International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 2, February - 2014

Cloud Based Smart Metering Security Access and Monitoring System in the Real Time Environment

Nageshwar Dev yadav
Computer Science And Engineering(Information Security)
Disha institute Of Management And Technology
Raipur, India

Prof. Akash Wanjari
Computer Science And Engineering(Information Security)
Disha institute Of Management And Technology
Raipur, India

Prof. Somesh Dewangan
Computer Science And Engineering(Information Security)
Disha institute Of Management And Technology
Raipur, India

***Abstract*— 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.The present electric power system structure has lasted for decades; it is still partially proprietary, energy inefficient, physically and virtually (or cyber) insecure, as well as prone to power transmission congestion and consequent failures. Recent efforts in building a smart grid system have focused on addressing the problems of global warming effects, rising energy-hungry demands, and risks of peak loads. One of the major goals of the new system is to effectively regulate energy usage by utilizing the backbone of the prospectively deployed Automatic Meter Reading (AMR), Advanced Meter Infrastructure (AMI), and Demand Response (DR) programs via the advanced distribution automation and dynamic pricing models, Cloud Computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance.**

Keywords: Cloud data, privacy, smart grid, encrypted data, metering data, Sensor, Motor, LCD, Micro controller

I. INTRODUCTION

Cloud Computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing data storage, processing and bandwidth.

A simple example of cloud computing is Yahoo email, Gmail, or Hotmail etc. All you need is just an internet connection and you can start sending emails. The server and email management software is all on the cloud (internet) and is totally managed by the cloud service provider Yahoo, Google etc. The consumer gets to use the software alone and enjoy the benefits. The analogy is, 'If you need milk , would you buy a cow ?' All the users or consumers need is to get the benefits of using the software or hardware of the computer like sending emails etc. Just to get this benefit (milk) why should a consumer buy a (cow) software /hardware?

Cloud computing is broken down into three segments: "application" "storage" and "connectivity." Each segment serves a different purpose and offers different products for businesses and individuals around the world. In June 2011, a study conducted by V1 found that 91% of senior IT professionals actually don't know what cloud computing is and two-thirds of senior finance professionals are clear by the concept, highlighting the young nature of the technology. In Sept 2011, an Aberdeen Group study found that disciplined companies achieved on average an 68% increase in their IT expense because cloud computing and only a 10% reduction in data center power costs

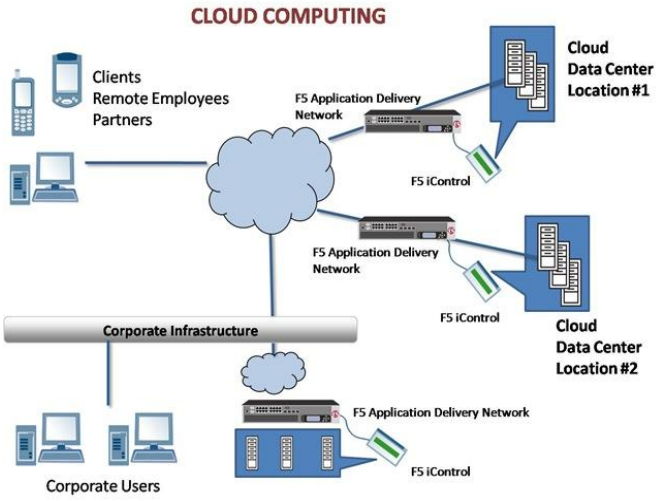

Figure 1. Cloud Computing

II. BACKGROUND AND RELATED WORKS

Proposed a privacy-preserving range query scheme, named PaRQ, for smart grid. An HVE based range query predicate is constructed to realize the range query on encrypted metering data. The PaRQ allows users to store their data on cloud servers in encrypted form, and range queries can be executed by using cloud server's computational capabilities. A requester with authorized query tokens can obtain the correct session keys to retrieve the metering data within specific query ranges. Security analysis demonstrates that the PaRQ can achieve data confidentiality and privacy and preserve query privacy. Performance evaluation shows that the PaRQ can significantly reduce computation and communication overhead, as well as response time.

In Figure-2, 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 their metering data to a local area gateway, e.g., a wireless 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.

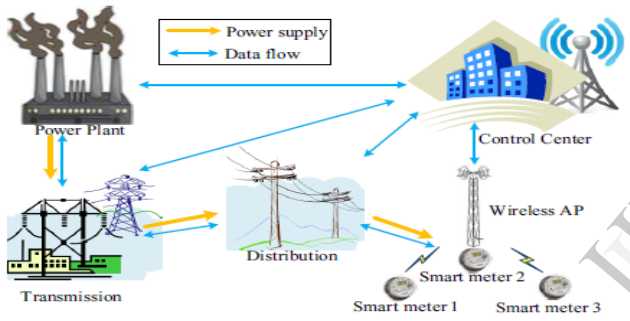

Figure 2. The Conception Smart Grid Architecture

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. Our focus is on how to outsource residential users' metering data to a cloud server in encrypted form and how to operate a range query over the encrypted metering data with the help of the control center (CC). Specifically, we consider a typical residential area, which is composed of a CC, two cloud servers: the CS1 and CS2, a requester S and some residential users U = {U1;U2; :::;Uv}. A residential user is the data owner, who encrypts his data by using a secret session key before outsourcing

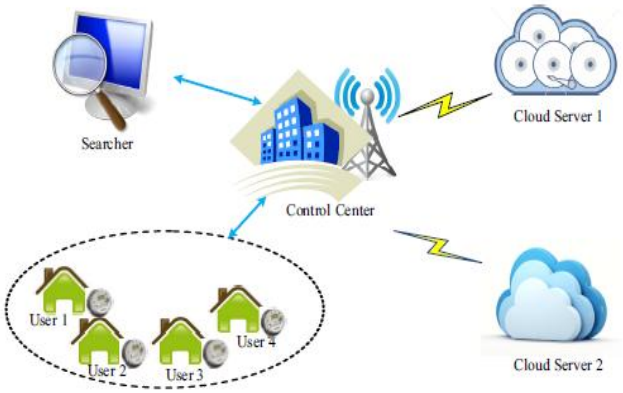

Figure 3. System model of PaRQ

the data to the CSs. There are two cloud servers: Cloud Server 1 (CS1) stores data cipher texts; Cloud Server 2 (CS2) stores session key's cipher texts and indexes. Both servers are semi-trusted, honest but curious. We assume that either the CS1 or CS2 might be compromised and controlled by an adversary seeking to link users' cipher texts with their keys, but the adversary cannot control both CSs. The control center is a trusted proxy (it operates on behalf of the utility companies), which can help users to deposit their data to cloud servers and generate query tokens for requesters to retrieve data from the servers. The requester can query the encrypted data on the cloud servers by depositing his entitling tokens to the CS2. The CC consists of two main components: a cipher text forwarder, and a query translator which always operates within the secure environment. The forwarder on the CC needs to add a unique index to the data cipher texts and the session key's cipher texts. To preserve the query privacy, the requester's query needs to be translated into two tokens, so that the CS2 can evaluate this query without disclosing its real value.Maintaining the Integrity of the Specifications

A. Security and Privacy in Smart Grid

Security and privacy are critical to the development of wireless networks, especially for the real-time data audit strategy in smart grid. The smart grid interpretability panel cyber security working group presents some guidelines for smart grid cyber

security, including security strategy, architecture, and high-level requirements. Reviews the cyber security and privacy issues in smart grid and discusses some security and privacy solutions for smart grid. Lu et al. use a super-increasing sequence to structure multidimensional data and encrypt the structured data by the holomorphic paillier cryptosystem technique. Li et al. propose an authentication scheme based on merkle tree for smart grid. Acs and Castelluccia exploit the privacy-preserving aggregation technique of time-series data in smart meters. They employ a differential privacy model in which users add noise to their electricity metering and the aggregator can successfully obtain the sum of the metering with a very large probability. In summary, few works focus on the query, especially range query over encrypted data in smart grid, which is really significant for user's metering data audit.

B. Range Query

Recently, the problem of querying encrypted data has been deeply investigated in both cryptography and database communities. One of the widely studied approaches is public key encryption with keyword search (PEKS). PEKS can protect users' data privacy and certain query privacy. However, most of PEKS schemes, such as the Searchable Encryption Scheme for Auction (SESA), only can be applied for equality checks. Range query over the encrypted data with numeric attributes is more difficult, and most of the existing literatures cannot achieve data and query privacy simultaneously. Roughly speaking, there are four categories of solutions that have been developed for range queries: order-preserving encryption (OPE), bucketization (Bucket), HVE and special data structure traversal. OPE-based technique is to ensure that the order of plaintext data is preserved in the ciphertext domain. This allows direct translation of range predicate from the original domain to the domain of the ciphertext. However, the coupling distribution of plaintext and ciphertext domains might be exploited by attackers to guess the scope of the corresponding plaintext for a ciphertext. Bucket-based technique uses distributional properties of the datasets to partition and index data for efficient querying while trying to keep the information disclosure to a minimum. Queries are evaluated in an approximate manner where the returned set of records may contain some false positives. In an HVE-based approach, two vectors over attributes are associated with a ciphertext and a token, respectively. Under the predicate translator, the ciphertext matches the token if and only if the two vectors are component-wise equal Several HVE schemes have been proposed in literatures. All of them use bilinear groups equipped with bilinear maps, and each constructs a proper method to hide attributes in an encrypted vector. However, it is expensive to compute exponentiation and pairing in a composite-order group. Jong proposes a new HVE scheme that not only works in prime-order groups, but also requires a shorter token size and fewer pairing computations. However, Jong's scheme cannot be directly applied in the smart grid applications where data are high in dimension, variety or both. Some specialized data structured for range query evaluation are trying to preserve notions of semantic security of the encrypted data, such as B+ tree etc. Recently, Shi et al. propose a searchable encryption scheme that supports multidimensional range queries over encrypted data (MRQED). The MRQED utilizes an interval tree structure to form a hierarchical representation of intervals for each dimension and stores multiple cipher texts corresponding to a single data value on the server, i.e., each one corresponds to a range. If it is applied to a single-dimensional data with values belonging to a domain of size N. The cipher text representation is O(logN) times the actual data. If the MRQED is applied to a piece of data with l dimensions, each query requires l time's complexity to execute.

C. Dependability Analysis Method

There are two types of quantitative dependability analysis methods: combinatorial models and state-space models. Reliability block diagrams fault tree analysis fault mode effect analysis attack tree attack graph and privilege graph are the main representatives of combinatorial models. The easy construction and explicit presentation make the combinatorial methods a good choice for dependability analysis. However, the limitation of capability to model large and complicated networks makes them less competitive than state-space models. State-space models include Markov chain, Markov reward model Markov regenerative process supplementary variable approach, stochastic Petri nets stochastic process algebra etc. Markov chain is the foundation of various state-space methods in dependability analysis. Markov reward process assigns rewards to the transitions of states in CTMC, while Markov regenerative process chooses some regenerative points in CTMC or semi-CTMC to simplify the modelling analysis. Stochastic process algebra uses a process to model the actions of components, making it suitable for modelling resource-sharing systems. As the impressive mathematical tools, SPNs are widely used to the dependability analysis in the recent years. Compared with other dependability analysis methods, SPNs can capture the relationships between actions and states of distributed networks in the simple and concise way, which provides a great advantage over Markov chain and other state-space models. Moreover, various existing results can be applied to SPNs to address the state-space explosion problem faced by all the state-space methods. Thus, we adopt the SPNs model to analyze the dependability of control center networks in smart grid.

1) Electricity Pricing:- To schedule the electricity load, the utility company adopts the conventional direct load control (DLC) strategy where smart switches are installed inside of houses such that the house appliances can be turned off during a high-demand period. The DLC enforces the customers to abandon the control of their appliances at certain conditions. Recently, in Ontario, Canada, a Time-Of-Use (TOU) pricing strategy has been widely adopted by utility companies, e.g., Hydro One Waterloo North Hydro [15]. TOU means that the electricity unit price changes according to the time of the day. The Ontario Energy Board (OEB) divides daily and seasonal TOU periods into three categories: off-peak, midweek, and on-peak. TOU enables the customers to view the electricity usage online and potentially influences electricity usage behaviour of the customers. Though the period settings of TOU can be updated, TOU is neither truly dynamic nor related to the real-time usage. Therefore, TOU may cause some inappropriate situation. For example, in a pre-defined on-peak period, when total electricity usage is in fact low, the oversupplied electricity cannot be economically stored as electrical energy and the customers should be given more incentive to consume more electricity. However, the high on-peak price discourages the electricity consumption of the customers. As a great benefit of smart grid, the dynamic pricing (DP) strategy ensures enough flexibility for the customers (i.e., without setting an upper bound of usage) and is more friendly to meet their demands. In this paper, we propose a new DP strategy by relating the price to the electricity usage in real time, and therefore the high on-peak price issue is avoided.

2) Security and Privacy:- in Smart Grid Security and privacy are critical to the development of real-time DP strategy in

smart grid. As the electricity usage information is frequently exchanged between the customers, the CGs, and the utility companies, to prevent the security attacks and the privacy violations is critical.Khurana summarized security, trust, and privacy issues in a comprehensive smart grid system. They presented the security and privacy challenges of smart grid system design such as transmission substations, policy-based data sharing, and attestation for constrained smart meters. Lu et al. proposed an efficient and privacy-preserving aggregation scheme (EPPA) for smart grid communications. The EPPA uses a super-increasing sequence to construct multi-dimensional data, and encrypts the structured data by the homomorphic Paillier cryptosystem technique. For data communications from the customers to the operation center, data aggregation is performed directly on cipher texts at gateways without decryption, and the aggregation result of the original data can be obtained at the operation center. Acs and Castelluccia exploited the privacy- reserving aggregation technique of time-series data in smart meters. The proposed scheme employs a differential privacy model in which the customers add noise to their electricity usage and the aggregator can successfully obtain the sum of the usage with a very large probability. However, in the smart grid, the sum of the usage of the customers is very critical since it directly influences the electricity price and accordingly the electricity usage behaviour of the customers. Thus, the customer electricity usage needs to be frequently and accurately collected. This requirement imposes a large amount of communication overhead on the customers and the utility company. In this paper, we propose a distributed pricing strategy where the CGs distributed interacts with the local customers and ensure the dynamic price information to be delivered in a timely fashion. We regard the CGs as the proxies of the utility company and explore the privacy issues for this scenario.

3) Crypto-technique:- Homomorphic Encryption encryption provides the addition and multiplication operations over ciphertexts; a user is able to process the plaintext without knowing the secret keys. With this property, homomorphic encryption is widely used in data aggregation and computation specifically for privacy-sensitive content. We review the homomorphic encryption scheme in which serves a building block of our proposed UDP scheme.

III. System Model and Preliminary

A. System Model

We consider the control center networks consisting of one control center and N substation networks, as shown in Fig. 1. In the control center, SCADA servers, database, and application servers are linked with local area networks (LAN), which are protected by the firewalls. If a component in the control center suffers from failure or various attackers, it can be repaired rapidly through user interface. Moreover, backup ervers are used to improve the dependability. The control center in one region also connects with the control centers in other regions through secure wide area networks (WAN). Since the control center is well protected, we assume that it cannot be intruded from other control centers. However, it can be attacked from the substation networks. N substation networks are connected to the control center through dedicated link or frame relay networks. Substation networks are responsible for collecting data from intelligent electronic devices (IEDs). Site engineers can log into the substation networks to restore failed components. Meanwhile, hackers can also intrude into substation networks if they can succeed in passing through the firewalls. These substations networks are connected with unsecure WAN, thus a substation may be at risk when another substation is compromised.

B. Security Requirements

We identify the security requirements for our PaRQ. In our security model, the CC is trustable, and residential users U = {U1;U2; :::;Uv} are honest as well. However, there exists an adversary A in the system intending to eavesdrop and invade the database on cloud servers to steal the individual users' reports. In addition, A can also launch some active attacks to threaten the data privacy and query privacy. Therefore, in order to prevent A from learning the users' data and to detect its malicious actions, the following security requirements should be satisfied in range query applications for smart grid.

• 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 CS2, 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 CS2 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 CS2.

C. Designing Goal

To enable effective range query over encrypted metering data under the aforementioned model, our design goal is to develop a privacy- reserving range query scheme over encrypted data for smart grid, and to achieve the security of the data and efficient range query as follows. The security requirements should be guaranteed in the proposed scheme. As stated above, if the smart grid does not consider the security, the residential users' privacy could be disclosed, and the real-time power metering reports could be steeled. Therefore, the proposed scheme should achieve the data confidentiality and privacy, as well as the query privacy. The performance efficiency should be achieved in the proposed scheme. As range query are operated over encrypted multidimensional data, compared with existing chemes, the proposed PaRQ

scheme should improve the communication, computation and response time.Equations

IV. PROPOSED WORK

In this project we are using the DC motor which can be used to indicate the analogue meters that are being used in the houses and industries today, as the power is consumed the meter will start to rotate and these rotations are read by the sensor as shown in the block diagram above . These data are then fed to the micro controller which will display the number of units consumed and the cost. The units are then fed to the PC using the serial port interface .

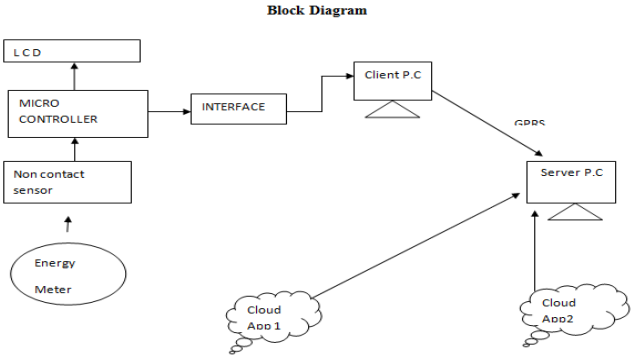

Figure 4. Privacy-Preserving Smart Metering

The client PC will send the data received from the hardware to server machine to encrypt. The server encrypts the data and stores the encrypted key in Google App1 and Google App2. So the security is maintained. Whenever the user requests for the data from cloud, the user has to give the secret keys used at the time of data storage. If correct the user can get to know the required details. The email will be sent to the user whenever he request for the bill.

V. ACKNOWLEDGMENT :

I am very much grateful to Department of CSE, DIMAT to give me opportunity to work on image encryption. I sincerely express my gratitude to Mr. Akash Wanjari of Dept. of MCA, DIMAT for giving constant inspiration to complete this work. I am also thankful to Mrs. Preeti Tuli, Prof. Somesh Dewangan, Dept. of CSE, DIMAT for helping me directly and indirectly during this work. I am really thankful to my all friends for their blessing and support.

VI. REFERENCES

[1] 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.
[2] 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.
[3] 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.
[4] 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.
[5] "Decentralized controls and communications for autonomous distribution networks in smart grid," IEEE Transactions on Parallel and Distributed Systems, vol. 4, no. 1, pp. 66–77, 2013.
[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 highlevel requirements," http://csrc.nist.gov/publications/nistir/ir7628/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.
[11] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu, "Securing smart grid: cyber attacks, countermeasures, and challenges," IEEE Communications Magazine, vol. 50, no. 8, pp. 38–45, 2012.
[12] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, "An efficient merkle tree based authentication scheme for smart grid," IEEE Systems Journal, to appear.
[13] G. Acs and C. Castelluccia, "I have a dream!(differentially private smart metering)," in Proc. the 13th international conference on Information hiding. Springer, 2011, pp. 118–132.
[14] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. Advances in Cryptology (Eurocrypt'04), 2004, pp. 506–522.
[15] M. Wen, R. Lu, J. Lei, H. Li, X. Liang, and X. Shen, "SESA: An efficient searchable encryption scheme for auction in emerging smart grid marketing," Security and Communication Networks, to appear.
[16] A. Boldyreva, N. Chenette, and A. O'Neill, "Order-preserving encryption revisited: Improved security analysis and alternative solutions," in Proc. Advances in Cryptology (CRYPTO'11). Springer, 2011, pp. 578– 595.
[17] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in Proc. ACM international conference on Management of data (SIGMOD'04), 2004, pp. 563–574.
[18] B. Hore, S. Mehrotra, M. Canim, and M. Kantarcioglu, "Secure multidimensional range queries over outsourced data," The VLDB Journal, vol. 21, no. 3, pp. 333–358, 2012.
[19] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Proc. Theory of Cryptography Conference (TCC'07), 2007, pp. 535–554.
[20] J. Park, "Efficient hidden vector encryption for conjunctive queries on encrypted data," IEEE Transactions on Knowledge and Data Engineering, vol. 23, no. 10, pp. 1483–1497, 2011.
[21] J. Katz, A. Sahai, and B. Waters, "Predicate encryption is supporting disjunctions, polynomial equations, and inner products," in Proc. Advances in Cryptology (EUROCRYPT'08). Springer, 2008, pp. 146–162.
[22] V. Iovino and G. Persiano, "Hidden-vector encryption with groups of prime order," in Proc. Pairing-Based Cryptography (Pairing'08). Springer, 2008, pp. 75–88.
[23] E. Shi, J. Bethencourt, T. Chan, D. Song, and A. Perrig, "Multidimensional range query over encrypted data," in Proc. the IEEE Symposium on Security and Privacy (SP'07), 2007, pp. 350–364.
[24] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in Proc. Advances in Cryptology (CRYPTO'01). Springer, 2001, pp. 213–229.
[25] B. Libert and J. Quisquater, "The exact security of an identity based signature and its applications," Tech. Rep. 2004, eprint.iacr.org/2004.
[26] J. Daemen, V. Rijmen, and A. Proposal, "Rijndael," in Proc. the First Advanced Encryption Standard Candidate Conference, National Institute of Standards and Technology (NIST), 1998.