ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 6, 1278-1285 (2020)

www.astesj.com

ASTESJ

ISSN: 2415-6698

Time Granularity-based Privacy Protection for Cloud Metering Systems

Hesham Aly El Zouka[*,1], Mustafa Mohamed Hosni[2]

[1]Computer Engineering Department, Arab Academy for Science, Technology, and Maritime Transport, Alexandria, 22206, Egypt

[2]Managing Director of OMIKRON Technologies, Electrical Engineering Department, Alexandria Faculty of Engineering, Alexandria, 22206, Egypt

ARTICLE INFO

Article history:
Received: 22 August, 2020
Accepted: 25 September, 2020
Online: 16 December, 2020

Keywords:
Smart Meter
Zero Knowledge Proof
Authentication
Security
Privacy
Cloud

ABSTRACT

Due to the advent of cloud computing and Internet of Things, smart meters have become a crucial part of smart cities. Smart meters generate vast amounts of fine-grained data that can immediately provide useful information to electricity consumers, such as automatic billing, load monitoring, and dynamic time pricing. This will make the electricity consumers more energy-efficient and self-organized in IoT and cloud computing technology. Smart meters also enable two-direction flow of energy and balance the measurement of inflows and outflows of energy between the meter and electric utility's central system through remote reporting. Besides, they help designers integrate renewable energy generation, such as solar rooftops to cover remaining energy needs. However, smart meters entail some severe security challenges. From a security point of view, these meter readings have a potential threat on personal privacy and the collected meter data. They may also reveal some details about consumer's lives. Thus, the data acquisition from those meter readings is expected to incorporate privacy requirements and application demands. In addition, the collected raw data from various meter readings needs to be collected from IoT smart metering sensors and stored in the cloud to be accessed and analyzed by electricity consumers. Subsequently, this considerable information Is prone to privacy threats and security vulnerabilities as the transmission of data to the cloud is most likely to cause a data breaching. In this paper the privacy and confidentiality of meter readings is protected through trusted platform module, which will allow the electricity provider to get the energy consumption at a periodic time granularity.

1. Introduction

The future smart meters are expected to provide details on individual appliance consumption and enable customers to access electricity safely and economically [1]. These technologies lead the trend to shift from conventional power grid to smart grid that uses sensors, smart meters, advanced communication systems and information technologies to create monitoring and visualizing real-time electricity information. But these technologies pose threats to individual's privacy as they can simply reveal one's daily activities [2]. Fine-grained electricity consumption aggregation scheme for smart meters can be used to reveal some information about consumers' lives and their activities. It can be also used to detect the presence or absence of occupants [3], [4]. In addition, transmitting the smart meter data to private or public cloud storage will allow the household consumers to monitor their usage, change their energy habits, adjust their electric power consumption, and give them better management to their energy costs. Real-time monitoring, then, can be accessed via the cloud using mobile browser, or any PC/Mac browser in the world. Subsequently, these meter readings and information are prone to privacy and security threats as the transmission of data to the cloud is most likely to cause a data breaching. In this paper, a storage outsourcing in the cloud is considered secure where the external storage is often untrusted or only semi-trusted. In addition, privacy-preserving analytics for IoT and cloud-based smart metering system is ensured by using a trusted hardware module which is used in conjunction with generated random number generator. The proposed framework guarantees an

[*]Corresponding Author: Hesham El Zouka, AAST, P.O. Box: 1029 Alexandria, Egypt, helzouka@aast.edu

https://dx.doi.org/10.25046/aj0506152

improved secure data storage of IoT smart meter reading and provides real-time measures of electricity consumption and the estimations of the consumption during operations.

In this system, the consumer grants the service company a meter reading request service at a time of charging and the granted utility company is only allowed to get the power readings during that granted time. This system also provides practical security measures and protects the privacy of consumers who have smart meters at their homes. Also, a privacy model is provided here to achieve the privacy requirement and experience that the proposed system may have a significant effect on privacy-preserving systems if the system is built under the assumption that the utility provider is semi-honest.

In addition, strong access configuration and authentication management protocols should be constructed in IoT - cloud outsourcing process, and any unauthorized access should be utilized and reported. Moreover, due to the lack of privacy and security issues, sensitive personal data can be revealed to third parties such as utility companies and cloud service providers. Today, energy might be collected and stored for future use as per demand. Additionally, data analysis programs can be used to improve the efficiency of power consumption of a particular meter.

It is true, of course, that adding memory or a processor to the smart meter will enhance its security services capabilities, but contradictorily, the cost of implementing these smart meters will be increased dramatically. The proposed security system in this paper is designed to support multiple time segment granularities and let the meter readings to be stored securely on the cloud. It also comprises the design, construction, and operation of proposed two-way communication scheme, which ensures secure and reliable connections between the smart meters and getaways.

The rest of this paper is structured as follows. Section II discusses the architecture and characteristics of smart metering system with the cloud computing. The related work is given in Section III. The system design and modeling are presented in Section IV. Results in terms of system implementation, authentication, security and privacy are presented and discussed in Section. V. The performance analysis of the proposed system is discussed in Section VI. In the final section, the conclusion and future work are presented.

2. Cloud Metering Infrastructure

Smart technologies like the IoT, artificial intelligence (AI), and other digital technologies are providing new opportunities to smart grid network, and can be used to control, monitor, maintain production, transmission, and consumption of electricity in smart metering systems. Many benefits could be obtained through the deployment of the smart grid services in cloud computing, in order to achieve energy savings. Cloud computing is also used to speed up communication with telemetry devices [5]. Moreover, power grid technology can be combined with smart meters to reduce the energy consumption in the peak demand and, hence, improve cost savings.

However, fine-grained technical approaches can cause security and privacy concerns for smart meter users. Current smart/interval meters can record electricity consumption in 30-minute intervals; however, the new generation of smart meters use more advanced technology and could convert all time units to seconds. Mechanisms for large-scale distributed sensor networks and other complex issues are likely to be addressed in order to prevent personal privacy from being breached and prevent revealing detailed information of one’s daily activities. It should be made clear that smart meters record the energy usage exactly in the same way as the standard meters, and send this data to the consumers and the utility provider, on a required time interval, which allows consumers to monitor their power consumption at very fine time granularities. As opposed to the conventional method of electricity billing [6], the proposed approach does not require a person from the electric companies to read the number of units of energy consumed in the meter. The proposed system can play an important role in minimizing overall energy consumption and, hence, making significant contribution to energy efficiency and power saving.

One of the most important aspects of the proposed privacy-preserving energy scheme is its capability of providing a fine-grained smart meter access, while preserving the privacy of consumers based on an encryption scheme.

Therefore, the proposed fine-grained anonymous metering system will encourage consumers to use limited electricity during peak hours, especially when energy demand is high and inform them with their consumption patterns, and challenge them to fully utilize potential while saving costs. Finally, a Load Monitoring Center (LMC) will be introduced in attempt to access the sum of meter readings from various smart meter-time resolutions (e.g. half-minute, one minute, five minute, etc.).

Some previous studies have focused on privacy, security, and accuracy issues of plug load monitoring system in smart grid environment [6]. Other related studies have focused on payment predication and automatic bill generation. Various privacy-preserving models were proposed to protect the individual's privacy and minimize the energy consumption [7]. However, most of the corrupted meters will disclose the activities of users by measuring their usage frequency. Furthermore, cyber security can be utilized to characterize the surrounding magnetic field of smart meter, which in turn will expose some vulnerabilities with the data being transmitted from smart meters. To solve such problems, many researchers have developed and investigated a wide variety of approaches over the years in order to prevent disclosing the consumer living activities and invade their privacy. In this paper, cloud computing offers an alternative storage model to the traditional in-house smart meter model. This is a quite effective way, so that the data stored in the cloud will be secured by using multiple levels of encryption and, hence, only authenticated consumers would be getting access to it. All meter readings will be read at specified time intervals and readings will be stored in a secure cloud-based server which will be accessible from anywhere through a web browser or any mobile device. The meter reading privacy will, then, be protected within the cloud environment, and, as a result, only authorized household consumers will get permission to access the sensitive content in the cloud.

The Cloud metering system (CMS) proposed here consists of three main parts: trusted identity module, cloud storage unit, and the utility service provider. The trusted identity module is embedded on a smart meter for the purpose of securing the metering services. The external cloud storage allows consumers to do their reading remotely, with no need to buy expensive equipment or hire large IT staffs. The energy service provider pools consumers' services, and demand different time granularities [9]. The proposed model has a mechanism to manage and grant meter readings to the utility company at specific time and date.

The utility company, then, can get energy readings at specific time intervals by analyzing meter data stored in the cloud. Meter readings are securely sent over the mobile network to be stored in the cloud for monitoring and analysis purposes. The meter construction and two-way communications capability will enable the system to process remote connections and disconnections of power service [10], [11]. The smart meters have the ability to measure, store, and report both energy inflows and outflows [12], [13]. The utility provider then, aggregates the consumption data from the storage system on the granted date in order to balance between the privacy requirements and the functionality of the system. Also, a privacy model is considered, as the meter readings should not be exposed to unauthorized persons or processes during transmission, storage and retrieving [14], [15]. Figure 1 illustrates the construction of the proposed CMS model.

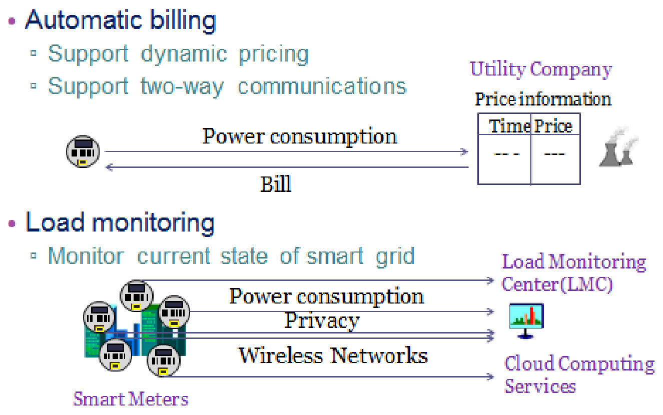


Figure 1: CMS Architecture

Clearly, the privacy is preserved by hiding smart meter's individual readings. Thus, sensitive data should be inaccessible to eavesdroppers. For example, data utilization, visualization, detection of emerging failures, centralized and decentralized operations and controls, all need to be considered when designing a secure network. There are complex security requirements to be deployed either on the cloud or on the smart meter with potentially limited resources like authentication and ID management. Thus, strong authentication protocols should be implemented in the cloud network to provide protection against privacy violations. Meanwhile, unauthorized users are rejected through the use of access control or privacy features. Without cloud, smart meters cannot preserve consumer privacy and confidentiality. On the other hand, sensitive data or meter readings should be encrypted before being outsourced to the cloud. [16], [17].

3. Related Work

Different secure architectures and data aggregations have been proposed to reduce the cost of digital signatures in smart meters. All these schemes aim to protect the transferred readings of energy data. There are different types of smart metering architectures, some are of a meter and others are of many meters. The former contribute to the billing applications and the later contribute to applications such as load monitoring.

Aggregation and the role of Trusted Third Parties (TTP} has been discussed in [18]. The role of a trusted third party is to validate and safeguard protected meter readings on the basis of privacy policies of third party services. Others have used cryptographic primitives. [19]-[21], for example, smart meters can greatly benefit from accessing cloud processing and storage services if security measures, like homomorphic encryption, are applied. This can be achieved by encrypting smart meter data before storage takes place in the cloud.

This model is quite unique when it comes to the aggregation of meters' readings using zero knowledge protocol and tamper proof signature.

As for [22] and [23], they replaced tamper proof signature by TPM. Mc Laughlinet al [24] propose an approach to privacy-preserving data aggregation being transmitted using a random noise. This random noise must be chosen in a manner that is transparent and does not affect the validity of aggregated data from smart meters. They also presented a privacy-preserving technique that is based on inserting the result of three aggregation functions for any given neighborhood in a short time period ψt. Based on these functions, the aggregation technique is implemented in such a way that the aggregator can produce an accurate aggregate number while maintaining the confidentiality of individual meter reading.

Moreover, [25] have proposed an approach that can utilize privacy settings on smart meters by using secret sharing scheme combined with symmetric encryption. The paper [26] has proposed a hybrid approach that uses random noise and pseudorandom sequences to preserve the privacy of readings collected from smart meters. Their proposed system supports load monitoring and billing applications as they claimed in their paper. However, most of the privacy preserving approaches in smart metering systems concentrate on the sensitivity of meter readings in attempt to protect time-series in general and not designed for very fine time granularities. Also, it is not clear which reading is considered sensitive and how it should be handled. While privacy-preserving solutions have been studied, users' privacy concerns have been not fully defined and the privacy of smart meter readings has not been formally addressed. Currently, many gaps exist between linking the meter readings to the status of specific applications. Appropriate regulatory protections vary from one application to other.

In this paper, the privacy of smart meter users is preserved by providing a flexible platform that supports multiple time granularities. In addition, the provided storage services of these smart metering systems are highly dependent on the cloud infrastructure. To ensure authenticity and integrity, a trusted platform module will be employed in this paper. The suggested module will be used to create signatures over the data to be signed.

4. System Design and Modeling

In this section, time scale notation, metering system and the proposed security model are described along with a brief introduction to the proposed privacy requirement.

4.1. Time Scale Notations

At the lowest level of time granularity S1, time is divided into several time units T1, T2, ….,Tn of 1 ms. Each time interval unit Ti is allocated to weight wi. At the startup routine, all the weights are equal, and the system entity structures extension to integrate weight hierarchies and time granularities into real time workflow. Automatically, a time granularity S is defined to support different applications. An example of three different time granularities, S1 , S2 and S3is shown in Figure2.

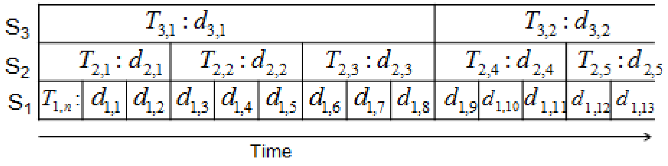


Figure 2: Time Granularities System

4.2. Smart Metering Process

The proposed metering system consists of a meter, an external cloud storage platform and the cloud service provider SPi which has a key pair: a public key (PK1) and a private key (SK1).

Figure3 shows an example of the proposed platform with a cloud computing architecture. Supposedly, a meter is fully trusted and the storage platform as well as the cloud service provider are honest, as they follow specific procedures in extracting individual meter readings from storage devices and communication links. If a consumer has a meter SM that records energy consumption d_1 at time unit T_1, H agrees time granularities Si with different service providers SP_i, and constructs SM by storing S_1.

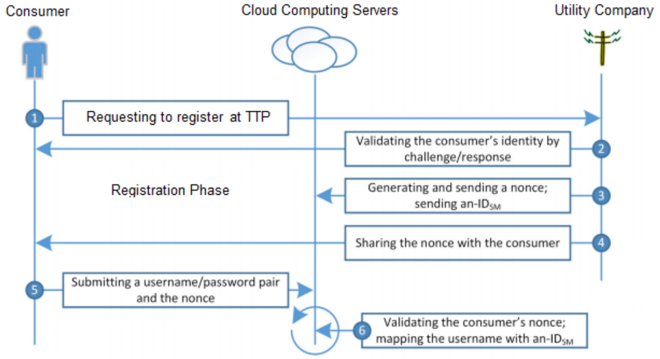
Meter M, then, encrypts the meter reading d1 as C_1 and stores C_1 into the cloud storage system. By getting the access right at a given time granularity S_i, an energy consumption di at time interval T_i is a sum of meter readings:

$$d_i = \sum_{S=(j-1)/i+1}^{j} d_1 \tag{1}$$

The proposed model consists of 3 layers, hardware layer, application layer and Kernel layer. The hardware layer consists of all hardware modules including the precision measurement unit, the platform module and a communication and processing module. As for the kernel layer, it has a set of modules that interacts with hardware layer. Then comes the application layer that is constructed upon the kernel layer to offer facilities such as cloud network management service, transaction service and web edge for monitoring current meter readings which can be stored on the cloud. This allows easy access to such readings from anywhere through any web-based interface application.

5. Trust Assumptions and Security Requirements

The meter readings can be transferred directly to the cloud using a Trusted Third Party (TTP) encryption, which is responsible for the registration of consumers and servers. TTP can manage meter data using standard Internet connections and has the capability to provide data confidentiality, data integrity and fraud prevention. Due to these capabilities, the consumers can utilize the best authentication and registration features. Hence, home residents can easily monitor and control home electricity facilities through computer and smart phones over the TTP. The whole registration, authentication method is illustrated in Figure 3.


Consumer
Cloud Computing Servers
Utility Company
1
Requesting to register at TTP
2
Validating the consumer's identity by challenge/response
Registration Phase
3
Generating and sending a nonce; sending an-ID_{SM}
4
Sharing the nonce with the consumer
5
Submitting a username/password pair and the nonce
6
Validating the consumer's nonce; mapping the username with an-ID_{SM}

Consumer Authentication Process

The residential home has local renewable resources, energy storage and electrical appliances that are able to adjust power consumption behavior and predict demand-capacity. It then works with a set of service providers as each service provider primarily delivers access of meter readings at a time periodically. In addition, each network/service provider SP_i with a key pair (private and public) has a demanded time granularity Si, and the startup time at the initial time granularity $T_{i,j}$ can be approximated by the following equation :

$$T_{i,j} = \left(\sum_{v=(j-1)/si+1}^{j} T_i \right) modN \tag{2}$$

Therefore, a network provider can compute the energy consumption di at time Ti by editing the encrypted meter readings as long as it knows a random value ri of sometime unit Ti . Then, the energy consumption di can be easily calculated by the following equation:

$$T_{i,j} = \left(\sum_{v=(j-1)/si+1}^{j} \mathrm{d}_i \right) modN \tag{3}$$

The consumer appliances, local renewable energy generators, smart grid utility will all be connected by the cloud and controlled by smart home meter which has the skill of getting consumption information from cloud services.

This smart-home meter is also capable of static scheduling and runtime scheduling to reduce the total cost of electricity energy while sustaining power requirements [27].

From security point of view, the consumer appliances should give the corresponding random numbers rito SPi in order to permit the right access of meter reading at a specific time Si to a network provider SP$_i$. In order to reduce the communication cost of random number ri derives the next one r$_{i,j+1}$ by using a shared PRNG where a random number is generated so that the equation would be:

$$r_i = \left(\sum_{v=(j-1)/si+1}^{j} T_i \right) modN \tag{4}$$

Where the time granularity Si is derived from r1 using the pseudorandom number generator g1. The consumer, then, will securely give ri, Si to the service provider SPi in order to grant the right access. SPi can consequently, derive other random numbers.

5.1. Trust Model

Let h be a crypto system and has h function where the encryption and decryption procedures used by the network provider SP$_i$ to authenticate the communication parties and to create a secure connection. The consumer will, then, share random number generator g: with SP$_i$, correspondingly. Then, the consumer will configure a meter SM by setting initial state number of a specific time Si.

The TPM and SM will generate a master key K by the using a seed θ, the sequence number SN and the hash algorithm h. The session key k is securely saved in the TPM of SM which creates a seed key K$_i$ by using the session key K and description D$_i$. M, then, computes r$_i$, and encrypts it by using public key PK$_i$ as r$_i$ and stores n$_i$ to the external data storage system.

5.2. Usability Goal

Permanent data storage mechanisms are urgently needed for the development of smart-meter system which aims at reducing the electricity cost at a residential home by scheduling the power demands according to a rich set of power – related data that can describe the dynamic status of smart grid, local power generation, energy consumption of consumer appliances, sensor data, weather data and occupants' activity data.

All this data will be stored in the cloud by a data base that is implemented by MYSQL which will also support queries over data and metadata from the smart home systems.

$$c_i = \left(\sum_{v}^{j\pi i} c_1 \right) mod\ N \tag{5}$$

where $\eta_{i,[j/\pi i]}= enc_{pki}^{i}\ (d_{i,[j/\pi i]})$

Meaning that the service provider SPi gets the encrypted power assumption di of every time unit T$_i$, for j ≥ 1 since di< N. In the next part, the privacy requirement that is proposed here is defined and it is proven that the proposed system meets it. Moreover, it is shown that managing meter data collections and billing are secure.

5.3. Privacy-Preserving Requirement

Privacy here requires that a network provider SP$_i$ cannot get energy consumption di at specific time intervals S$_v$, where j ≥ 1 and v < I. Paying into consideration that if SP$_i$ cannot get energy consumption at specific time intervals S$_{i-1}$, it wouldn't get energy consumption at any time intervals S$_v$ for v < i – 1. The privacy preserving requirement here is to keep the time granularity adapted to a prior time constraints when determining the maximum time boundary. For example, a demand phase continues first when A adoptively gets meter readings di at time intervals T$_1$, j as j = 1 and C returns back to A the encrypted meter readings C1. A, then, specifies to enter the experiment phase at (j* - 1) + 1. A then chooses two challenge sets meter readings for a time ∈ {0 , 1}. The intersection of the two sets is that the consequential di , j* are the same as illustrated in the following equation:

$$\sum_{v=\pi_{i-1}(j^*-1)+1}^{\pi i-1 j^*} d_i^0 = \sum_{v=\pi_{i-1}(j^*-1)+1}^{\pi i-1 j^*} d_j^1 \tag{6}$$

After reading the encrypted meter data, A passes to the second phase. For a second time, A adaptively indicates a meter reading dj for subjective time interval Ti and C automatically returns the encrypted meter reading C1 back to A. Hence, a smart metering scheme satisfies the privacy preserving requirement against a network provider SPi for any probabilistic polynomial time function T bounded adversary A attacking the real process.

Table 1: Implementation analysis of the proposed system

Initialization phase	Computation cost (ms)	Storage cost
Registration phases	≤ 10 ms	1592 B
Generating a nonce number	1.2 ms	2 B
Encrypting a meter reading	< 12 ms	19
Session key exchange	4.3 ms	17 B
Data transmission phase	2.8 ms	68 B

5.4. Storage System Security

The meter readings are shown to be securely stored in the cloud storage devices, bearing in mind that each network provider has more information than the storage devices and that the proposed metering algorithm is securely integrated with privacy-preserving scheme.

The security requirement of cloud storage is the collective processes, technologies and controls that ensure that only authorized and legitimate users can store, access and use storage resources. The attacker A has the same role of the storage system, but without the knowledge of the stored pseudorandom number r. Hence, the metering systems satisfy the secure storage constraints by considering any probabilistic parameterized polynomial time algorithms which are employed by the users during the initialization and the security phases, assuming that all encryption algorithms used by network provider SPi are completely secure.

6. Performance Analysis and Results

The performance of the offered smart metering system is examined in terms of benefit-to-cost ratio and storage cost. Moreover, a specific scenario is considered where four time measures; years, months, hours, and seconds are used in the smart meter. The utilization of the system shows that the time of the generated key is the highest among the transmitted and authentication time.

In addition, the proposed system minimizes the overhead of the authentication process as compared to the other know authentication algorithms in smart metering networks because the key used in transfer time as well as the key used in the verification time produce a lower amount of overhead. As shown in Table 1, it is obvious that the encryption time is the highest among the authentication and transfer time.

It is also obvious, from the table, that the time complexity for key generation is in the order of O(log n) and it takes nearly less than 20 seconds on average to be accomplished. Despite the long generation time and relatively low encryption time, the total key transfer time range is 0.6 to 3 seconds, whereas the total key authentication time range is 0.8 to 5 seconds.

Noticing that the scheduling scheme produces a total of N sub-keys of the size of 32 bits and that the encryption system used by network providers is standard RSA encryption. The proposed system showed that the generated 2048-bit key of RSA algorithm takes significantly longer than the 1042-bit key. A commercial Information on Trusted Platform Module (TPM) chip is used to enhance the performance of cryptographic system in terms of space and speed, which is capable of supporting a 1024-bit signature in 50 ms and 2048-bit RSA signature in 250 ms.

The TPM can be initiated to cope with multiple security services, including the protection and secure storage of the keys. TMP can be used also to cope with RSA algorithm for key signing and encrypting data.

It is also assumed that calculating Si optimal additions is not slower than the estimated time complexity to factor 1024-bit RSA modulus, and the fastest known factorization algorithm requires around 265 times complexity to factor a 1024-bit signature. The task of generating a 1024-bit RSA signature, would take less than 100 ms to be generated.

Thus, the complexity of encrypting a meter reading takes less than 35 ms. Additionally, the storage cost of a meter is considered to be constant and the cost of storing data in the cloud system is analyzed as follows: for each reading, the cloud system stores an encrypted data reading of (log2 n) bits. In order to grant the access right to a network provider SPi, a cipher text is stored in the cloud storage system at the first time interval T1.

Consequently, for every Ti time unit at time granularity S1, an encryption of a nonce digits is stored. In the proposed model, the cloud storage efficiency of encrypted data reading of a month is around 325 MB, and as for the storage cost of encrypted data for a month is about 3.4 MB, which make the overall storage cost of the cloud storage system for a meter system per month is fewer than 126.3 MB.

Level of trust operations of cloud network providers includes encryption, modular arithmetic and the computation of nonce numbers are all within efficient range and work under all standard reference conditions required by secure service providers. The computation efficiency of meter system is analyzed as follows: large keys are converted into small keys by using MD5 hash algorithm and the data encryption takes place during the initialization process.

The calculation in the initialization process is subject to the computation of generated RSA keys. As the encrypting of a nonce takes 2 ms, the initialization itself takes 2 seconds. At T1, the meter reading is encrypted by using the nonce r1 that on average, takes between 10 – 15 ms to be completed.

On the other hand, the efficiency analysis and the security analysis show that the proposed protocol is secure and efficient ; the efficiency is verified by ns2 simulation results, which show a high authentication rate. The average time for the authentication phase is between 1 and 2 ms, and the average time of key exchange protocol is also utilized and was in the range of 1 to 7 ms.

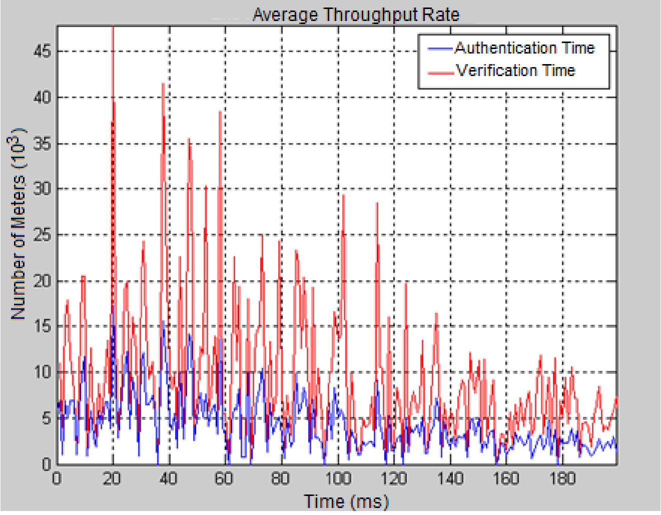


Figure 4: End-to-End Delay

The verification time has been calculated for various security measures in accordance with the key generation time and the key computation time to prevent intruders from decrypting the keys.

The simulation results showed that the elapsed time to complete the verification process including the key exchange protocol and the hash function is approximately equal to the total time required for exchanging of all smart meter readings within the communication channel.

The performance analysis of this system for varying number of meters is presented in Figure 4 and Figure 5, respectively. In the former figure, the measured end-to-end delay between the creation and aggregation of the meter readings at the cloud server and the readings response time at the utility company is illustrated by implementing the authentication protocols.

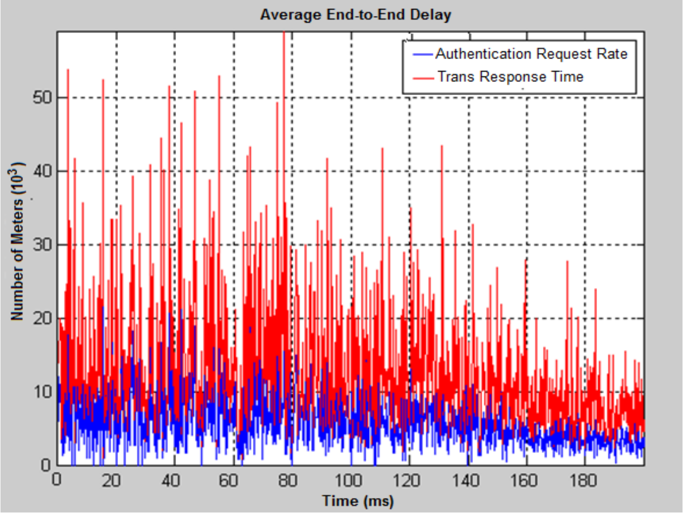


Figure 5: Throughput Rate

Cleary, the delay is affected by the time slot where the meter is assigned in the schedule of time granularity created by the users. Another reason for the increase in the message delay is the computational overheads taking place at the communication layers of the network. Furthermore, the suggested authentication scheme reduced the response time and the communication overhead in the proposed smart metering system because the verification time and the key transfer time produce minimum amount of data overhead. It is noted from Figure 5 that the generation time of the key pair is the lowest among the computation time and verification time. It is clear also from the figure that the generation time of the key-pair was performed in less than 9 ms. When considering the key exchange time over different network bandwidth, the key transfer time was quite high compared with key verification time. The average transfer time was less than one second and the verification time was the 6.2 ms on average. To avoid the risk of key-guessing attack and code replication attack, a strong crypto system together with a secure digital signature were used interchangeably to encode smart meter readings during transmission between the cloud server and the smart meters. As for the results, the proposed security and meter privacy preservation scheme in this paper have offered alternative ways for preserving the cloud storage and time granularity while still providing privacy in smart meters.

7. Conclusion and Future Work

In this paper a data processing and storage system that is applicable to smart meters with many modules that is connected as an internet of things via the public network and uses the full strength of cloud computing and secures users' privacy and the confidentiality of data exchanged on the grid by encrypting smart meter data before sending to the cloud for the sake of processing and storage with the help of a homomorphic asymmetric key cryptosystem. Each smart meter includes a set of public and private keys to which the grid operator can access and the household owner, on the other hand, can only access the decryption key corresponding to their own smart meter. With the help of the homomorphic feature of the cryptographic technique, several methods are created to enable most of the computing works to be done directly on the data encrypted by the cloud which is the main focus of this model. The smart reading system which is proposed in this paper considers an external storage cloud server and supports multiple time granularities in a privacy preserving manner against host-but-curious providers. The consumer gives different time granularities to different service providers. It is shown in this paper that a service provider gets power consumption of the consumer at only the granted time granularity. The security analysis in this paper confirms that the proposed security protocol preserves the overall privacy of the smart meter readings by allowing an efficient authentication and key management protocol for cloud-based smart metering systems. The performance of the proposed system is analyzed in terms of computation cost and storage cost of a meter. The results confirm also that the key generation time is the highest among the transfer and the verification time. Furthermore, the suggested scheme reduced the overhead of the authentication time as compared to the other existing authentication schemes in smart metering systems. The analysis also provides a solid step towards the practical construction of privacy in cloud-based smart grid technologies.

References

[1] G. Lobaccaro, S. Carlucci, and E. Lofstrom,"A review of systems and technologies for smart homes and smart grids," Energies, **9**(5), 1–33, 2016. https://doi.org/10.3390/en9050348

[2] Dark Reading. Smart meter hack shuts off the lights. Available at: http://www.darkreading.com/perimeter/smart-meter-hack-shuts-off-the-lights/d/d-id/1316242.

[3] B. J. Murrill, E. C. Liu, and R. M. Thompson,"Smart Meter Data:Privacy and Cybersecurity," CRS Report for Congress [Online]. Available: http://www.fas.org/sgp/crs/misc/R42338.pdf.(accessed on April 2018).

[4] M. Weiss, A. Helfenstein, F. Mattern, T. Staake, Leveraging smart meter data to recognize home appliances, in: 2012 IEEE International Conference on Pervasive Computing and Communications (PerCom), IEEE, 190–197, 2012.

[5] S. Bera, S. Misra, and J. J. Rodrigues, "Cloud computing applications for smart grid: A survey," IEEE Transactions on Parallel and Distributed Systems, **26**(5), 1477-1494, 2015. https://doi.org/10.1109/ISGT-Asia.2012.6303140

[6] J. Zhou, R. Q. Hu, and Y. Qian, "Scalable distributed communication architectures to support advanced metering infrastructure in smart grid," IEEE Transactions on Parallel and Distributed Systems, **23**(7), 1632-1642, 2012.

[7] L. Ji, W. Lifang, and Y. Li, "Cloud Service based intelligent power monitoring and early-warning system," in Innovative Smart Grid Technologies-Asia (ISGT Asia 2012), IEEE, 1-4, 2012. https://doi.org/10.1109/ISGT-Asia.2012.6303140

[8] M. Akbar, D.Z.A. Khan, "Modified nonintrusive appliance load monitoring for nonlinear devices," in: Multitopic Conference, 2007. INMIC 2007. IEEE International, IEEE, , 1–5, 2007.

[9] X. Fang, D. Yang, and G. Xue, "Evolving smart grid information management cloudward: A cloud optimization perspective," IEEE Transactions on Smart Grid, **4**(3), 111-119, 2013.

https://doi.org/10.1109/TSG.2012.2230198

[10] N. Lu, P. Du, P. Paulson, F. Greitzer, X. Guo, and M. Hadley, “A multi-layer, hierarchical information management system for the grid,” in Proc. of IEEE Conf. on Power and Energy Society General Meeting, 632 – 642, Sept. 2012.

[11] Fournet, C., Kohlweiss, M., Danezis, G., Luo, Z.: Zql: A compiler for privacy-preserving data processing. In: Proceedings of the 22Nd USENIX Conference on Security. 163–178. SEC’13, USENIX Association, Berkeley, CA, USA, 2013.

[12] P. Deng, L. Yang, A secure and privacy-preserving communication scheme for advanced metering infrastructure, in: Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES, IEEE, 1–5, 2012.

[13] A. Rial, G. Danezis, Privacy-preserving smart metering, in: Proceedings of the 10th Annual ACM Workshop on Privacy in the Electronic Society, ACM, 49–60, 2011.

[14] Jo, H.J.; Kim, I.S.; Lee, D.H. Efficient and privacy-preserving metering protocols for smart grid system. IEEE Trans. Smart Grid, **7**, 1732–1742, 2016.

[15] Kursawe, K.; Danezis, G.; Kohlweiss, M. Privacy-Friendly Aggregation for the Smart-Grid. In Proceedings of the 11th International Conference on Privacy Enhancing Technologies (PETS’11), Waterloo, ON, Canada, 27–29, July 2011.

[16] J.L. Hennessy, D.A. Patterson, Computer Architecture: A Quantitative Approach, Elsevier, 2012.

[17] G.E. Blelloch, B.M. Maggs, Parallel algorithms, in: Algorithms and Theory of Computation Handbook, Chapman & Hall/CRC, 25–27, 2010.

[18] Le Métayer, D.: Privacy by design: A formal framework for the analysis of architectural choices. In: Proc. of the Third ACM Conference on Data and Application Security and Privacy. 95–104. CODASPY ’13, ACM, New York, NY, USA, 2013.

[19] Garcia, F., Jacobs, B.: Privacy-friendly energy-metering via homomorphic encryption. In: Cuellar, J., Lopez, J., Barthe, G., Pretschner, A. (eds.) Security and Trust Management, Lecture Notes in Computer Science, vol. 6710, 226–238. Springer Berlin / Heidelberg , 2011.

[20] N.P. Smart, F. Vercauteren, Fully homomorphic encryption with relatively small key and ciphertext sizes, in: Public Key Cryptography–PKC 2010, Springer, 420–443, 2010.

[21] F.D. Garcia, B. Jacobs, Privacy-friendly energy-metering via homomorphic encryption, in: Security and Trust Management, Springer, 2011, 226–238.

[22] J. Zhao et al., “Privacy Protection Scheme Based on Remote Anonymous Attestation for Trusted Smart Meters, IEEE Transaction, Smart Grid. 2016.

[23] Gong, Y.; Cai, Y.; Guo, Y.; Fang, Y. A privacy-preserving scheme for incentive-based demand response in the smart grid. IEEE Trans. Smart Grid, **9**(4), 3313-3320, 2016. https://doi.org/10.1109/TSG.2016.2626317

[24] McLaughlin, S.; McDaniel, P.; Aiello, W. Protecting consumer privacy from electric load monitoring. In Proceedings of the 18th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 17–21 October 2011.

[25] S. Fahl, M. Harbach, T. Muders, and M. Smith. Confidentiality as a service–usable security for the cloud. In TrustCom, 153–162, 2012.

[26] Backes, M.; Meiser, S. Differentially private smart metering with battery recharging. In Data Privacy Management and Autonomous Spontaneous Security; Springer Science + Business Media: New York, NY, USA, 2014; 194–212. Available online: https://eprint.iacr.org/2012/183.pdf. (accessed on 26 August 2018).

[27] D.P. Rodgers, Improvements in multiprocessor system design, in: ACM SIGARCH Computer Architecture News, **13**, IEEE Computer Society Press, . 225–231, 1985.