International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 10 – No.6, March 2016 – www.ijais.org

# A Fog Computing based Smart Grid Cloud Data Security

Ahmad Almadhor
Electrical and Computer Engineering Department
University of Denver

## ABSTRACT

Today's electricity grid is sprouting into the smart grid which should be dependable, supple, effcient, and supportable. To fulfill these necessities, the smart grid draws on a lot of center advances. Advanced Metering Infrastructure (AMI). These advances or progressions encourage simple also, quick aggregation of different information, e.g. fine-grained meter readings. Various security and protection concerns with respect to the accumulated information/data emerge or arise, since explorations has demonstrated that it is conceivable to reason and extract user behavior from smart meter readings. Thus, these meter readings are extremely touchy and require suitable assurance. Smart grid is bleeding edge power grid. It takes in communication framework/network with information system as one more savvy system for strong and safe base. Cloud computing has made and propelled over the earlier years transforming into a certified choice for Smart Grids system because of the flexibility, openness, interoperability execution and most basic its execution. Regardless of the way that smart grid using two way communication and cloud there are still some break provisions as for security which have to ponder on.

## Keywords

Smart Grid, Cloud Computing, Security, IoT, Power Grid

## 1. INTRODUCTION

Smart grid is the substitution of maturing power system by insightful power system joining Energy Information and Communication Technology (ICT) and Technology (ET). The usage of smart grid innovations altogether expand the unpredictability of taking care of information/data in data management model, which implies the general expense of information/data control in the information management model increments [Zhong Fan et al]. Cloud based information incorporation offers more elevated amount of adaptability, productive information sharing approaches, easy handling of data for profoundly complex frameworks and better outsourcing for innovative entities. Henceforth, an outline of effective model and choice of suitable reproduction apparatus is needed for general expense diminishment of information management. A cutting edge distributed computing worldview termed as cloud computing innovation assumes a key part in data management by serving extensive data centre’s utilizing cloud suppliers with huge stockpiling/storage and services of computations [Wu C et al]. The novel smart grid strategy is extraordinarily charming front line electrical power framework design. It takes in communication networks and power distribution networks as one all the more sharp system, and goes about as two-way smart information and control streams/flows. In perspective of that savvy decisions and streamlining on usages of power as demonstrated by the state of the electrical power, system and customers dynamical needs are possible. According to NIST's hypothetical model, the Smart Grid comprises seven consistent domains i.e. Mass Generation, Transmission, Customer, Distribution, Service Provider, Markets and Operations. The beginning four areas are the two way power and information streams. The last three areas are information assembling and power organization/management in the Smart Grid. In this way, to interconnect this entire communication framework/network accepts a basic part. Smart grid is genuine application, which oblige web for correspondence so to finish wise functionalities it strongly subject to communication framework/network. In smart grid information set away or stored on cloud storage, customers and buyers can direct collaborate with this data. On account of that, stresses of steady quality and security of this data ending up being more fundamental and crucial. Nowadays masters, academic professionals are taking a shot at fundamental security concerns assurance/confidentiality, data reliability, availability. In smart grid information present on cloud is greatly fragile to attack. Aggressor tries to get passage of information open on smart meters, which will be to a great degree hazardous for both customer and buyer. As smart grids enthusiastically rely on upon communication framework or network security for insider data, robbery strike is a basic. Standard security frameworks are not prepared to fulfill security need of this innovative technology. As needs be, there is exact need of best course of action, which competent thwart data mishap, and misuse of data. In this research article we outline the data security issues in a cloud for the smart grid with respect to fog computing, and focus on an innovative proposed approach fog computing for cloud data security to provide security elucidations for cloud data security in smart system.

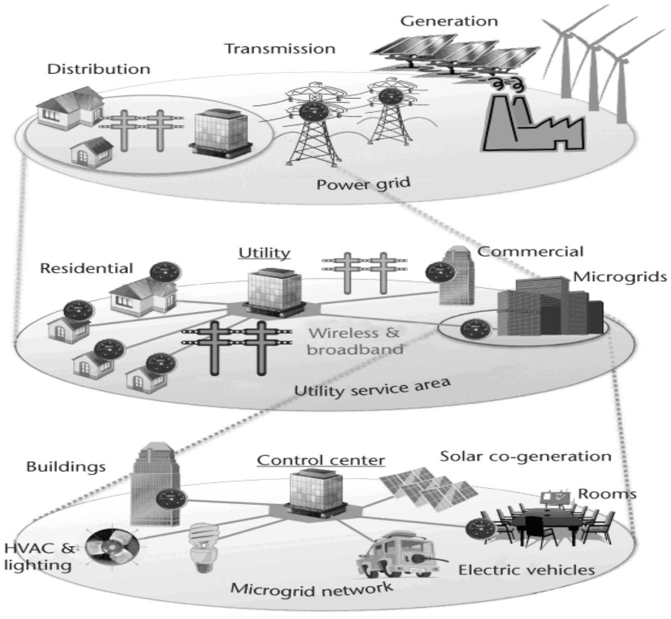
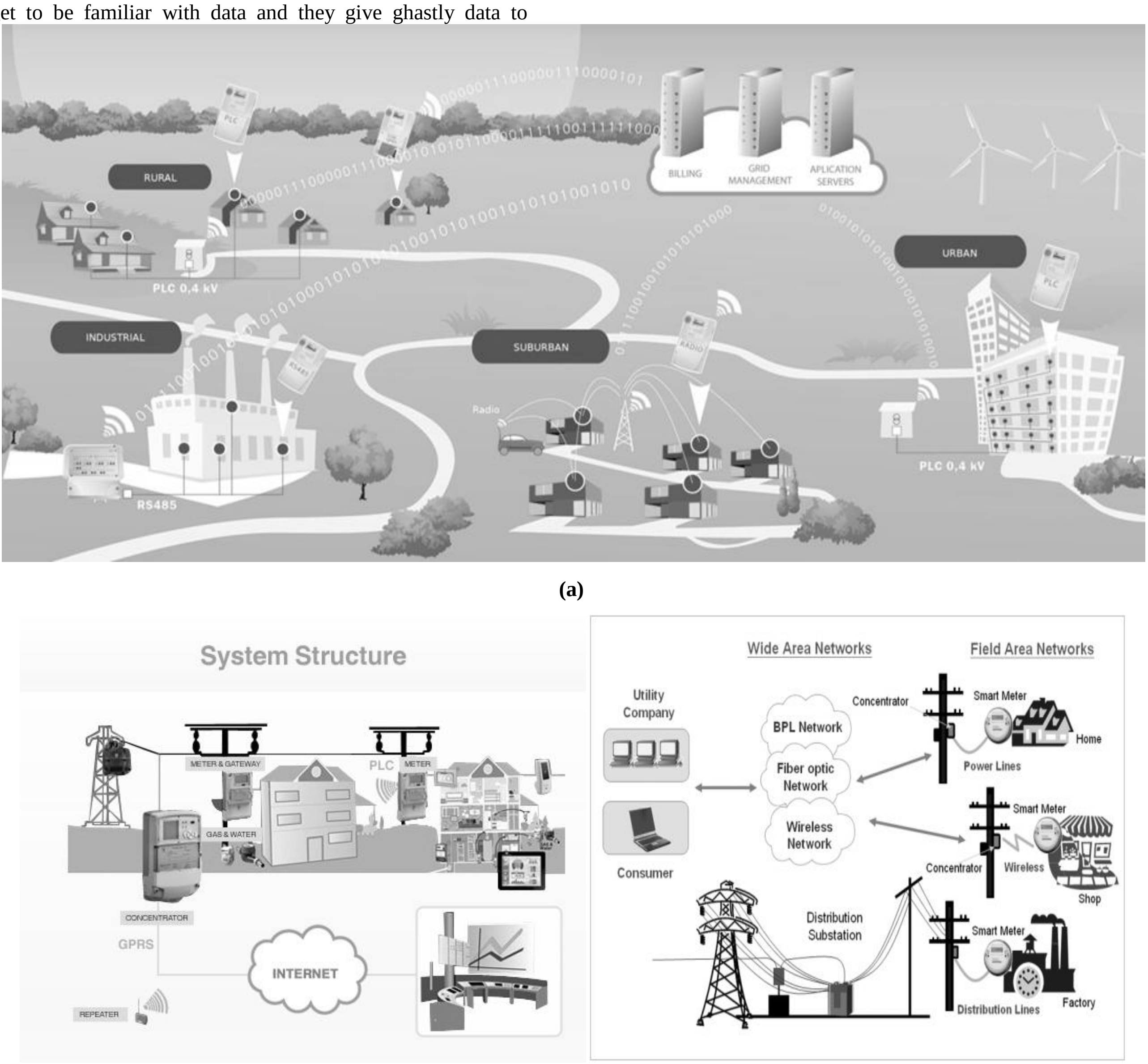


**Figure 1: Smart Grid infrastructure**

Authors of [G. Dán et al, Y. Huang, H et al, T. Liu et al, Y. Huang et al, M. Esmalifalak et al, A. Tarali et al, R. B. Bobba et al, Q. Yang et al, B. Gou et al] proposed various estimations, algorithms and methods in perspective of physics law, which recognize all around illustrated terrible data. [Y. Liu et al] states that in smart grid, Data theft strike has strong effect on system. They contemplated that unapproved persons get to be familiar with data and they give ghastly data to particular variables and on hand systems get evade for terrible estimation finding in power system, learning/knowledge of the power system setups is mishandled Smart grid is not as long-established power system where control center were separated, guaranteed. Smart grids have limitless smart metering infrastructure, distributed inside connected with the communication framework/network as shown in Fig 2.



**(a)**

**(b)** **(c)**

**Figure 2 (a, b, c): Advanced Metering Infrastructure**

## 2. LITERATURE REVIEW:

With progressions, current developments cyber attacks approaches moreover get improved due to that it is not troublesome now to break any protected communication network [H. Khurana et al, R. Q. Hu et al, A. Giani et al]. Aggressors can interfere into smart meters and overhaul readings to trap or anger charging system [P. McDaniel et al]. In legitimate field, in light of strike on data there is strong likelihood to bother demand and supply structure/system balance, addition in cost of energy, mixed up decisions due to misleader control center [T. Liu et al, J. Lin et al]. In case if intruders do well to get to data, it results in vital damage on national power infrastructure [P. McDaniel et al]. So as stated above, ambushes on data in smart grid can make imperative destruction for power infrastructure so it shows up there is necessity for strong security instrument or approach. Here the accentuation primarily on cyber security, towards the security elucidations for secure cloud by exercising decoy information technology, which have, come to call fog computing. Despite the way that Fog computing is similar to cloud however noteworthy qualification is that its closeness to end customers, support for mobility, its impenetrable geographical movement. It is therefore necessary shifting towards fog computing for security because of it holds up Internet of things (IoT) applications that demands flexibility backing and broad assortment of Geo-distribution taking in location awareness and low latency aspects. The authors using this development or technology to dispatch disinformation strikes against malicious insiders. With help of this scheme, they can keep vindictive insiders from perceiving the veritable sensitive data from fake pointless data. Fog computing is one of the profitable system which gives decoy technology. This technology mainly goes for recognizing the unapproved access employing customer behavior profiling and fake data implies decoy reports. The customer behavior profiling complete exercising data access patters. At the point when the passageway or access distinguished as unapproved, the decoy information delivered and brought into play to misdirect the intruder. The decoy reports may be honey archives/files, honey pots and decoy false information. The smart grid is viewed as the cutting edge power network and is required to address the deficits and issues of the present power grid [Farhangi, H]. It envelops a canny management and networking of power generators, power buyers, and power storage in the distribution system and energy transmission. For doing as such, the smart grid draws on different innovations [Ockwell, G], counting the Advanced Metering Infrastructure (AMI) [National Energy Technology] which is deep-seated for constant estimations and time-of-utilization meters. By means for smart meter devices consumers, energy utilization information can be watched and gathered at exceptionally successive time periods, e.g. every second. Such fine-grained meter readings facilitate vibrant pricing estimating and permit to conjecture demand of energy [Quinn E.L]. In addition, utility suppliers can encourage load balancing, pack load attenuation, and more effcient system administration. On the other hand, with the brilliant's smart grid and its popularity in our every day lives, new difficulties and concerns arise in specific about energy prosumer security [Clements, et al, Eckert, C et al], a prosumer being a producer of energy and customer in the meantime. Research has demonstrated that it is conceivable to derive and deduce private and personal subtle elements of prosumers' day by day lives from fine-grained meter readings [Molina-Markham et al]: Data Mining advancements take into consideration the extraction of occupants' ways of life comprising breakfast, lunch, and supper exercises or wake, vicinity, nonattendance, and rest cycles. As indicated by [Cavoukian et al], there will be the enticement to offer such data, e.g. utilization of energy or machine information, either in identifiable client level, anonymized, on the other hand in accumulated structure to outsiders, e.g.marketers looking for business pick up. In this way, securing prosumers' smart meter readings is a specific test in the smart grid, particularly once meter readings are discharged to outsiders. To handle this concern [Park, J et al, Pretschner] present bring into play control ideas to the smart grid area. As opposed to other information security instruments, similar to get to control that screens and controls who can get to and communicate with delicate information, utilization control is worried with how information could possibly be utilized once initial access to it has been conceded. Information or data utilization necessities, as do not disperse my meter readings are specified in use control arrangements and are upheld by the utilization control infrastructure. The essential security concerns are checking or verification at various levels of entryways and furthermore if there ought to emerge an event 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 opportunity that customer can mess around with its own specific smart meter, spoof IP addresses and report false readings, for his individual or harmful manners of thinking. [Peng Yong et al] in 2012 brought into play cryptographic approaches as a piece of their arrangement/design to come to an end examination result of secure cloud storage. Authors observed in their explorations about Smart Grid strikes and potential countermeasures [Zubair A. Baig et al]. Fig 3, displaying the security goals which have been discussed and outlined by almost all researchers.

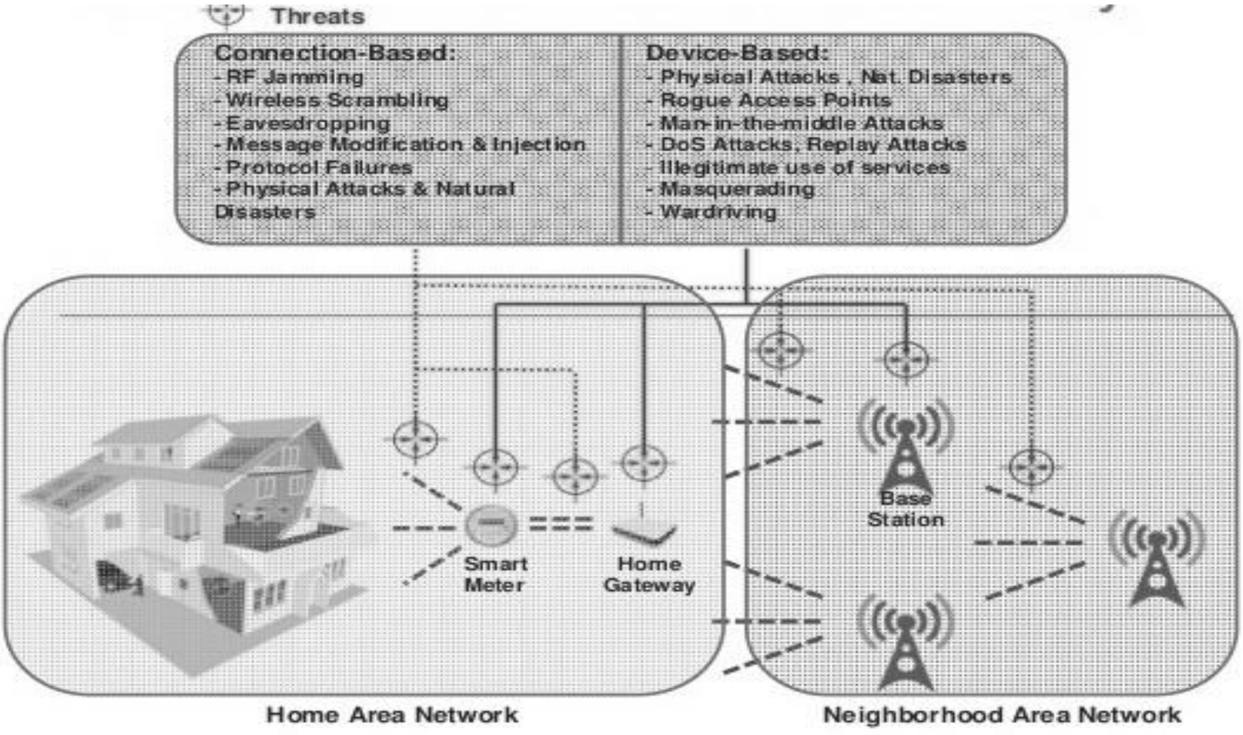

Threats
Connection-Based:
- RF Jamming
- Wireless Scrambling
- Eavesdropping
- Message Modification & Injection
- Protocol Failures
- Physical Attacks & Natural Disasters
Device-Based:
- Physical Attacks , Nat. Disasters
- Rogue Access Points
- Man-in-the-middle Attacks
- DoS Attacks, Replay Attacks
- Illegitimate use of services
- Masquerading
- Wardriving
Smart Meter
Home Gateway
Base Station
Home Area Network
Neighborhood Area Network

**Figure 3: Smart Grid Security Issues**

In 2011 there is strategy "SPARSH" projected by [Rohit Ranjan et al]. This is a biometric method employing thumb impression to confer security. This approach fill in as verification/authentication and exhibits useful while downloading and exchanging or uploading records from cloud. Then again, the declaration of Steve Kirsch of oneID have to be considered, which he said in fog computing social event, that there is a parable that biometric is well-built protection plan than whatever else in light of the fact that your fingerprints may get stolen from things which you are using . He furthermore said that passwords are frightful security is another myth; the way we are employing passwords isn't correct [Fog Computing Conference]. Think in like manner recommended that fog computing can be constructive for security in light of the fact that it focus on to recognize unapproved access through customer behavior profile that is decoy course of action or method. With decoy system, if access is unapproved it gave fake reports, which perplex assailant [Salvatore J. Stolfo et al]. Fake records may be honey pots, honey archives or any wrong bills, records that are not discriminating. This system pleasing because of two sureness's (i): It checks whether customer is authorized or not. 2: If customer is not a genuine customer puzzle it for fake records.

## 3. THE UTILIZATION OF FOG TO SECURE CLOUD:

At present cloud storage is a comprehensively used technology to store information because it have wide storage space. On the other hand, information set away or stored in cloud available thoroughly where anyone can get to it. The most basic thing should notice that when customer store information he absolutely clueless that where and how data will be secured and who will get to it. So taking all things into account customer need affirmation that his business data nobody will access without rights. Standard encryption technique is not capable enough to make it unsuccessful to balance data burglary ambush. By applying encryption technique to the information, we can't comprehend outright protection to private data. To make the smart grid safe and sound from insider data theft strike it is feasible to change from cloud to fog. Fog Computing is staggering platform for IoT's application like smart grid in light of the way that it satisfies mobility and proximity solicitations [Maher Abdelshkour]. The ultimate objective is to cutoff data loss to pull off a deterrent disinformation strike technique are going to draw on by the authors. This sheltered cloud service finished pulled off after two components cleared up [Salvatore J. Stolfo et al] in as underneath:

### 3.1 Consumer Behavior Profiling

This is behavior based security strategy. In this phase it limit access to customer that how, when, the amount of information he will get to. Supplier or supervisor keep up log of legitimate customers and set criteria for analyzing information. Behavior of typical customer interminably verified to see whether there is any abnormal behavior happened in user's data. According to customer behavior and getting the opportunity to time, system will prepared to see bizarre access.

### 3.2 Decoy Technology

When weird behavior recognized, it gave some fake reports. To do these things a couple traps set within records systems this traps are just decoy reports. These reports get set by genuine customer, camouflages or intruders completely clueless of this. So if any unapproved individual found suspicious to system he gave fake data. Right when unapproved customer gets fake data, he acknowledges that he is overseeing exceptional data. That suggests here succeeds to dumbfound customer due to that data disaster turned away. Thusly, in this way cloud data secured, and this approach is being used by the authors [Mayur Subhash Chavan] in smart grid to accomplish a paramount security elucidations.

For smart grid when consumer needs to get data from appropriated smart grid storage, for instance, customer information like area, name et cetera, bills information, need to pay charges should take after below security confirmations.

- Login.
- Enter check/verification code.
- Answer mandatory or test questions.

Right when customer passes these three stages, he can get to be familiar with data, which he needs and prepared to download/upload records as show in Fig 4.

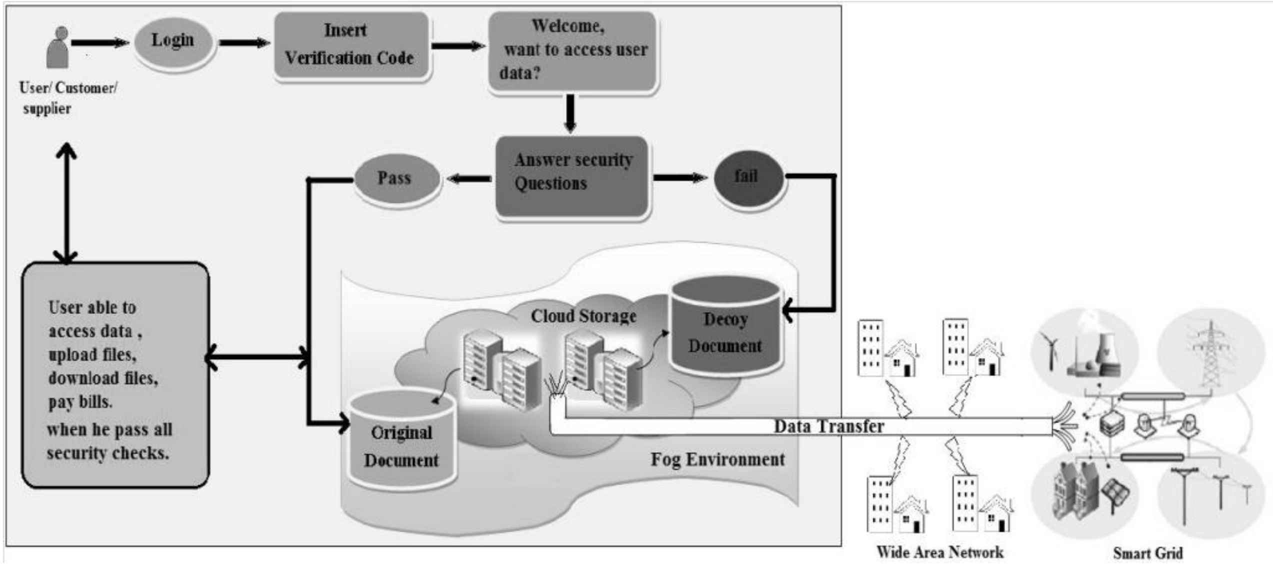

Login
Insert Verification Code
Welcome, want to access user data?
User/ Customer/ supplier
Answer security Questions
Pass
fail
User able to access data , upload files, download files, pay bills. when he pass all security checks.
Cloud Storage
Decoy Document
Original Document
Data Transfer
Fog Environment
Wide Area Network
Smart Grid

**Figure 4: Proposed Security Solution [Mayur Subhash Chavan]**

Customer must be an enrolled customer. Right when customer endeavor to login he will get one affirmation code. Affirmation code here means one time password, which he needs get access to an account. After that if, customer need to download or upload data he needs to breeze through security watches that is test questions if answer correctly then prepared to access to data. If customer fails to answer so, he will get fake/decoy data, which he acknowledges is special. Fake/decoy data put with special or original data away or in storage. Here nobody can go into cloud storage clearly; they have to experience fog environment, which made for security of data on cloud. In perspective of fog decoy document, unapproved customer will not be capable to reach to one of a kind of original document or record. Also, this how system make it to surprise mugger.

## 4. CONCLUSION

With the smart grid emergence an a lot of energy prosumers' fortification concerns emerge in light of the fact that research has demonstrated that it is conceivable to conclude private subtle elements of occupants' way of life from meter readings , particularly when those are discharged to cloud-based third-party smart grid services. We assessed data burglary strikes appear in smart grid cloud data storage. Here we outlined to offer response for such data attack with fog computing. Fog computing is another promising approach to manage securing individual and business data in the cloud. In the first place it screen unapproved access through customer behavior profile and after that second decoy chronicles or document set away in the Cloud near to the usage access. If there is any nasty behavior recalled that it confused or served the attacker with diversion reports (decoy documents).

## 5. REFERENCES

[1] "G. Dán et al", "Stealth attacks and protection schemes for state estimators in power systems," in Proc. Smart Grid Communications (SmartGridComm), 2010.

[2] "Zhong Fan et al", "Smart Grid Communications: Overview of Research Challenges, Solutions, and Standardization Activities", IEEE Communication Surveys & Tutorials, Vol.15, No.1, 2013,pp. 21-38.

[3] "Wu C et al", "A real-valued genetic algorithm to optimize the parameters of support vector machine for predicting bankruptcy", Expert System Applications 2007; 32(2):397–408.

[4] "Y. Huang et al", "Bad data injection in smart grid: attack and defense mechanisms," Communications Magazine, IEEE, vol.51, pp. 27-33, 2013.

[5] "A. Tarali et al", "Bad data detection in two-stage state estimation using phasor measurements," in Proc. Innovative Smart Grid Technologies (ISGT Europe), 2012.

[6] "Y. Huang, H et al", "Defending false data injection attack on smart grid network using adaptive cusum test," in Proc. 2011 Information Sciences and Systems (CISS), 2011.

[7] "T. Liu et al", "A Novel Method to Detect Bad Data Injection Attack in Smart Grid," in Proc. IEEE INFOCOM Workshop on CCSES, 2013.

[8] "R. B. Bobba et al", 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.

[9] "Q. Yang et al", "On False Data Injection Attacks against Power System State Estimation: Modeling and Countermeasures," IEEE Transactions on Parallel and Distributed Systems, 2013.

[10] "P. Yong et al", "Secure cloud storage based on cryptographic techniques", The Journal of China Universities of Post and Telecommunications, vol. 19, sup. 2, pp. 182-189, 2012.

[11] "M. Esmalifalak et al", "Bad Data Injection Attack and Defense in Electricity Market Using Game Theory Study", IEEE Transactions on Smart Grid, vol.4 , pp:106-169, 2012.

[12] "B. Gou et al", "A pre-procedure of bad data detection for smart grid monitoring" in Power and Energy Society General Meeting, IEEE, 2012.

[13] "H. Khurana et al", "Smart-grid security issues," Security & Privacy, IEEE, vol.8, pp. 81-85, 2010.

[14] "R. Q. Hu et al", "Cyber security for smart grid communications: part II [Guest Editorial]," Communications Magazine, IEEE, vol.51, pp. 16-17, 2013.

[15] "Y. Liu et al", "False Data Injection Attacks against State Estimation in Electric Power Grids,", Proceedings of the 16th ACM conference on Computer and communications security, 2009.

[16] "A. Giani et al ", "Smart Grid Data Integrity Attacks,", IEEE Transactions on Smart Grid, vol.4 , pp:1244-1253, 2013.

[17] "Zubair A. Baig et al", " An Analysis of Smart Grid Attacks and Countermeasures" Journal of Communications Vol. 8, No. 8, August 2013.

[18] "Rohit Ranjan et al", "SPARSH"-Data Security in Cloud, ijetae 10 Oct 2011.

[19] "P. McDaniel et al", "Security and privacy challenges in the smart grid," Security & Privacy, IEEE, vol.7, pp. 75-77, 2009.

[20] "Fog Computing Conference Speakers Explain How to Improve IoT Security" Available online at http://www.fogcomputingworld.com/topics/fogcomputin g/ articles/ November 2014

[21] "J. Lin et al", "On false data injection attacks against distributed energy routing in smart grid," in IEEE/ACM Third International Conference on Cyber-Physical Systems (ICCPS), , 2012.

[22] "Park, J et al", The UCONABC usage control model. ACM Trans. Inf. Syst. Secur. 7(1), 128{174 (Feb 2004), http://doi.acm.org/10.1145/984334.984339

[23] "Mayur Subhash Chavan", DESIGN OF SECURE FRAMEWORK FOR CLOUD DATA SECURITY IN SMART GRID WITH FOG COMPUTING, IJESMR , Aug 2015

[24] "Farhangi, H", The path of the smart grid. Power and Energy Magazine, IEEE 8(1), 18{28 (Jan 2010)

[25] National Energy Technology Laboratory for the U.S. Department of Energy: Advanced Metering Infrastructure. Tech. rep., U.S. Department of Energy (Feb 2008)

[26] ”Ockwell, G”, The DOE's "7 Traits of a Smart Grid". Fortnightly's Spark (Oct 2009) Quinn, E.L.: Smart Metering & Privacy: Existing Law and Competting Policies. Tech. rep., Colorado Public Utilities Commission (2009)

[27] ”Molina-Markham et al”, Private memoirs of a smart meter. In: Proc. 2nd ACM Workshop on Embedded Sensing Systems for Energy-E_ciency in Building. pp. 61{66 (2010)

[28] ”Clements, et al”, Cyber-security considerations for the smart grid. In: Power and Energy Society General Meeting, 2010 IEEE. pp. 1{5 (Jul 2010)

[29] “Salvatore J. Stolfo et al”, “Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud” IEEE CS Security and Privacy Workshops pp 125-128, 2012.

[30] ”Maher Abdelshkour”, “IoT, from Cloud to fog”, online Avalaible at http://blogs.cisco.com/perspectives/iotfromcloudtofogcomputing

[31] ”Eckert, C et al”, Sicherheit im Smart Grid - Herausforderungen und Handlungsempfehlungen. Datenschutz und Datensicherheit - DuD 35, 535{541 (2011)

[32] “Cavoukian et al”, SmartPrivacy for the Smart Grid: embedding privacy into the design of electricity conservation. Identity in the Information Society 3, 275{294 (2010)

[33] “Pretschner”, A.: An Overview of Distributed Usage Control. In: Proc. 2nd Conf. Knowledge Engineering: Principles and Techniques. Romania (Jul 2009)

[34] “Quinn E.L” , Smart Metering & Privacy: Existing Law and Competting Policies. Tech. rep., Colorado Public Utilities Commission (2009)