A Secure Cloud Computing Based Framework for Big Data Information Management of Smart Grid

Joonsang Baek, Quang Hieu Vu, Joseph K. Liu, Xinyi Huang, and Yang Xiang, *Senior Member, IEEE*

Abstract—Smart grid is a technological innovation that improves efficiency, reliability, economics, and sustainability of electricity services. It plays a crucial role in modern energy infrastructure. The main challenges of smart grids, however, are how to manage different types of front-end intelligent devices such as power assets and smart meters efficiently; and how to process a huge amount of data received from these devices. Cloud computing, a technology that provides computational resources on demands, is a good candidate to address these challenges since it has several good properties such as energy saving, cost saving, agility, scalability, and flexibility. In this paper, we propose a secure cloud computing based framework for big data information management in smart grids, which we call "Smart-Frame." The main idea of our framework is to build a hierarchical structure of cloud computing centers to provide different types of computing services for information management and big data analysis. In addition to this structural framework, we present a security solution based on identity-based encryption, signature and proxy re-encryption to address critical security issues of the proposed framework.

Index Terms—Big data, cloud computing, secure, information management, smart grid

1 Introduction

1.1 Big Data Analysis in Smart Grid

Smart grids have recently been adopted in electronic grid renovation plans of many countries, replacing traditional power grids. One of the reasons is that compared to traditional power grids, smart grids bring significant improvement in the efficiency, reliability, economics, and substantiality of electricity services [18]. As an example, the ENEL Telegestore project in Italy [38], which is widely regarded as the first commercial project using smart grid technology, delivers annual savings of approximately 500 million Euros [37]. Following the success of Telegestore, several other smart grid projects have been proposed. They include the Hydro One project [10] in Canada, the Evora InovGrid project [26] in Portugal, and the Modellstadt Mannheim (Moma) project [36] in Germany.

While smart grids bring in several benefits to electrical power grids, their deployment is often limited to small regions (e.g., within a city or a small province). There are several challenges that prevent smart grids to be deployed at a larger scale (e.g., in the whole country), one of which is information management that is related to information gathering, information storing, and information processing [5], [14], [17]. Since there are a large number of front-end intelligent devices, managing a huge amount of information received from these devices is not an easy task. In a preliminary estimation at one utility, the amount of data required to process transactions of two million customers could reach 22 gigabytes [44] per day. It is definitely a big challenge to manage this set of big data, which may include the selection, deployment, monitoring, and analysis of smart grid data. More importantly, a real-time information processing is usually required in the smart grid. Any delay may cause a serious consequence in the whole system which has to be avoided as much as possible.

- *J. Baek is with the Electrical and Computer Engineering Department, Khalifa University of Science, Technology and Research, Abu Dhabi, UAE. E-mail: jsbaek@gmail.com.*
- *Q.H. Vu is with the Etisalat BT Innovation Centre (EBTIC), Khalifa University of Science, Technology and Research, Abu Dhabi, UAE. E-mail: quang.vu@kustar.ac.ae.*
- *J.K. Liu is with the Department of Infocomm Security (ICS), Institute for Infocomm Research, Singapore. E-mail: ksliu9@gmail.com.*
- *X. Huang is with the School of Mathematics and Computer Science, Fujian Normal University, Fuzhou 350000, China. E-mail: xyhuang81@gmail.com.*
- *Y. Xiang is with the School of Information Technology, Deakin University, Burwood, Victoria, Australia. E-mail: yang.xiang@deakin.edu.au.*

Manuscript received 28 Feb. 2014; revised 15 Aug. 2014; accepted 12 Sept. 2014. Date of publication 18 Sept. 2014; date of current version 10 June 2015. Recommended for acceptance by R. Ranjan, L. Wang, A. Zomaya, D. Georgakopoulos, G. Wang, and X.-H. Sun.
For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below.
Digital Object Identifier no. 10.1109/TCC.2014.2359460

1.2 Assistance from Cloud Computing

Cloud computing has become popular recently due to several advantages over traditional computing models. Typical advantages include flexibility, scalability, agility, energy efficiency, and cost saving [24]. For this reason, it has been expected to be a dominant computing model in the future. By employing cloud computing in smart grids, we not only address the issue of large information management but also provide a high energy and cost saving platform. It is because 1) the framework can scale very fast to deal with changes in the amount of processing information and 2) it can provide a high utilization of computing resources.

Actually, prior to our work, initial efforts have been devoted to prove that cloud computing can satisfy requirements of information management in these systems [4], [40]. In particular, in [40], properties of smart grid and cloud computing were analyzed to prove the relationship between them. Furthermore, in [4], use cases of a smart grid were discussed to understand detailed requirements of information

management, and cloud computing properties were studied to show that they meet the requirements. Nevertheless, none of these works comes up with a *concrete* design for information management in smart grids besides rather abstract analyses.

1.3 Our Approach

Motivated by the previous work, in this paper, we introduce a design of *Smart-Frame*, a flexible, scalable, and secure information management framework for smart grids based on cloud computing technology. Our basic idea is to build the framework at three *hierarchical* levels: *top*, *regional*, and *end-user* levels in which the first two levels consist of cloud computing centers while the last level contains end-user smart devices. The top cloud computing center takes responsibility of managing general devices and accumulation of data across the regional cloud computing centers which are placed in the lower level in the hierarchy. The regional cloud computing centers are in turn in charge of managing intelligent devices, which have lower hierarchical level than the regional cloud computing centers in specific regions (e.g., within a city), and processing data of these devices.

In addition to this general framework, we propose a security solution for the framework based on identity-based encryption (IBE) and signature [6], [43], and identity-based proxy re-encryption [22]. Providing information security for smart grids is very important since much of the information in smart grids is sensitive and needs to be strictly protected. Information leakage in smart grids can lead to vulnerabilities that affect not only individuals but also the whole nation because leaked information can be used to launch attacks to both individuals and the whole smart (power) grids at the national level.

The main idea of our security solution for the Smart-Frame is to allow all the involved entities, i.e., top and regional cloud computing centers and end-users to be represented by their identities which can be used as encryption keys or signature verification keys. The entities in the lower level can use the identities of higher-level entities to encrypt their data for secure communication with the entities in the higher level. For example, the regional centers use the top cloud's entity to encrypt their messages. By employing an identity-based re-encryption scheme, the information storages, which are components of regional clouds, can re-encrypt the received confidential data from the end-user devices so that services requested by the end-users decrypt and process the confidential data without compromising the information storages' private keys. One of the obvious benefits we can gain from applying identity-based cryptography to the Smart-Frame is that through using identities rather than digital certificates which depend on traditional public key infrastructure (PKI), we can save significant amount of resources for computation and communications and resolve scalability issues. The saving gained from the elimination of digital certificate in the big data environment is especially momentous.

1.4 Our Contributions

To summarize, our contributions in this paper are twofold:

- *We introduce Smart-Frame*. A cloud computing based framework for big data information management in smart grids, which provides not only flexibility and scalability but also security features.
- We present a security solution for the proposed framework based on identity-based encryption and proxy re-encryption schemes, which provides secure communication services for the Smart-Frame. We further implement the prototype of our proposed solution to show its practicality.

The rest of this paper is organized as follows. In Section 2, we review the related work. Through Sections 3 and 4, we present the Smart-Frame. In particular, Section 3 focuses on the general architecture of the Smart-Frame while Section 4 deals with its security issues and proposed a solution based on identity-based cryptography. Finally, we demonstrate a simple prototype implementation in Section 5 and conclude the paper in Section 6.

2 Related Work

In this section, we review the related work about smart grid information management (Section 2.1), smart grid security management (Section 2.2), and finally the basics of identity-based encryption and proxy re-encryption schemes respectively (Sections 2.3 and 2.4).

2.1 Smart Grid Information Management

Smart grid information management usually involves three basic tasks: information gathering, information processing, and information storing. For information gathering, since smart grids have to collect information from heterogeneous devices at different locations, the main research challenge is to build efficient communication architecture. Several solutions have been proposed to address this challenge and most of them can be found in the recent surveys such as [17], [46], and [5]. In terms of information processing, data integration also lays a challenge as information can be received from a number of devices, which may use different data structures to handle the information. Fortunately, a proposal for standardization of data structures used in smart grid applications has recently been proposed to address this issue of data inter-operability [25]. However, how to process a large amount of data efficiently still remains as a big challenge. Cloud computing appears to meet this demand and also satisfy challenges of information storing. As a result, initial works on cloud computing and smart grids have been produced. In [40] properties of smart grid and cloud computing were analyzed to prove that cloud computing is a good candidate for information management in smart grids. Similarly, in [4], use cases of a smart grid were discussed to understand detailed requirements of information management and cloud computing properties were studied to show that they meet the requirements. These two works are different from ours in that they only presented analysis while we introduce a concrete design for the platform as well as a security solution for it.

2.2 Other Approaches to Smart Grid Security

Due to their large-scale deployment, smart grids suffer from several security vulnerabilities [28]. Since any security breach in smart grids may lead to a big loss, there are initiatives to address security challenges in this type of systems. For examples, authors of [15], [27], [32], and [8] proposed different methods to address the security issues related to

information processing of smart meters while Zhang et al. [49] and Wei et al. [48] respectively introduced security frameworks to control the consistency of security requirements across all smart grid components and to protect smart grids against cyber attacks. On the other hand, Metke and Ekl [35] discussed key components for security in smart grids and Rogers et al. [39] presented an authentication and integrity approach that used digital signatures and timestamps. Recently identity-based cryptography was considered as good apparatus for secure cloud computing and grid computing as discussed in [30], [33], and [42].

Coates et al. [9], Kuntze et al. [29], and Hamlyn et al. [23] proposed security architectures for smart grid. The security architectures that proposed by Coates et al. and Kuntze et al. [29] can be categorized as trusted computing based architecture, according to Wang and Lu [47]. Coates et al.'s architecture proposed in [9], a trust system is deployed near or at the SCADA center to validate identities and inputs, assess security risks, detect defective or malicious data and trigger appropriate alerts. In [29], Kuntze et al. proposed hardware design for distributed trust computing to establish a security infrastructure for power networks. The security architecture that Hamlyn et al. proposed in [23] is a role-based network architecture in which an authentication network structure is realized based on functional roles.

In addition to the security architectures for smart grid, secure aggregation protocols were proposed by Li et al. [31] and Bartoli et al. [3]. The secure aggregation protocols pursue the bottom-up traffic model (i.e., device-to-center), which is spread widely in power systems, for example, meter-reading in the advanced metering infrastructure network. Other efforts include securing distributed networking protocol 3.0 protocols for US power systems using IPSec or TLS and IEC 62351 [12], which is a standard proposed to handle the security for a series of protocols including IEC 61850 [11], a recent standard for substation communication.

Our work is inspired by these works but we provide a new security framework based on identity-based proxy re-encryption, different from those considered in the previous work. More precisely, [42] is mainly concerned with a new identity-based key agreement protocol based on RSA primitive, which is different from ours. Li et al. [30] discusses applying identity-based signature (IBS) schemes in non-hierarchical cloud environment. The main focus of [33] is to construct identity-based key agreement protocol in general grid computing environment while our work focuses specifically on providing our Smart-Frame with security framework based on identity-based encryption/signature and identity-based proxy re-encryption schemes. We note that in the recent work by Tysowski and Hasan [45], the proxy re-encryption technique is applied to provide mobile applications in clouds with security. Although our work is related to theirs as our security framework is based on cloud computing, we specifically apply identity-based cryptographic techniques to address the scalability issues of smart grid applications.

2.3 Basic Identity-Based Cryptographic Schemes

Two very basic cryptographic building blocks for the security of the Smart-Frame are identity-based encryption and identity-based signature schemes.

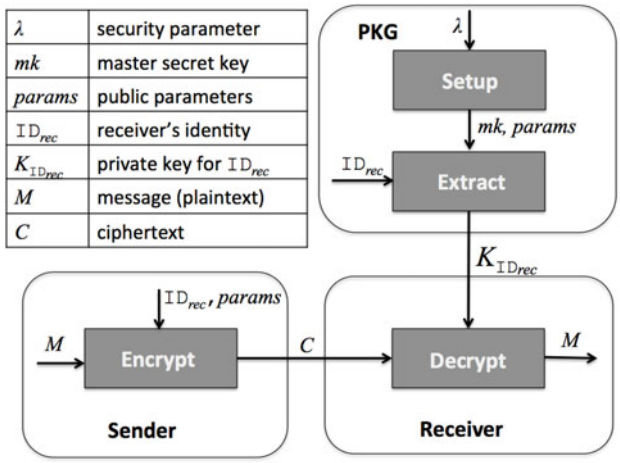


Fig. 1. Overview of identity-based encryption.

Introduced by Shamir in 1984 [43], identity-based cryptography is to eliminate the requirement of checking the validity of certificates in traditional public key infrastructure. In an identity-based encryption scheme, the private key generator (PKG), a trusted party, first generates secret master key mk and public parameter $params$. Note that $params$, which is long-term, will be given to every party that is involved. Once a receiver submits his/her identity, denoted by $\mathtt{ID}_{rec}$, the PKG computes the private key $K_{\mathtt{ID}_{rec}}$ associated with $\mathtt{ID}_{rec}$ by running the private key extraction algorithm Extract providing its master secret key mk as input. Here, the identity $\mathtt{ID}_{rec}$ can be *any string* such as an email address, a telephone number, etc. Note that the distribution of the private keys can be done in a similar way as digital certificates are issued in normal public key cryptography: Users would authenticate themselves to the PKG and obtain private keys associated with their identities. Secure channel may have to be established between the PKG and the users depending on the situation to prevent eavesdropping.

Now any sender who is in the possession of $\mathtt{ID}_{rec}$, encrypts a plaintext message M into a ciphertext C by running the Encrypt algorithm. Upon receiving C, the receiver decrypts it by running the Decrypt algorithm providing the private key $K_{\mathtt{ID}_{rec}}$ obtained from the PKG previously as input. The basic operations of the IBE scheme are illustrated in Fig. 1.

An identity-based signature scheme [43] can be described as follows. Likewise, when the signer submits his/her identity $\mathtt{ID}_{sig}$, the PKG computes the private key $K_{\mathtt{ID}_{sig}}$ associated with $\mathtt{ID}_{sig}$ by running the Extract with the master secret mk. Using $K_{\mathtt{ID}_{sig}}$, the signer can sign a message M to create a corresponding signature σ by running the Sign algorithm. Providing the message M, the signer's identity $\mathtt{ID}_{sig}$, and the signature σ, any party (verifier) can verify whether the signature σ is valid one or not. The basic operations of the IBS scheme are illustrated in Fig. 2.

Note that both IBE and IBS avoid the use of digital certificates but provide implicit certification of each user within the system as only the user who successfully registered his/her identifier and obtained the corresponding private key can conduct decryption or produce a valid signature. We remark that although the IBS scheme had already been realized by Shamir in 1984 [43], practical realization of

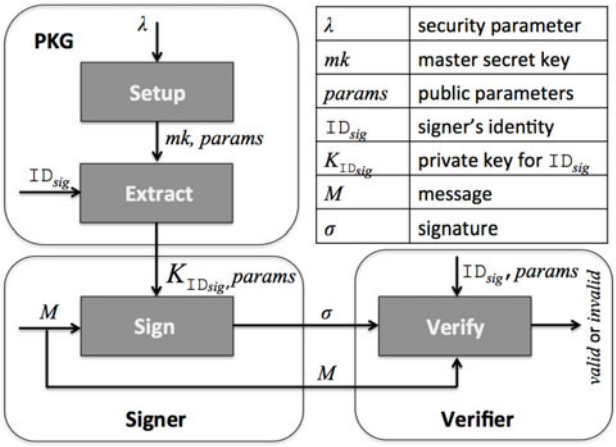


Fig. 2. Overview of identity-based signature.

identity-based encryption was accomplished by Boneh and Franklin [6] in 2001.

2.4 Identity-Based Proxy Re-Encryption

Proxy re-encryption lets a proxy to transform a ciphertext produced under Alice's public key in such a way that the transformed ciphertext can be decrypted under another party Bob's private key. The concept of proxy re-encryption was first introduced by Mambo and Okamoto [34], whose main goal was to achieve efficiency better than "decrypt-and-encrypt" approaches. The first fully functioning proxy re-encryption scheme was proposed by Ateniese et al. [1]. Compared with the previous approaches, their proxy re-encryption scheme was unidirectional, so it does not require delegators to reveal their secret keys to anyone in order to allow proxy to re-encrypt their ciphertexts.

Since Ateniese et al.'s work, numerous proxy re-encryption schemes with various functionalities have been proposed. Among them, the *identity-based proxy re-encryption* scheme proposed by Green and Ateniese [22] is closely related to our Smart-Frame. In an identity-based proxy re-encryption scheme, a delegator allows a proxy to transform an encryption under Alice's identity into one encrypted one under Bob's identity. The proxy then uses re-encryption keys to conduct the transformation without being able to learn any information about the plaintext. Also, no information about the private keys of Alice and Bob would be deduced from the re-encryption keys. Note that identity-based proxy re-encryption combine the two functionalities of IBE and proxy re-encryption without compromising the security. Note also that Green and Ateniese's identity-based proxy re-encryption scheme [22] is based on the pairing like Boneh and Fraklin's IBE scheme.

3 Smart-Frame

In this section, we discuss our proposed Smart-Frame from three main perspectives: system architecture (Section 3.1), logical components (Section 3.2), and information management (Section 3.3).

3.1 General System Architecture

The overall architecture of the Smart-Frame is shown in Fig. 3.

In this architecture, a smart grid can be divided into several regions each of which is managed by a cloud computing center that can be setup from either a public cloud or a private cloud. The role of a regional cloud computing center is to manage intelligent devices in the region as well as to provide an initial processing for information received from these devices. Besides regional cloud computing centers, there is a special cloud computing center at the top level, which is in charge of managing and processing data for the whole grid. In each of these cloud computing centers, the following cloud computing services could be deployed:

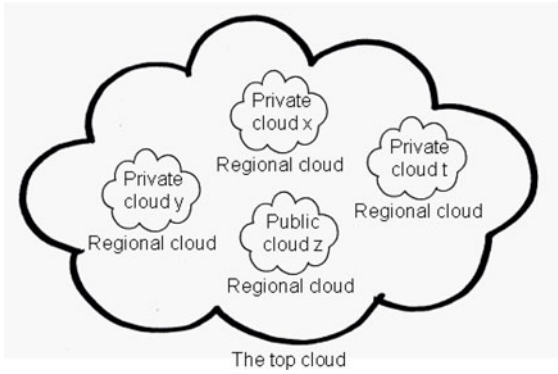


Fig. 3. Overview of the architecture of the Smart-Frame.

- *Infrastructure-as-a-service (IaaS)*. This type of service forms the backbone of the system. It helps to provide resources on demand for all applications and services deployed in the system. Main tasks of information management in smart grids such as information gathering, information processing, and information storing, are all executed inside this layer of service.
- *Software-as-a-service (SaaS)*. While IaaS is the backbone of the system, all smart grid services will be deployed as SaaS at the top of the system. Examples include services that allow customers to save or optimize their energy usage such as Google Power Meter [21].
- *Platform-as-a-service (PaaS)*. PaaS provides tools and libraries to develop cloud computing applications and services. Salesforce [41] is a typical PaaS example, which provides libraries to develop some specific types of applications in saleforce or fieldforce domains. In smart grid domain, since a number of applications could be required to follow special security requirements and have to allow lawful interceptions, it is useful to have a general PaaS that has already integrated these requirements to implement applications.
- *Data-as-a-service (DaaS)*. DaaS could be deployed to provide useful information for statistics purpose. Since smart grid data is often extremely large, it is useful to provide such statistics services for users. Statistics can be used for optimization purposes for not only electricity users but also electricity providers at different levels.

3.2 Logical Component View

Among cloud computing services presented in Section 3.1, while IaaS is the backbone of the system, we classify other services into clusters according to functionality they provide

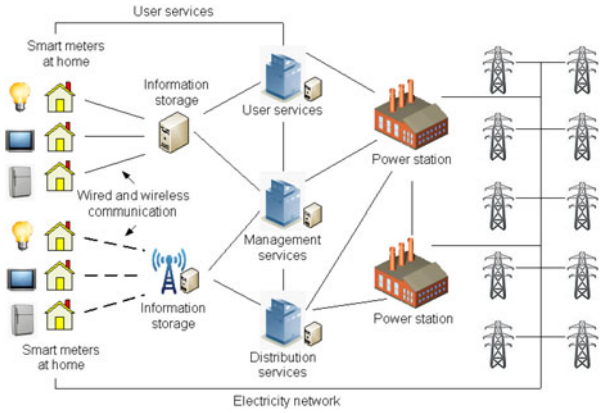


Fig. 4. Functional cloud computing service clusters.

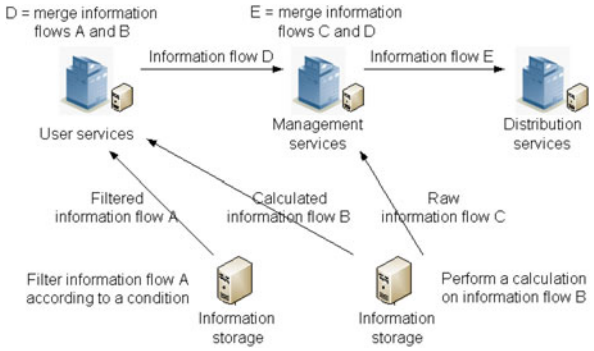


Fig. 5. An example of information flow schedule.

in order to ease the management. In our framework, we propose to use four main functional clusters as follows:

- *Information storages*. These are main storages keeping all smart grid information received from front-end intelligent devices. These storages are designed to accept information from different transportation modes through both wired and wireless channels. For optimization purpose, statistics services are also located in this cluster.
- *General user services*. This type of services consists of all services an electricity user needs to use. Typical examples are services that allow users to monitor, control or optimize the usage of their electric utilities. The majority of SaaS fall into this type of service. PaaS that provides libraries for user services also falls into this cluster.
- *Control and management services*. This type of services includes all services needed for system management such as governance service, monitoring service, task scheduling service, and security service.
- *Electricity distribution services*. This type of services is directly related to electricity distribution. Examples are distribution management service, optimization service, and quality of service measurement.

The above four types of services are illustrated as in Fig. 4. Note that besides information storages, all other types of services can be linked to the electricity grid. Note also that among these functional clusters, while information storages and user services usually exist in regional clouds, management and distribution services can be found in both regional and top clouds.

3.3 Information Flow Management

Since smart grids need to handle huge amount of data, it is extremely important to manage information flows efficiently. In the Smart-Frame, we suggest a centralized service to manage information flows. This service takes inputs as both information requests from service clusters and general statistics (e.g., the amount of information, time of arrival) from information storages. Using these inputs, the service generates an information flow schedule, which specifies sources and destinations of information flows as well as how they are processed (e.g., which specific operators are applied on information flows and where they are applied). Both information storages and services clusters need to follow this schedule for execution. Fig. 5 shows an example of information flow schedule. Note that since information amount and requests in smart grid may change with time, each information flow schedule has an expiry time. After this time, a new schedule has to be generated and distributed again to all parties.

4 Security Solution for Smart-Frame

4.1 Security of Smart-Frame Supported by Identity-Based Cryptography

Since security is a major concern in the smart grids, it is of great importance for our Smart-Frame to provide a solution to address that. As mentioned earlier, one of the huddles for widely deploying security solutions based on public key cryptography is the high cost for maintaining PKI. We envision that Identity-based cryptography can be a good solution (though it is not perfect) for resolving this problem since identity-based cryptography has the following advantages in regards to the Smart-Frame security.

1) Under traditional public key cryptography, each participating entity must *locate* and *verify* the public keys of the receivers. This is especially burdensome for end-user devices in our Smart-Frame, which are usually assumed as limited in power and networking capacity.
2) Although traditional public key cryptography is scalable in theory, a number of issues regarding user interfaces for maintaining public-key certificates (involving certificate revocation) have to be resolved. However, since any identifier strings can serve as encryption key or signature verification keys, identity-based cryptography could provide better *scalability* for the system. This is important in Smart-Frame in which numerous end-user devices can join and leave the system often.
3) For the convenience of the participating entities in the system, implementing key recovery is easy using identity-based cryptography. In contrast, in traditional public key cryptography, key recovery system is hard to implement requiring to keep secure database of private and public key pairs of the users. Due to the generic nature that private keys can be derived from the users' identities and master key of the private key generator, no secure database can be required for the system based on identity-based cryptography.

4) In terms of encryption, traditional public key cryptography always require a setup phase to generate public-keys of the receiving parties. However, identity-based cryptography does not need such phase and users can encrypt their messages using the receiving parties' identities even before the receivers get the private keys form the PKG. This can be useful in the Smart-Frame where *availability* is an issues in the power grid. Availability will be assured by minimizing the time and frequencies for updating identities (public-keys).
5) Identities used as public keys in identity-based cryptography are flexible and *versatile* in format and description. They do not have to be restricted like the X.509 certificate format used in traditional public key cryptography. This *versatility* will be useful in our Smart-Frame in which identities can describe participating entities more flexibly.

There is, of course, a key escrowing problem in identity-based cryptography. However, this can be relatively a mild issue for our setting as the Smart-Frame is mainly concerned with power grids which cannot fully be open to public network. In this setting, confidentiality, integrity and availability will have more priorities.

Note that Shamir already showed that a functional IBS scheme can be constructed using the RSA primitive [43]. More recent work by Galindo and Garcia demonstrated that a very efficient IBS scheme can be constructed using discrete-logarithm primitive [19]. In terms of IBE, it would be difficult to compare the performance of IBE schemes with that of normal public-key encryption schemes as the latter can be constructed using a number of different kinds of computational primitives. In general, IBE schemes would slightly be more costly than most efficient public key encryption schemes such as ElGamal-style encryption schemes based on elliptic curves, due to the pairing operations which have been used in many functional IBE schemes since Boneh and Franklin's IBE scheme [6]. However, we note that research has been being performed actively to improve the performance of pairing computation as surveyed in [7].

4.2 High Level Description

In realizing the security framework for the Smart-Frame, we make the following assumptions:

- There is a private key generator that can issue private keys for top and regional clouds, and end-users when they register. We assume that the PKG is a party that has responsibility and capacity of maintaining the Smart-Frame usually at the national level and its credential is fully trusted.
- The top cloud, regional clouds and end-users (e.g., smart meters at home) are identified by unique strings, which are to be used as encryption keys or signature verification keys.
- Each entity will obtain a private key associated with its identity, so it can decrypt the confidential data.
- Each entity will send confidential data to the entity which is only one-level higher. That is, the end-users send confidential data to the entities in the regional cloud only. Similarly entities in the regional cloud can send confidential data to the top cloud only.
- Each entity will authenticate data using the private key obtained from the PKG.

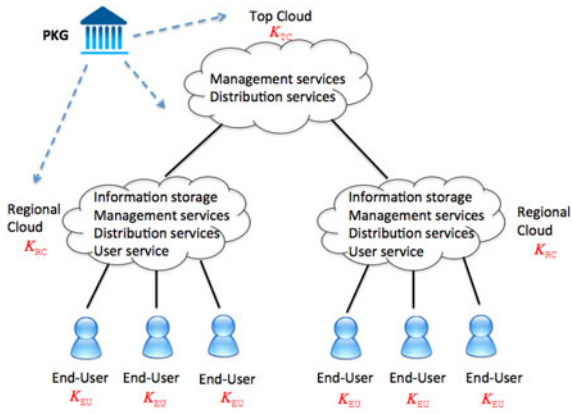


Fig. 6. Hierarchical architecture.

Based on the above assumptions, our main idea can be described using the following scenario, which is also depicted in Fig. 6. At the top of the hierarchy is the top cloud, which consists of power stations, distribution services or management services. Below the top cloud, there are regional clouds that consist of general user services and information storages. These regional clouds, in turn, have higher hierarchy than smart (intelligent) end-user devices (simply we call "end-users"), which are at the bottom of the hierarchy. Based on the principle of identity-based cryptography, the PKG will generate private keys for top cloud and any entities in regional clouds and end-users. Using their identifiers and private keys, each entity can utilize IBE schemes to secure information flow depicted in Fig. 5. In addition to IBE schemes, any parties can authenticate their data employing IBS schemes.

Another important security issue that should be addressed is to make it possible for an information storage in the regional cloud to forward the received confidential data (ciphertexts) from the end-users to specific services in such a way that the services decrypt the ciphertexts correctly but the secrecy of the information storage's private key is never compromised. That is, the information storage performs heavy tasks of distributing confidential data to various services residing in the regional cloud while maintaining the security of cryptographic keys held by the information storage. We employ an identity-based proxy re-encryption scheme to achieve this. In the setting of identity-based proxy re-encryption, end-users can protect their data as the data are always encrypted with the identity of the information storage. When an end-user wants a specific service to receive, use and process its data, the information storage generates a re-encryption key using its identity and the identity of the requested service. The information storage then uses the generated re-encryption key to re-encrypt the confidential data encrypted using the information storage's identity so that the target service can receive, decrypt, and process the data. Note that the information storage takes care of heavy load of re-encryption but the services in the regional cloud cannot break the confidentiality of

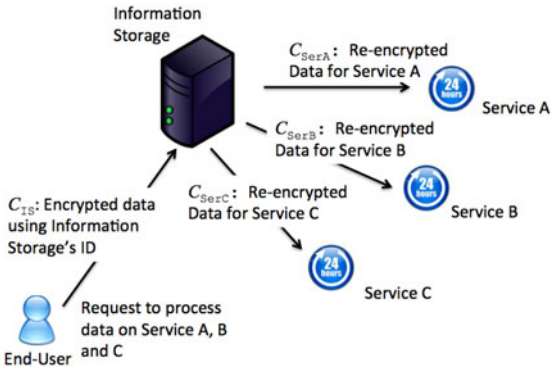


Fig. 7. Proxy re-encryption.

the data which they not entitled to process. An example is illustrated in Fig. 7 where the end-user agrees to let services A, B, and C to receive and use its data.

The details of our security framework are more formally described as follows. Note that TC, RC, and EU denote top cloud, regional cloud, and end-user respectively. We assume that the regional cloud consists of information storage IS and services $\mathtt{SerA}_1, \mathtt{SerA}_2, \ldots, \mathtt{SerA}_n$. For the sake of convenience of the description, we assume that SerA represents each service, i.e., $\mathtt{RC} = \{\mathtt{IS}, \mathtt{SerA}\}$. We also assume that IS and SerA are independently run, and do not share confidential information nor collude. Additionally, we assume that the basic identity-based cryptographic schemes IBE and IBS, which the following security framework unitize, are as described in Section 2.3.

- Key Generation
  - Setup: Given a security parameter λ, the PKG generates a secret master key mk and a set of parameters $params$. The PKG distributes $params$ to all the clouds and end-users.
  - ExtractTCKey: Upon receiving a top cloud's identity TC, the PKG generates a private key $K_{\mathtt{TC}}$ associated with TC by running the private key extraction algorithm Extract providing TC as input. We denote this process by $K_{\mathtt{TC}} \leftarrow \mathsf{ExtractRCKey}(params, mk, \mathtt{TC})$.
  - ExtractISKey: Upon receiving an identity of the information storage in the regional cloud, denoted by IS, the PKG generates a private key $K_{\mathtt{IS}}$ associated with IS by running the private key extraction algorithm Extract providing IS as input. We denote this process by $K_{\mathtt{IS}} \leftarrow \mathsf{ExtractISKey}(params, mk, \mathtt{IS})$.
  - ExtractServiceKey: Upon receiving an identity of the service A in the regional cloud, denoted by SerA, the PKG generates a private key $K_{\mathtt{SerA}}$ associated with SerA by running the private key extraction algorithm Extract providing SerA as input. We denote this process by $K_{\mathtt{SerA}} \leftarrow \mathsf{ExtractServiceKey}(params, mk, \mathtt{SerA})$.
  - ExtractEUKey: Upon receiving an end-user's identity EU, the PKG generates a private key $K_{\mathtt{EU}}$ associated with EU by running the private key extraction algorithm Extract providing EU as input. We denote this process by $K_{\mathtt{EU}} \leftarrow \mathsf{ExtractEUKey}(params, mk, \mathtt{EU})$.
- Encryption to Information Storage (in Regional Cloud)
  - Encrypt2IS: Each end-user can encrypt a message M into a ciphertext $C_{\mathtt{IS}}$ by running the IBE encryption algorithm Encrypt with $params$ and the identity IS of the information storage in the regional cloud. We denote this process by $C_{\mathtt{IS}} \leftarrow \mathsf{Encrypt2IS}(params, \mathtt{IS}, M)$.
  - DecryptIS: Each regional cloud can decrypt a received ciphertext C to M by running the IBE decryption algorithm Decrypt with the private key $K_{\mathtt{IS}}$ associated with the information storage's identity IS. We denote this process by $M \leftarrow \mathsf{DecryptIS}(params, K_{\mathtt{IS}}, C_{\mathtt{IS}})$.
- Encryption to Top Cloud
  - Encrypt2TC: Each information storage in the regional cloud can encrypt a message M into a ciphertext $C_{\mathtt{TC}}$ by running the IBE encryption algorithm Encrypt with $params$ and the top cloud's identity TC. We denote this process by $C_{\mathtt{TC}} \leftarrow \mathsf{Encrypt2TC}(params, \mathtt{TC}, M)$.
  - DecryptTC: The top cloud can decrypt a received ciphertext C to M by running the IBE decryption algorithm Decrypt with the private key $K_{\mathtt{TC}}$ associated with the top cloud's identity TC. We denote this process by $M \leftarrow \mathsf{DecryptTC}(params, K_{\mathtt{TC}}, C_{\mathtt{TC}})$.
- Proxy Re-encryption by Information Storage
  - RKGen: Providing its own private key $K_{\mathtt{IS}}$, its identity IS and the server A's identity SerA as input, the information storage in the regional cloud generates a re-encryption key $RK_{\mathtt{IS}\rightarrow\mathtt{SerA}}$. We denote this process by $RK_{\mathtt{IS}\rightarrow\mathtt{SerA}} \leftarrow \mathsf{RKGen}(K_{\mathtt{IS}}, \mathtt{IS}, \mathtt{SerA})$.
  - Reencrypt: The information storage in the regional cloud re-encrypts the ciphertext $C_{\mathtt{IS}}$ using the re-encryption key $RK_{\mathtt{IS}\rightarrow\mathtt{SerA}}$ and obtains a ciphertext $C_{\mathtt{SerA}}$. We denote this process by $C_{\mathtt{SerA}} \leftarrow \mathsf{Reencrypt}(RK_{\mathtt{IS}\rightarrow\mathtt{SerA}}, C_{\mathtt{IS}})$.
  - DecryptService: The service A decrypts $C_{\mathtt{SerA}}$ using its private key $K_{\mathtt{SerA}}$. We denote this by $M \leftarrow \mathsf{DecryptService}(K_{\mathtt{SerA}}, C_{\mathtt{SerA}})$.
- Signature Generation by End-Users
  - SignEU: Each end-user can generate a signature σ for a message M using the private key $K_{\mathtt{EU}}$ associated with its identity EU. We denote this process by $\sigma \leftarrow \mathsf{SignEU}(params, K_{\mathtt{EU}}, M)$.
  - VerifyEU: Any party can verify a signature σ for some message M using $params$ and the identity of the end-user, EU. We denote this process by $d \leftarrow \mathsf{VerifyEU}(params, \mathtt{EU}, \sigma, M)$, where d is either "accept" or "reject".
- Signature Generation by Entities in Regional Cloud
  - SignIS: Each information storage in the regional cloud can generate a signature σ for a message M using the private key $K_{\mathtt{IS}}$ associated with its identity IS. We denote this process by $\sigma \leftarrow \mathsf{SignIS}(params, K_{\mathtt{IS}}, M)$. Each service in the regional cloud (denoted by SerA as a representative) can also generate a signature in the same way.

- VerifyIS: Any party can verify a signature σ for some message M using $params$ and the information storage's identity IS. We denote this process by $d \leftarrow \mathsf{VerifyIS}(params, \mathtt{IS}, \sigma, M)$, where d is either "accept" or "reject". The signatures generated by a service in the regional cloud (denoted by SerA as a representative) can be verified in the same way.

- Signature Generation by Top Cloud
  - SignTC: The top cloud can generate a signature σ for a message M using the private key $K_{\mathtt{TC}}$ associated with its identity TC. We denote this process by $\sigma \leftarrow \mathsf{SignTC}(params, K_{\mathtt{TC}}, M)$.
  - VerifyTC: Any party can verify a signature σ for some message M using $params$ and the identity of the top cloud, TC. We denote this process by $d \leftarrow \mathsf{VerifyTC}(params, \mathtt{TC}, \sigma, M)$, where d is either "accept" or "reject".

4.3 Instantiations of the Security Framework Based on Pairing-Based IBE, ID-Based Proxy Re-Encryption Schemes and IBS

We now give concrete instantiations of the proposed security framework, which are based on Boneh and Franklin's IBE [6] and scheme and Green and Ateniese's identity-based proxy re-encryption [1] scheme. Both schemes relay on the $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, where $\mathbb{G}_1$ and $\mathbb{G}_2$ are groups of prime order q, is an (admissible) bilinear pairing, which has the following properties:

1) Bilinearity: For all $a, b \in \mathbb{Z}_q^*$, $e(g^a, h^b) = e(g, h)^{ab}$.
2) Non-degeneracy: $e(g, h) \neq 1$.
3) For the sake of practicality, e has to be efficiently computable.

Confidentiality Service

- Key Generation
  - Setup: The PKG generates $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order q and an admissible pairing $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, a generator $g \in \mathbb{G}_1$ and a hash function $\mathcal{H}_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$ and $\mathcal{H}_2 : \mathbb{G}_2 \rightarrow \{0,1\}^n$ for some positive integer n, which is the size of plaintexts. It then picks $s \in \mathbb{Z}_q$ at random and computes $u = g^s$. The top cloud sets secret master key $mk = s$ and a set of public parameters $params = (\mathbb{G}_1, \mathbb{G}_2, e, g, u, \mathcal{H}_1, \mathcal{H}_2)$. The PKG distributes $params$ to top and regional clouds and end-users.
  - ExtractTCKey: Upon receiving a top cloud's identity TC, the PKG computes $\mathcal{H}_1(\mathtt{TC})^s \in \mathbb{G}_1$ and returns $K_{\mathtt{TC}} = \mathcal{H}_1(\mathtt{TC})^s$ as a private key.
  - ExtractISKey: Upon receiving an identity of the information storage in the regional cloud, denoted by IS, the PKG computes $\mathcal{H}_1(\mathtt{IS})^s \in \mathbb{G}_1$ and returns $K_{\mathtt{IS}} = \mathcal{H}_1(\mathtt{IS})^s$ as a private key.
  - ExtractServiceKey: Upon receiving an identity of the service A in the regional cloud, denoted by SerA, the PKG computes $\mathcal{H}_1(\mathtt{SerA})^s \in \mathbb{G}_1$ and returns $K_{\mathtt{SerA}} = \mathcal{H}_1(\mathtt{SerA})^s$ as a private key.
  - ExtractUserKey: Upon receiving a user's identity EU, the PKG computes $\mathcal{H}_1(\mathtt{EU})^s \in \mathbb{G}_1$ and returns $K_{\mathtt{EU}} = \mathcal{H}_1(\mathtt{EU})^s$ as a private key.

- Encryption to Top Cloud[1]
  - Encrypt2TC: Any entity in the regional cloud can encrypt a message M using $params$ and the top cloud's identity TC as follows. First, pick $r \in \mathbb{Z}_q$ at random, and compute $C_1 = g^r$ and $C_2 = M \cdot e(u, \mathcal{H}_1(\mathtt{TC}))^r$. Finally, output $C_{\mathtt{TC}} = (C_1, C_2)$ as a ciphertext.
  - DecryptTC: Using the private key $K_{\mathtt{TC}} = \mathcal{H}_1(\mathtt{TC})^s$, the top cloud can decrypt a received ciphertext $C_{\mathtt{TC}} = (C_1, C_2)$ into M, where $M = C_2/(e(C_1, K_{\mathtt{TC}})$.

- Encryption to Information Storage
  - Encrypt2IS: Any end-user can encrypt a message M using $params$ and the information storage's identity IS as follows. First, pick $r \in \mathbb{Z}_q$ at random, and compute $C_1 = g^r$ and $C_2 = M \cdot e(u, \mathcal{H}_1(\mathtt{IS}))^r$. Finally, output $C_{\mathtt{IS}} = (C_1, C_2)$ as a ciphertext.
  - DecryptIS: Using the private key $K_{\mathtt{IS}} = \mathcal{H}_1(\mathtt{IS})^s$, the information storage can decrypt a received ciphertext $C_{\mathtt{IS}} = (C_1, C_2)$ into M, where $M = C_2/e(C_1, K_{\mathtt{IS}})$.

- Proxy Re-encryption by Information Storage
  - RKGen: The information storage identified by IS obtains a re-encryption key by computing $RK_{\mathtt{IS} \rightarrow \mathtt{SerA}} = (R_1, R_2, R_3)$ where $R_1 = g^{\tilde{r}}$ and $R_2 = T \cdot e(u, \mathcal{H}_1(\mathtt{SerA}))^{\tilde{r}}$ and $R_3 = K_{\mathtt{IS}}^{-1} \cdot \mathcal{H}_2(T)$ for random $\tilde{r} \in \mathbb{Z}_q$ and $T \in \mathbb{G}_2$.
  - Reencrypt: Suppose that the re-encryption key $RK_{\mathtt{IS} \rightarrow \mathtt{SerA}}$ is parsed as (R_1, R_2, R_3). The service A re-encrypts the ciphertext $C_{\mathtt{IS}} = (C_1, C_2)$ by computing a new ciphertext $C_{\mathtt{SerA}} = (C_1, C_2 \cdot e(C_1, R_3), R_1, R_2)$.
  - DecryptService: Let $C_{\mathtt{SerA}} = (C_1', C_2', R_1', R_2') = (C_1, C_2 \cdot e(C_1, R_3), R_1, R_2)$. Given $K_{\mathtt{SerA}} (= \mathcal{H}_1(\mathtt{SerA})^s)$, the service A computes $T = R_2'/e(K_{\mathtt{SerA}}, R_1')$. Then, it computes $M = C_2'/e(C_1', \mathcal{H}_2(T))$.

Authentication Service

Below, we describe the instantiation of the IBS based on Gentry and Silverberg's IBS scheme [20] from pairings. Note that we only describe the case of top cloud as the rest are very similar.

- Key Generation
  - The Setup procedure is the same as that of the IBE scheme except that another hash function $\mathcal{H}_2 : \{0,1\}^* \rightarrow \mathbb{G}_1$ will be used in the signature generation. Let $mk = s_0$ and $params = (\mathbb{G}_1, \mathbb{G}_2, e, g_0, u, \mathcal{H}_1, \mathcal{H}_2)$, where $u = g_0^{s_0}$, be the PKG's master secret key and a set of public parameters respectively. The key extraction procedures for regional cloud and end-user are exactly the same as those of the IBE scheme.
- Signature Generation by Top Cloud
  - SignTC. Using its private key $K_{\mathtt{TC}} (= \kappa = g_1^{s_0})$, each regional cloud generates a signature σ for message M as follows. First, compute $g_1 = H_1(\mathtt{TC}) \in \mathbb{G}_1$ and $g_M = \mathcal{H}_1(\mathtt{TC}, M) \in \mathbb{G}_1$. Then,

1. Basically the encryption algorithm is the same for all the entities involved except that identities are changing. We, however, describe each party's encryption process separately for completion.

pick $r \in \mathbb{Z}_q$ at random, and compute $\sigma_1 = \kappa g_M^r$ and $\sigma_2 = g_0^r$. Finally, output $\sigma = (\sigma_1, \sigma_2)$ as a signature.

– VerifyTC. Any party can verify a signature σ for the message M using $params$ and the top cloud's identity TC. To do this, a verifier needs to confirm that $e(g_0, \sigma_1) = e(u, g_1)e(\sigma_2, g_M)$.

4.4 Security Analysis

The correctness of the IBE scheme can easily be shown. The correctness of the ID-based proxy re-encryption scheme can be proven as follows. Let $C_{\mathtt{SerA}} = (C_1', C_2', R_1', R_2') = (C_1, C_2 \cdot e(C_1, R_3), R_1, R_2)$. Since $K_{\mathtt{SerA}} = \mathcal{H}_1(\mathtt{SerA})^s$, we have

$$\begin{aligned} R_2'/e(K_{\mathtt{SerA}}, R_1') &= R_2'/e(\mathcal{H}_1(\mathtt{SerA})^s, R_1) \\ &= T \cdot e(u, \mathcal{H}_1(\mathtt{SerA}))^{\tilde{r}}/e(\mathcal{H}_1(\mathtt{SerA})^s, R_1) \\ &= T \cdot e(g^s, \mathcal{H}_1(\mathtt{SerA}))^{\tilde{r}}/e(\mathcal{H}_1(\mathtt{SerA})^s, R_1) \\ &= T \cdot e(\mathcal{H}_1(\mathtt{SerA})^s, g^{\tilde{r}})/e(\mathcal{H}_1(\mathtt{SerA})^s, R_1) \\ &= T. \end{aligned}$$

Also, note that

$$\begin{aligned} C_2''/e(C_1', \mathcal{H}_2(T)) &= C_2 \cdot e(C_1, R_3)/e(C_1, \mathcal{H}_2(T)) \\ &= C_2 \cdot e\big(C_1, K_{\mathtt{IS}}^{-1} \cdot \mathcal{H}_2(T)\big)/e(C_1, \mathcal{H}_2(T)) \\ &= C_2 \cdot e\big(C_1, K_{\mathtt{IS}}^{-1}\big) \\ &= M \cdot e(u, \mathcal{H}_1(\mathtt{IS}))^r \cdot e\big(C_1, K_{\mathtt{IS}}^{-1}\big) \\ &= M \cdot e(g^r, \mathcal{H}_1(\mathtt{IS})^s) \cdot e\big(C_1, K_{\mathtt{IS}}^{-1}\big) \\ &= M \cdot e(C_1, K_{\mathtt{IS}}) \cdot e\big(C_1, K_{\mathtt{IS}}^{-1}\big) \\ &= M. \end{aligned}$$

Thus, the correctness of the ID-based proxy re-encryption holds.

Note also that the verification algorithm of the signature scheme is also valid since $e(g_0, \sigma_1) = e(g_0, \kappa g_M^r) = e(g_0, \kappa)$ $e(g_0, g_M^r) = e(g_0, g_1^{s_0})e(g_0^r, g_M) = e(u, g_1)e(\sigma_2, g_M)$.

The security of the Boneh-Fraklin IBE and the Green-Ateniese proxy re-encryption can directly applied to the security of the above scheme. More precisely, the security of above scheme meets the security notion of IBE, i.e., IND-ID-CPA (indistinguishability against identity and chosen plaintext attacks) and the security notion of identity-based proxy re-encryption, i.e., IND-PrID-CPA (indistinguishability against proxy identity and chosen plaintext attacks) in the random oracle model assuming that the bilinear Diffie-Hellman (BDH) problem [6] is intractable. Note that the BDH problem is to compute $e(g, g)^{abc} \in \mathbb{G}_2$, given $g^a, g^b, g^c \in \mathbb{G}_1$, where $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is an (admissible) bilinear pairing, which is known to be intractable.

In terms of authenticity, the above IBS scheme is unforgeable against chose message attack in the random oracle model assuming that computational Diffie-Hellman (CDH) problem in group $\mathbb{G}_1$. (The CDH problem is to compute g^{ab}, given $g^a, g^b \in \mathbb{G}_1$.)

5 Prototype Implementation

5.1 Overview

As a proof-of-concept, we implemented a simple prototype for our proposed framework. In our implementation, all cloud computing centers, both regional centers and the top cloud center, were built based on Eucalyptus [16], a popular open source cloud computing platform. By using Eucalyptus, we aim to provide infrastructure-as-a-service to the platform users. We chose Eucalyptus for our framework because of the following reasons.

- It is fully compatible with the industry standard amazon web services cloud APIs.
- It supports all major virtualization technologies including Xen, KVM, and VMware vSphere.
- It can be developed and extended easily and be installed smoothly on all major Linux OS distributions such as Ubuntu, RHEL/CentOS, openSUSE, and Debian.

On top of the Eucalyptus platform, to support the security for the framework, we provide the following services.

- *Identity registration*. Identity registration is used to register identities of all components that need to send or receive information in the framework. As an example, smart meters, intelligent sensors and all other front-end devices need to register their identities before they are allowed to send information to the cloud storage. On the other hand, cloud computing components and services need to register their identities before they can receive or provide information. When an identity is registered, a private key associated with the identity is generated for the registered component.
- *Data encryption and data decryption*. Data encryption is used to encrypt data before it is sent through the network. In general, before sending the data, the sender uses the identity of the target receiver as the key to encrypt the data. Given that the target receiver is the only one who holds the private key to decrypt the data, this way the security of data is retained. On the other hand, data decryption is used by a receiver of ciphertext to decrypt the previously encrypted data (ciphertext) to obtain original data.

These above services were implemented based on the Java-based cryptographic library for pairing operation called *JPair* developed by Dong [13]. Given the platform and basic security services, all information management tasks as well other types of services can be implemented on top of the platform.

5.2 A Specific Scenario of the Platform Usage

As an example, we give a specific scenario of the platform usage. Suppose that a regional center (server) identified by a string "AD_EC" for controlling electricity in Abu Dhabi, United Arab Emirates. Suppose also that a smart meter identified by a string "SM1" which resides in a household in AlMata, a region of Abu Dhabi, will encrypt a message regarding the daily usage of electricity. Let this message be "SM1||50kW||AlMata". This scenario is realized in our proposed security framework as follows:

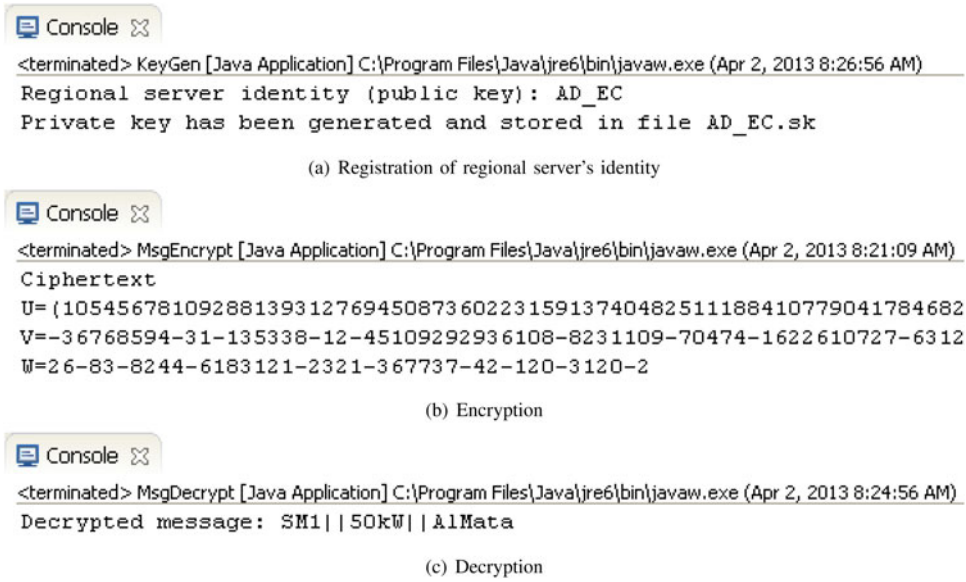


Fig. 8. Basic processes for encryption and description in the Smart-Frame.

- In the first step, the regional center (server)'s identity `AD_EC` is registered using the *identity registration* service. After registration, the private key associated with the identity is issued. Fig. 8a demonstrates this process which is displayed in console. Note that `AD_EC.sk` denotes the private key associated with regional server (center)'s identity `AD_EC`.
- In the next step, the smart meter uses the regional center (server)'s identity `AD_EC` to encrypt its message regarding the daily usage of electricity by calling the *data encryption* service. Fig. 8b demonstrates this process, displayed in console. Note that the ciphertext, consisted of three components `U`, `V` and `W`, is longer than the original message due to the redundancy added by the encryption algorithm to guarantee strong security.
- In the final step, the regional center uses its private key `AD_EC.sk` to decrypt the ciphertext by calling the *data decryption* service. Fig. 8c demonstrates this process, displayed in console. The decrypted message is "`SM1||50kW||AlMata`" which is interpreted as "The daily usage of electricity recorded in Smart Meter 1 in household in AlMata is 50kW".

6 Conclusion

In this paper, we have introduced the Smart-Frame, a general framework for big data information management in smart grids based on cloud computing technology. Our basic idea is to set up cloud computing centers at three hierarchical levels to manage information: top, regional, and end-user levels. While each regional cloud center is in charge of processing and managing regional data, the top cloud level provides a global view of the framework. Additionally, in order to support security for the framework, we have presented a solution based on identity-based cryptography and identity-based proxy re-encryption. As a result, our proposed framework achieves not only scalability and flexibility but also security features. We have implemented a proof-of-concept for our framework with a simple identity-based management for data confidentiality. Our immediate next step is to also support proxy re-encryption for the framework.

Acknowledgments

The authors of this paper would like to thank Dr. Changyu Dong at the University of Strathclyde for providing the source code that implements bilinear pairing in Java. This source code has been used in our prototype implementation to support identity-based management services. This paper is an extended version of the work originally presented at the 7th IEEE International Conference for Internet Technology and Secured Transactions (ICITST'12) , London, United Kingdom, December 2012, titled "Smartframe: A flexible, scalable, and secure information management framework for smart grids" [2]. This version differs from the previous one in that it contains completely revised security model based on identity-based proxy re-encryption and implementation results are included. Xinyi Huang is supported by National Natural Science Foundation of China (61472083), Fok Ying Tung Education Foundation (141065), Ph.D. Programs Foundation of Ministry of Education of China (20123503120001), Program for New Century Excellent Talents in Fujian University (JA14067), and Distinguished Young Scholars Fund of Department of Education, Fujian Province, China (JA13062).

References

[1] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM Trans. Inf. Syst. Security*, vol. 9, no. 1, pp. 1–30, 2006.

[2] J. Baek, Q. Vu, A. Jones, S. Al-Mulla, and C. Yeun, "Smart-frame: A flexible, scalable, and secure information management framework for smart grids," in *Proc. IEEE Int. Conf. Internet Technol. Secured Trans.*, 2012, pp. 668–673.

[3] A. Bartoli, J. Hernandez-Serrano, M. Soriano, and M. Dohler, "Secure lossless aggregation for smart grid M2M networks," in *Proc. IEEE Conf. Smart Grid Commun.*, 2010, pp. 333–338.

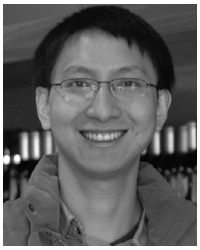
[4] K. P. Birman, L. Ganesh, and R. V. Renesse, "Running smart grid control software on cloud computing architectures," in *Proc. Workshop Comput. Needs Next Generation Electric Grid*, 2011, pp. 1–33.

[5] Z. Bojkovic and B. Bakmaz, "Smart grid communications architecture: A survey and challenges," in *Proc. 11th Int. Conf. Appl. Comput. Appl. Comput. Sci.*, 2012, pp. 83–89.
[6] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *Proc. 21st Annu. Int. Cryptol. Conf. Adv. Cryptol.*, 2001, vol. 2139, pp. 213–229.
[7] X. Boyen, "A tapestry of identity-based encryption: practical frameworks compared," *Int. J. Appl. Cryptograph.*, vol. 1, no. 1, pp. 3–21, 2008.
[8] C.-K. Chu, J. K. Liu, J. W. Wong, Y. Zhao, and J. Zhou, "Privacy-preserving smart metering with regional statistics and personal enquiry services," in *Proc. 8th ACM SIGSAC Symp. Inf., Comput. Commun. Soc.*, 2013, pp. 369–380.
[9] G. M. Coates, K. M. Hopkinson, S. R. Graham, and S. H. Kurkowski, "A trust system architecture for SCADA network security," *IEEE Trans. Power Delivery*, vol. 25, no. 1, pp. 158–169, Jan. 2010.
[10] R. Davies, "Hydro one's smart meter initiative paves way for defining the smart grid of the future," in *Proc. Power Energy Soc. Gen. Meeting*, 2009, pp. 1–2.
[11] *IEC 61850: Communication Networks and Systems in Substations*, IEC 61850. Dec. 2013.
[12] *IEC 62351: Data and Communication Security*, IEC 62351, May 2007.
[13] C. Dong. Jpair [Online]. Available: https://personal.cis.strath.ac.uk/changyu.dong/jpair/intro.html, Oct. 2010.
[14] J. Duff, "Smart grid challenges," in *Proc. Workshop High Perform. Trans. Syst.*, 2009, [Online]. Available: http://www.hpts.ws/papers/2009/session4/duff.pdf
[15] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proc. 1st Int. Conf. Smart Grid Commun.*, 2010, pp. 238–243.
[16] Eucalyptus. [Online]. Available: http://www.eucalyptus.com, 2014.
[17] Z. Fan, P. Kulkarni, S. Gormus, C. Efthymiou, G. Kalogridis, M. Sooriyabandara, Z. Zhu, S. Lambotharan, and W. Chin, "Smart grid communications: Overview of research challenges, solutions, and standardization activities," *IEEE Commun. Survey Tutorials*, vol. 15, no. 1, pp. 21–38, Jan. 2012.
[18] H. Farhangi, "The path of the smart grid," *IEEE Power Energy Mag.*, vol. 8, no. 1, pp. 18–28, Jan./Feb. 2010.
[19] D. Galindo and F. Garcia, "A Schnorr-like lightweight identity-based signature scheme," in *Proc. 2nd Int. Conf. Cryptol. Africa*, 2009, pp. 135–148.
[20] C. Gentry and A. Silverberg, "Hierarchical ID-based cryptography," in *Proc. 8th Int. Conf. Theory Appl. Cryptol. Inf. Security: Adv. Cryptol.*, 2002, pp. 548–566.
[21] Google PowerMeter. [Online]. Available: http://www.google.com/powermeter/about, 2011.
[22] M. Green and G. Ateniese, "Identity-based proxy re-encryption," in *Proc. 5th Int. Conf. Appl. Cryptograph. Netw. Security*, 2007, vol. 4521, pp. 288–306.
[23] A. Hamlyn, H. Cheung, T. Mander, L. Wang, C. Yang, and R. Cheung, "Trust infrastructures for future energy networks," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2008, pp. 1–7.
[24] B. Hayes, "Cloud computing," *Commun. ACM*, vol. 51, no. 7, pp. 9–11, 2008.
[25] IEEE, *P2030/D7.0 draft guide for smart grid interoperability of energy technology and information technology operation with the electric power system (EPS), and end-user applications and loads*, P2030/D670, 2011.
[26] Inovgrid. [Online]. Available: http://www.inovcity.pt/en/pages/inovgrid.aspx, 2010.
[27] G. Kalogridis, C. Efthymiou, S. Denic, T. Lewis, and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *Proc. 1st Int. Conf. Smart Grid Commun.*, 2010, pp. 232–237.
[28] H. Khurana, M. Hadley, N. Lu, and D. Frincke, "Smart-grid security issues," *IEEE Security Privacy*, vol. 8, no. 1, pp. 81–85, Jan./Feb. 2010.
[29] N. Kuntze, C. Rudolph, M. Cupelli, J. Liu, and A. Monti, "Trust infrastructures for future energy networks," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2010, pp. 1–7.
[30] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-based authentication for cloud computing," in *Proc. 1st Int. Conf. Cloud Comput.*, 2009, vol. 5931, pp. 157–166.
[31] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smartgrids using homomorphic encryption," in *Proc. IEEE Conf. Smart Grid Commun.*, 2010, pp. 327–332.
[32] H. Li, R. Mao, L. Lai, and R. Qiu, "Compressed meter reading for delay-sensitive and secure load report in smart grid," in *Proc. 1st Int. Conf. Smart Grid Commun.*, 2010, pp. 114–119.
[33] H. Lim and K. G. Paterson, "Identity-based cryptography for grid security," *Int. J. Inf. Security*, vol. 10, no. 1, pp. 15–32, 2011.
[34] M. Mambo and E. Okamoto, "Proxy cryptosystems: Delegation of the power to decrypt ciphertexts," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. E-80, no. 1, pp. 54–63, 1997.
[35] A. Metke and R. Ekl, "Smart grid security technology," in *Proc. Eur. Conf. Innovative Smart Grid Technol.*, 2010, pp. 1–7.
[36] Moma. [Online]. Available: http://www.modellstadt-mannheim.de, 2012.
[37] National Energy Technology Laboratory for the U.S. Department of Energy, "Modern grid benefits," *White Paper*, 2007.
[38] S. Rogai, "ENEL Telegestore Project," Economic Commission for Europe, Committee on Sustainable Energy, Steering Committee of the Energy Efficiency 21, Ad Hoc Group of Experts on Energy Efficiency, Investments for Climate Change Mitigation, Eighth meeting, Geneva, 31 May 2006. [Online]. Available at http://www.unece.org/fileadmin/DAM/ie/se/pp/adhoc/adhoc8May06/2_Rogai.pdf
[39] K. Rogers, R. Klump, H. Khurana, A. Aquino-Lugo, and T. Overbye, "An authenticated control framework for distributed voltage support on the smart grid," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 40–47, Jun. 2010.
[40] S. Rusitschka, K. Eger, and C. Gerdes, "Smart grid data cloud: A model for utilizing cloud computing in the smart grid domain," in *Proc. 1st Int. Conf. Smart Grid Commun.*, 2010, pp. 483–488.
[41] Salesforce. [Online]. Available: http://www.salesforce.com
[42] C. Schridde, T. Dórnemann, E. Juhnke, B. Freisleben, and M. Smith, "An identity-based security infrastructure for cloud environments," in *Proc. IEEE Wireless Commun., Netw. Inf. Security*, 2010, pp. 644–649.
[43] A. Shamir "Identity-based cryptosystems and signature schemes," in *Proc. CRYPTO Adv. Cryptol.*, 1984, vol. 196, pp. 47–53.
[44] M. Shargal and D. Houseman, "The big picture of your coming smart grid," *Smart Grid News*, Mar. 2009. (Online). Available: http://www.smartgridnews.com/artman/publish/commentary/The_Big_Picture_of_Your_Coming_Smart_Grid-529.html
[45] P. K. Tysowski and M. A. Hasan, "Hybrid attribute- and re-encryption- based key management for secure and scalable mobile applications in clouds," *IEEE Trans. Cloud Comput.*, vol. 1, no. 2, pp. 172–186, Jul.–Dec. 2013.
[46] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," *Comput. Netw.*, vol. 55, no. 15, pp. 3604–3629, 2011.
[47] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *IEEE Trans. Power Delivery*, vol. 57, no. 5, pp. 1344–1371, Apr. 2013.
[48] D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde, "An integrated security system of protecting smart grid against cyber attacks," in *Proc. Eur. Conf. Innovative Smart Grid Technol.*, 2010, pp. 1–7.
[49] T. Zhang, W. Lin, Y. Wang, S. Deng, C. Shi, and L. Chen, "The design of information security protection framework to support smart grid," in *Proc. Int. Conf. Power Syst. Technol.*, 2010, pp. 1–5.

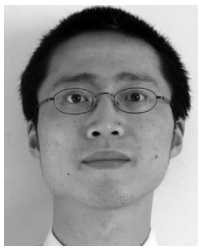
Joonsang Baek received the PhD degree from Monash University, Australia. He is currrently an assistant professor at the Department of Electrical and Computer Engineering, Khalifa University of Science, Technology and Research (KUSTAR), UAE. Before joining KUSTAR, he was a scientist at the Institute for Infocomm Research (I2R), Singapore. His research interests include the field of cryptography and information security. He has published his work in a number of reputable journals and conference proceedings. He has also served as chairs and program committee members for a number of international conferences on information security and cryptography.

Quang Hieu Vu received the PhD degree from Singapore-MIT Alliance (SMA), a collaboration program among three universities: Massachusetts Institute of Technology (MIT), National University of Singapore (NUS), and Nanyang Technological University (NTU) in 2008. He is currently a senior researcher of Etisalat BT Innovation Center (EBTIC) in United Arab Emirates (UAE). Prior to joining EBTIC, he was a research fellow at NUS in Singapore, a research associate at Imperial College London in United Kingdom, and a scientist at the Institute for Infocomm Research (I2R) in Singapore. His research interests include distributed systems (in particular peer-to-peer and cloud computing), optimization problems (in particular query optimization), and network security. He has published several papers at top conferences and journals such as SIGMOD, VLDB, ICDE, VLDB Journal, and *IEEE Transactions on Knowledge and Data Engineering (TKDE)*. In 2009, he published a book, *Peer-to-Peer Computing: Principles and Applications*.

Joseph K. Liu received the PhD degree in information engineering from the Chinese University of Hong Kong in July 2004, specializing in cryptographic protocols for securing wireless networks, privacy, authentication, and provable security. He is currently a research scientist in the Infocomm Security Department at the Institute for Infocomm Research, Singapore. His research interests include particularly lightweight security, cyber security, security in physical systems, and cloud computing environment.



Xinyi Huang received the PhD degree from the School of Computer Science and Software Engineering, University of Wollongong, Australia, in 2009. He is currently a professor at the Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, China. His research interests include cryptography and information security. He has published more than 80 research papers in refereed international conferences and journals. His work has been cited more than 1,500 times at Google Scholar (H-Index: 21). He is in the editorial board of *International Journal of Information Security* (*IJIS, Springer*) and has served as the program/general chair or program committee member in more than 60 international conferences.



Yang Xiang received the PhD degree in computer science from Deakin University, Australia. He is currently a full professor at the School of Information Technology, Deakin University. He is the director of the Network Security and Computing Lab (NSCLab). His research interests include network and system security, distributed systems, and networking. In particular, he is currently leading his team developing active defense systems against large-scale distributed network attacks. He is the chief investigator of several projects in network and system security, funded by the Australian Research Council (ARC). He has published more than 130 research papers in many international journals and conferences, such as *IEEE Transactions on Computers, IEEE Transactions on Parallel and Distributed Systems, IEEE Transactions on Information Security and Forensics*, and *IEEE Journal on Selected Areas in Communications*. Two of his papers were selected as the featured articles in the April 2009 and the July 2013 issues of *IEEE Transactions on Parallel and Distributed Systems*. He has published two books, *Software Similarity and Classification* (Springer) and *Dynamic and Advanced Data Mining for Progressing Technological Development* (IGI-Global). He has served as the program/general chair for many international conferences such as ICA3PP 12/11, IEEE/IFIP EUC 11, IEEE TrustCom 13/11, IEEE HPCC 10/09, IEEE ICPADS 08, and NSS 11/10/09/08/07. He has been the PC member for more than 60 international conferences in distributed systems, networking, and security. He serves as the associate editor of *IEEE Transactions on Computers, IEEE Transactions on Parallel and Distributed Systems, Security and Communication Networks* (Wiley), and the editor of *Journal of Network and Computer Applications*. He is the coordinator, Asia for IEEE Computer Society Technical Committee on Distributed Processing (TCDP). He is a senior member of the IEEE.