A Privacy Preserving Techniques to Improve Privacy and Efficiency of Smart Grid Technology

Nazimunisa, Avvaru Padmaja, V Swarna Kamalam, Mehveen Mehdikhatoon
Sree Dattha Institute of Engineering & Science, Hyderabad.
Bhoj Reddy Engineering College for Women, Hyderabad.

Abstract – In the smart grid, a full measurement and collection system called the advanced metering Infrastructure (AMI) replaces traditional electromechanical meters. The AMI collects fine-grained, time-based information and transmits them to various parties through a communication network, enabling the integration of demand-side resources into the wholesale market and hence the demand response (DR). The load-following strategy, where a power plant adjusts its power supply to match the fluctuating demand, has been dominant in the traditional power grid operations. However, this strategy incurs a high cost in terms of environment, grid reliability, and operational efficiency. On the contrary, the smart grid places great emphasis on the DR strategy where consumers shape their power demand to match the supply.

Index Terms – Smart grid, AMI, DRP, metering.

1. INTRODUCTION

Cloud computing type of “Internet-based computing" where different services such as servers, storage and applications are delivered to an organization's computers and devices through the Internet. Research on the topic of trust in this domain has focused largely on privacy-preserving access authority sharing .In this paper. We propose a shared authority based privacy-preserving authentication protocol to address the privacy issue for cloud storage. The users may want to access and share each other’s authorized data fields to achieve productive benefits, which brings new security and privacy challenges for the cloud storage.

The scope of our project for SAPAs is to define the data integrity and availability is low during data’s sharing. When anonymous ID binding with the data’s during sharing time the quality of dependable cloud storage service for users very poor. So enhancing this method by using Cryptographic algorithm is used to identify this problem and also to improve the privacy and security of the model. Proxy re-encryption is applied by the cloud server to provide data sharing among the multiple users.

Where fine-grained metering data are required to analyze individual demand curtailments, and hence, need to be attributable. This assumption does not hold in incentive-based demand response (IDR) programs where fine-grained metering data are required to analyze individual demand curtailments, and hence, need to be attributable.

Few of problems with the existing work is, Data integrity and availability user need not utilize public key cryptography, and can dynamically derive the symmetric keys during decryption. The attribute based access control mechanism is designed to achieve that a user can decrypt the contents if and only if its identity attributes satisfy the content provider’s policies.

2. LITERATURE SURVEY

According to Dan Boneh, Short Group Signatures, 2014, we construct a short group signature scheme. Signatures in our scheme are approximately the size of a standard RSA signature with the same security. Security of our group signature is based on the Strong Diffie-Hellman assumption and a new assumption in bilinear groups called the Decision Linear assumption. We prove security of our system, in the random oracle model, using a variant of the security definition for group signatures recently given by Bellare,Micciancio, and Warinschi.

As per Giuseppe Ateniese and Breno de Medeiros, Efficient Group Signatures without, Trapdoors, 2007, Group signature schemes are fundamental cryptographic tools that enable unlinkably anonymous authentication, in the same fashion that digital signatures provide the basis for strong authentication protocols. In this paper we present the first group signature scheme with constant-size parameters that does not require any group member, including group managers, to know trapdoor secrets. This novel type of group signature scheme allows public parameters to be shared among organizations. Such sharing represents a highly desirable simplification over existing schemes, which require each organization to maintain a separate cryptographic domain.

According to Cheng-Kang Chu and Wen-Guey Tzeng, Identity-Committable Signatures and Their Extension to Group-Oriented Ring Signatures, 2011, We introduce a new notion of identity-committable signatures (ICS) to ensure the anonymity of Deep Throat" inside a group. A member of an organization can sign a message on behalf of himself (regular signature) or the organization (identity- committed signature). In the latter case, the signer's identity is hidden from anyone, and can be opened by himself only. We describe the requirements of ICS and give the formal de¯nition of it. Then we extend the notion of ICS to group-oriented ring signatures

(GRS) which further allow the signer to hide his identity behind multiple groups. We believe a GRS scheme is more e±cient and practical than a ring signature scheme for leaking secrets. Finally, we provide concrete constructions of ICS and GRS with information-theoretic anonymity, that is, the identity of the signer is fully-protected.

A per Cheng-Kang Chu And Wen-Guey Tzeng, Efficient Identity-Committable Signature and Group-Oriented Ring Signature Schemes 2003, Jae Choon Cha1 and Jung Hee Cheon2, Identity-Based Signature from Gap Diffie-Hellman Groups,2004, Private Memoirs of a Smart Meter by Andr´es Molina-Markham, Prashant Shenoy, Kevin Fu, Designing Privacy-preserving Smart Meters with Low-cost Microcontrollers by Andres Molina-Markham, George Danezis, Security and Privacy in the Smart Energy Grid by Martin Erich Jobst, A QoS Guided Scheduling Algorithm for Grid Computing by Xiaoshan He1and A QoS Guided Scheduling Algorithm for Grid Computing by Xiaoshan He1were explained about on these technologies.

3. RELATED WORK

System Shared access authority is achieved by anonymous access request matching mechanism with security and privacy considerations (e.g., authentication, data anonymity, user privacy, and forward security).Attribute based access control is adopted to realize that the user can only access its own data fields. Proxy re-encryption is applied by the cloud server to provide data sharing among the multiple users.

A new privacy challenge during data accessing in the cloud computing to achieve privacy-preserving access authority sharing. Authentication is established to guarantee data confidentiality and data integrity. Data anonymity is achieved since the wrapped values are exchanged during transmission. User privacy is enhanced by anonymous access requests to privately inform the cloud server about the users' access desires.

While instrumental to the implementation of DR, finegrained metering data collected by the AMI can be used to determine occupant activities, raising serious privacy concerns [8]. Research studies on non-intrusive load monitoring (NILM) have shown the possibility of deducing appliance usage patterns from fine-grained metering data. The appliance usage patterns can be further analyzed to learn the health status, daily routines or unusual behaviors such as "you slept late at night" and "your child is left alone at home" . Hence, a growing number of research activities have been carried out to address privacy issues in the AMI.

4. PROPOSED WORK

In this paper, we propose a privacy-preserving scheme for smart grid technology, which enables the demand response provider (DRP) to compute individual demand curtailments and demand response rewards while preserving customer privacy. Moreover, a customer identity and ownership of power usage profile in certain situations such as legal disputes. We focused on privacy and efficiency in our scheme by using cryptographic algorithms identity-committable signatures (ICS) and partially blind signatures.

System Algorithms:

Algorithm: Cipher text policy attribute based encryption (CP-ABE).

When a users wants to sharing the data's from one to another the cloud serves the authenticated anonymous key for both users. This key performed both users when a data sharing encryption and decryption is achieved. When users shares the information by the cloud server with the same symmetric key.

In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous Attribute Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt.

The challenger runs the Setup algorithm and gives the public parameters, PK to the adversary.

Phase 1. The adversary makes repeated private keys corresponding to sets of attributes S1,... ,Sq1 . Challenge. The adversary submits two equal length messages M0 and M1. In addition the adversary gives a challenge access structure $A*$ such that none of the sets S1,... ,Sq1 from Phase 1 satisfy the access structure. The challenger flips a random coin b, and encrypts Mb under $A*$. The ciphertext $CT*$ is given to the adversary.

Phase 2. Phase 1 is repeated with the restriction that none of sets of attributes Sq1+1,... ,Sq satisfy the access structure corresponding to the challenge. Guess. The adversary outputs a guess b' of b. The advantage of an adversary A in this game is defined as $Pr[b' = b] - 1\ 2$. We note that the model can easily be extended to handle chosen-ciphertext attacks by allowing for decryption queries in Phase 1 and Phase 2.

The following game models the user privacy. The rationale is that the curious DRP cannot tell which one of two honest users is responsible for a particular interaction under the extreme

condition that all other interaction sequences have been specified by the curious DRP. The particular interaction could be during pseudonym registration, settlement, querying, and revocation, but not during real identity registration or metering, because real identity is to be known in real identity registration, and no real identity is revealed by the smart meter in metering. Our definition also guarantee that the settlement interactions are unlikable.

• *System Parameter*. The malicious adversary *A* creates and publishes the system parameter.

Interactions. Adversary *A* can make the following four types of interactions freely with *C*, who acts on behalf of two honest users *U*0;*U*1.

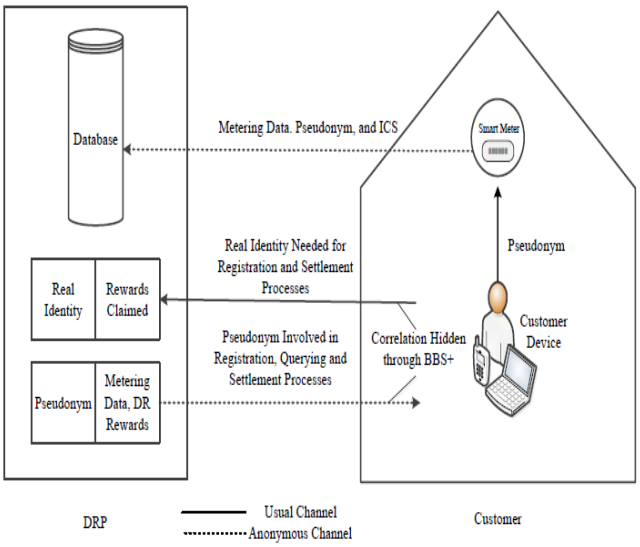
• *Registration* ($b \in \{0; 1\}$). *A* interacts with *C* who acts on behalf of *Ub* in the registration protocol. The value *b* is specified by *A*.

• *Querying* ($b \in \{0; 1\}$). *A* interacts with *C* who acts on behalf of *Ub* in the querying process. The value *b* is specified by *A*.

• *Settlement* ($b \in \{0; 1\}$). *A* interacts with *C* who acts on behalf of *Ub* in the settlement process with value *d*. The value *b* is specified by *A*.

• *Revocation* ($b \in \{0; 1\}$). *A* interacts with *C* who acts on behalf of *Ub* in the revocation process. The value *b* is specified by *A*.

Challenge. *A* chooses a type of interaction among pseudonym registration, querying, settlement, and revocation.



The DRP creates two accounts for a customer, one associated with his real identity and the other associated with his pseudonym. The real identity can be any information that uniquely identifies the customer, such as the account number or telephone number. Since a customer can only enroll in a single IDR program at a time, the DRP needs to make sure that a customer does not register multiple pseudonyms. This is achieved with the anonymous ticket: the customer obtains a ticket when he registers the real identity and presents it to the DRP when he anonymously registers the pseudonym. In the metering process, the smart meter collects metering data, constructs signatures on them, and sends them together with its pseudonym to the DRP through the anonymous channel. The DRP stores the data by pseudonym in the database and analyzes the data for operational and settlement purposes.

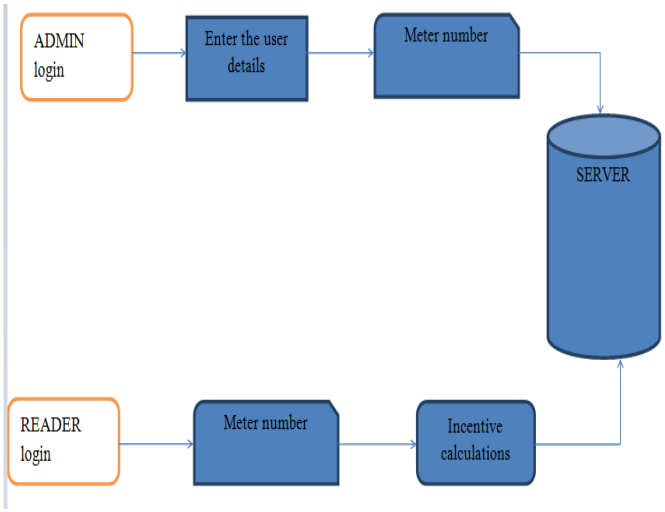


Fig.2. System Architecture

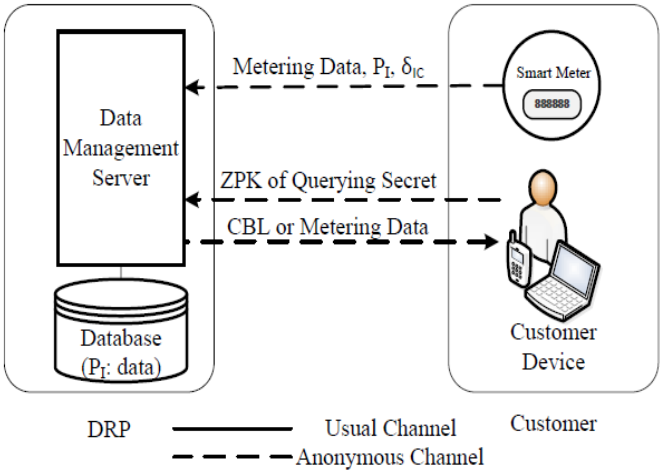


Fig.3. Metering Process [18]

5. IMPLEMENTATION

System Shared access authority is achieved by anonymous access request matching mechanism with security and privacy considerations (e.g., authentication, data anonymity, user privacy, and forward security).Attribute based access control is adopted to realize that the user can only access its own data

fields. Proxy re-encryption is applied by the cloud server to provide data sharing among the multiple users.

Modules Description:

User Interface Design

In this module we design the windows for the project. These windows are used to send a message from one peer to another. We use the Swing package available in Java to design the User Interface. Swing is a widget toolkit for Java. It is part of Sun Microsystems' Java Foundation Classes an API for providing a graphical user interface for Java programs. In this module mainly we are focusing the login design page with the Partial knowledge information. Application Users need to view the application they need to login through the User Interface GUI is the media to connect User and Media Database and login screen where user can input his/her user name, password and password will check in database, if that will be a valid username and password then he/she can access the database.

Admin login and register

This module is used to admin to upload users registration. Here admin want to register the meter number of the particular users and the location details. This will be used for readers login time to calculate their incentives.

Reader login

This module is used to reader login. After the reader login they need to fill the incentive calculation according to usage. The incentive is calculated considering the maximum current registered by the admin.

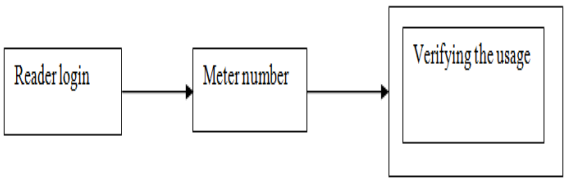


Fig.4. Reader login

Incentive calculation:

This module is used to calculate the incentive. The incentive is calculated by the reader. If the users reach the certain maximum power the incentive will calculated automatically. Smart meter will shows the how much power will the user used.

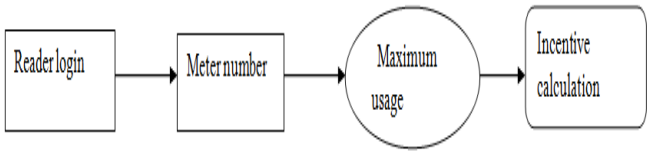


Fig.5. Incentive Calculation

User login

This module is used for user's login. After user login they need to give a particular meter number. Then it will separately show their bill with incentive details.

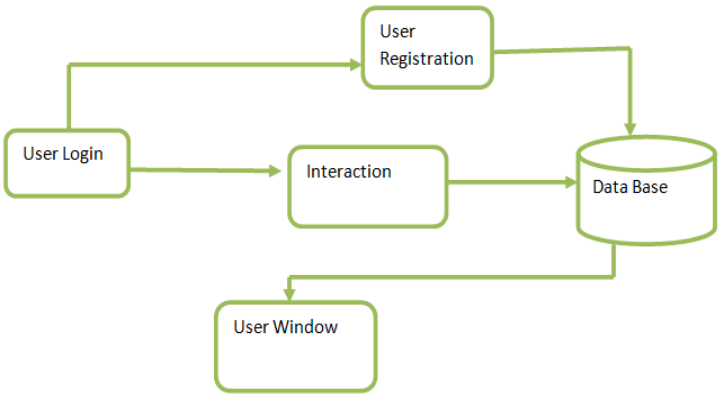


Fig.6. Modules Flow

6. RESULTS

In this paper we propose a shared authority based privacy-preserving authentication protocol to address the privacy issue for cloud storage. The users may want to access and share each other's authorized data fields to achieve productive benefits, which brings new security and privacy challenges for the cloud storage. The results proved that the system works and gives good results.

Registration		Metering			Querying		Settlement	
Customer	DRP	Customer	Smart Meter	DRP	Customer	DRP	Customer	DRP
22	14	0	0	0	2	1	48	21
1	6	0	0	0	0	1	3	9
4	6	0	0	0	0	5	13	16
1	2	0	0	0	0	1	2	3
3	2	0	0	5	0	1	6	2
2	0	0	0	0	0	0	2	0

Table.1. Performance Analysis

Fig.7.New Registration

Fig.8.Metering Number and Incentive Calculation

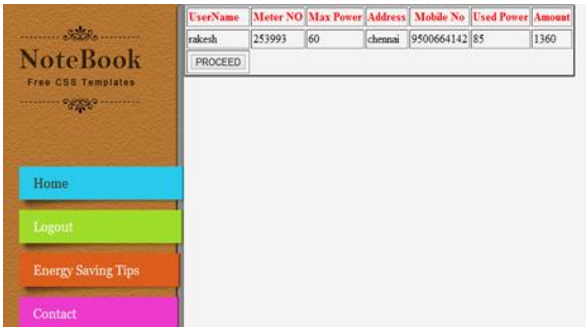


Fig.9. Show Experimental results

7. CONCLUSION

In this paper, used fine-grained metering technology for demand data response. It gives good privacy for the users' data with unique identity. The data integrity can be done with DRP by using re-identification. Finally this scheme provides solutions for IDR programs with efficiency and giving privacy solutions. But we failed in explaining the solutions for different issues in metering process.

8. FURTURE ENHANCEMENT

In the future, the proposed methodology can be extended by limiting the trust level in the CS. This will further enhance the system to cope with insider threats. Moreover, the response of the methodology with varying key sizes can be evaluated.

REFERENCES

[1] Benefits of Demand Response in Electricity Markets and Recommendations for Achieving Them, U.S. Dept. Energy, Washington, DC, USA, Tech. Rep., Feb. 2006.
[2] A. Ipakchi and F. Albuyeh, "Grid of the future," IEEE Power Energy Mag., vol. 7, no. 2, pp. 52–62, Mar./Apr. 2009.
[3] C. Goldman, M. Reid, R. Levy, and A. Silverstein, "Grid of the future," Lawrence Berkeley Nat. Lab., Univ. California, Berkeley, CA, USA, Tech. Rep. LBNL-55281, 2010.
[4] EnerNoc. (2008). The Demand Response Baseline. [Online]. Available: http://www.naesb.org/pdf4/dsmee_group2_022609w2.pdf
[5] G. W. Hart, "Non-intrusive appliance load monitoring," Proc. IEEE, vol. 80, no. 12, pp. 1870–1891, Dec. 1992.
[6] D. C. Bergman et al., "Distributed non-intrusive load monitoring," in Proc. IEEE PES Innov. Smart Grid Technol. (ISGT), Anaheim, CA, USA, 2011, pp. 1–8.
[7] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, "Private memoirs of a smart meter," in Proc. ACM Workshop Embedded Sens. Syst. Energy Efficien. Build., Zurich, Switzerland, 2010, pp. 61–66.
[8] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology. Berlin, Germany: Springer, 1985, pp. 47–53.
[9] J. C. Cha and J. H. Cheon, "An identity-based signature from gap Diffie–Hellman groups," in Public Key Cryptography—PKC 2003. Berlin, Germany: Springer, 2002, pp. 18–30.
[10] C.-K. Chu and W.-G. Tzeng, "Identity-committable signatures and their extension to group-oriented ring signatures," in Information Security and Privacy. Berlin, Germany: Springer-Verlag, 2007, pp. 323–337.
[11] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," SIAM J. Comput., vol. 18, no. 1, pp. 186–208, 1989.
[12] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in Proc. Adv. Cryptol. (CRYPTO), Santa Barbara, CA, USA, 1987, pp. 186–194.
[13] J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups," in Proc. Adv. Cryptol. (CRYPTO), Santa Barbara, CA, USA, 1997, pp. 410–424.
[14] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in Proc. Annu. Int. Cryptol. Conf. (CRYPTO), Santa Barbara, CA, USA, 1992, pp. 129–140.
[15] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Proc. Annu. Int. Cryptol. Conf. (CRYPTO), Santa Barbara, CA, USA, 2004, pp. 41–55
[16] M. H. Au, W. Susilo, and Y. Mu, "Constant-size dynamic k-TAA," in Proc. 5th Int. Conf. Security Cryptogr. Netw., Maiori, Italy, 2006, pp. 111–125.
[17] K. Coughlin, M. A. Piette, C. Goldman, and S. Kiliccote, "Estimating demand response load impacts: Evaluation of baseline load models for non-residential buildings in California," Lawrence Berkeley Nat. Lab., Berkeley, CA, USA, Tech. Rep. LBNL-63728, 2008.

Authors

Ms. Nazimunisa received M.Tech (CSE) from Jawaharlal Nehru Technological University (JNTUH), Hyderabad. Her research interest includes Data Mining, Computers. Now she is working as an Assistant Professor in CSE Dept, Sree Dattha Institute of Engineering and Science, Hyderabad.

Ms.Avvaru Padmaja, received M.Tech (CSE) from Jawaharlal Nehru Technological University (JNTUH), Hyderabad. Her research interest includes Data Mining, Network Security & Cloud Computing. Now she is working as an Assistant Professor in CSE Dept, Sree Dattha Institute of Engineering and Science, Hyderabad.

Ms.V Swaranakamalam, received M.Tech (CSE) from Jawaharlal Nehru Technological University (JNTUH), Hyderabad. Her research interest includes Data Mining, Network Security. Now she is working as an Assistant Professor in CSE Dept, Bhoj Reddy Engineering College for Women, Hyderabad.

Ms. Mehveen Mehdikhatoon, received M.Tech (CSE) from Jawaharlal Nehru Technological University (JNTUH), Hyderabad. Her research interest includes Data Mining. Now she is working as an Assistant Professor in CSE Dept, Bhoj Reddy Engineering College for Women, Hyderabad.