Abstract*--Exposure of key is the fundamental drawback of ordinary digital signatures. If the private key of a signer is compromised, all signatures of that signer becomes unworthy, future signatures are invalidated and no previously issued signatures can be trusted. The concept of forward secure signature is used to preserve the validity of past signatures even if the current secret key is compromised. The issue of key exposure is more severe in a ring or in a closed group. The exposure of one user's secret key renders all previously obtained ring signatures invalid if that user is one of the ring members. Hence Forward security is a necessary requirement on ring signatures. In ID based Ring Signature with forward security, to verify a user, only the identities of ring users are used, together with the pair of message and signature are needed. As one can see, the elimination of certificate validation, which is a costly process, saves a great amount of time and computation. This saving will be more critical if a higher level of anonymity is needed by increasing the number of users in the ring. ID-based ring signature is more preferable in the setting with a large number of users such as energy data sharing in smart grid.**

***Keyword: Smart grid, ID based ring signature, forward security.***

## I. INTRODUCTION

### i. Traditional System

Costly certificate verification in the traditional public key infrastructure (PKI) becomes a drawbackfor this solution to be scalable. A smart grid contains huge number of nodes/junctures and each node will have enormous number of consumers (end users). This results in high transmission of data within a grid. Due to its openness, a smart grid is vulnerable to a number of security threats

By employing traditional authentication and security mechanisms may provide security but impacts the efficiency of the smart grid due to high transmission of data.The number of users in a data sharing system could be huge (example: A smart grid with a country size) and leads to high computation and communication cost.

Suppose there are 10,000 users in the ring, the verifier of a traditional public key based ring signature must first validate 10,000 certificates of the corresponding users, after which one can carry out the actual verification on the message and signature pair which is a costly process, saves a great amount of time and computation. This saving will be more critical if a higher level of anonymity is needed by increasing the number of users in the ring.

This saving will be more critical if a higher level of anonymity is needed by increasing the number of users in the ring.

### ii. Smart Grid

A smart grid is an electronic grid which consist of many features which enables to not only conserve electricity usage but also allows people to use renewable resources effectively including smart meters, smart appliances, renewable energy resources, and energy efficiency resources. Electronic power conditioning and control of the production and distribution of electricity.

Users in a 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. From the collected data a statistical report is created, and
one can compare their energy consumption with others. This ability to access, analyzes, and responds to much more precise and detailed data from all levels of the electric grid is critical to efficient energy usage.

**Anonymity**

Energy usage data contains variety of information of consumer, from which one can extract the number of persons in the home, the types of electric utilities used in a specific time period, etc.

**Data Authenticity**

In the situation of smart grid, the statistic energy usage data would be misleading if it is forged by adversaries.

**Access Control:-**

Only eligible users can have the access to the data.

**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.

**Availability**

There are other security issues in a data sharing system which are equally important, such as availability.

## II. RELATED WORK

In the two remarks on public key cryptography the issue with security of the key is discussed. Where once the private key is compromised the previously issued data and the validity of the future data becomes useless. This issue of key exposure is more sensitive in a closed group[2]. To overcome this drawback we go with forward security. Where even though the current key of the signer is compromised the past and the future keys which were issued remains protected as random keys are generated each time of the data transfer.

In 2010 P. P. Tsang, et al proposes "A suite of non-pairing ID-based threshold ring signature schemes with different levels of anonymity". The public key of each user is easily computable from a user's public identity (like email address, residential address, etc.). A private key generator (PKG) then computes private keys from. This public key property avoids the need of certificate validation. This type of validation required necessary in traditional public-key. [12]

Traditional digital signature scheme which works with certificate verification process is not much effect in a group which consists of larger number of members which is both time and cost consuming in a large group or a ring where each time when a data is transferred the time consuming certificate verification is done[3].

RSA algorithm is cheaper than D-H operation. To be more clearly using RSA encryption is much cheaper than D-H encryptionin terms of time and space[4] .While the RSA decryption entails to be more or less the same cost with D-H operations.

## III. PROPOSED SYSTEM

Forwarded secure Identity-based (ID-based) ring signature which eliminates the process of certificate verification which combines the ID Based crypto system and ring signature. In this project further enhance the security of ID-based ring signature by providing forward security.In future smart grid will become an essential factor for efficient utilization of both the renewable and non-renewable energy resources and to save electricity charges. As the users of a smart grid require privacy so that their personal identity is not compromised and also that they require an efficient analysis on their and others electricity usage.

As traditional system makes use of certificate verification process which is both time consuming and costly. And also that the expectation of smart grid users is to not compromise their identity ID based ring signature scheme is used.

By which the anonymity of the user is preserved and also that the user who is accessing the data is assured to be authentic. By doing so the costly certificate verification process can be eliminated, this is not required as the user of the grid is known and authenticated.

Smart grid with certain number of users will be managed by an administrator who has the ability to add, remove and group the authenticated users to a group which can be secreted under some criteria say for example based on the locality. After being added to a group the user can access other electricity usage and gain a reasonable knowledge from it.

A simple example regarding the uploading of data by the by a group or a ring which consist of six members including owner (Figure1).

There are three sections involved in this process were the data is to be uploaded or others data is to be viewed.The administrator is a person who manages the addition of new members by performing verification for the user to be trusted person, adding to locality according to their request, removing the user etc.

### Ring Signature

Ring signature is one type of group-oriented signature with privacy protection on each user. A user can sign individually on behalf of a group on his own choice and send to the other persons in the group as depicted in Figure 2. Any verifier can be frustrated that a message has been signed by one of the members in this group also called the Rings but the actual identity of the user is hided from the originality. Ring signatures could be used for whistle blowing membership authentication for an ad hoc networks and many other applications which do not want complicated group formation stage but require signer anonymity.

.

**Advantage**

- The first ID-based ring signature scheme was proposedin 2002 which can be proven secure in the random oracle model.
- Due to its natural framework, ring signature in ID based Cryptosystem has a significant advantage over its counterpart in traditional public key system.
- The first ID-based ring signature scheme claimed to be secure in the standard model because it is under the trusted setup assumption.

ID-based ring signature is more preferable in the setting with a large number of users such as energy data sharing in smart grid:

**Step 1**: The energy data owner who is present in the group sends his data with the signature which contains the public identity of any one member of the group. This phase only

needs the public identity information of ring members, such as residential addresses, and does not need the collaboration from any ring members.

**Step 2**: Data owner uploads his personal data of electronicusage, together with a ring signature and the identity information of all ring members.

**Step 3**: By verifying the ring signature, one can be assured that the data is indeed given out by a valid resident (from the ring members) while cannot figure out who the resident is. Hence the anonymity of the data provider is ensured together with data authenticity. Meanwhile, the verification is efficient which does not involve any certificate verification


**FIGURE 1**: Energy Usage uploading of ring members to the data center by ID based ring signature.

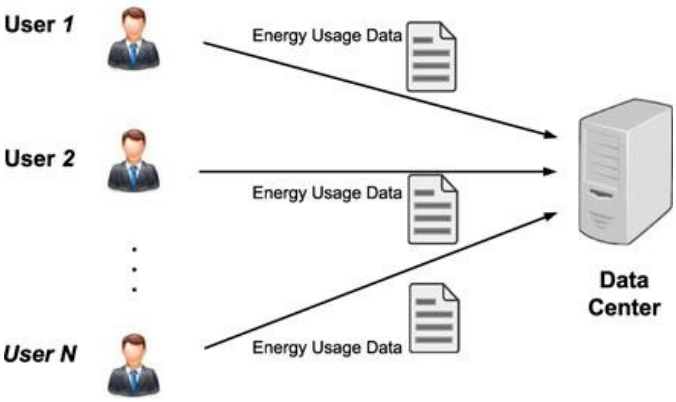



FIGURE 2: Energy usage data sharing in smart grid. [3]

## IV. EXPERIMENTAL RESULT

The applications home page consists of the login page where there are options to both register as a new customer to host a request to join a group in a locality or if it is a registered user; he or she can directly login and either upload his data or view others report.

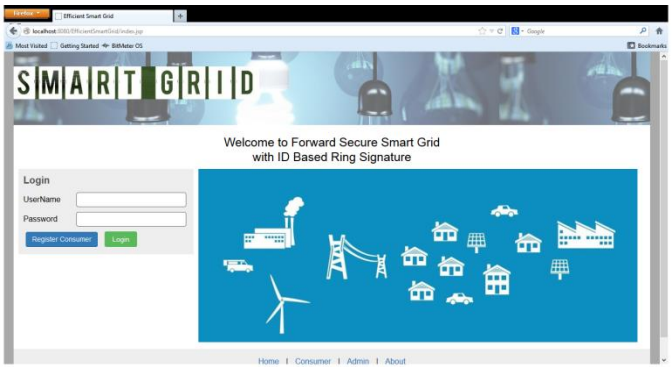
The administrator has the ability to add the user who has registered to a locality. The administrator does the verification of checking the user to be trusted person by direct verification. Then the user is added to the system. Based on the customer's request the new locality is added to the database.

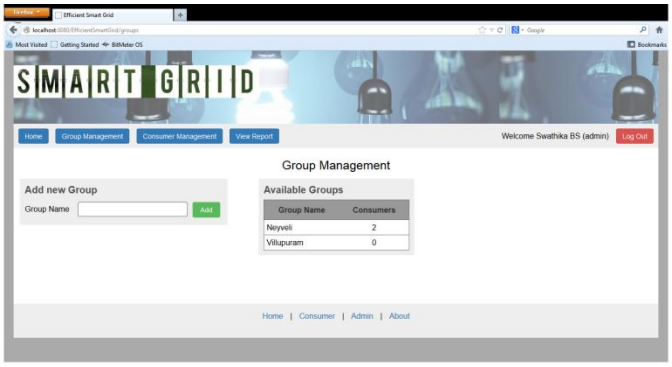
The above are the steps involved in only the registration and addition of users to the system to a locality based on the request.

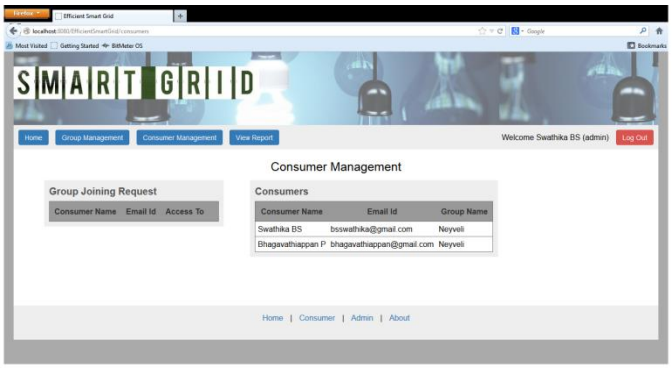
As the users are registered and known to be trusted, verification of the user each time when he or she is trying to access the data is unnecessary.

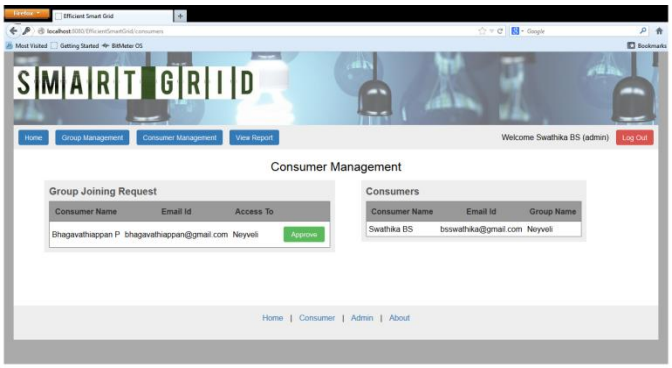
ID based ring signature comes to play only when the data is to be uploaded to the center by the user or when the user tries to access others data.

By which the authenticity and anonymity of the user is preserved. Each time when the user logs in to his account certificate verification is not necessary.






## V. CONCLUSION

The aim of the above proposed system is to provide a user in a ring or a group an authentic data sharing with compramising their identity. And also that the verification of certificate is not required each time when the authorised user tries to access the data center makes it more efficient that is eliminating the need of certificate verification which is time consuming and costly. This system suites well only for a closed group and cannot be extended to a open network.There might be risk in adding unknown members to a group as their validity cannot be trusted.

## REFERENCE

[1] J. Han, Q. Xu, and G. Chen, "Efficient ID-based threshold ring signature scheme," in Proc. IEEE/IFIP Int. Conf. Embedded Ubiquitous Comput., 2008, pp. 437–442.

[2] Ross Anderson "Two remarks on public key cryptography" Technical reports published by the University of Cambridge Computer Laboratory.

[3] Xinyi Huang, Joseph K. Liu, Shaohua Tang, Member, IEEE, Yang Xiang, Senior Member, IEEE,Kaitai Liang, Li Xu, Member, IEEE, and JianyingZhou"Cost effective authentic and anonymous data sharing" ,2015.

[4] J. Herranz, "Identity-based ring signatures from RSA," Theor. Comput. Sci., vol. 389, no. 1-2, pp. J 100–117, 2007.

[5] . Herranz and G. S_aez, "Forking lemmas for ring signatureschemes," in Proc. 4th Int. Conf. Cryptol. India, 2003, vol. 2904,pp. 266–279.

[6] R. Anderson, "Two remarks on public-key cryptology," Manuscript,Sep. 2000. (Relevant material presented by the author in an invited lecture at the Fourth ACM Conference on Computer and Communications Security.)

[7] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A practical and provably secure coalition-resistant group signature scheme," in Proc. 20th Annu. Int. Cryptol. Conf. Adv. Cryptol., 2000, vol. 1880, pp. 255–270.

[8] H. Xiong, Z. Qin, and F. Li, "An anonymous sealed-bid electronic auction based on ring signature," I. J. Netw. Secur., vol. 8, no. 3, pp. 235–242, 2009.

[9] G. Yan, D. Wen, S. Olariu, and M. Weigle, "Security challenges in vehicular cloud computing," IEEE Trans. Intell. Transp. Syst., vol. 14, no. 1, pp. 284–294, Mar. 2013.

[10] J. Yu, R. Hao, F. Kong, X. Cheng, J. Fan, and Y. Chen, "Forwardsecure identity-based signature: Security notions and construction," Inform. Sci., vol. 181, no. 3, pp. 648–660, 2011

[11] J. Yu, F. Kong, H. Zhao, X. Cheng, R. Hao, and X.-F. Guo, "Noninteractive forward-secure threshold signature without random oracles," J. Inform. Sci. Eng., vol. 28, no. 3, pp. 571–586, 2012.

[12] P. P. Tsang, M. H. Au, J. K. Liu, W. Susilo, and D. S. Wong, "A suiteof non-pairing ID-based threshold ring signature schemes withdifferent levels of anonymity (extended abstract)," in Proc. 4th Int.Conf. Provable Security, 2010, vol. 6402, pp. 166–183.