ISSN 2349-6193
Impact Factor (PIF): 2.243

IJESMR

International Journal OF Engineering Sciences & Management Research

DESIGN OF SECURE FRAMEWORK FOR CLOUD DATA SECURITY IN SMART GRID WITH FOG COMPUTING

Asst. Prof. Mayur Subhash Chavan
[1]Department of Computer Engg, PICT , Pune, Maharashtra,India

Keywords: Cloud computing, Fog computing, Smart grid, Security.

ABSTRACT:

Smart grid is next generation power grid. It combines communication network with information system as one smarter system for reliable and safe infrastructure. Cloud computing has developed and evolved over the past years becoming a real choice for Smart Grids infrastructure because of the scalability, availability, interoperability performance and most important its performance. Though smart grid using two way communication and cloud there are still some loop holes regarding security which need to focus.

In smart grid information present on cloud is very sensitive to attack. Attacker tries to gain access of information available on smart meters, which will be very dangerous for both customer and consumer. As smart grid heavily relies on communication network security for insider data, theft attack is an important. Traditional security mechanisms are not able to fulfil security requirement of this new trend power grid. Therefore, there is exact need of best solution, which able prevent data loss, and misuse of data. Towards the end paper addresses issues in smart grid for data security in cloud, previous work regarding the topic and focus on new approach fog computing for cloud data security. With this new technique fog computing, we are trying to give security solution for cloud data security in smart grid.

INTRODUCTION:

The new smart grid approach is very attractive next generation electrical power network trend. It combines power distribution network and communication networks as one smarter system, and act as two-way interactive information and control flows. Because of that intelligent decisions and optimization on electricity usages according to the state of the electrical power, system and customers dynamical needs are possible.

According to NIST's conceptual model, the Smart Grid consists of seven logical domains: Transmission, Bulk Generation, Customer, Distribution, Service Provider, Markets and Operations. The first four feature the two way power and information flows. The last three feature information collection and power management in the Smart Grid. Therefore, to interconnect this entire communication network plays an important role.

Smart grid is real world application, which need internet for communication so to achieve interactive functionalities it heavily dependent on communication network. In smart grid information stored on cloud storage, customers and consumers can directly interact with this data. Due to that, concerns of reliability and security of this data becoming more and more critical and essential. Nowadays researchers are working on primary security concerns privacy, data integrity, availability.

Researchers [1-9] proposed many algorithms based on physics-law, which detect well-designed bad data. Liu and Ning [10] states that in smart grid, Data theft attack makes strong influence on system. They concluded that unauthorized persons get access to data and they provide bad data to certain variables and existing techniques get bypass for bad measurement detection in power system, knowledge of the power system configurations is exploited

Smart grid is not as traditional power grid where control center were isolated, protected. Smart grid have large advance-metering infrastructure, distributed internally connected to the communication network. With advances modern technologies cyber attack techniques also get improved due to that it is not difficult now to crack any secure communication network [13-15].

Attackers can intrude in to smart meters and update readings to fool or disturb billing system [11]. In organizational field, because of attack on data there is strong possibility to disturb demand and supply system balance, increase in cost of energy, erroneous decisions due to misleader control center [3, 12]. In case if terrorists succeed to access data, it results in significant damage on power infrastructure of nation [11].

ISSN 2349-6193
Impact Factor (PIF): 2.243

IJESMR

International Journal OF Engineering Sciences & Management Research

So as stated in above paragraphs attacks on data in smart grid can make significant damage for power infrastructure so it shows there is need for strong security mechanism. Here our focus mainly on information/cyber security, towards the end paper articulate security solution to secure cloud by using decoy information technology, which we have, come to call fog computing. Though Fog computing is similar to cloud but major difference is that its proximity to end users, support for mobility, its dense geographical distribution. We are switching to fog computing for security because of it supports internet of things applications that demands mobility support and wide range of Geo-distribution in addition to location awareness and low latency features. We are using this technology to launch disinformation attacks against malicious insiders. With help of this idea, we can prevent malicious insiders from distinguishing the real sensitive data from fake worthless data. Fog computing is one of the useful technique which provides decoy technology. Decoy technology mainly aim at detecting the unauthorized access using user behaviour profiling and fake data means decoy files. The user behaviour profiling get done using data access pattern. Once the access detected as unauthorized, the decoy information generated and used to misguide the intruder. The decoy documents may be honey-files, honey-pots and other bogus information.

The rest of the paper organized as follows: Section II we review related work on security mechanisms for cloud data security. In section III, Securing clod using fog. Rough layout of proposed system in section IV.

RELATED WORK

The main security issues are authentication at different levels of gateways as well as (in case of smart grids) at the smart meters installed in the consumer's home. Each smart appliance and smart meter has an IP address. There is possibility that user can tamper with its own smart meter, spoof IP addresses and report false readings, for his personal or malicious motives. Peng Yong et al. in 2012 used cryptographic techniques in their design to achieve research results of secure cloud storage [16]. Author analyzed in their survey about Smart Grid attacks and possible countermeasures [17]. Almost all researchers mentioned following security goals for smart grid as in table below.

Table 1- Attack Types and its Effects

ATTACK TYPE	ATTACK DETAILS	AFFECTED SECURITY TYPE	AFFECTED AREA
Malware spreading and device attacks	Tampers with the devices and tries to control them	Availability, Integrity, Confidentiality, Non-repudiation, Denial of service attack	Smart Meter, SCDA, Home Area\ Neighborhood area networks
Data Injection And Replay Attack	Tries to compromise the data in the network traffic and extract private user information.	Confidentiality, Privacy, Integrity	Smart Grid data, Home Area\ Neighborhood area networks
Eavesdropping, Man-in-the-middle-attack and traffic analysis	It aims to learn the network traffic in order to take advantage of the vulnerabilities.	Integrity, Availability, Confidentiality, DOS , Privacy	Smart Grid network Home Area\ Neighborhood area networks

(*Source: summarized from Bela Genge, Adela Beres and Piroska Haller 2014*)

In 2011 there is technique "SPARSH" proposed by researchers in this area [18]. This is a biometric technique using thumb impression to provide security. This technique work as authentication and proves advantageous while downloading and uploading files from cloud. However, we have to consider a statement of Steve Kirsch of oneID, which he mentioned in fog computing conference of nov 2014, that there is myth that biometric is strong security solution than anything else because your fingerprints might get stolen from things which you are using . He also added that passwords are bad security is another myth, the way we are using passwords is wrong [19]. Study also proposed that fog computing can be useful for security because it focus on to detect unauthorized access through user behaviour profile that is decoy technique. With decoy technique, if access is unauthorized it served with fake documents, which confuse attacker [20]. Fake documents might be honey-pots,

ISSN 2349-6193
Impact Factor (PIF): 2.243

IJESMR

International Journal OF Engineering Sciences & Management Research

honey-files or any wrong bills, files that are not important. This technique helpful because of two facts 1: It checks whether user is legal or not. 2: If user is not a legal user confuse it with fake documents.

SECURING CLOUD USING FOG

Cloud storage is now a widely used to store information because it have extensive storage space. However, information stored in cloud available globally where anyone can access it. The most important thing should notice that when user store information he completely unaware that where and how data will be stored and who will access it. So in that case user need assurance that his business data nobody will access without rights. Traditional encryption method is used nut it unsuccessful to prevent data theft attack. By applying encryption technique to the information, we cannot realize total protection to confidential data.

To secure smart grid from insider data theft attack it is feasible to switch from cloud to fog. Fog computing is great platform for internet of thing application like smart grid because it satisfies demands of proximity and mobility [21].

Our aim is to limit data loss to achieve a preventive disinformation attack technique we are going to use here. This secure cloud service achieved through following two features explained [20] in as below:

1. ***USER BEHAVIOR PROFILING***
   This is behavior based security technique. In this stage it limit access to user that how, when, how much information he will access. Administer or Supplier maintain log of legal users and set criteria for assessing information. Behavior of normal user continuously checked to recognize whether there is any abnormal behavior occurred in user's data. According to behavior of user and accessing time, system will able to recognize abnormal access.
2. ***DECOY TECHNOLOGY***
   Once abnormal behavior detected, it served with some fake documents. To do these things some traps placed within files systems this traps are nothing but decoy files. These files get placed by legal user, masquerades totally unaware of all this. So if any unauthorized person found suspicious to system he served with decoy data. When unauthorized user gets decoy data, he assumes that he is dealing with original data. That means system here succeeds to confuse user due to that data loss prevented.

   Therefore, this way cloud data secured, and this approach we are using to achieve secure solution in smart grid.

LAYOUT OF PROPOSED SYSETM

To secure smart grid cloud data we are combining the approach mentioned in above section. For smart grid when customer or consumer wants to get data from cloud storage of smart grid i.e information of bills, user information (address, name etc), want to pay bills should follow some security checks, which are as below.

1. Login.
2. Enter verification code.
3. Answer challenge questions.

When user passes these three stages, he can get access to data, which he wants and able to download/upload files. Below figure 1 articulate this things.

ISSN 2349-6193
Impact Factor (PIF): 2.243

IJESMR
International Journal OF Engineering Sciences & Management Research

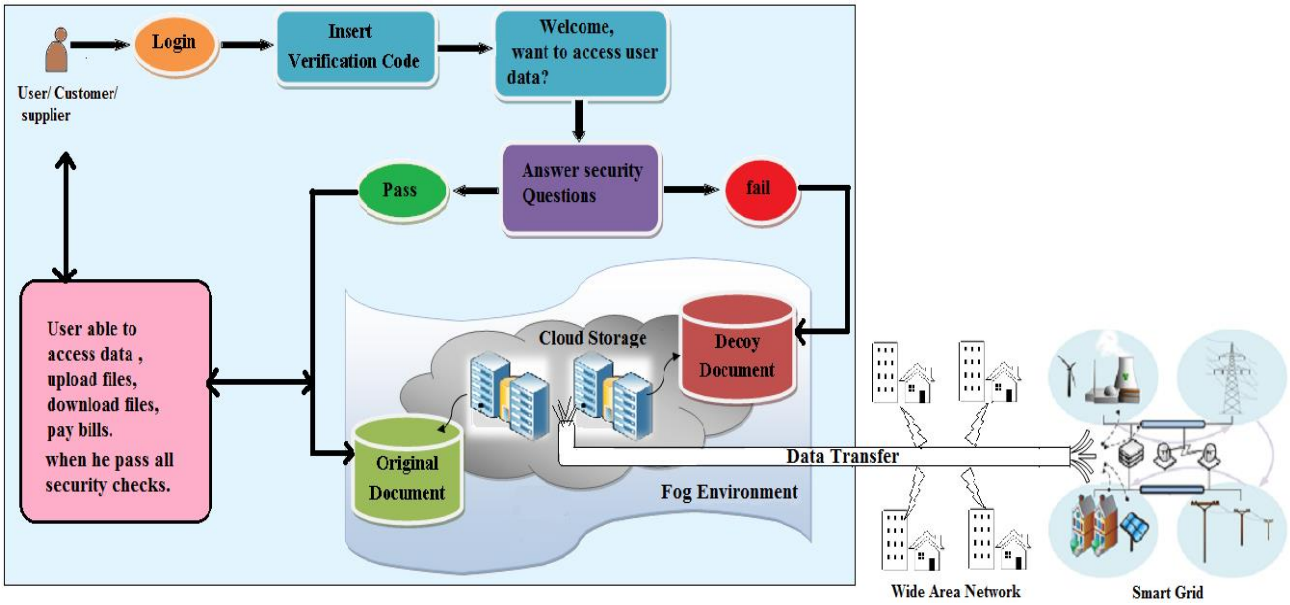

Figure 1: Layout of Proposed system

User must be a registered user. When user try to login he will get one verification code. Verification code here means one time password, which he needs to enter into account to get entry. After that if, user want to upload or download data he has to pass security checks that is challenge questions if he answer it correct then able to access to data. If user fails to answer questions, he will get decoy data, which he assumes is original. Decoy data placed with original data in storage. Here nobody can enter into cloud storage directly; they have to pass through fog environment, which created for security of data on cloud. Because of fog created in form of decoy document, unauthorized user not able to reach to original document. And this how system succeed to confuse attacker.

CONCLUSION

In this paper, we reviewed data theft attacks appear in cloud data storage of smart grid. Here we trying to give solution to such data attack with fog computing. Fog computing is a new promising approach to secure personal and business data in the Cloud. First it monitor unauthorized access through user behaviour profile and then second decoy documents stored in the Cloud alongside the user's real data also serve as sensors to detect unauthorized access. If there is any malicious, behaviour recognized it served with decoy documents.

ACKNOWLEDGEMENTS

I take this opportunity to express my deep sense of gratitude towards my colleagues and friends, I always thankful for their indispensable support, priceless suggestions and for most valuable time lent as and when required.

REFERENCES

[1] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in Proc. Smart Grid Communications (SmartGridComm), 2010.
[2] Y. Huang, H. Li, K. A. Campbell and Z. Han, "Defending false data injection attack on smart grid network using adaptive cusum test," in Proc. 2011 Information Sciences and Systems (CISS), 2011.
[3] T. Liu, Y. Gu, D. Wang, X. Guan and Y. Gui, "A Novel Method to Detect Bad Data Injection Attack in Smart Grid," in Proc. IEEE INFOCOM Workshop on CCSES, 2013.
[4] Y. Huang,et al., "Bad data injection in smart grid: attack and defense mechanisms," Communications Magazine, IEEE, vol.51, pp. 27-33, 2013.

ISSN 2349-6193
Impact Factor (PIF): 2.243

IJESMR

International Journal OF Engineering Sciences & Management Research

[5] M. Esmalifalak, G. Shi, Z. Han and L. Song, "Bad Data Injection Attack and Defense in Electricity Market Using Game Theory Study", IEEE Transactions on Smart Grid, vol.4 , pp:106-169, 2012.
[6] A. Tarali and A. Abur, "Bad data detection in two-stage state estimation using phasor measurements," in Proc. Innovative Smart Grid Technologies (ISGT Europe), 2012.
[7] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt and T. J. Overbye, "Detecting false data injection attacks on dc state estimation," in Proc. Preprints of the First Workshop on Secure Control Systems, 2010.
[8] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang and W. Zhao, "On False Data Injection Attacks against Power System State Estimation: Modeling and Countermeasures," IEEE Transactions on Parallel and Distributed Systems, 2013.
[9] B. Gou and R. Kavasseri, "A pre-procedure of bad data detection for smart grid monitoring" in Power and Energy Society General Meeting, IEEE, 2012.
[10] Y. Liu, P. Ning and M. K. Reiter, "False Data Injection Attacks against State Estimation in Electric Power Grids,", Proceedings of the 16th ACM conference on Computer and communications security, 2009.
[11] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," Security & Privacy, IEEE, vol.7, pp. 75-77, 2009.
[12] J. Lin, W. Yu, X. Yang, G. Xu and W. Zhao, "On false data injection attacks against distributed energy routing in smart grid," in IEEE/ACM Third International Conference on Cyber-Physical Systems (ICCPS), , 2012.
[13] H. Khurana, M. Hadley, N. Lu and D. A. Frincke, "Smart-grid security issues," Security & Privacy, IEEE, vol.8, pp. 81-85, 2010.
[14] R. Q. Hu, Y. Qian, H. Chen and H. T. Mouftah, "Cyber security for smart grid communications: part II [Guest Editorial]," Communications Magazine, IEEE, vol.51, pp. 16-17, 2013.
[15] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar and K. Poolla, "Smart Grid Data Integrity Attacks,", IEEE Transactions on Smart Grid, vol.4 , pp:1244-1253, 2013.
[16] P. Yong, Z. Wei, X. Feng, D. Zhong-hua, G. Yang and C. Dong-qing, "Secure cloud storage based on cryptographic techniques", The Journal of China Universities of Post and Telecommunications, vol. 19, sup. 2, pp. 182-189, 2012.
[17] Zubair A. Baig , Abdul-Raoof Amoudi, " An Analysis of Smart Grid Attacks and Countermeasures" Journal of Communications Vol. 8, No. 8, August 2013.
[18] Rohit Ranjan1, Gaurav Sonwani, Nikita Surana, "SPARSH"-Data Security in Cloud, ijetae 10 Oct 2011.
[19] "Fog Computing Conference Speakers Explain How to Improve IoT Security" Available online at http://www.fogcomputingworld.com/topics/fogcomputing/ articles/ November 2014
[20] Salvatore J. Stolfo, Malek Ben Salem, Angelos D. Keromytis, "Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud" IEEE CS Security and Privacy Workshops pp 125-128, 2012.
[21] Maher Abdelshkour "IoT, from Cloud to fog", online Avalaible at http://blogs.cisco.com/perspectives/iotfromcloudtofogcomputing