Efficient Privacy-preserving Authentication for Automated Billing Infrastructure in Smart Grids

Inchara M
MTech PG Student
MCE Hassan
Dept of ECE
Hassan India

Triveni C L
Assistant Professor
MCE Hassan
Dept Of ECE
Hassan, India

Abstract: The concept of smart grid has emerged as a convergence of traditional power system engineering and information and communication technology. It is vital to the success of next generation of power grid, which is expected to be featuring reliable, efficient, flexible, clean, friendly, and secure characteristics. Security has turned into a significant issue when the uses of huge information are drastically developing in cloud processing. The advantages of the execution for these rising innovations have enhanced or changed administration models and enhance application exhibitions in different points of view. Moreover, since millions of smart meters create a huge amount of data, a privacy-preserving authentication scheme in smart grid should not only be secure but also efficient in terms of communication and computation cost. In this proposed approach, we describe smart grid goals and tactics, and present a securing the smart grid. Following a brief discussion about major challenges in smart grid developmentOur proposed approach intends to specifically scramble information also, utilize protection characterization techniques under planning requirements. They improve traditional advanced metering infrastructure (AMI) and meter data management (MDM) functionality with robust data analytics and operational data storage and management capabilities.This approach is intended to boost the security assurance scope by utilizing a specific encryption system inside the required execution time necessities.

Index Terms-Cloud Processing ,Big Data, Smart Grid

I. INTRODUCTION

Smart grid combines traditional grid and information and control technologies. It allows decentralized two-way transmission and reliability and efficiency-driven response, and aims to provide improved reliability (e.g., self-healing, self-activating, automated outage management), efficiency (e.g., cost-effective power generation, transmission, and distribution), sustainability (e.g., accommodation of future alternative and renewable power sources), consumer involvement, and security. Smart meters (SMs) are important components of smart

grid. They are two-way communication devices deployed at consumers premise, records power consumption periodically. With smart meters, smart grid is able to collect realtime information about grid operations and status at an operation center, through a reliable communications network deployed in parallel to the power transmission and distribution grid.Being one of specialized standards has empowered enormous information to be broadly connected in numerous mechanical areas and also investigated in late inquires about.

Smart grid also automates reliable power distribution by engaging and empowering customers in utility management. It exposes customers' detailed real-time electricity use information (through smart meters) to utility companies, which may then change electricity price accordingly or even adjust customers' usage by preinstalled load control switches in order to help flatten demand peaks. Customers are allowed to access their own real-time use information through smart grid services. In order to lower their own energy costs and enjoy uninterrupted activities, they will be willing to use energy efficient appliances and tend to shift power use from peak times to nonpeak times. One of the security concerns is caused by decoded information transmissions because of the huge volume of information. Considering a satisfactory execution level, numerous applications forsake utilizing figure messages in versatile cloud information transmissions.

Table 1: Smart grid goals and tactics

Goals	Tatics
Reliability	Automated real-time monitoring and control of equipments;smart metering and dynamic pricing.
Efficiency	Accommodation of alternative power sources and smart appliances; active management of electric vehicle charging; optimized power generation, transmission and distribution
SecuritY	Accommodation of alternative power sources and smart appliances;active management of electric vehicle charging; optimized power generation, transmission and distribution

Collects data such as energy consumption, hourly readings and auto-recovery of missing values. Your utility does not have to maintain an internal process for collecting billing data, because this function is delivered by Titanium as a service flow that can be directly integrated with your utility's billing system. Remote collection of meter readings reduces operational labour costs and allows utilities to meet new regulations limiting consumption estimations. This marvel can bring about protection spillage issues since plain messages are unchallenging for enemies to catch data in an assortment of routes, for example, sticking, observing, and parodying.

Cloud Computing security challenges and it's also an issue to many researchers; first priority was to focus on security which is the biggest concern of organizations that are considering a move to the cloud. The use of cloud computing brings a lot of advantages including reduced costs, easy maintenance and reprovisioning of resources. The first real use of the concept of cloud computing was in 2002 by the company Amazon Web Services, when it leased its resources to companies during periods off celebrations (when there was no peak usage of its IT) on demand.

II. Related Works

Cloud is a between connective stage for PC clients, which underpins data sharing among different gatherings crosswise over particular framework. Remote correspondences between clients for the most part bring individual data through an assortment of channels, including long range interpersonal communication locales and foundation. Securing information administration, stockpiling, and transmissions are three essential angles that have been investigated in the earlier inquires about.

The data of individual consumers in the region can be aggregated at a local gateway (GW) and forwarded in a compact form to the operation center in order to save communication bandwidth. To preserve user privacy, local gateways should not beable to access the content of consumers data. To enable them to perform data aggregation, homomorphic encryption techniques may be applied for encrypting consumers data. In this technique, a specific linear algebraic manipulation toward the plaintext is equivalent to an other one conducted on the ciphertext. This unique feature allows the local gateway to perform summation and multiplication-based aggregation on received consumer data without decrypting them. Wang et al. concentrated on building up an approach offering a safe cloud framework that could bolster security protecting open inspecting. This examination had investigated the technique for characterizing foes from the information stockpiling side. In any case, the dangers in the information transmissions were not tended to with the goal that this sort of arrangement may bring about security spillages before the inspecting activities.

An efficient Privacy preserving Authentication for Lossless Data Aggregation scheme that protects user privacy under eavesdropping and false data injection attacks. In our scheme, the control center stores received data encrypted in a database at all times to enhance user privacy. The control center decrypts the total sum using the homomorphic encryption, only when service providers or customers who have authority request their energy usage. Thus, the control center is able to spread the computation overhead over a period of time. Moreover, our scheme considers both scenarios for data collecting. So, the control centre can query both the total consumption of a group and individual smart meters while providing user privacy even when the aggregator is compromised.

An efficient privacy-preserving demand response (EPPDR) scheme which employs a homomorphic encryption to achieve privacy-preserving demand aggregation and efficient response. In addition, an adaptive key evolution technique is further investigated to ensure the users' session keys to be forward secure. Security analysis indicates that EPPDR can achieve privacy-preservation of electricity demand, forward secrecy of users' session keys, and evolution of users' private keys. In comparison with an existing scheme which also achieves forward secrecy, EPPDR has better efficiency in terms of computation and communication overheads and can adaptively control the key evolution to balance the trade-off between the communication efficiency and security level.By and by, these investigates for the most part focus on danger discoveries by utilizing an assortment of examination strategies. Our examination proposes an approach that intends to build the rate of encoded information while thinking about the estimation of the information encryptions.

Be that as it may, there are assortments of vulnerabilities despite the fact that numerous entrance control models have been created. Information transmissions in remote systems make an expansive number of chances for assailants to interrupt the interchanges and take information. Protection can be debilitated even a few information portions are caught by enemies in light of the propelled information mining systems. In this paper, we build up a novel approach that specifically encode information keeping in mind the end goal to ensure protection notwithstanding amid the information transmission process. The selective data encryptions depend on the return value of the sensitive data weights and data attributes in order to reduce the chance of sensitive data leakage when hackers apply data hacking techniques.

III PROPOSED FRAMEWORK

In this section, we present our data sharing framework, which consists of five parts: System initialization, Proxy encryption, Proxy re-encryption and Secure data sharing. Before plugging into the details, we first review the preliminaries, including homomorphic encryption and proxy re-encryption.

A. Preliminaries

1) Homomorphic Encryption: Homomorphic encryption is a special form of encryption that allows anyone with ciphertexts of messages (m1, • • • ,mt) to output a ciphertext of message f(m1, • • • ,mt) for some desired function f without knowing the decryption key. If the function f could be any function, then the homomorphic encryption is a fully homomorphic encryption. A concrete homomorphic encryption scheme is composed of the following algorithms.

Algorithm 1

Require: Alice wants to outsource data record $d = d_1, \ldots, d_n$ (Note: The master private key pr_a is known only to Alice; pr_b is known to both Alice and Bob; pk_a and pk_b are public.)

```
   {Steps 1 - 13 performed by Alice}
1: Picks n + m random numbers $r_1, \ldots, r_{n+m}$ ($r_i \in Z_N$ , for
   $1 \leq i \leq n + m$)
2: Generates $d = d_1 + r_1, \ldots, d_n + r_n, r_{n+1}, \ldots, r_{n+m}$
3: $E_{pka} (d) \leftarrow E_{pka} (d_1), \ldots, E_{pka} (d_{n+m})$
4: if $S = \emptyset$ then
5:   for i := 1 to n + m do
6:     Compute $E_{pkb} (\alpha_i)$
7:   end for
8:     $Epk_b (\alpha) \leftarrow Epk_b (\alpha 1), \ldots, Epk_b (\alpha n+m)$
10:    Add $T_b^d$ to $T^d$
11:    Else
```

```
12:   $T_b^d$ = null
13:   end if
```

d. However, similar steps can be used for all data records in the cloud.

For a data record d, the cloud checks whether Bob is authorized to access d by using the authorization token list T^d associated with

If there is no entry related to Bob in T^d, then the cloud simply aborts Bob's request. On the other hand, if there exists an entry for Bob, i.e., T_b^d, then the cloud proceeds as follows:

- Uses the proxy re-encryption key $rk_{pka \to pkb}$ in T_b^d and con-verts E_{pka} (d) to E_{pkb} (d) by computing E_{pkb} (d_1), . . . ,E_{pkb} (d_{n+m}) .
- Computes E_{pkb} ($d_i + \alpha_i$) ← E_{pkb} (d_i) $+_h$ E_{pkb} (α_i) mod

N^2, for $1 \le i \le n + m$. Where $+_h$ is the additive homo-morphic property and N is the group size which is also part of pk_b i.e., the public key of Bob.

- Sends E_{pkb} ($d_1 + \alpha_1$), . . . , E_{pkb} ($d_{n+m} + \alpha_{n+m}$) to Bob.

Upon receiving the data from the cloud, Bob decrypts each entry using his secret key pr_b (which is sent by Alice during Stage 1). That is, Bob performs D_{pkb} (E_{pkb} ($d_i + \alpha_i$)) to get $d_i + \alpha_i$, for $1 \le i \le n + m$.

Note that, Bob is able to successfully decrypt only those at-tributes that he is authorized to access. The attributes he is not authorized to access will yield a value of 0 upon decryption be-cause $d_i + \alpha_i = d_i$ only if Bob has access rights to the ith attribute of d. The detailed steps involved in the Data Access process be-tween Bob and the cloud for a data record d are given in Algorithm 2.

4) User Revocation - Alice revokes Bob's access to data record d by simply instructing the cloud to remove the authorization token T_b^d corresponding to E_{pka} (d). Here, we assume that the cloud acts as a semi-honest party (honest but-curious); which follows the rules of the protocol but is free to later use the intermediate re-sults it sees to compromise the security. However, since the data is in encrypted form and the encryption scheme is probabilisitic, the intermediate results computed by the cloud are random values uniformly distributed in Z_N .

5) User Rejoin - Let Bob be the user who was revoked earlier

Algorithm 2 Data_Access(d)

Require: Bob sends a data request to the cloud (Note: the private key pr_b is only known to Alice and Bob.)

```
{Steps 1 - 10 performed by the cloud}
  1: Receive data request from Bob
  2: if No entry for Bob in $T^d$ then
  3:   Abort
  4: else
  5:   for i := 1 to n + m do
  6:     $E_{pkb}(d_i) \leftarrow$ PRE.ReEnc($E_{pka}(d_i)$, $rk_{pka \to pkb}$ )
  7:     $E_{pkb}(d_i + \alpha_i) \leftarrow E_{pkb}(d_i) +_h E_{pkb}(\alpha_i) \bmod N^2$
  8:   end for
  9:   Sends $E_{pkb}(d_i + \alpha_i)$ to Bob, for $1 \le i \le n + m$
  10: end if
{Steps 11 - 14 performed by Bob}
  11: if Bob is authorized to access d then
  12:   Receive data from the cloud
  13:   $d_i + \alpha_i \leftarrow D_{prb}(E_{pkb}(d_i + \alpha_i))$, for $1 \le i \le n + m$
  14: end if
```

by Alice on a data record d .

2) **Proxy Re-Encryption** Proxy re-encryption (PRE) allows a semi-trusted interme-diary, called an oracle, to re-encrypt data for delivery to a specific user without requiring the data to be decrypted and re-encrypted. Furthermore, a key pair can be generated to allow the encrypted data to be delivered in a re-encrypted form such that the end user, we will call Bob, can decrypt the data while the oracle cannot. More formally, we define it as follows:

Definition 1. Let x be the data owned by Alice with public key pk_a . Without loss of generality, assume that T (the oracle) knows the proxy re-encryption key denoted as $rk_{pka \to pkb}$, where pk_b is the Bob's public key. If Alice computes E_{pka} (x) and hands it to , then T re-encrypts it for Bob:

$$\text{PRE.ReEnc}(E_{pka}(x), rk_{pka \to pkb}) \to E_{pkb}(x) \qquad (1)$$

where PRE.ReEnc() is the proxy re-encyrption function. After this,
T sends the output E_{pkb} (x) to Bob who can decrypt it to retreive x using his private key pr_b.

The observation is that T can first operate on the encrypted data sent by Alice, i.e., E_{pka} (x), using additive homomorphic proper-ties and applies the PRE scheme on the updated data. Therefore, the combination of additive homomorphic properties with the PRE scheme will benifit the data owners to shift the work load to T (i.e., the cloud who is computationally unbounded) and will provide a medium for T to operate on the encrypted data.

In this system there are two actors one is Admin and another is User, Admin has to provide the sensitive data training set to the system. Data user can able to register and login with the registration credentials. Once data user logged in he can able to upload and download the file as he wish. Fig.1 shows this process clearly.

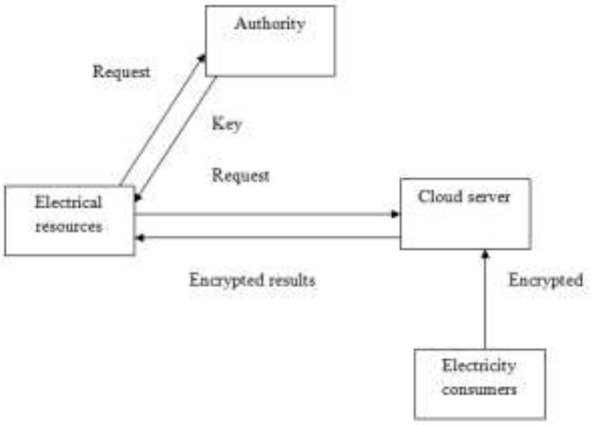


Fig 1: System Architecture

When the data user request the data, The following process are take place

- System Model
- System initialization
- Proxy encryption
- Proxy re-encryption
- Secure data sharing

The first process focus on how the electricity consumption reports are securely shared among the distributed generation resources. In particular, advantages of the data-as-a-service (DaaS) model in cloud computing is taken, where the system is composed of the following parties: the trusted authority (TA), many electricity consumers (ECs), many energy resources (Ers) and the cloud server. The TA is responsible for generating the system parameters and the certificate for the public key of each ER. The Ecs produce the electricity consumption reports that are outsourced to the cloud server. To achieve the confidentiality, the electricity consumption reports should be encrypted by using the public key of the corresponding ER where the consumed electricity comes from. In order to make a smart decision on the power generation, price and others, each ER would like to do analysis on the electricity consumption reports corresponding to itself or other Ers. Before doing the analysis, the ER should obtain the analysis rights from other Ers.

Second process describes about TA generates the system parameters, including the security parameter λ, the ER generates its own public/private key pair (pk; sk) by running PRE:KeyGen(λ), and the public key pk is implemented in the device of the EC who will consume the electricity generated by the ER. Furthermore, each ER should obtain the certificate cert for its public key from the TA.

Proxy encryption concentrates about before uploading the electricity consumption reports to the cloud server, the consumer encrypts the electricity consumption reports m by running PRE:Enc (pk;m) → c, where pk is the public key of the corresponding ER. The encrypted reports are stored on the cloud server, where ID contains the necessary information to identify the reports, such as address and the ER's identity information.

Proxy re-encryption is a special kind of public key encryption, which allows a semi-trusted proxy with some information to transform a ciphertext under one public key into another ciphertext under another public key. However, the corresponding message cannot be revealed during the transformation process. A concrete proxy re-encryption scheme is composed of the following five algorithms.

Secure data sharing process describes about The decryption algorithm is a deterministic algorithm that takes the private key sk and a ciphertext c as input, and outputs the corresponding message m. Cloud server shares reports with ER in secure manner.

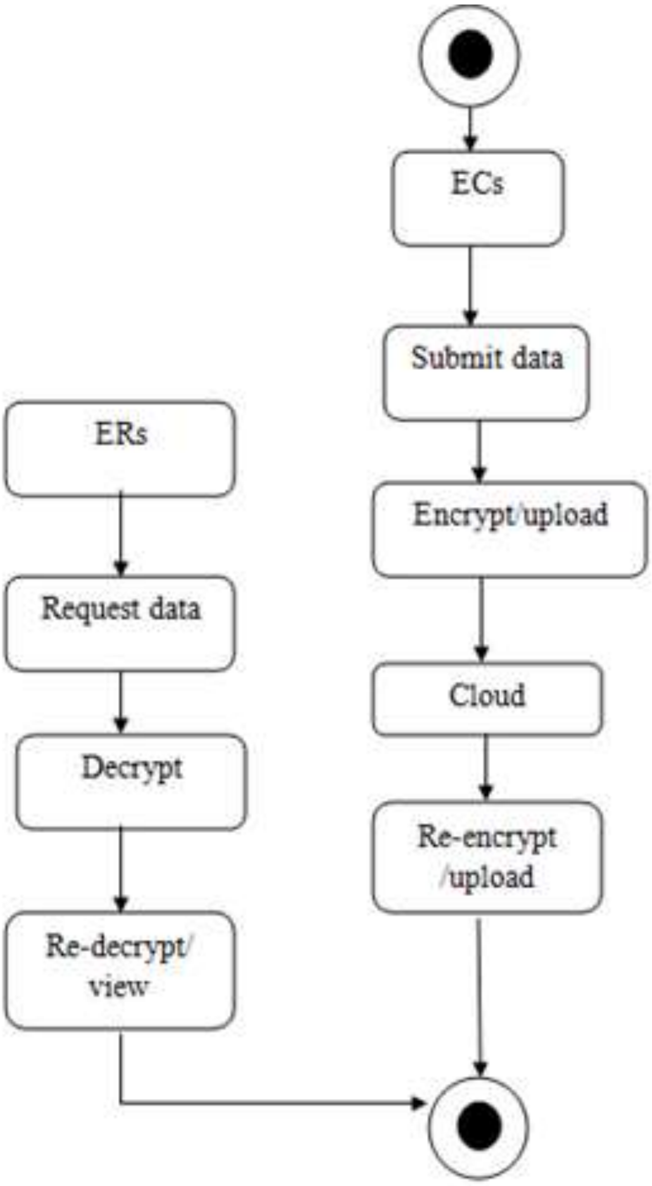
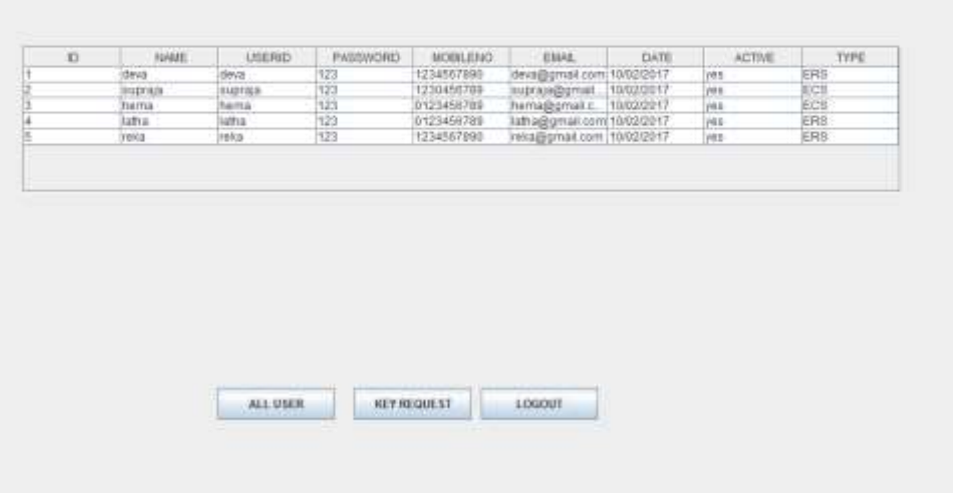


Fig 2: Activity Diagram for process

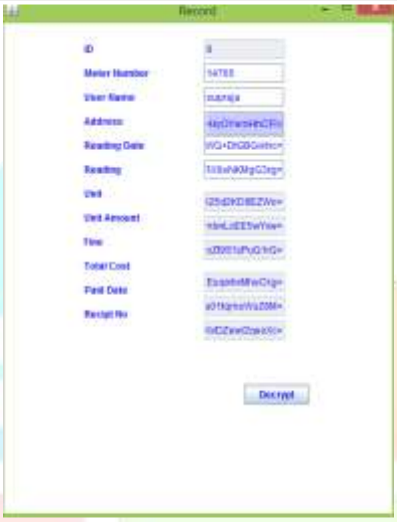
IV Performance evaluation

In this section, we evaluate the computation and observation of the proposed framework

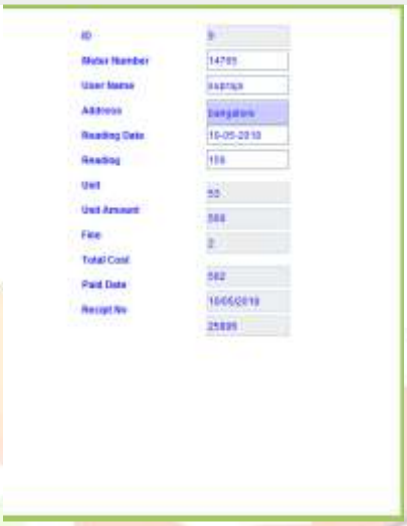
The user should enroll to the authority login where all the records of the enrolled users are recorded and the users are provided with the unique key using which the users can get the information about the electricity usage bills which will be in the encrypted form and it is decrypted using the unique provided to the individual user



ID	NAME	USERID	PASSWORD	MOBILENO	EMAIL	DATE	ACTIVE	TYPE
1	deva	deva	123	1234567890	deva@gmail.com	10/02/2017	yes	ERS
2	supraja	supraja	123	1230456789	supraja@gmail....	10/02/2017	yes	ECS
3	hema	hema	123	0123456789	hema@gmail.c...	10/02/2017	yes	ECS
4	latha	latha	123	0123456789	latha@gmail.com	10/02/2017	yes	ERS
5	reka	reka	123	1234567890	reka@gmail.com	10/02/2017	yes	ERS



ID: 9
Meter Number: 14785
User Name: supraja
Address: 4kyDhwrbHnCFIo
Reading Date: WQ+DtGBGxthc=
Reading: 1i1IsNKMgG3rg=
Unit: I25dDKD8EZWo=
Unit Amount: nbnLzEESwYw=
Fine: sZ8051sPuQ1rG=
Total Cost: EsqshMwCrg=
Paid Date: a01KpmsWsZ0M=
Recipt No: 0dDZewDzak9c=



ID: 9
Meter Number: 14785
User Name: supraja
Address: bangalore
Reading Date: 10-05-2018
Reading: 158
Unit: 55
Unit Amount: 588
Fine: 2
Total Cost: 582
Paid Date: 10/05/2018
Recipt No: 25895

By providing this unique the generated bill is secured and the data in the smart grid is secured by the fully homomorphic encryption and evaluation algorithm. In the future work the enhancement of the security efficiency can be included.

V Conclusion

In this paper, we have proposed a data sharing framework for the smart grid. The proposed framework mainly studies how to keep the smart grid still smart in the sense that electricity consumption reports can be analyzed by the distributed energy resources, while the consumer's privacy in the reports can still be protected. To the best of our knowledge, the proposed framework is the first attempt to consider the above problem, and a possible solution has been given by using a combination of homomorphic encryption and proxy re-encryption technique.

REFERENCES

[1] M. Jacobs, "13 of the Largest Power Outages in History and What They Tell Us About the 2 003 Northeast Blackout," Available at: http://blog.ucsusa.org/2003-northeast-blackout-and-13-of-thelargest- power-outages-in-history-199, 2013.
[2] D. Bobkoff, "10 Years After The Blackout, How Has The Power GridChanged?," Available at: http://www.npr.org/2013/08/14/210620446/10- years-after-the-blackout-how-has-the-power-grid-changed, 2013.
[3] K. Alfaheid, "Secure and compromise-resilient architecture for advanced metering infrastructure," MASc Thesis, University of Ontario Institute of Technology, 2011.
[4] R. Deng, J. Chen, X. Cao, Y. Zhang, S. Maharjan, and S. Gjessing, "Sensing-performance tradeoff in cognitive radio enabled smart grid," IEEE Trans. Smart Grid, vol. 4, no. 1, p. 302-310, 2013.
[5] H. Liang, B. Choi, W. Zhuang, and X. Shen, "Towards optimal energy store-carry-and-deliver for phevs via v2g system," in Proc. IEEE International Conference on Computer Communications (INFOCOM), 2012, p. 1674-1682.
[6] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: An efficient and privacy preserving aggregation scheme for secure smart grid communications," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 9, p. 1621-1631, 2012.
[7] X. Li, X. Liang, R. Lu, X. Lin, H. Zhu, and X. Shen, "Securing smart grid: Cyber attacks, countermeasures and challenges," IEEE Commun. Mag., vol. 58, no. 8, p. 38-45, 2012.
[8] F. Tao, Y. Cheng, D. Xu, L. Zhang, and B. Li. CCIoT-CMfg: cloud computing and internet of things-based cloud manufacturing service system. IEEE Transactions on Industrial Informatics, 10(2):1435–1442, 2014.
[9] G. Wu, H. Zhang, M. Qiu, Z. Ming, J. Li, and X. Qin. A decentralized approach for mining event correlations in distributed system monitoring. Journal of parallel and Distributed Computing, 73(3):330–340, 2013.
[10] F. Li, B. Luo, and P. Liu, ''Secure Information Aggregation for Smart Grids using Homomorphic Encryption,'' in Proc. IEEE Int. Conf. SmartGridComm, 2010, pp. 327-332.
[11] E. D. Knapp and R. Samani, *Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure*. Waltham, MA: Syngress, 2013.

[12] A. Ipakchi and F. Albuyeh, "Grid of the future," *Power and Energy Magazine, IEEE*, vol. 7, no. 2, pp. 52–62, 2009.
[13] Z. M. Fadlullah, M. M. Fouda, N. Kato, A. Takeuchi, N. Iwasaki, and Y. Nozaki, "Toward intelligent machine-to-machine communications in smart grid," *Communications Magazine, IEEE*, vol. 49, no. 4, pp. 60– 65, 2011.
[14] E. L. Quinn, "Smart metering and privacy: Existing laws and competing policies," *Report for the Colorado Public Utilities Commision*, 2009.
[15] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *Proceedings of the 1st International conference on Smart Grid Communications*. IEEE, Oct. 2010.
[16] F. D. Garcia and B. Jacobs, "Privacy-friendly energy-metering via homomorphic encryption," in *Proceedings of the 6th International Workshop on Security and Trust Management*. Springer Berlin Heidelberg, Sep. 2010.
[17] G. Acs and C. Castelluccia, "I have a DREAM! (differentially private smart metering)," in *Proceedings of the 13th International Conference on Information Hiding*. Springer Berlin Heidelberg, May 2011.
[18] E. Shi, T.-H. H. Chan, E. G. Rieffel, R. Chow, and D. Song, "Privacypreserving aggregation of time-series data," in *Proceedings of 18th Annual Network and Distributed System Security Symposium*, Feb. 2011.
[19] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 23, no. 9, pp. 1621–1631, 2012.
[20] Z. Erkin and G. Tsudik, "Private computation of spatial and temporal power consumption with smart meters," in *Proceedings of the 10th International Conference on Applied Cryptography and Network Security*. Springer Berlin Heidelberg, June 2012.
[21] S. Yu,W. Zhou, R. Doss, andW. Jia. Traceback of DDoS attacks using entropy variations. IEEE Transactions on Parallel and Distributed Systems, 22(3):412–425, 2011.
[22] Y. Li, W. Dai, Z. Ming, and M. Qiu. Privacy protection for preventing data over-collection in smart city. IEEE Transactions on Computers, 65:1339–1350, 2015.
[23] S. Yu,W. Zhou,W. Jia, S. Guo, Y. Xiang, and F. Tang. Discriminating DDoS attacks from flash crowds using flow correlation coefficient. IEEE Transactions on Parallel and Distributed Systems, 23(6):1073–1080, 2012.
[24] Y. Yu, M. Au, G. Ateniese, X. Huang, W. Susilo, Y. Dai, and G. Min. Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage. IEEE Transactions on Information Forensics and Security, PP(99):1, 2016.
[25] L. Weng, L. Amsaleg, A. Morton, and S. Marchand-Maillet. A privacy-preserving framework for large-scale content-based information retrieval. IEEE Transactions on Information Forensics and Security, 10(1):152–167, 2015.
[26] K. Gai, M. Qiu, H. Zhao, and J. Xiong. Privacy-aware adaptive data encryption strategy of big data in cloud computing. In The 2nd IEEE International Conference of Scalable and Smart Cloud (SSC 2016), pages 273–278, Beijing, China, 2016. IEEE.
[27] Y. Zhang, C. Xu, S. Yu, H. Li, and X. Zhang. SCLPV: Secure certificateless public verification for cloud-based cyber-physical social systems against malicious auditors. IEEE Transactions on Computational Social Systems, 2(4):159–170, 2015.
[28] C. Wang, S. Chow, Q. Wang, K. Ren, and W. Lou. Privacy-preserving public auditing for secure cloud storage. IEEE Transactions on Computers, 62(2):362–375, 2013.
[29] K. Gai, L. Qiu, M. Chen, H. Zhao, and M. Qiu. SA-EAST: security aware efficient data transmission for ITS in mobile heterogeneous cloud computing. ACM Transactions on Embedded Computing Systems, 16(2):60, 2017.
[30] C. Lai, M. Chen, M. Qiu, A. Vasilakos, and J. Park. A RF4CEbased remote controller with interactive graphical user interface applied to home automation system. ACM Transactions on Embedded Computing Systems, 12(2):30, 2013.
[31] S. Backhaus, R. Bent, J. Bono, R. Lee, B. Tracey, D. Wolpert, D. Xie, and Y. Yildiz. Cyber-physical security: A game theory model of humans interacting over control systems. IEEE Transactions on Smart Grid, 4(4):2320–2327, 2013.
[32] K. Gai, M. Qiu, H. Zhao, and W. Dai. Privacy-preserving adaptive multi-channel communications under timing constraints. In The IEEE International Conference on Smart Cloud 2016, page 1, New York, USA, 2016. IEEE.