A Review on Cloud-based Privacy Preserving Schemes for Smart Meters

MUAHAMMAD TANVIR ALAM[1]
University of Toronto
Department of Electrical and Computer Engineering
Toronto, Canada
tanvir.alam@mail.utoronto.ca

Abstract Smart meters are used to have efficient energy management by the utilities using information driven approach. The requirements of scalable, elastic, reliable and shareable resources for deploying and running a Smart Grid utility's software architecture strongly fits within the capabilities provided by Cloud platforms. Indeed, some data warehouse vendors are already considering Cloud deployments for Smart utilities. However, a growing concern is ensuring privacy of personally identifiable data within the information integration platform of the utility provider in an area. In this survey, we present a synthesized overview of existing works integrating cloud computing in the existing smart grid architecture, in order to have client privacy preserved for energy supply. Also, we compare and evaluate these privacy preserving solutions against feasibility and practicality.

Keywords: privacy, smart meter, cloud, survey

(Received Jan 9th, 2016 / Accepted 16th Jun, 2016)

1. Introduction

Smart Grids have been a key enabler for Smart Energy, which refers to power networks that can intelligently integrate the behaviors and actions of all stakeholders connected to it, for example, generators, customers and those that do both –in order to efficiently deliver sustainable, economic and secure electricity supplies [1]. Currently, most of the Western electric utilities are being transitioned to Smart Power Grids that use large scale smart meter deployments at power consumers for real time communication using Internet protocols. The goal is to have efficient energy management by the utilities using information driven approach. For instance, the resource needs for the utility varies over the time of the day, with peak operation occurring during the day and information processing needing to slow down at night. Such informatics approach has given rise to many new models for demand forecasting in order to use direct and indirect information from diverse sources along with data mining and machine learning techniques for more accurate, adaptive and real time predictions. The data intensive applications and models require the use of scalable platforms to deploy and operate in a reliable manner. These requirements of scalable, elastic, reliable and sharable resources for deploying and running a Smart Grid utility's software architecture strongly fits within the capabilities provided by Cloud platforms [37]. Indeed, some data warehouse vendors are already considering Cloud deployments for Smart utilities [37]. Denmark now has its first cloud-based smart metering solution, targeted at small utilities and communities that previously could not afford such technologies [1].

As a result of the internet presence in cloud platforms, smart meter data have a greater exposure to cyberattacks or unprecedented access to consumer data. This could lead from hacking of smart meter data to power theft. Another growing concern is ensuring privacy of personally identifiable data within the utility's information integration platform. In this article, we investigate the privacy aware architectures and system designs of cloud based platforms for smart meters. The literature surveyed is within the past seven years to date which is the timeframe of cloud applications beginning to explore solutions for privacy aware smart metering.

2. Background

Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services [5]. The services referred to as Software as a Service (SaaS). The datacenter hardware and software is referred to as a Cloud. Internal datacenters of a business or other organization that are used for internal purposes are called private Cloud. On the other hand, a cloud is referred to as public when it is made available in a pay-as-you-go manner to the public, the service in such case being sold is Utility Computing. Thus, Cloud Computing is the sum of SaaS and Utility Computing [5]. Another type of cloud is called hybrid cloud where the private and public clouds are integrated together to perform several tasks which are capable of handling the requirements of private and public organizations. Apart from SaaS, two other types of services rendered in clouds are called Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). IaaS model includes storage and virtual machines as hardware platform to the users on demand basis. PaaS is responsible for the development and delivery of programming models to IaaS. Users can access such programming models through cloud and execute their programs [8]. The main properties that make cloud computing a good candidate to be deployed in smart grid are elasticity, shared and metering architecture. Elasticity refers to the capability of expanding and reducing according to the demand of the users. Service cost can be reduced by sharing resources among resources in a grid. Lastly, cost optimization mechanisms are offered to grid users, enabling them to provision and pay for their consumed resources only, which is offered by smart metering architecture.

The smart meter architecture is well described in [1]. Figure 1 depicts the data intelligence framework of a smart meter. The first component is the types of data stored or captured which can be broken down into consumption or measurement, power generation, power quality and events such as power failures, meter status etc. External data such as information analysis from temperature changes, geography and consumer information could be combined with these types of data. Accurate analysis of these captured or stored data can lead to many potential opportunities for generating value from such data.

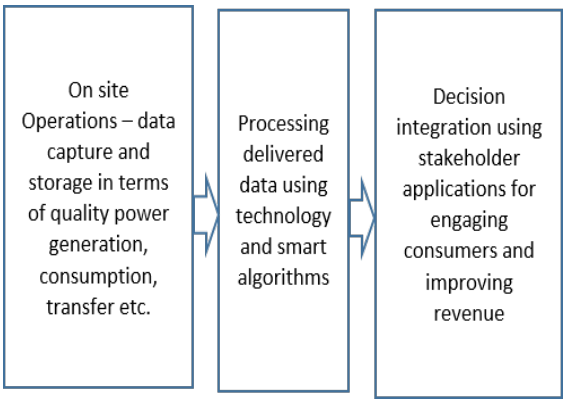

Figure 1: Smart Meter Framework

In the current metering environment, a meter is expected to have the capabilities to capture of electricity usage in real time or near real time, to provide the possibility of remote and local reading of the meter, to enable meter to control remotely or even terminate supply, and to link to other commodity supply for instance gas, water etc. In order to deliver these modern metering capabilities, it becomes imperative that data analytics technologies (which is the second component of smart meter framework) have to keep improving. The basic requirements of the tools and technologies are more reliable and faster transfer and storage of data and appropriate skills and resources being available in an organization. Therefore exploratory analytics tools such as clustering, visualization, unsupervised machine learning techniques and approach such as application driven directed activities are being utilized to address stakeholder or business requirements. Throughout the paper, we use the terms user, consumer, client and stakeholder interchangeably. Cloud computing plays integral role of hosting and providing tools and analytics building blocks. In order to identify the transformer loading patterns, the meters connected to individual transformers can be aggregated together. A simple cloud based web site can help customers relate power consumption to household activity. Smart applications can be deployed that may generate load forecasting on a time series data of the clients. Metering intelligence could be applied to benefit utility providers as well for instance, to set up dynamic and flexible tariff structures to improve efficiency in electricity markets by better representing the costs of producing and delivering electricity at different times. Finally, the deeper understanding of the dynamics of supply and demand combined with forecasting can result in enabling pricing

intelligence in terms of wholesale electricity cost, retail services cost, as well as costs of any regulatory requirements. The benefits such as on demand self-service, resource pooling and use of a cloud service on pay-per-use or charge per-use basis can result in huge volume of data generated and collected and hence, the growing concern of consumer privacy and unauthorized usage remains.

3. Motivation

While demand response, distributed generation, resource scheduling, and real-time pricing models contribute to the heterogeneity of a smart grid, effective authentication and authorization techniques are required for the preservation of user-privacy. Not only security aspects in smart grid like threat detection, cyber-physical attacks are necessary to be implemented, proper privacy policy needs to be implemented to motivate participation of customers. Cloud platform plays a significant role to provide solutions for these scenarios. A few surveys are available in the literature that address the cloud computing applications in smart grid ([38], [8], [1], [21], [18]). Smart meter challenges related to big data and the enablement of autonomous grid operation are investigated by Subhani *et al* [38]. A synthesized overview of the current state of research on smart grid development in the areas of cloud-based energy management, information management, and security is provided in [8]. A comprehensive survey of smart electricity meters and their utilization focusing on key aspects of metering process and the different technologies used to satisfy stakeholder interests is furnished in [1]. Security issues with defense mechanisms in smart grid for cloud-based software platforms are presented in [21], [18]. However, trust management under smart integration and adaptation to emerging fields using clouds in Smart Grid is still in an embryonic state. As such, we report recent advancements using cloud platforms, specifically for smart meter data to preserve consumer privacy and confidentiality.

Briefly, the main contributions of this paper are the following: (i) we present a survey of the existing cloud based privacy aware architectures for smart meter data after introducing the significance of cloud presence and its privacy requirements; (ii) we compare and evaluate these solutions against feasibility and practicality; and suggest recommendations for future work.

The rest of the paper is organized as follows. Section four depicts how cloud computing can be rendered integrating with smart meter data. Privacy objectives for smart meter data and defense mechanisms are furnished in section five and six respectively. The feasibility and practicality of these defense mechanisms are discussed in section seven. Finally, we conclude the article in section eight with the future research direction.

4. Cloud Computing in Smart Environment

The phases of smart grid include power generation, transmission and distribution [8], [21]. First, is the bulk generation of electricity that can be supported by numerous renewable and non-renewable power plants such as solar or wind farms, thermal and hydro plants etc. The transmission and distribution of power line to the smart meter enabled smart city is the other phases of smart grid. Here smart meters are deployed in the user premises. Depending upon the requirements in the scope of service or utility providers, the cloud integrated here could be private or public cloud supporting SaaS, PaaS or IaaS. This cloud platform is capable of storing and analysing power usage data collected by smart meters on real time basis via wide area network (WAN) connection (see figure 2).

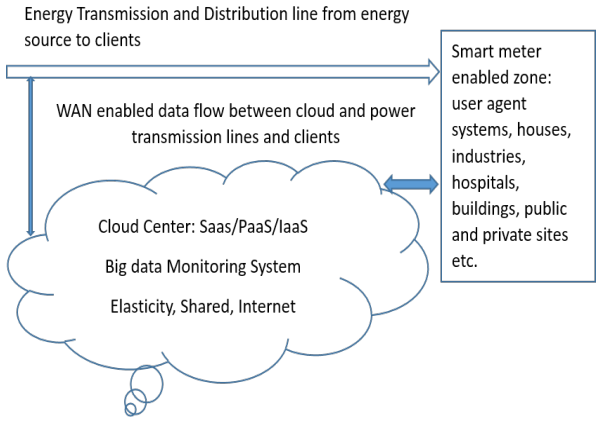

Figure 2: Cloud Support in Smart Grid

The cloud control center may consist of the backend servers that support various applications deployed on cloud infrastructure in order to provide data intelligence of smart meters. Moreover the control center is connected with the power lines to control, monitor and administer all the grid related operations ranging from generation to transmission to distribution on the click of the button. The cloud technology for data storage, management and monitoring involve extensive

processing power that require dedicated resources are usually implemented in a distributed manner to fasten up all the computations. The examples of various areas of big data management applications include energy management, dynamic demand response management, suggestions for billing and dynamic pricing for clients, trading system, auto-alert systems, market management, outage management, transmission management, distribution management, meter data management and so forth.

5. Privacy Objectives

Authenticity and Authorization. Authenticity refers to data that comes from a trusted source whereas authorization refers that only authorized users or personnel should be permitted at any time to access sensitive information and specific operations as the cloud users or users of smart meter system. Again the challenge lies both in trust building and providing the same level of authenticity in all communication phases in the heterogeneous infrastructure of the cloud. With different computing capabilities of different hardware, the deployment of same key infrastructure to implement cryptographic measure such as digital signature may not be trivial.

Access control and Integrity. Access control is yet another critical component where correct policies need to be implemented to identify involved entities in time appropriate manner for the purpose of data availability. This is to control the consumption behaviour of smart meters and all applications taking part in the public cloud. Integrity refers to data originating from the cloud or from the smart meters must not be altered so that they can be trusted at every step and state of the communication process.

Data privacy against Utility. Smart meters are capable of reading data from each appliance-the refrigerator, kettle, toaster, washing machine etc. since each of these devices has its own energy fingerprint, or appliance load signature, A glimpse on these data can easily reveal accurate information what appliances a consumer uses and how often. Hence, a common worry for consumers is that intelligent monitoring devices such as smart meters, which may transmit power-usage information to the utility as frequently as every 15 minutes, would make them vulnerable to thieves, annoying marketers, and police investigations etc. In order to further discuss this critical issue, figure 3 provides example of hourly measurements of household energy. Such daily measurements of energy usage reveal whether a house is inhabited or not, indicating when the inhabitants are away for a weekend, or for a couple of weeks, on holidays etc. More frequent measurements can reveal even more information. For instance, devout people of certain religion gets up at five in the morning for their first prayers, and can thus be singled-out, with some level of certainty. Similarly, long-term detailed insight in power consumption can enable data mining and profiling in various ways. For instance, the utility provider operators can observe certain patterns, like when the fridge switches on and how much electricity it uses, the operators can even observe if such a fridge becomes old or less efficient and needs to be replaced soon etc. Efficient engineering to protect consumer privacy without compromising the benefits of smart meters is the challenge where research contribution is underway. The review presented in this survey, is centered around this privacy objective. However, building the trust in such engineering schemes is still a not won war which makes confidentiality to be a significant property of communications between smart meters and cloud. Specific measures are required to provide it, especially on the public cloud platform.

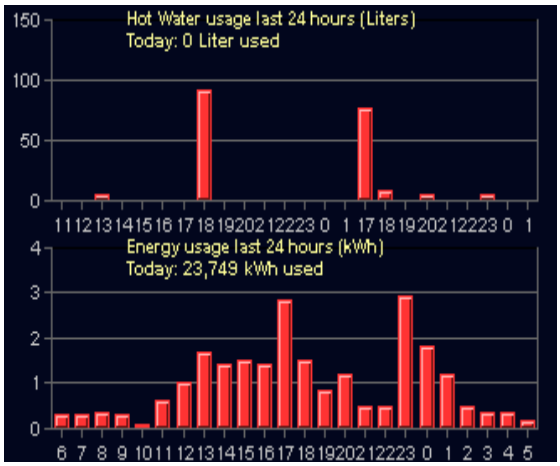

Figure 3: Ex. for hourly measurements of energy from bwired.nl

6. Defense Mechanisms

6.1 General guidelines

A few defense mechanisms for cloud based smart meter data is provide in [19] by Ghansah and in [30]. First, Ghansah argues to implement stringent well defined policies for password and authentication, and

regularly audit these policies to help ensure that the policies are properly being followed and abided. Any deviation to these policies should be tackled by the management in an unbiased and strict fashion. The popular DNP (distributed network protocol) and SCADA (supervisory control and data acquisition) protocol that are used with smart meter data communications suffer from replay attack, message spoofing attacks, sniffing attacks, response delay attacks, network scanning attacks etc. Hence, layered approach such as installation of IPS (intrusion protection system) and IDS (intrusion detection system), fine grained firewall rules and software updates in timely fashion should be carried out. Intrusion prevention and detection systems play a vital role to provide a robust mechanism to detect even the latest attack/intrusion types by anomaly detection process. Well formulated firewall level can help to combat DOS (denial of service) attack by implementing rate limiting technique in addition to unauthorized network connection requests, network scanning attacks and various backdoor attacks. Digital signatures and proofs of storage should be used for keeping the integrity of the data. On the other hand, operational privacy can be achieved by using private information retrieval, searchable encryption and anonymous routing. Ghansah further describes that it is mandatory to update the underlying software, applications and operating systems with the latest patches and updates [19]. Significant importance should be given in the application design phase to protect the cloud services against common attacks like zero day attacks, buffer overflow attacks, heap overflow attacks etc. Smart grid network (SGN) is a complex network connecting billions of devices and users together, so is the patch updating process [19]. The importance of producing temper proof devices or smart meters to enhance physical security is also emphasized.

While the discussion in [19], [30] is healthy mainly for overall security of cloud servers dealing with meter sensitive data, the report fails to identify client privacy deeply in terms of data being interpreted by the employees of service providers which is the central focus of this review. However, the authors do mention to educate the employees for social engineering attacks. But this still does not solve the privacy-preserving billing and barter of energy between the utility provider and the smart meters. In fact, previous studies [22] have shown that energy signatures of home appliances can be used to remotely eavesdrop at activities within homes, thus exposing a wealth of private information to anyone with access to such usage data. Furthermore, even when not all appliances can be identified within a person's electricity profile, the surrounding context and the use of statistical tools along with information that is willingly shared in the Internet can be used to intrude at the life of individuals [26].

6.2 Encryption

Wang *et al* proposes that smart meter clients should encrypt their data using their own key and store encrypted data in the cloud [39]. As a result, each user can securely access and retrieve data from the cloud without compromising data privacy. In addition, without sharing any secret keys before computation, arbitrary combinations of additions and multiplications can be efficiently evaluated on data of multiple users without revealing the inputs, intermediate or final results to the cloud. The proposal is significant in the sense that the computation is non-interactive to clients and hence clients only need to provide encrypted data initially and remain offline until they receive the encrypted output. The phenomenon here is to use the model of two non-colluding cloud servers which has been previously used in [13], [29], or outsourcing using multi-party computation. Single-server model may not completely eliminate interactions between the user and server because of the impossibility of program obfuscation. Therefore, two cloud servers belonging to two different cloud service providers can be used to free users from interactions in secure outsourced computation which is referred as multi key model. Due to the concerns of privacy leak in the cloud, each user encrypts its outsourced data under its own public key before outsourcing to cloud server A. As a result, multiple keys operate the outsourced computation over encrypted cloud data, hence all the data stored on cloud server A are encrypted, so as all the data transferred between cloud server A and cloud server B during the computation. The transfer of data may also be further blinded which is the purpose of multi key model. This design seemed to be elegant in terms of privacy, since neither of the two cloud servers is able to reveal the content of each user's data, intermediate or final results of outsourced computation. Moreover, users are totally free from interactions during the computation since the outsourced computation in the cloud does not require any interactions among users or between a user and a cloud server. However, the work is only tested under small message space. The underlying proxy re-encryption schemes used in the work can only support a small message space which may limit the practical

application of the work dealing with big data space in real time. It is apparent that the number of smart meters in the network may vary from some few thousand to several millions indicative of the usage benefit of elasticity feature of cloud computing.

Wen *et al* [40] argue that widely studied approaches such as public key encryption with keyword search (PEKS) for data privacy are limited to equality checks. They addressed the privacy issues in financial auditing under Privacy-Preserving Range-Query (PaRQ) scheme over encrypted metering data. This scheme addresses the data confidentiality and privacy problem by introducing an HVE (Hidden Vector Encryption) technique. Several work on HVE technique is available in the literature [10], [31] which basically suggests that two vectors over attributes are associated with a cipher text and a token, respectively. Under a translator, the cipher text matches the token if and only if the two vectors are component wise equal [10].

The PaRQ allows a smart meter client to store metering data on a cloud server 1 in an encrypted form and the related encrypted key in cloud server 2 via middle tier called, control center (see figure 4). When the client data is needed for instance for billing or auditing purpose, only an authorized requester (to particular cloud servers) can send its range query to the control center to retrieve the metering data. The control center forwards the query tokens to the requester with which the requester requests the related keys from cloud server 2. Finally, the requester can retrieve data from cloud server 1 via the encrypted keys forwarded from cloud server 2. Here the PaRQ constructs a hidden vector encryption based range query predicate to encrypt the searchable attributes and session keys of the encrypted data. The requester's range query can be transferred into two query tokens, which are used to find the matched query results [40]. Only requesters with authorized query tokens can access the cloud server 2, and they can obtain the correct session keys when their query vectors in the tokens are satisfied with the encryption vectors. This way metering data can be decrypted and encrypted only by the authorized requesters.

Albeit promising, the PaRQ proposes an alternate solution using encryption for privacy of smart metering data by restricting the access of the requester. However, the work failed to benchmark with the usage of other range query techniques such as order-preserving encryption, bucketization etc. and a ready to use techniques out of this for range query schemes while applied under cloud based platforms. As such more investigation is expected to be carried out in this area. Moreover, the authorized requesters still can dig into the appliance load specific data of the clients by performing smart analysis over range of query results. Nonetheless, the simulation work offered in the work shows computation reduction and less communication overhead due to multidimensional parallel data access and the access restriction posed on the requesters.

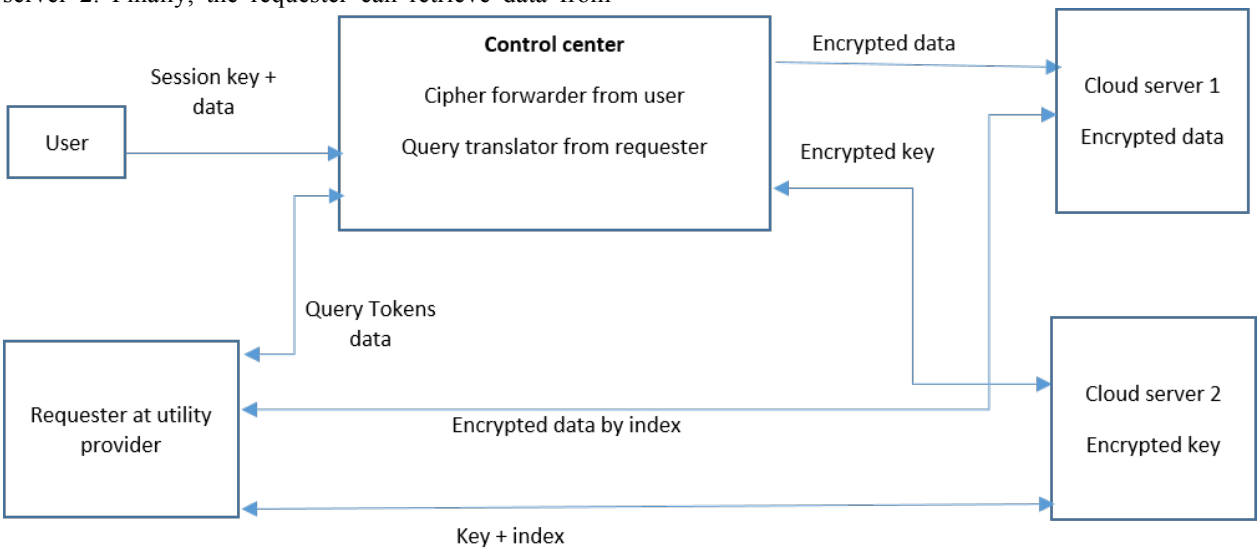

Figure 4: PaRQ Scheme

6.3 Data Aggregation

Data aggregation is another technique among others in order to protect privacy of clients. Importance is provided for efficient and secure data aggregation in [23], [15], [33], [24], [6]. Although the work in [23], [15], [33] did not propose the computation to be done in a control center, rather in a distributed manner using arbitrary set of designated nodes in the networks, the concept is rendered on cloud based platforms in [3], [25], [6]. Efficient encryption can be achieved with effective aggregation process. The ideology here is to divide one specific billing period of a user into a set of time slots. The smart meter deployed at the user's household randomly encrypts the timeslot data and forwards to the local cloud server to perform the encrypted power data aggregation and partially de-blinds the encrypted power data using its own secret key. Due to the aggregation process, the utility company can have the knowledge of the total power consumption for one specific user in the billing period T, but not the user's real-time power consumption. The cloud server should know nothing about the user except the fact that the server assists with data aggregation.

The cloud control center may consist of multiple cloud servers. These cloud servers can be distributed with the energy consumption values of users. Each smart meter (SM) breaks its energy consumption report in disjoint subsets and forwards each one to a replica cloud server. For example, the daily readings can be broken in intervals of e.g., one hour, so that every replica gets a fraction of the original report. This approach may still leak information to a malicious cloud server. However, the disclosed readings may not allow a precise representation of the user activities and profile. Instead of sending plain but partial measurements to different cloud servers, each SM can use secret sharing ([36], [6]) to break its readings in multiple shares so that at least t shares are necessary to recover the original measurement, suggesting at least t cloud servers (CS) are required to obtain individual measurements. The cloud servers can concurrently sum their shares obtained from either different SMs or from the same SM at different times. After that, the summed shares are forwarded to the utility provider (UP) who can recover the collective measurements. By virtue of the homomorphic properties of the secret sharing scheme, the recovered measurement corresponds to the aggregated sum of the individual readings. This way, the UP obtains the total consumption values, but gets no information about individual measurements.

Algorithm 1 below presents the process of distributing trust or secret sharing among cloud servers. Here, each SM generates a random polynomial *r()* of degree *t-1*. Let *g, h* be two generators of a group, such that computing discrete logarithms in this group is computationally hard. Furthermore, let i_x denote the private key of CS_x. and $p_x = h^{i_x}$ is its registered public key. The value *r(0)* corresponds to a secret measurement which is recoverable only when t tuples of the same group are used by the cloud servers (or utility provider) to reconstruct the secret. The public keys of cloud servers have to be known to all SMs. Each SM picks a polynomial with coefficient a_y chosen at random and sets a_0 which is equal to the secret measurement (see step 2 and 3 in algorithm 1). Using the public keys of cloud servers, SM keeps this polynomial secret but publishes the related commitments and the encrypted shares as in step 4. To reconstruct the secret value, each cloud server uses its private key to obtain the share $S_x = h^{r(x)}$ by computing P_x^{1/i_x} (step 5). The final measurement can be constructed by all t cloud servers working together using Lagrange interpolation (*Lx* is a Lagrange coefficient). Refer to [36] for detail interpolation process of step 6.

Algorithm 1: Secret sharing among cloud servers

1) SM knows public key p_x of Cloud Server x (CS_x)
2) SM sets $a_0 =< cons_y, timestamp_y >$
3) SM generates random polynomial, $r(i) = a_0 + \sum_{y=1}^{t-1} a_y i^y$
4) SM publishes to *CSx* the encrypted share: $P_x = P_x^{r(x)}$ and commitment: $C_y = g^{a_y}$
5) Using private key, *CSx* decrypts and computes $S_x = P_x^{1/i_x}$
6) All involved t cloud servers collectively reconstruct, $\prod_{x=1}^{t} S_x^{L_x} = h^{a_0}$

The work presented in [23], [15], [24] are similar in terms of computation effort as they all refer to avoid using computationally expensive homomorphic cryptosystem. Both smart meters and the control center will have strong impact based on the choice of encryption/decryption scheme in addition to data aggregation. Asymmetric encryption is more

computationally expensive than symmetric encryption such as AES (Advanced Encryption Standard) and triple-DES (Data Encryption Standard) etc. It can be noted that in the traditional encryption approach, with no in-network aggregation, each smart meter will encrypt its message once with the public key, while the cloud server needs to decrypt N messages. Whereas with the data aggregation approaches, every smart meter needs to encrypt the message once with asymmetric encryption, but the cloud server device only needs to apply one asymmetric decryption (to the final aggregation result). Moreover, the shared and elastic feature of cloud computing can easily facilitate distributed computation of aggregation (for instance multiplication of the cipher-text) before the availability of data access by the utility provider requesters. However, one may argue that data aggregation may be reverse-engineered with appropriate recognition pattern to track the appliance load signature, and hence the privacy offered depends on trust relationships and data policies that govern aggregators.

Microsoft researchers in [35] suggests the usage of protocol that will involve both aggregation and anonymization using a single cloud server. The meter registers encrypted readings with a server in the cloud using web technologies. Users can access a billing portal, that delivers a web page to perform the privacy preserving computations for billing similar to [6], but using a single cloud server. The control runs on the ASP.NET web-client: it downloads and decrypts the readings and the tariff policy, computes and proves the bill, and uploads it for verification back to the server. The decrypted readings never leave the client side controller. The concept here is to allow users to perform and prove the correctness of computations based on readings of their own devices, without disclosing any fine grained consumption before forwarding for utility approval. This method will require development of robust application that will preserve both user privacy and the accommodation of wider variety of tariff policies. The application must not allow the users to make any unethical changes.

6.4 Anonymization

Georgios Kalogridis and Costas Efthymiou of Toshiba presented a solution in [17] using the technique called data anonymization/escrow. Part of the work was later extended by Dimitriou and Karame in [16] under cloud platform where the report servers perform data escrow. The concept of anonymization presents the same argument as in [23], [15] that the utility doesn't necessarily need to know to whom this data belongs. In other words, energy data, does not need to be tied to a specific household to be useful in managing the grid. An anonymous Internet proxy server can hide a computers IP address before sending data to other networks.
Similarly, Toshibas system would hide a smart meter address before sending energy-usage data to utilities. A third-party escrow service (which cloud be cloud based local distribution controller), would take charge of anonymizing and managing detailed energy-usage data. The escrow service could be the smart meter manufacturer or other trusted party that will communicate with the encrypted data-collecting components embedded in the smart meter. The only identifiable information a utility should be receiving directly from the smart meter would be the information it already receives i.e., billing information and monthly energy use. For this, Kalogridis and Efthymiou introduced two separate IDs to be embedded in the smart meter, rather than a single ID as is the case with standard smart meters: HFID, or High-Frequency ID (anonymous) and LFID, or Low-Frequency ID (attributable). These two IDs are attached to metering-related messages that are transmitted from the smart meter to the utility for the high-frequency and low-frequency metering data [17]. High frequency refers to the meter readings a smart meter transmits to the utility often enough (e.g. every few minutes) to suggest information related with the private life of electrical data user. Low-frequency metering data, which are the meter readings a smart meter transmits to the utility scarcely enough (e.g. every week or month) to offer adequate privacy. It is found in practice that the vast majority of meter readings are sent using the HFID.

The only way for the HFID to be anonymous from the start, and to remain so, is for it to never be known to the utility or the smart meter installer. However a utility needs be sure that messages being received from a specific HFID can be authenticated, i.e. verified to be legitimate, as the utility will not know which HFIDs are valid. Hence, is the requirement of 3rd party escrow service or cloud service provider!

Simply aggregating data would not allow the utility provider to apply demand-side or load shedding management at the smart meter level (which, the escrow service will still allow). Allowing each smart meter to anonymize its data through an aggregator would result in the aggregator receiving a number of anonymous meter readings every few minutes, without any way of correlating these readings with what went on before, which would destroy some of the value of having a

unique anonymous ID per smart meter. Unique anonymous IDs should allow the substation or aggregator to detect electricity theft or similar situations where its own meter readings do not match up with the summation of readings from the individual smart meters that are connected to it. The 3rd party escrow service is further justified for the following reason. Suppose that we simply allow a block of smart meters to aggregate their data in a local area as in [23], [15]. This would apparently hide the parts of the sum attributed to individual smart meters, and the aggregated message can be considered to be anonymized. However, a separate mechanism for authenticating each smart meter is required, and the utility provider should not perform the authentication mechanism in order not to hamper user privacy.

The smart meter manufacturer can assign two unique IDs (just like MAC addresses for IEEE 802.x devices are unique, for example) to each smart meter that is produced, only one of which (LFID) is visible to the utility, both during the procurement and deployment procedures. Essentially, the manufacturer (and, if different, the 3rd party escrow/cloud service provider) is the only party which is aware (and has a record) of the connection between a valid HFID/LFID pair. In this case, strong data privacy policy need to be enforced to be complied by the escrow service provider. For instance, escrow service provider will only know about the relationship between a valid HFID and LFID, and not access or process the stored data. Of course, this solution would require protocols and standardization.

A secure protocol setup mechanism described in [32] is applied for anonymization. The client has to apply for anonymous data profile (ADP) which is when the process of anonymization is initiated by the system. The protocol messages for this process are digitally signed to reassure integrity. They are required to be encrypted too to reassure communications confidentiality. In addition, they should include timestamps and/or a random nonce (number used once) message for added integrity and reliability. Finally, a shared Certification Authority (CA) is used for key management and cross verification purposes. The detailed protocol exchanges are described in [14].

Once the ADP has been set up, the smart meter chooses a random number as an initial meter reading and then proceeds to send frequent updates to the data aggregator. This random number is chosen only after appropriate random time intervals have passed, in order to remove the correlation between LF and HF meter readings that are sent out from the SM. The utility could send a control message to the relevant aggregator which could be forwarded on to the anonymous ID in case any control management is necessary during the process.

Unfortunately, the proposed method by Toshiba researchers [17], [20] may not offer sufficient smart metering privacy protection. The degree of anonymity or conversely the weakness of escrow service depends on the random time interval. The average value of this time interval needs to be large enough to allow a large enough anonymity set to be created. The size of the anonymity set defines the anonymity of ADP. The automated initial set up process of ADP should be intelligent enough to mitigate any passive attacks from utility for non-intrusive analysis that should make it hard to link ADP with clients. If ADP is not set up, then there is no anonymity. Furthermore, the security of ADP setup depends primarily on trustworthiness of the escrow entity. Assuming that ADP process will be kept confidential by the escrow service and the smart meter, it is still difficult to quantify how hard it is for the utility to deduce this secret. Nonetheless, the work contributes an additional layer of security towards the direction of privacy concerns.

6.5 Energy Trade using Digital Currency

The work in [16], [27], [2] go one step further on top of data aggregation and anonymization to preserve user privacy. The work in [27] did not specify whether the system requires a cloud platform. However, M. Alam *et al* in [2] refer that cloud computing can play integral role for the proposed privacy preserving scheme. The use of software driven controller in a cloud platform is a good fit as the testbed [2]. Dimitriou and Karame [16] promoted the work of Toshiba researchers with the help of local community based report or technical servers. The use case scenario of these work is as follows. The smart grid was designed to support the smart integration of the (surplus) energy originating from home owners within the smart grid; home owners can produce energy (e.g., from solar power) and sell their surplus back to the utility provider (see figure 5). This is especially important for small rural areas that are remote from the utility provider. By gathering the surplus of energy from end-users of the grid back to other users of the smart grid, the provider minimizes energy distribution costs and increases the utility of the grid. To promote this scenario, the smart meters will have access to the Internet, at least intermittently, through some open access and secure Wi-Fi

infrastructure. Part of the other assumptions is a secure data storage through a dedicated cloud based transaction server that supports autonomous cryptographic functionality. These can be facilitated via control commands (controller) in an operating system for the smart meters. The controller (which may be hosted by a transaction/cloud server) is able to keep track (if allowed) how much energy is fed or withdrawn into the grid by particular group of users in an area. The buy and sell orders for energy are submitted to a public order-book or database stored in a local cloud server.

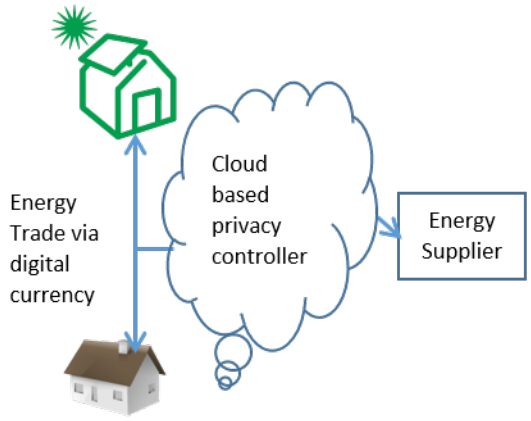

Figure 5 Energy Trade via Bitcoin

The buying and selling of energy among the users is sort of alternate solution to the other solution Toshiba researchers proposed to preserve privacy. The other solution of Toshiba researchers takes an entirely different approach [20]: It anticipates of having an extra rechargeable battery or two and that running a few appliances partially off a battery, rather than directly off the grid, would hide the fact that those appliances are in use. If the battery is connected to electricity supply and intelligently route power from both the battery and the grid to the appliances, then the smart meter will record a very different load signature one that does not identify appliances. It is apparent that some electricity will be lost in the diversion, so there would be a trade-off of some efficiency for privacy. This scheme does not require 3rd party service like cloud of things though how best to optimize both cost and privacy using such a system is still to be decided. Producing and trading energy among the users in an area enhances similar privacy as long as the transaction is unknown to utility provider or the main energy supplier of the area. In the case of anonymous trading within users, the 3rd party cloud structure is required to facilitate such blinded trading.

Digital currency such as Bitcoin [28] can be used to enhance privacy preserving trading of energy due to the anonymous nature of the currency. Bitcoin uses peer-to-peer technology that relies on digital signatures to prove ownership and a public history of transactions to prevent double-spending. Under smart learning mechanism, the cloud based local controller can continuously convert locally produced renewable energy to digital currency based on the rate and price of energy. However, the usage of such currency might not be trivial due to the high volatility in price of Bitcoin and the independent usage policy of users. The governing body of the locality/country may recognize digital currency and provide incentive, may be in the form of tax return if users voluntarily report energy trade. A fixed price for the digital currency can be stamped in the form of a certificate/voucher for such trade that can later be cashed through a financial institution. In order to preserve anonymity of trade, the voucher should not contain distinguisher to relate to participating users in the trade or transaction time.

Bitcoin provides support for making deposits to third parties, in this case the cloud based controller. It allows transactions to be associated with a "lock time"; which as such allows transactions to remain pending until the lock time is exceeded [34]. Here both utility provider or an energy supplier and the client/user can act as either buyer or seller. A transaction can be replaced if both parties agree during a lock time. Based on a heuristic method or some smart algorithm and the local energy demand, the cloud will advertise an optimal price to the clients. A buyer can use Bitcoin to "commit" to a given seller user that the seller will eventually receive a (monetary) reward if the seller correctly executes the required tasks. With the price agreement set, this can be achieved by issuing a transaction with a lock time (e.g., 1 day or 1 month) in committed Bitcoin that requires the signatures of both the buyer and seller (energy producer). Note that the cloud based controller will blind these signatures. The buyer will forward the appropriate Bitcoin to the controller once the transaction agreement is made. No information need to be compromised if the buyer is another user/client, however the seller may have the right to know if the potential buyer is the utility provider or energy supplier of the area. Bitcoin can ensure that transactions cannot be double-spent once they are included in the Bitcoin block chain. Moreover, transactions/deposits can be publicly verifiable by all participating parties in the cloud. This implies that the

deposit of Bitcoin can be blocked by the buyer with the help of controller under the condition if the seller does not inject appropriate energy into the grid or execute the required tasks to honor the agreement.

A typical anonymous trading steps in between home owners via the controller is as follows. Once the price is negotiated, the cloud based controller (or the transaction server) must not negotiate privacy of the users with other users or UP during the process. The appropriate amount of Bitcoin can be forwarded or uploaded by the buyer using a user friendly interface of controller. The controller obtains consumption values and outputs measurements from smart meters and include in the uploaded Bitcoin lock time. If both trading parties agree to register the transaction, only then it is recorded in the order-book with their signatures which is reported to the UP. The controller may generate certificate/voucher on the trade which may later be used for reference purpose. Lastly, Bitcoin is exchanged once the appropriate energy is fed to the buyer's grid. If the home owners do not agree to record the transaction, the controller reports UP only the amount of energy traded to facilitate computing energy savings in the area without knowing the user information and amount of Bitcoin traded [2]. Note that Bitcoin reveals no information about the underlying SM or home owner. In order to ensure that bitcoin are untraceable and to protect the privacy of users, Bitcoin can be blindly signed by UP with a certificate (The signature blinding method is discussed in [11]). Hence, Bitcoins are not associated with a particular user, but solely contain a unique identifier (to track spent Bitcoins only), date, and the amount of energy that the Bitcoin is worth. This ensures that the UP cannot insert distinguishers (e.g., unique identifiers) particularly to track users while signing a given transaction message. This will make sure that no information is leaked about the identity of user throughout the purchase of issuing certificate/voucher and Bitcoin. However, only to prevent double spending of the digital currency, it is possible that the UP keeps track of some unique identifiers of spent Bitcoins (e.g., by means of a hash-table). But that does not harm the user privacy.

Any predefined billing policy used by UP over forwarded consumption values and outputs from smart meters via controller, need to be known by the smart meters in advance, but can be updated on demand through a request to UP. The cloud based controller can be seen as a trusted intermediary whose sole role is to strip away any information that may serve as a quasi-identifier for the corresponding SM. Therefore, the controller will digitally sign the trading consumption tuples and forward to the UP at the end of a billing period without compromising user privacy i.e., via blind signature [11]. In order to make the process more privacy aware, a group signature (furnished in [12]) can be used to authenticate a SM or sign a report, for user to UP trade. To ensure k-anonymity in the signing of SMs, at least k SMs in an area need to hold the same group signature key. The method of aggregation discussed above can be applied by the controller to aggregate these values before forwarding the collective summary to the UP. This will make sure that the trading report masks the individual consumption/fed values, provided that the number of participating SMs is large enough to smooth out individual energy patterns. For very small number of participating users, the cloud based controller can wait till enough information of several energy purchase is available and then randomize before forwarding to UP. The wait period need not to be less than equal to a billing period since the trading report should not affect the monthly bill charged by UP. The timestamp information of trade does not need to be forwarded to UP, rather used for the computation purpose of controller. For user to user trade, the Bitcoin is forwarded via controller (after verifying for double-spending) either at the beginning/end of the energy withdrawn/fed from the grid.

7 Discussion

Generally speaking, the privacy preserving schemes are still under studied compared to smart grid features offered. Based on the work reviewed, the effect of number of participants is well observed most of the time. The encryption work including PaRQ allow users to store their data on cloud servers in encrypted form, and range queries can be executed by using cloud servers computational capabilities. A requester with authorized query tokens can obtain the correct session keys to retrieve the metering data within specific query ranges. It is taken these days no communication scheme would allow data to flow without a secure protocol. Though, the work offers less computation overhead, the scheme needs to be enhanced for large data set. The scheme provides restriction to the requesters' side. However, the tracking of specific times and locations of energy consumption in specific areas of the home may still be vulnerable in this technique. These activities are indifferent whether number of smart meter participants are large or small which is shown in Table 1.

It might be considered practical to let the utility provider create the groups of smart meters whose readings are aggregated based on network topology or

geographical features. In that case, the following attack is possible: Assume the cloud service provider provides the utility supplier with the aggregated energy consumption of, say, groups containing 25 smart meters each. The utility provider could now create a group with one real smart meter and 24 fake smart meters each of which reports a pre-determined value chosen by the utility supplier. By submitting electricity consumption values for each of them and subtracting them from the retrieved sum, it would be easy to compute the actual power consumption of the 25th smart meter. This demands that the total number of real customers is known to the cloud so that attempting this sort of attack can be detected. The work in [4] proposes the cloud to consist of multiple group controllers, each of which controls group of smart meters that do not collide and that are responsible for key management for each group.

The secret sharing via aggregator can provide good privacy if the number of smart meter participants and the number of cloud servers used is large enough (table 1). Otherwise, the security flaws have been identified in [7] for small number of aggregator servers used. In order to reduce costs, it would make more sense, especially for the smaller utility companies, to outsource their data communication and processing operations to a cloud service using virtual machines. A further limitation of secret sharing is that the public keys of the cloud servers need to be available to the smart meters, preferably via bootstrapping phase. This may constraint the cloud service providers to some extent. As such, the smart meters used by households have to be tamper resilient; and the private consumer electricity consumption data is processed in the cloud only for computing the aggregated electricity consumption and will be disposed of as soon as the aggregation is finished.

Table 1: Comparison of Cloud Based Privacy Schemes

Cloud based schemes	Privacy impact for less participants	Privacy impact for many participants
Encryption [40], [39], [13], [29]	Average	Average
Aggregation [3], [25], [24], [6]	Average	Good
Anonymization [17], [20]	Average	Good
Digital Currency [16], [27], [2]	Good	Good

A few flaws in anonymization has been discussed before. In addition to the number of smart meter participants, the ADP setup process depends on client data profile. All smart meters are required to share a Certification Authority (CA) for key management and cross verification purposes. Additionally, they should be encrypted to reassure communications confidentiality. Also, they should include timestamps and/or a random nonce (number used once) message for added integrity and reliability, such as protection against reply attacks. There may be situations where temporary lifting of the anonymity provided by this solution is required. A simple example could be the detection of power theft, e.g. when there is a disparity between the reported meter readings in an area and that of the distribution substation serving that area. Other example includes newly registered smart meters of the area that needs to be included by the existing aggregator cloud. The triggering back of anonymization needs to be graceful enough not have the hiccups of re-setup of the complete ADP.

The trading of energy is a better option regardless of number of users participating. This process encourages energy to be locally produced rather than supplied by energy supplier. The utility provider will not have accurate picture of load signature of the smart meter data. The storage and diversion of energy might incur some energy loss, but anonymous trade is possible via cloud as automated 3rd party trader. In addition, the cloud can apply data aggregation or secret sharing before the forwarding the client data to UP. The scheme seems very sound if client trust is achieved in such use case scenario. However, for the anonymous trade via cloud, a token needs to be generated which could be in the form digital or crypto currency. The price volatility will need to be dealt with. The work in [16], [2] shows how the cloud transaction server can lock down the transaction price of the digital currency used; and generate certificate without inserting any distinguishers to identify a certificate to a client, so that a central bank can be used to redeem the digital currency used for such transaction. To promote this, strict policies need to be enforced so that the revenue agency of the country recognizes such transaction or digital currency (rather than profit making commodity) and may provide tax incentive etc. to the clients who voluntarily discloses such transaction during tax return or so.

Even after all the technology in place, the question remains who or what will implement the privacy aware methods? The work in [9] shows that the solutions involved 3rd party services can provide better privacy.

But the researchers say many consumers don't trust the third party cloud responsible for such operations. What about the cloud security itself? Trust is particularly low in some European countries, where electric utilities have been deregulated and consumers regularly switch providers. Educating clients in a remote area might not be trivial or practical. Robust privacy policies must be made available to smart meter users. They should be given the ability and process to challenge organization-compliance with their state privacy regulations and organizational privacy policies as well as their actual privacy practices. Available choices can be presented to all users to this regard. Only personal information that is required to fulfill the stated purpose should be collected from individuals. Treatment of the information should conform to these privacy principles. Information should only be used or disclosed for the purpose for which it was collected and should only be divulged to those parties authorized to receive it. As the consumer awareness grows, the faster the gap of consumer trust vs cloud based solutions are to be narrowed for the privacy preserving methods to be of any benefit.

8 Conclusions

Most of the available survey literature focus on cyber security and cloud based applications in smart grid whereas the privacy schemes have received low attention. To fill out this void, in this article, we provided a synthesized overview of existing works integrating cloud computing in the existing smart grid architecture, in order to have client privacy preserved for energy supply. It is easy to perceive that the combination of different approaches will result in better privacy although in general networks, they will cause overhead problems or delay issues. For some time-critical operations, limited bandwidth and less connectivity features in the smart grid may hinder the implementation of anonymity for privacy. More in-depth research is required to develop such a promising power grid in the near future. This should include the criteria of robust power theft detection and cyber security while making the smart meter data of clients more privacy aware at the same time. Moreover, dynamic and time-dependent data consumption are to be utilized by the supplier to create predictions of a user's energy demand in the future and as such of the locality. Realizing privacy friendly method for calculating such predictions is another subject for future research. However, one must realize that privacy and the ability to create predictions potentially conflict with each other and this conflict should be investigated further to quantify the trade-off in the field of Smart Metering. Nonetheless, from this surveyed work, we can see that the use of cloud computing applications in smart grid is one of the useful techniques to overcome issues related to smart meter data privacy despite the existence of some technical challenges.

References

[1] Alahakoon D. and Yu X. "Smart electricity meter data intelligence for future energy systems: A survey," IEEE Transactions on Industrial Informatics (future issue) DOI 10.1109/TII.2015.2414355, p. 1, 2015.

[2] Alam M., Li H., and Patidar A. "Smart trading in smart grid using bitcoin," Computer and Information Science, vol. 8(2), pp. 102–112, 2015.

[3] Alohali B., Merabti M., and Kifayat K. "A cloud of things (cot) based security for home area network (han) in the smart grid," in IEEE Eighth International Conference on Next Generation Mobile Applications, Services and Technology, 2014, DOI:10.1109/NGMAST.2014.50.

[4] Alohali B., Merabti M., and Kifayat K. "A secure scheme for a smart house based on cloud of things (cot)," in IEEE 6th Computer Science and Electronic Engineering Conference, 2014.

[5] Armbrust M., Fox A., Grifth R., Joseph A. D., Katz R., Konwinski A., Lee G., Patterson D., Rabkin A., Stoica I., and Zaharia M. (2009, Feb.) Above the clouds: A berkeley view of cloud computing. [Online]. Available: http://radlab.cs.berkeley.edu/

[6] Baktir S. "Privacy preserving smart grid management in the cloud," in IEEE International conference on IT Convergence and Security, DOI:10.1109/ICITCS.2014.7021799, 2014, pp. 1–4.

[7] Bao H. and Lu R. "Comment on privacy-enhanced data aggregation scheme against internal attackers in smart grid," IEEE Transactions on Industrial Informatics, DOI 10.1109/TII.2015.2500882, 2015.

[8] Bera S., Misra S., and Rodrigues J. "Cloud computing applications for smart grid: A survey," IEEE Transactions on Parallel and Distributed Systems, vol. 26, p. 1477, May 2015.

[9] Bohli J., Sorge C., and Ugus O. "A privacy model for smart metering," in IEEE International Conference on Communications Workshops, DOI:10.1109/ICCW.2010.5503916, May 2010, pp. 1–5.

[10] Boneh D. and Waters B. "Conjunctive, subset, and range queries on encrypted data," in in Proc. TCC, 2007, pp. 535–554.

[11] Chaum D. Blind Signatures for Untraceable Payments. 10.1007/978-1-4757-0602-4.18: Springer-US, 1983.

[12] Chaum D. and Heyst E. Group Signatures. Volume 547 of the series Lecture Notes in Computer Science pp 257-265: Advances in Cryptology EUROCRYPT, 1991.

[13] Chow S. S. M., Lee J. H., and Subramanian L. "Two-party computation model for privacy-preserving queries over distributed databases," in in NDSS, 2009.

[14] Dent A. W. and Mitchell C. J. User's guide to cryptography and standards. Artech House, 2005.

[15] Dong X., Zhou J., Alharbi K., Lin X., and Cao Z. "An elgamal based efcient and privacy-preserving data aggregation scheme for smart grid," in 2014 IEEE Globecom Wireless Networking Symposium, DOI: 10.1109/GLOCOM.2014.7037553.

[16] Dimitriou T. and Karame G. "Privacy-friendly tasking and trading of energy in smart grids," in ACM Proceedings of the 28th Annual ACM Symposium on Applied Computing, Mar 2013.

[17] Efthymiou C. and Kalogridis G. "Smart grid privacy via anonymization of smart metering data," in IEEE 1st conference on Smart Grid Communications, DOI: 10.1109/SMARTGRID. 2010.5622050, 2010, pp. 238 – 243.

[18] Genge B., Beres A., and Haller P. "A survey on cloud based software platforms to implement secure smart grids," in Proc. IEEE Power Engineering Conference (UPEC), 49th International Universities, DOI: 10.1109/UPEC.2014.6934607, 2014, pp. 1 – 6.

[19] Ghansah I. "Best practices for handling smart grid cyber security," California Energy Commission, California State University Sacramento, Tech. Rep., May 2014.

[20] Kalogridis G., Denic S. Z., Lewis T., and Cepeda R. "Privacy protection system and metrics for hiding electrical events," International Journal of Security and Networks (IJSN), special issue on security and privacy in smart grids, vol. 6(1), pp. 14–27, 2011.

[21] Kaur K. and Kumar N. "Smart grid with cloud computing: Architecture, security issues and defense mechanism," in Proc. IEEE Industrial and Information Systems (ICIIS), 9th International Conference on, DOI: 10.1109/ICIINFS.2014.7036578, 2014, pp. 1 – 6.

[22] Lam H. Y., Fung G. S. K., and Lee W. K. "A novel method to construct taxonomy electrical appliances based on load signature," IEEE Trans. on Consumer Electronics, vol. 53, pp. 653–660, May 2007.

[23] Li F., Luo B., and Liu P. "Secure information aggregation for smart grids using homomorphic encryption," in Smart Grid Communications (SmartGridComm), First IEEE International Conference on, DOI: 10.1109/SMARTGRID.2010.5622064, 2010, pp. 327 – 332.

[24] Li F., Luo B., and Liu P. "Secure and privacy-preserving information aggregation for smart grids," International Journal of Security and Networks (IJSN), special issue on security and privacy in smart grids, vol. 6(1), pp. 28–39, 2011.

[25] Maheshwari K., Lim M., Wang L., Birman K., and Renesse R. "Toward a reliable, secure and fault tolerant smart grid state estimation in the cloud," in IEEE conference on Innovative Smart Grid Technologies (ISGT), DOI: 10.1109/ISGT.2013.6497831, 2013, pp. 1–6.

[26] Molina-Markham A., Shenoy P., Fu K., Cecchet E., and Irwin D. "Private memoirs of a smart meter," in In the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Eciency in Buildings, Zurich, Switzerland, Nov 2010.

[27] Mihaylov M., Jurado S., Avellana N., Moffaert K. V., M. de Abril I., and Nowe A. "Nrgcoin: Virtual currency for trading of renewable energyin smart grids," in 11th International Conference on the European

Energy Market (EEM), DOI: 10.1109/EEM.2014.6861213, 2014, pp. 1–6.

[28] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system, 2008. [Online]. Available: http://bitcoin.org/bitcoin.pdf

[29] Nikolaenko V., Weinsberg U., Ioannidis S., Joye M., Boneh D., and Taft N. "Privacy-preserving ridge regression on hundred of millions of records," in in Proc. IEEE Security and Privacy, DOI: 10.1109/SP.2013.30, 2013, pp. 334 – 348.

[30] NIST. (2010, Aug.) Guidelines for smart grid cyber security (vol. 1-3). [Online]. Available: http://csrc.nist.gov/publications/PubsNISTIRs.html

[31] Park J. "Efficient hidden vector encryption for conjunctive queries on encrypted data," IEEE Trans. on Knowl. Data Eng., vol. 23, pp. 1483–1497, Oct. 2011.

[32] Pfitzmann A. and Hansen M. Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management a consolidated proposal for terminology, 2006. [Online]. Available: http://dud.inf.tu-dresden.de/

[33] Rajagopalan S. R., Sankar L., Mohajer S., and Poor H. V. "Smart meter privacy: A utility-privacy framework," in IEEE Smartgrid Communication, Cyber and Physical Security and Privacy, Oct. 2011, pp. 190–195.

[34] Reid F. and Harrigan M. "An analysis of anonymity in the bitcoin system," in Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third Inernational Conference on Social Computing (SocialCom), DOI: 10.1109/PASSAT/SocialCom.2011.79, 2011, p. 1318 1326.

[35] Rial A. and Danezis G. "Privacy-preserving smart metering," Technical Report Microsoft Research, 2010.

[36] Schoenmakers B. "A simple publicly verifiable secret sharing scheme and its application to electronic voting," in In Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology, 1999, pp. 148–164.

[37] Simmhan Y., Kumbhare A. G., Cao B., Prasanna V., and Hsieh M. "An analysis of security and privacy issues in smart grid software architectures on clouds," in Proc. IEEE 4th International Conference on Cloud Computing, 2011, DOI: 10.1109/CLOUD.2011.107.

[38] Subhani S., Gibescu M., and Kling W. "Autonomous control of distributed energy resources via wireless machine-to-machine communication; a survey of big data challenges," in Proc. IEEE 15th International Conference on Environment and Electrical Engineering (EEEIC), DOI: 10.1109/EEEIC.2015.7165381.

[39] Wang B., Li M., Chow S. S. M., and Li H. "Computing encrypted cloud data efficiently under multiple keys," in Communications and Network Security (CNS), 2013 IEEE Conference on, DOI: 10.1109/CNS.2013.6682768, 2013, pp. 504 – 513.

[40] Wen M., Lu R., Zhan K., Lei J., Liang X., and Shen X. "Parq: A privacy-preserving range query scheme over encrypted metering data for smart grid," IEEE Transactions on emerging topics in computing, Digital Object Identifier 10.1109/TETC.2013.2273889, vol. 1, pp. 178–191, 2013.