IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 3, May 2014.
www.ijiset.com
ISSN 2348 – 7968

A Hidden Vector Encryption Using Query Tokens in Cloud Computing

H.PRABHA[1], C.MENAGA[2]

[1] Assistant Professor, Computer science and Engineering , NPR College of Engineering and Technology Tamilnadu, India.

[2] PG Student, Computer science and Engineering , NPR College of Engineering and Technology Tamilnadu, India.

Abstract

Smart grid has emerged as a new concept and a promising solution for intelligent electricity generation, transmission, distribution and control by two-way communications. To prevent the private and sensitive information in the metering data from disclosure, data confidentiality and privacy should be achieved in financial audit for smart grid. A novel privacy-preserving range query (PaRQ) scheme over encrypted metering data to address the privacy issues in financial auditing for smart grid. A PaRQ allows a residential user to store metering data on a cloud server in an encrypted form. A PaRQ constructs a Elgammal algorithm for encrypting the data. The PaRQ constructs a hidden vector encryption based range query predicate to encrypt the searchable attributes and session keys of the encrypted data.

Keywords: *Hidden vector, Range Query, smart grid.*

1. Introduction

SMART grid has emerged as a new concept and a promising solution for intelligent electricity generation, transmission, distribution and control the use of robust two way communications and distributed computing technology improves the efficiency and reliability of power delivery and usage [2]. Currently, many utility companies begin to use smart grid information systems to collect real-time metering data at their control centers, via a reliable communication network deployed in parallel to the power transmission and distribution grid. In the smart grid information system, smart meters are deployed at residential users' premises as two-way communication devices, which periodically record the power consumption and report. This paper describes novel Private Stream Aggregation (PSA) algorithms which allow users to upload a stream of encrypted data to an untrusted aggregator, and allow the aggregator to decrypt (approximate) aggregate statistics for each time interval with an appropriate capability. We guarantee a strong notion of privacy. First, our aggregation scheme is aggregator oblivious, meaning that the aggregator is unable to learn any unintended information other than what it can deduce from its auxiliary knowledge and the desired statistics. Second, we guarantee distributed differential privacy for each individual participant, in the sense that the statistic revealed to the aggregator will not be swayed too much by whether or not a specific individual participates. Therefore, users may safely contribute their encrypted data, as presence in the system will not lead to increased risk of privacy breach. Our privacy guarantees hold even when the aggregator has arbitrary auxiliary information about an individual's inputs (but has not compromised her secret key). Such auxiliary information may be obtained from publicly available datasets, personal knowledge about an individual participant, or through collusion with a small subset of corrupted participants. The proposed privacy mechanisms represent a promising approach to ensuring user privacy in numerous applications, including cloud services, medical privacy, sensor network aggregation, and smart metering.

2. Related Works

In [1] Mi Wen Smart grid, envisioned as an indispensable power infrastructure, is featured by real-time and two-way communications. However, how to securely retrieve and audit the communicated metering data for validation testing is still challenging for smart grid. In this paper, we propose a novel privacy-preserving range query scheme over encrypted metering data, named PaRQ, to address the privacy issues in financial auditing for smart grid. Our PaRQ allows a residential user to store metering data on a cloud server in an encrypted form. When financial auditing is needed, an authorized requester can send its range query tokens to the cloud server to retrieve the metering data. Specifically, the PaRQ constructs a hidden vector encryption (HVE) based range query predicate to encrypt the searchable attributes and session keys of the encrypted data. Meanwhile, the requester's range query can be transferred into two query tokens, which are used to find the matched query results. Security analysis

ISSN 2348 – 7968

demonstrates that in the PaRQ, only the authorized requesters can obtain the query results, while the data confidentiality and query privacy are also preserved. The simulation results show that our PaRQ can significantly reduce communication and computation costs.

In [2] Elaine Shi et al. We consider how an untrusted data aggregator can learn desired statistics over multiple participants' data, without compromising each individual's privacy. We propose a construction that allows a group of participants to periodically upload encrypted values to a data aggregator, such that the aggregator is able to compute the sum of all participants' values in every time period, but is unable to learn anything else. We achieve strong privacy guarantees using two main techniques. First, we show how to utilize applied cryptographic techniques to allow the aggregator to decrypt the sum from multiple cipher texts encrypted under different user keys. Second, we describe a distributed data randomization procedure that guarantees the differential privacy of the outcome statistic, even when a subset of participants might be compromised.

In [3] Alexandra Boldyreva et al**.** we show that, for a database of randomly distributed plaintexts and appropriate choice of parameters, ROPF encryption leaks neither the precise value of any plaintext nor the precise distance between any two of them. The analysis here introduces useful new techniques. On the other hand, we show that ROPF encryption leaks approximate value of any plaintext as well as approximate distance between any two plaintexts, each to an accuracy of about square root of the domain size. We then study schemes that are not order-preserving, but which nevertheless allow e_cient range queries and achieve security notions stronger than POPF. In a setting where the entire database is known in advance of key-generation (considered in several prior works), we show that recent constructions of monotone minimal perfect hash functions" allow to efficiently achieve (an adaptation of) the notion of IND-O(ordered) CPA also considered by Boldyreva et al., which asks that only the order relations among the plaintexts is leaked. Finally, we introduce modular order-preserving encryption (MOPE), in which the scheme of Boldyreva et al. is prepended with a random shift cipher. MOPE improves the security of OPE in a sense, as it does not leak any information about plaintext location. We clarify that our work should not be interpreted as saying the original scheme of Boldyreva et al., or the variants that we introduce, are secure or insecure." Rather, the goal of this line of research is to help practitioners decide whether the options provide a suitable security-functionality trade for a given application.

In [4] Xiaohui Liang et al. smart sensing and wireless communication technologies enable the electric power grid system to deliver electricity more efficiently through the dynamic analysis of the electricity demand and supply. The current solution is to extend the traditional static electricity pricing strategy to a time-based one where peak-time prices are defined to influence electricity usage behavior of customers. However, the time-based pricing strategy is not truly dynamic and the electricity resource cannot be optimally utilized in real time. In this paper, we propose a usage-based dynamic pricing (UDP) scheme for smart grid in a community environment, which enables the electricity price to correspond to the electricity usage in real time. In the UDP scheme, to simplify price management and reduce communication overhead, we introduce distributed community gateways as proxies of the utility company to timely respond to the price enquiries from the community customers. We consider both community-wide electricity usage and individual electricity usage as factors into price management: a customer gets higher electricity unit price if its own electricity usage becomes larger under certain conditions of the community-wide collective electricity usage. Additionally, we protect the privacy of the customers by restricting the disclosure of the individual electricity usage to the community gateways. Lastly, we provide privacy and performance analysis to demonstrate that the UDP scheme supports real-time dynamic pricing in an efficient and privacy-preserving manner.

In [5] N. Ansari et al. The objectives and requirements of cyber security in the Smart Grid, with a focus on identifying fundamental differences between the Smart Grid and another large scale network paradigm, the Internet. Since cyber attacks mainly come from malicious threats in communication networks review cyber attacks in electric power systems and provide an extensive analysis of network vulnerabilities under important use cases in the Smart Grid. To efficiently counteract cyber attacks, it is essential to widely deploy attack prevention and defense strategies throughout the Smart Grid. Therefore, we conduct an evaluation of the existing solutions, including network and cryptographic countermeasures, by considering case studies and applications in the Smart Grid.

The Proposed system is a comprehensive survey of security issues in the Smart Grid. The communication architecture and security requirements, analyzed security vulnerabilities through case studies, and discussed attack prevention and defense approaches in the Smart Grid. Also summarized the design of secure network protocols to achieve efficient and secure information delivery in the Smart Grid cyber security is still under development in

ISSN 2348 – 7968

the Smart Grid, especially because information security must be taken into account with electrical power systems.

3. Existing System

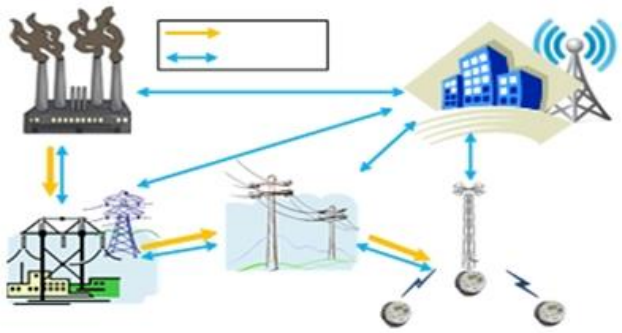


Fig 1: System Architecture

The use of robust two way communications and distributed computing technology improves the efficiency and reliability of power delivery and usage currently, many utility companies begin to use smart grid information systems to collect real-time metering data at their control centers, via a reliable communication network deployed in parallel to the power transmission and distribution grid. In the smart grid information system, smart meters are deployed at residential users' premises as two-way communication devices which periodically record the power consumption and report access point (AP). The gateway then collects and forwards data to a control center. Additionally, metering data in smart grid information systems should be periodically audited to ensure that the billing and pricing statements are presented fairly. Specifically, requesters, such as market analysts, are endowed with the task of querying smart grid information systems for auditing, analysis, accounting or tax-related activities. Thus, to prevent the private and sensitive information in the metering data from disclosure, data confidentiality and privacy should be achieved in financial audit for smart grid. However, the metering data in smart grid are surging from 10,780 terabytes (TB) in 2010 to over 75,200 TB in 2015 which is far beyond the control center's data management capability.

Outsourcing data to cloud servers is a promising approach to relieve the control center from the burden of such a large amount of data storage and maintenance. In this approach, users can store their data on cloud servers and execute computation and queries using the servers' computational capabilities Nevertheless, cloud servers might be untrusted, and intentionally share sensitive data with the third parties for commercial purposes. Therefore, data confidentiality is important in financial audit for smart grid. In addition, privacy concerns raise in financial auditing. For instance, utility usage patterns within short intervals may reveal the users' regular daily activities. In particular, data from a single house would reveal the activities of the residents when the individual resident is at home, when he/she is watching TV. If an attacker can query these data, data privacy might be violated. Therefore, users' data confidentiality and privacy should be protected and only authorized requesters can query the metering data. From the requester's perspective, the requester, who manages the data query for financial auditing, needs to frequently query the metering data by using date ranges and/or geographic regions etc. If the query is sensitive, the requesters may prefer to keep their queries from being exposed to servers. As a result, how to operate such range queries with guaranteed query privacy is also significant for smart grid. In this paper, we propose a Privacy-preserving Range Query(PaRQ) scheme over encrypted metering data for smart grid. The PaRQ addresses the data confidentiality and privacy problem by introducing an HVE technique. The main contributions of this paper are twofold.

Firstly, we construct a range query predicate based on the HVE. Specifically, the session keys and the searchable attributes of the encrypted data are hidden in the HVE based range query predicate. When a requester query the cloud server, the session keys, whose encryption vectors are satisfied with the range query vectors, are released to the requester, for decrypting the encrypted metering data. Secondly, we analyze the security strengths and evaluate the performance of the PaRQ. Security analysis demonstrates that the PaRQ can achieve user's data confidentiality and privacy, as well as requester's query privacy. Performance evaluation results show that our PaRQ can reduce the communication and computation overhead, and shorten the response time.

5. PROPOSED SYSTEM

• Data Confidentiality:

The residential user can utilize symmetric or asymmetric cryptography to encrypt the data before outsourcing, and successfully prevent the unauthorized entities, including eavesdroppers and cloud servers, from prying into the outsourced data.

• Data privacy:

Individual residential users' data should not be accessed by unauthorized requesters. It means that only requesters with authorized query tokens can access the *CS*2, and they

can obtain the correct session keys when their query vectors in the tokens are satisfied with the encryption vectors. Thus, only the authorized requester can decrypt the encrypted
Metering data.

• Query privacy:
As requesters usually prefer to keep their queries from being exposed to others, thus, the biggest concern is to hide their queries into tokens to protect the query privacy. Otherwise, if the query includes some sensitive information, such as "5 ≤ *priority* ≤ 7", then the *CS*2 could know the requester is querying some important users' metering data. Then, the requester or the query results could be traced or analyzed by the curious server *CS*2.

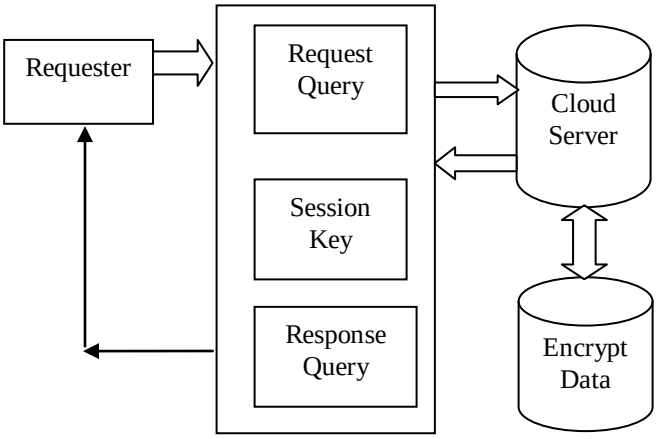


Fig 2:General Format

HVE based query predicate
HVE mainly consists of four phases: key generation, data encryption, token generation and data query.
Equality Query*:*
• In key generation phase, the TA distributes the public/private key pair (*PK; SK*) to a receiver.
• In data encryption phase, a user chooses a vector **x**=(*x*1… *xl*) ∈ Σ*l* to characterize its data and encrypts its data *m* into a cipher text CT using the receiver's public key.
• In token generation phase, the receiver chooses a vector **w** = (*w*1.....*wl*) ∈ (Σ∗)*l* to represent his query requirements and generate a query token *Tw*. The receiver sends *Tw* to the server.
• In data query phase, if **x** equals to **w**, the token can
Decrypt a cipher text by using the receiver's private keys. The matching condition is defined as following: let *s*(*w*) be the set of indexes *i* such that *wi* is not a wildcard in the vector **w** = (*w*1....*wl*).

HVE-based Session Key Encryption:
If each data has *l* searchable attributes, *Ui* chooses a vector **x***i* = (*xi*1…. *xil*)∈ Σ*l* to characterize its data *mi* in different dimensions. To encrypt *ksi* by using the CC's *PK* and the vector **x***i*, *Ui* divides each *ksi* into two parts: *ksi*L and *ksi*R. Then, *ksi*L is encrypted by using the encryption vector _≥(**x***i*); *ksi*R is
encrypted by using the encryption vector _≤(**x***i*). Thus, the *CS*2 can recover *ksi* only when both encryption vectors are satisfied with the corresponding query vectors in the range
query tokens. The HVE-based session key encryption details are as follows:
1) Firstly, *Ui* maps **x***i* to an encryption vector _≥(**x***i*) as Eq.
(2). Then, *Ui* selects two random numbers *ri*1*; ri*2 ∈ *Zp* and computes tags for the ciphertext *ksi*L by using the encryption vector _≥(**x***i*) as:C*i*
C*i* $_{L1}$ = *Y ri*1
C*i* $_{L2}$ = *Y ri*1
C$i_{L3,1}$ = (*h*1*uσ*≥(*xi*1)^{ri1}*V ri*2
Ci_{L3},*nl* = (*hnluσ*≥(*xinl*)*nl*)*ri*1*V ri*2
C*i*L4,1 = *ri*11 *Tri*2
C*i*L4,*nl* = *ri*1
C*i*L5 = *gri*2 *;*
C*i*L6 = Γ*ri*1*ksi*L*:*
Let CT*i*L = (C*i*L1*;*C*i*L2*;*C*i*L3,C*i*L4*;*C*i*L5*;*C*i*L6).
2) Secondly, *Ui* maps **x***i* to an encryption vector _≤(**x***i*) as Then, *Ui* selects two random numbers *r′*
*i*1*; r′i*2∈*Zp*, and computes tags for the ciphertext *ksi*R by using the encryption vector _≤(**x***i*):
C*i*R1 = *Y ri*1
C*i*R2 = *Y ri*1
C*i*R3,1 = (*h*1*uσ*≤(*xi*1)1)*ri*1*V ri*2
C*i*R3,*nl* = (*hnluσ*≤(*xinl*)*nl*)*ri*1*V ri*2
C*i*R4,1 == *ri*11 *Tri*2
C*i*R4,*nl* = *rinl Tr;*
C*i*R5 = *gri*2 *;*C*i*
R6 = Γ*ri*1*ksi*R*:*
Let CT*i*R = (C*i*R1*;*C*i*R2*;*C*i*R3,1*;* CR4,1;R5*;*C*i*R6).
Ciphertext Deposit: Ui deposits CT*i*L and CT*i*R to theCC as:

Ui → *CC* : *{*CT*i*L*;* CT*i*R*; t*2*}:*

The CC also adds the index *Indi* to the key ciphertext and transmits all of them to the *CS*2.

CC → *CS*2 : *{*CT*i*L*;*CT*i*R*; t*2*; Indi}*

Data Encryption:
We denote each data as *mi*. When *Ui* wants to report *mi* to the cloud server *CS*1, *Ui* randomly generates a session

key *ksi*. Then *Ui* encrypts its data into a cipher text CT*i*, where CT*i* = Enc*ksi* (*mi*). Enc(·) is a
Asymmetric encryption algorithm, e.g., ELGAMMAL
For each uploading interval

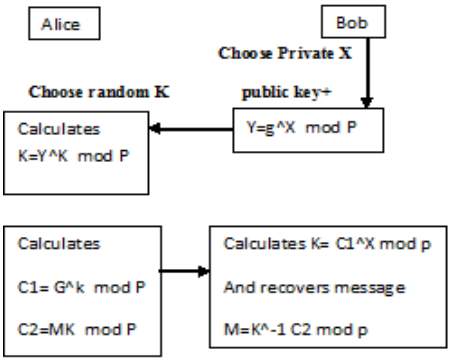
$$Ui \rightarrow CC : \{Ci; t1\}$$

"$A \rightarrow B : \{C\}$" means " A sends C to B". Then, the CC adds a unique index *Indi* to the data cipher text and transmits all of them to the *CS*1.

$$CC \rightarrow CS1 : \{Ci; t1; Indi\}$$

Elgammal=diffie Hellman key exchange+ encryption by multiplying mod p

Prime p and generator g are public key of bob



The elgammal encryption algorithm is more secure because it produces more than one cipher text for single plain text.

6. REFERENCES

[1] PaRQ: A Privacy-preserving Range Query Scheme over Encrypted Metering Data for Smart Grid Mi Wen, Member, IEEE, Rongxing Lu, Member, IEEE, Kuan Zhang, Jingsheng Lei, Xiaohui Liang, Student Member, IEEE, and Xuemin (Sherman) Shen, Fellow, IEEE.

[2] C. Lo and N. Ansari, "The progressive smart grid system from both power and communications aspects," IEEE Communications Surveys & Tutorials, vol. 14, no. 3, pp. 799–821, 2012.

[3] R. Zeng, Y. Jiang, C. Lin, and X. Shen, "Dependability analysis of control center networks in smart grid using stochastic petri nets," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 9, pp.1721–1730, 2012.

[4] 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 Transactions on Parallel and Distributed Systems,vol. 23, no. 9, pp. 1621–1631, 2012.

[5] C. Lo and N. Ansari, "Alleviating solar energy congestion in the distribution grid via smart metering communications," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 9, pp. 1607–1620, 2012.

[6] The Smart Grid Interoperability Panel-Cyber Security Working Group, "Nistir 7628 guidelines for smart grid cyber security: Smart grid cyber security strategy, architecture, and high-level requirements,"http://csrc.nist.gov/publications/nistir/ir 7628/nistir-7628 vol1.pdf, August 2010.

[7] X. Liang, X. Li, R. Lu, X. Lin, and X. Shen, "UDP: Usage-based dynamic pricing with privacy preservation for smart grid," IEEE Transactions on Smart Grid, vol. 4, no. 1, pp. 141–150, 2013.

[8] R. Yu, Y. Zhang, S. Gjessing, C. Yuen, S. Xie, and M. Guizani, "Cognitive radio based hierarchical communications infrastructure for smart grid," IEEE Network, vol. 25, no. 5, pp. 6–14, 2011.

[9] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proc. The IEEE International Conference on Computer Communications (INFOCOM'10), 2010, pp. 1–9.

[10] P. Sakarindr and N. Ansari, "Security services in group communications over wireless infrastructure, mobile ad hoc, and wireless sensor networks," IEEE Wireless Communications, vol. 14, no. 5, pp. 8–20, 2007.