http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (22): 6702-6709, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.6702.6709

The Security Issue of WSNs Based on Cloud Computing for Smart Grid

Guangrong Yue, Yuanpeng Xie and Hong Wen
National Key Laboratory of Science and Technology on Communications,
University of Electronic Science and Technology of China, 610054, Chengdu, China

Abstract: Wireless Sensor Networks (WSNs) have been widely recognized as a promising technology that can enhance electric power systems by monitoring and diagnosing power system to avoid the effect of equipments failure and natural accidents. However, the management of huge amount of high sensitive data generated and collected by sensor networks becomes the bottleneck of WSNs application in the smart grid. This study proposed a framework to combine WSNs with cloud computing to solve the data storing and access problems due to the low-power, small-size characteristics of WSNs. We pointed out pros and cons of the proposed system and analyzed security issues of the combination paradigm and offered some solutions to these problems. Our efforts try to make easier to collect and access large amount of data generated by sensor nodes and guarantee the confidentiality and the integrity of data.

Key words: Smart grid, security, WSNs, cloud computing, framework

INTRODUCTION

The smart grid is a efficiency, reliability and safety, electric power-grid infrastructure by taking advantages of the automated control and modern communication technologies (Gungor *et al*., 2010). Comparing with the existing power grid which suffers from the lack of pervasive and effective communications, monitoring, fault diagnostics and automation, the smart grid system can capture and analyze data related to power usage, delivery and generation efficiently via wireless sensor networks (WSNs) (Poovendran, 2010). The smart grid can diagnose power disturbances and outages to avoid the effect of equipmentsfailure and natural accidents by the information provided by the sensor nodes (Wen *et al*., 2013a).

Electric power systems contain three major subsystems, power generation, power delivery and power utilization. WSNs have been widely recognized as a promising technology that can enhance all these three subsystems. Sensor nodes can monitor the overall network and to communicate with the control center in the power utility in order to help operators decide the appropriate actions, in which it is highly urged to get sensing data in real-time. At the same time, the collected sensing data is needed to store for the future analysis and research. The bottleneck occurred when researchers found that it was difficult to process and store such huge amount of heterogeneous sensing data coming from different sorts of sensors due to the low-power, small-size characteristics of WSNs, which makes that it is hardly capable to get desired correct and useful data.

As a matter of fact, cloud computing is playing a more and more significant role in both academic and commercial areas recent years and it's assumed to be the next big thing in the foreseeable future. Basic services that cloud computing provides are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) and all these services have already been utilized in reality life instead of just being in theory studys.

As cloud computing may become ubiquitous in future (Hassan *et al*., 2009), researchers consider the probability of combining WSN with cloud computing to solve the problems which are owing to the unique property of WSNs. In fact, the combination does overcome some challenges such as storage problems and accessibility, the on-demand services characteristic that cloud services provide is an attracting property for the smart grid system (Zingirian and Valenti, 2012). But vulnerabilities still exist, especially in security issues. According to an International Data Corporation (IDC) survey in 2008, security is an main consideration issue. In this study, we focus on the security framework description for this new combination. In this study, we address the challenge of data management in WSNs for the smart grid. Firstly, we propose a cloud based architecture for collecting and accessing large amount of data generated by sensor nodes. Then we analyze the security issues of the new architecture and show how we guarantee the confidentiality and the integrity of data.

Corresponding Author: Guangrong Yue, National Key Laboratory of Science and Technology on Communications,
University of Electronic Science and Technology of China, 610054, Chengdu, China

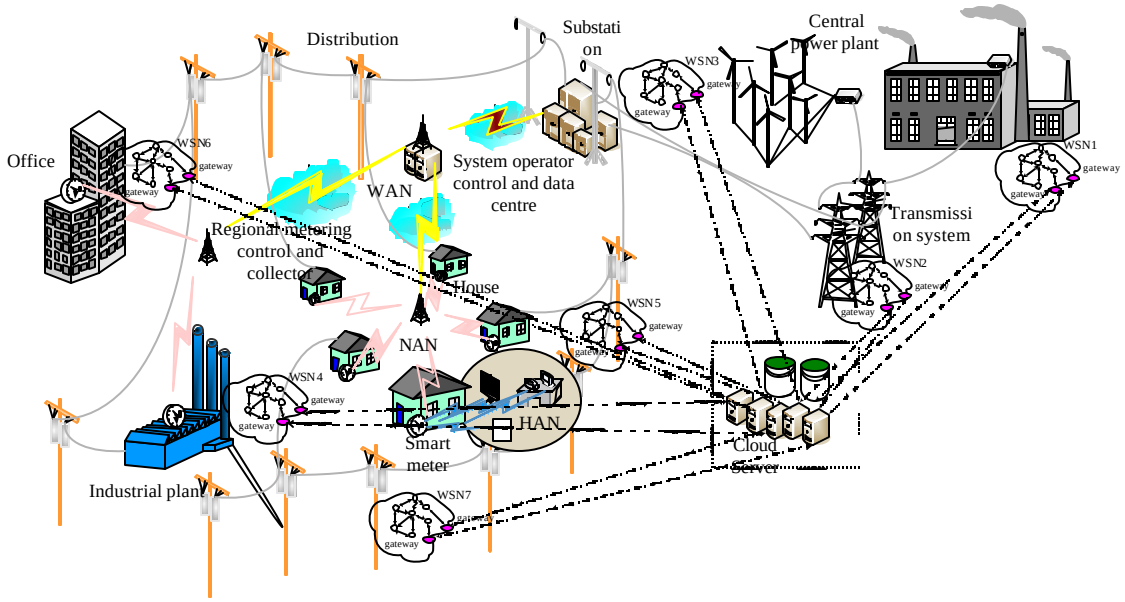

Fig. 1: Cloud-based WSNs for smart grid communications

The rest of study is organized as follows. Section 2 intruduces the cloud-based WSNs for smart grid communications. Related works are exhibited in section 3. The section 4 presents the framework for the new combination of WSN and cloud. The advantages and disadvantages of the combination will be shown in section 5. The security challenges of the new paradigm analysis is given in section 6. We conclude our work in section 7.

CLOUD-BASED WSNS FOR SMART GRID COMMUNICATIONS

The smart grid systems contain three major subsystems, power generation, power delivery and power utilization, as shown in Fig. 1. WSNs has been widely recognized to be of benefit to electric system automation applications. The sensor nodes take advantage of demographic, action, communication, situation, physical environment, location data, distance, temperature, sound, air pressure, time and lighting levels, which can map the physical characteristics of the environment to quantitative measurements and bring several advantages over traditional sensing including such as greater fault tolerance, improved accuracy, larger coverage area and extraction localized features.

For distributing energy power system the power generation may contain several bulk generation plant and many distributed small generation plant. A bulk generation plant may contain several generation units and several hundred actuators may control fuel, air and water flows to optimize heat rate and adjust generator output within each unit. In such harsh environments sensors nodes can be installed to monitor the generation systems without requiring any external power and also can be easily relocated and supplementary. Becuase of such advantages of sensor nodes, they are installed to monitor the delivery systems and power use in power delivery system. WSNs also are used in power utilization. For example, in a smart meter system WSNs can be used to detect real-time energy consumption, which can help improve business performance and technical reliability for power utility operations.

There has been a host of research results on WSNs for the smart grid (Wen *et al*., 2013b). However, all these efforts suffer from the shortcoming of a lack of consideration of data management. The problems how to store and access such huge amount of high sensitive data generated and collected by sensor networks should be solved in the new architectures. Combining WSNs with cloud computing will be a way to solve these problems. New cloud-based WSNs architecture will be presented to resolve the data storing and make easy information access.

RELATED WORK ABOUT CLOUD-BASED WSNS

In recent years, there were several researchers about integrating WSN into cloud, or so-called sensor-cloud, some of those researchers share a same framework model (Nguyen and Huh, 2011). In (Hassan *et al*., 2009), authors proposed a framework to enable to integrate WSN to

cloud computing by a content-based pub-sub model which simplified the integration and in order to deliver published sensor data, or events to appropriate users of cloud service who subscribed, it is needed to match published events with subscriptions efficiently. The authors presented a matching algorithm called Statistical Group Index Match (SGIM). The authors presented an architecture of the sensor cloud services based on subscription/notification model for Vehicle Communication Platforms (VCP). In (Zingirian and Valenti, 2012), according to this newly proposed model, VCPs made their components, including sensors and devices, to be available to the third-party vehicle monitoring applications. However, all these research results were lacking in discussions about security issues. (Nguyen and Huh, 2011) proposed an efficient secure multicast approach by combining group-key and time-key to minimize number of updated key for such dynamic scenario in publish/subscribe based sensor cloud. The study offered a new key management that could enhance the efficience of the system while it did not propose a useful approach to solve the real security issues of sensor-cloud. A model of combining WSN with cloud computing paradigm was proposed in (Eugster *et al*., 2003) and the authors did not use a pub/sub based model, they chose to utilize pipes and filters instead, which was mostly used in digital signal processing applications, according to the study, the paradigm also fitted well in WSNs, the results provided us with a new view to combine WSNs and cloud while it did not gave a method to guarantee the security of the sensor-cloud.

Framework Model

In our proposed framework, the publish/subscribe model (Eugster *et al*., 2003) is utilized as one of the major basic architecture. A pub/sub system (Eugster *et al*., 2003) enables subscribers to get their desired data from the system after they register to it and express the interested events, as long as the publishing data arrives at the interface of the system after filtering and classifying, the system sends the subscriptions to subscribers via some sorts of channel. In fact, a pub/sub system has already been the first choice for integrating WSN to cloud recently because of its very nature that subscribers can get the desired data in real-time or near real-time, due to which researchers in some special areas, e.g. , health care, climate change and diaster monitoring could get vital information in time.

Another basic architecture of the proposed framework is pipes and filters (Ganıma *et al*., 1995), which can always be noticed in digital signal processing but it also works well in domain of WSN (Kurschl *et al*., 2009). In our model, pipes do not store or process sensing data, their main purpose is buffering data and providing filters with a uniform format data instead. And the data is transmitted through an output port at the end of pipes. The output port is connected to a filter, whose main job is slightly modified the data from pipes via some algorithms designed to eliminate noise mixing in raw data. We make a filter chain which can be constructed by certain number of pipes and filters, a filter chain can be regarded as the gateway used to transmit sensing data to cloud. A simplified figure of a filter chain is shown in Fig. 2.

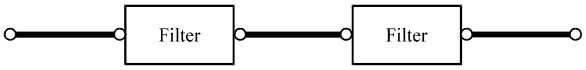

Fig. 2: A filter chain

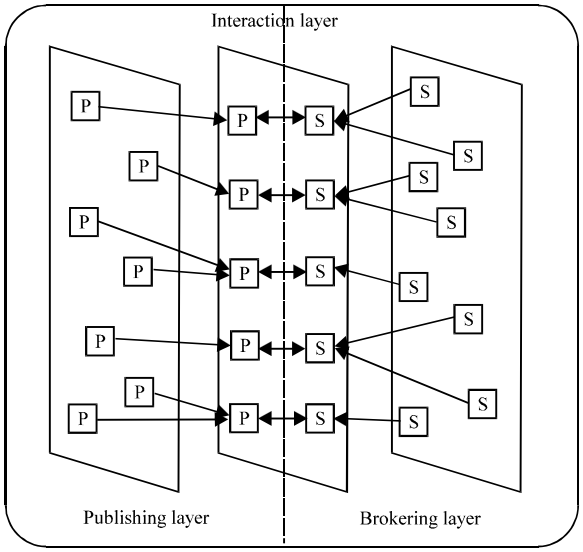

Fig. 3: Three layer architecture

The pub/sub system based model needs the three-layer architecture. As shown in Fig. 3, the architecture is composed by a publishing layer, an interaction layer and a brokering layer. A publishing layer receives sensing data from filter chains, as discussed above, filter chains have eliminated noise mixing in the sensing data from sensors, therefore, the publishing layer's job is to organize and classify these sensing data by a data model algorithm. And the organized data is transmitted to an interaction layer, where the data is compared by the data model algorithm, if a certain publication meets all requirements that a subscription needs, it will be classified into matched data and sent to the third layer, the brokering layer. Otherwise, the data will

be classified into mismatched data and transmitted to the IaaS or DaaS to be stored. What's more, an interaction layer not only receives organized data from a publishing layer, but also receives subscriptions from the brokering layer, which receives all those subscriptions coming from the consumers of the cloud services. As described, the three layers should use cloud services such as IaaS or DaaS due to the large amount of sensing data they may receive and process.

In a pub/sub based model, the most important job, which is also a challenging job, is to send appropriate publishing data to subscribers who desire the data. In the proposed framework, we present a data model to implement this vital but difficult goal. As we know, different kinds of WSNs will produce enormous amount of raw sensing data from heterogeneous sensors, which results in different formats of raw data, thus an efficient data model is imperative under such a circumstance. The data model we present is inspired by the data model proposed in (Nguyen and Huh, 2011), based on which our data model is composed by format, sensor ID, size, time, value and period. Therefore, a raw data can be expressed as a vector Publication<format; sensor ID; size; time; value; period>.

Format stands for the basic format of the raw data that a specific sensor produces, there are different kinds of formats decided by different kinds of sensors, for example, JPEG, WMA, TXT, PNG, WMV, etc. A sensor ID is the only sign of the source sensor that raw sensing data comes from, a specific sensor could produce lots of data, all these data shares one same sensor ID. The size of sensing data is defined by the data itself, a size identification can make this clear to interaction layers, for instance, if a subscription needs a publication whose data size is between 20 bytes and 30 bytes, then all the publications that beyonds the range are no longer in consideration for the subscription. As for time, as long as a sensor captures data from the environment it is in, the time that the capture occurs will be regarded as the time attributes of the raw data. A value sign represents the most important characteristic of sensing data, a subscriber choose certain data mostly by this attributes. The meaning it stands for differs from format to format, different kinds of sensors have different meanings. For example, for a temperature sensor, the value means specific numbers of the temperature. A period identification is a time cycle of the data, once a sensing data does not meet all requirements of subscriptions, it will be sent to the IaaS of cloud and all these data will be stored as a queue by time identification. As long as the stored time in IaaS beyonds the period value, it will be destroyed for good. The period identification is used to increase the utilization rate of the cloud services.

A subscription model is of same construction, except that some attributes is in a range instead of confirmed value. A subscription can be expressed as a vector: Subscription<format; sensor ID range; size range; time range; value range; application ID; consumer ID; period>.

One same sort of sensors which are utilized to the same purpose may have IDs in a range, for example, temperature monitoring sensors may own IDs in range of 10000 to 20000 and if consumers need accurate temperature data, they can add (10000, 20000) to the sensor ID range. A size range and time range can be understood in the same way, value range also differs from sensor to sensor. An Application ID and the consumer ID are used to find the consumer as long as certain data suits the subscription.

We can divide the framework into three parts: Cloud, WSN and bridge. On the WSN side, it works just like normal WSN systems except that all the sensing data are transported to the bridge, which is the filter chains and three layers in our circumstance. On the cloud side, consumers of cloud services mostly urge real-time data, that's the most valuable property of pub/sub based sensor-cloud, in order to implement the idea, the brokering layer is connected to specific applications of SaaS. Consumers can get their subscriptions by registering to the applications and browsing via the Internet.

The cloud-side workflow is as follows:

- Consumers of cloud services register their information and subscription to specific SaaS application
- The subscriptions are transmitted to the brokering layer, which will classify and organize the subscriptions by the subscription attributes
- Brokering layer sends the classified subscriptions to the interaction layer
- The subscriptions are compared with the publications coming from a publishing layer, if certain data suits the subscription, then the data will be sent to the SaaS application registered by the consumer and applications send the data to its consumer, otherwise, the publishing data will be sent to IaaS or DaaS of cloud

The WSN-side workflow is as follows(a publishing layer is on the cloud-side, since it uses IaaS services of cloud):

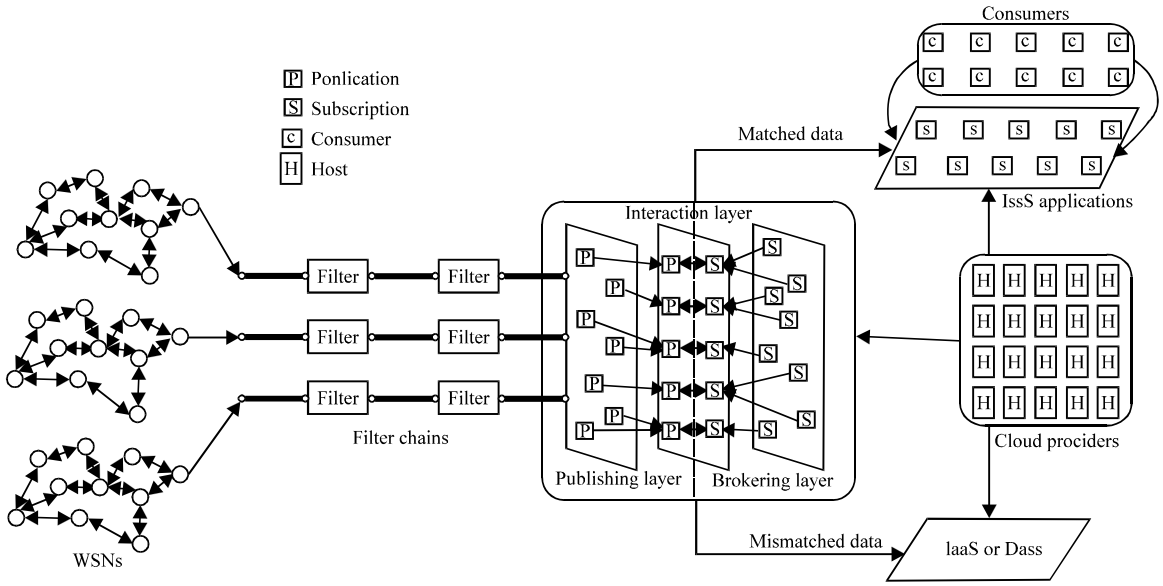

Fig. 4: The whole workflow

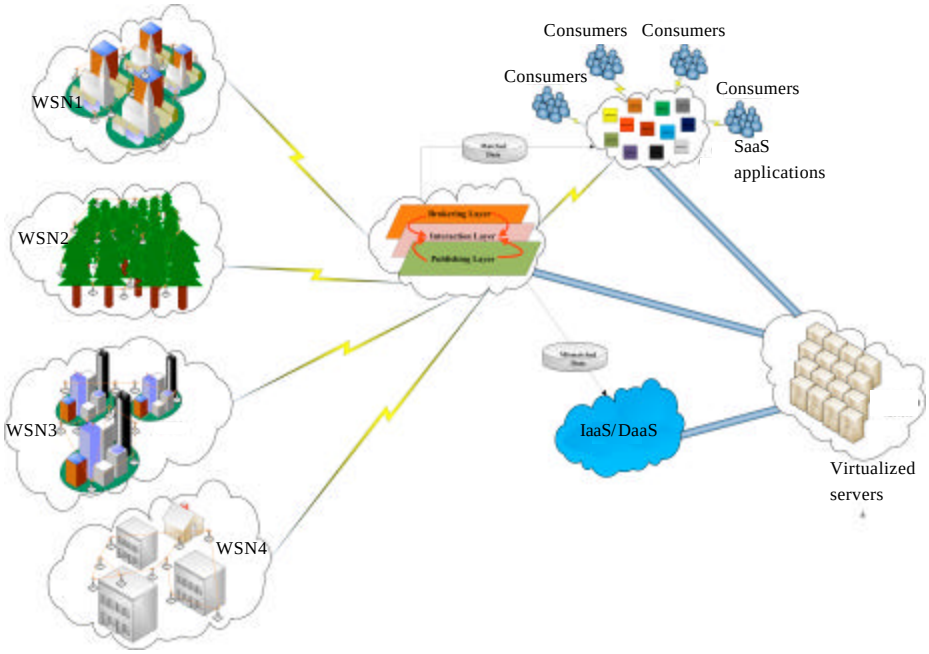

Fig. 5: General structure

- Sensors of WSNs capture data from the around environment and transmit the data to a filter chain
- Filter chains buffer and slightly modify the data by eliminating noise within the raw data
- Modified data is sent to the publishing layer, where the data is organized and classified by data models
- The Publishing layer transmits the data to an interaction layer

The whole workflow is shown in Fig. 4 and 5 illustrates the general structure of the integration.

ADVANTAGES AND DISADVANTAGES

As discussed above, there are both opportunities and challenges that integrating WSNs and cloud could offer, we will conclude the pros and cons of the combination in this section.

Advantages:

- Storage

This may be the most intuitive advantage of the combination, after all, the amount of sensing data from heterogeneous sensors could increase incredibly in a short period, which causes the so-called data burs, this kind of problem could be solved by cloud services like IaaS and DaaS.

- On-demand Services

One of the purposes of the integrating framework is that consumers could choose to get what they want from WSNs instead of everything coming from WSNs.

- Ubiquitous network access

For consumers, another important reason to choose this new paradigm is that they can access to sensing data as long as they can access to the Internet instead of via traditional ways.

- Real-time processing ability

As we have discussed, there are several areas requiring real-time data to process related work, for instance, health care, disaster monitoring, climate change and so on. The pub/sub model could satisfy such demands.

Disadvantages:

- Data format

There still lacks standard metrics for sensing data at present, which means the interfaces on data-receiving side of the paradigm are facing problems in selection and classification. And different data formats need different APIs to be programmed.

- Network bandwidth

As mentioned before, data burst is an ordeal for network bandwidth, if the data amount is too huge for existing bandwidth to maintain transmitting sensing data, the real-time capability is of no use.

- Billing model

The state-of-the-art Billing model of cloud computing is not regulated, which may make consumers who are waiting for a standard cloud service billing model more confused. If the billing model can be standardized, it is an another advantage of cloud computing instead of an opposite one.

SECURITY CHALLENGES

In this study, the security challenges we discuss mainly focus on data security through the whole workflow, especially on the architecture integrating WSNs to cloud instead of data security in WSNs or cloud services.

We will analyze the security issues of the combination according to the workflow priority.

First of all, we begin with WSN-side, as we can see in Fig. 4, WSNs send sensing data to filter chains, in this transversion, security issues inside WSNs are in same condition as independent ones, which are not the main objectives in this study, but we should know that key management is still the most useful and popular way to defend attacks from adversaries. In (Nguyen and Huh, 2011), authors proposed an efficient key management for secure multicast in sensor-cloud, in the study, the key management is combined by grouping key and time key to minimize number of updated key in a sensor-cloud environment.

As discussed above, the three layers are all on cloud-side, security issues in cloud should be considered for sensing data which is going to a publishing layer. In the integrated paradigm, all the three layers are actually DaaS or IaaS services that cloud provides to store the coming data in huge amount temporarily. As a result, a publishing layer can be regarded as an cloud control interface to access to cloud services. According to (Somorovsky *et al*., 2011), a successful attack on a cloud control interface grants the attacker a complete power over the victim's account, with all the stored data included. And the authors' research results claimed that the cloud control interfaces of public cloud could be attacked by novel signature wrapping and advanced XSS techniques. In addition, several countermeasures were discussed in the study.

As long as the data is transmitted to the publishing layer, it is utilizing cloud services like IaaS or DaaS, security challenges of which must be overcome since then. There are plenty of research results about cloud security, in conclusion, a secure cloud should at least satisfy 4 basic urges of consumers [15], say availability, confidentiality, data integrity, control:

- Availability

Cloud providers should offer services that consumers could get and use at any places and any time. There are mainly two methods to enhance availability in cloud, which are virtualization and redundancy.

Currently, cloud technology is mainly based virtual machine, since cloud providers can provide separated virtualized memory, virtualized storage, virtualized CPU cycles, so users can always get them.

Large cloud provider enterprises build data centers in multiple regions all over the world to protect files they store from failing in one particular region and spreading to other regions. For example, Google set three replications for each object stored in it, all these redundancy strategies are enhancing the availability for consumers to get whatever they want at any time and any place.

Besides these concerns on availability, don't trust HTTP protocol too much as it is a stateless protocol for attackers, which may cause unauthorized access to the management interface of cloud infrastructures:

- Confidentiality

Confidentiality has been a huge barrier for cloud providers to popularize cloud to consumers since it comes out. It is understandable that consumers cannot trust the cloud services, after all, nobody knows what will happen to the files, especially important and confidential ones, once they are placed in cloud vendors' hosts.

There basically exist two common approaches in current cloud infrastructures, say physical isolation and encryption. Physical isolation specifically means virtual physical isolation as cloud services are transmitted via public networks. In this context, virtual physical isolation are using VPN and firewalls to secure database (Zhou *et al*., 2010). Encrypting vital and confidential data before placing it in cloud infrastructures is another method to enhance confidentiality of cloud. But do not count on that approach too much because novel methods of breaking cryptographic algorithms are discovered (Grobauer *et al*., 2011).

- Data integrity

Data integrity ensures consumers that their storing data is not modified by others or collapsing owing to system failure. An easy method is making plenty of copies of consumers' files, which is a good but highly-cost way. Or cloud vendors can employ a new kind storage equipment, Zetta system, which is suitable for data integrity of cloud. Besides these two methods, a "cloud security capture application" (Sunte, 2010) could be in use to show consumers when and where their data was modified or transmitted.

- Control

It is a sophisticated work to control a cloud system, a control work mainly includes deciding what resource could be utilized in what occasions.

In order to own a secure control system, cloud vendors may need a specialized operating system. Virtualization based cloud services make it difficult to overcome defects in security control because of the insufficient control mechanisms that virtualized networks offer. And poor key management procedures of virtualized based cloud services make it wors. Because virtual machines don't have a fixed hardware infrastructure and cloud-based content is often geographically distributed, it is a very tough task to ensure a secure control in cloud (Liu and Wassell, 2011).

CONCLUSION

The smart grid can diagnose power disturbances and outages to avoid the effect of equipments failure and natural accidents by the information provided by the sensor nodes. contain three major subsystems, power generation, power delivery and power utilization. WSNs have been widely recognized as a promising technology that can enhance electric power systems. However, the management of huge amount of high sensitive data generated and collected by sensor networks becomes the bottleneck of WSNs application in the smart grid.

This study intruduces a framework to integrate WSNs to cloud to solve the data storing and access problems due to the low-power, small-size characteristics of WSNs. We pointed out pros and cons of the proposed system and analyzed security issues of the combination paradigm and offered some solutions to these problems.

ACKNOWLEDGMENT

The study is supported by the NSFC (Grant No. 61032003, 61271172 and 61071100), RFDP (Grant No. 20120185110030 and 20130185130002) and SRF for ROCS, SEM.

REFERENCES

Eugster, P.Th., P.A. Felber, R. Guerraoui and A.M. Kermarrec, 2003. The many faces of publish/subscribe. ACM Comput. Surv., 35: 114-131.

Gamma, E., H. Richard, R. Johnson and J. Vlissides, 1995. Design Patterns: Elements of Reusable Object-Oriented Software. Addison-Wesley, Massachusetts.

Grobauer, B., T. Walloschek and E. Stocker, 2011. Understanding cloud computing vulnerabilities. IEEE Secur. Privacy, 9: 50-57.

Gungor, V.C., B. Lu and G.P. Hancke, 2010. Opportunities and challenges of wireless sensor networks in smart grid. IEEE Trans. Ind. Electr., 57: 3557-3564.

Hassan, M.M., B. Song and E.N. Huh, 2009. A framework of sensor-cloud integration opportunities and challenges. Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication, January 11-12, 2009, Suwon, South Korea, pp: 618-626.

Kurschl, W., S. Mitsch and J. Schoenboeck, 2009. Modeling distributed signal processing applications. Proceedings of 6th International Workshop on Body Sensor Networks, Auguse 5-7, 2009, Berkeley, USA., pp: 103-108.

Liu, R. and I. Wassell, 2011. Opportunities and challenges of wireless sensor networks using cloud services. Proceedings of ACM International Conference On Emerging Networking Experiments And Technologies, December 6-9, 2011, Japan, pp: 1-7.

Nguyen, T.D. and E.N. Huh, 2011. An efficient key management for secure multicast in Sensor-Cloud. Proceedings of the 1st ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering, May 23-25, 2011, Jeju Island, pp: 3-9.

Poovendran, R., 2010. Cyber-physical systems: Close encounters between two parallel worlds [Point of View]. Proc. IEEE, 98: 1363-1366.

Somorovsky, J., M. Heiderich, M. Jensen, J. Schwenk, N. Gruschka and L. Lo Iacono, 2011. All your clouds are belong to us: Security analysis of cloud management interfaces. Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop, October 21-22, 2011, Chicago, USA., pp: 3-14.

Sunte, L., 2010. Cloud computing: Security risk. Proceedings of the 48th Annual Southeast Regional Conference, April 15-17, 2010, Oxford, MS, USA, pp: 1-5.

Wen, H., S.Q. Li, X.P. Zhu and L. Zhou, 2013. A Framework of the PHY-layer approach to defense against security threats in cognitive radio networks. IEEE Networks, 27: 34-39.

Wen, H., Y.F. Wang, X. Zhu, J. Li and L. Zhou, 2013. Physical layer assist authentication technique for smart meter system. IEE Commun., 7: 189-197.

Zhou, M., R. Zhang, W. Xie, W. Qian and A. Zhou, 2010. Security and privacy in cloud computing: A survey. Proceedings of the 6th International Conference on Semantics Knowledge and Grid, November 1-3, 2010, Beijing, pp: 105-112.

Zingirian, N. and C. Valenti, 2012. Sensor clouds for intelligent truck monitoring. Proceedings of the Intelligent Vehicles Symposium, June 21-23, 2012, Alcala de Henares, Spain, pp: 999-1004.