*ICIT 2015 The 7th International Conference on Information Technology*
doi:10.15849/icit.2015.0030 © ICIT 2015 (http://icit.zuj.edu.jo/ICIT15)

# *ENSURING SMART GRID DATA SECURITY AT CLOUD DATA CENTRES*

*E.Chaitanya Krishna*
Asst.System Engineer,
Tata Consultancy Servies,Bangalore,India

*Dr. K. Venkataramana*
Department of Computer Science,
KMM Institute of Post Graduate Studies,Tirupati
Email:ramanakv4@gmail.com

*Dr.Sulaiman AlMuhteb*
Department of Computer Science,S.V.University,Tirupati

*Prof..M.Padmavathamma*
Department of Computer Science,S.V.University,Tirupati

***Abstract:*** **In the world of evolving technologies the energy like solar or electricity and utilities industry, plays major role includes smart meters and smart grids, which provides companies with exceptional capabilities for forecasting demand, determining customer usage patterns, preventing outages, minimizing the loss and more. Advances in technologies and its usage generates unprecedented data volume, speed and complexity which should be preserved securely for later usage for accurate predictions. Managing the large volume information generated by short-interval reads of smart meter data by various smart devices is a challenge for existing IT resources in storing them and also ensuring the privacy of sensitive customer meter data is also a major issue in smart meter deployments. Security should be provided for data which is stored at data centers at cloud and also at local energy distributer centers at two tiers. In this paper we focus on security regarding storage of big data at data centres as well as at local distribution such as databases. So we propose MDET (Multiple Data Encryption Technique) which allows encryption of each record two times at storage centres by using Generator based encryption technique. In this technique the data in the database is encrypted twice so that the data record should be decrypted once at data centre as well as at the local distribution centre by private keys at two levels so that privacy of consumer data is not lost at either data storage centre at cloud or at local distribution centre.**

***Keywords---Smart grid, Goals of smart grid, Functions of smart grid, Securing Grid data, Big Data centres, Encryption and Decryption.***

## I. INTRODUCTION

A **Smart Grid** as a digitally enabled electrical grid that combines modern IT technology with Electrical system that gathers, distributes and acts on information about the behavior of all participants (suppliers and consumers) in order to improve the efficiency, importance, reliability, economics, and sustainability of electricity services . The deployment of advanced metering infrastructure (AMI) and intelligent supervisory control and data acquisition (SCADA) systems is essentially all about improving the amount and quality of data that utilities have on supply and distribution. Data is the fundamental currency of the smart grid. A clear understanding of how this data is generated, what it consists of and the benefits it can be used to deliver is critical to realizing the fullest possible returns from smart grid investments. Over the past 50 years, electricity networks have not kept pace with modern

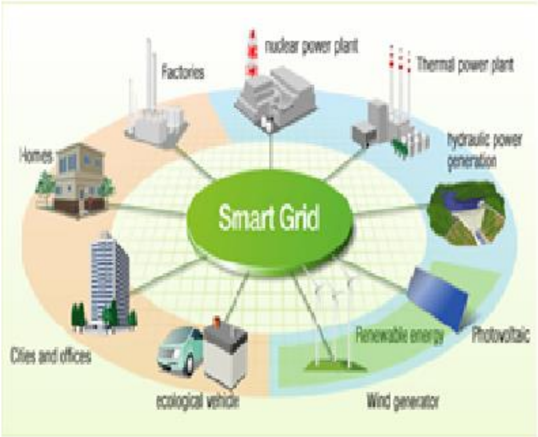

**Fig-1 SMART GRID**

challenges, such as: Data storage, Security threats, from either energy suppliers or cyber-attack, national goals to employ alternative power generation sources whose intermittent supply makes maintaining stable power significantly more complex. In general, data management design in any context should optimize outcomes in two ways. First, it should extract clean, consistent and well understood information that drives targeted benefits for the business. And second—having identified those benefits—it should minimize the costs of infrastructure needed to obtain and process the data necessary to deliver these benefits. Before inception of Smart grids the data relating to distribution of electricity collection is very rudimentary like consumption data on customer premises one data point a month per customer. But Smart grids have changed things. The deployment of advanced metering infrastructure (AMI) and intelligent supervisory control and data acquisition (SCADA) systems is essentially all about improving the amount and quality of data that utilities have on supply and distribution. The advent of AMI has increased the level of data collection dramatically from megabytes to Exabyte which requires Data centres and cloud infrastructure. Modern Smart grid data should be maintained at data centres at cheap cost , also should be guarded against unauthorized access at service provider level as well as at data centre level [8].

A smart grid is a large-scale system that extends from a power generation facility to each and every power consuming device such as home appliance, computer, and phone. This large-scale nature has increased the possibilities of remote operation of power management and distribution system. With energy being a premium resource, ensuring security against theft, abuse, and malicious activities in a smart grid is of prime concern.

The challenges of ensuring cybersecurity in a smart grid are diverse in nature due to the diversity of the components and the contexts where smart grids are deployed. Deploying a smart grid without strong and diligent security measures can allow advanced cyber-attacks to remain undetected, which can eventually compromise the entire system [9]. Inadequate security measures can also compromise the stability of the grid by exposing it to, for example, utility fraud, loss of confidential user information and energy-consumption data [10].

The cyber security objectives can be classified into the following three categories [9, 11]. (i)Integrity. Protecting against the unauthorized modification or destruction of information. Unauthorized information access opens the door for mishandling of information, leading to mismanagement or misuse of power. (ii)Confidentiality. Protecting privacy and proprietary information by authorized restrictions on information access and disclosure.(iii)Availability. Ensuring timely and reliable access to information and services. Availability can be compromised by disruption of access to information which undermines the power delivery. To ensure above, for securing smart grid data we have proposed an MDET algorithm for providing privacy and secrecy for data at data centres storage.

## II. ARCHITECTURE OF SMART GRID

An electrical grid is not a single entity but an aggregate of multiple networks and multiple power generation companies with multiple operators employing varying levels of communication and coordination, most of which is manually controlled. Smart grids as show in Fig-1 increase the connectivity, automation and coordination between these suppliers, consumers and networks that perform either long distance transmission or local distribution tasks. This paradigm is changing as businesses and homes begin generating more wind and solar electricity, enabling them to sell surplus energy back to their utilities. Modernization is necessary for energy consumption efficiency, real time management of power flows and to provide the bi-directional metering needed to compensate local producers of power. Although transmission networks are already controlled in real time, many in the US and European countries are antiquated by world standards, and unable to handle modern challenges such as those posed by the intermittent nature of alternative electricity generation, or continental scale bulk energy transmission. Smart Grids are profitable for industrial sector in various like aluminum processing, cement manufacturing, food processing etc. which should function in accordance with by greenhouse emission standards. [4] Smart Grid uses computer communication networks which requires security [5].

## III. GOALS OF THE SMART GRID

Latency of the data flow is a major concern, with some early smart meter architectures allowing actually as long as 24 hours delay in receiving the data, preventing any possible reaction by either supplying or demanding devices.

### *A. Smart Energy Demand*

Smart energy demand describes the energy user component of the smart grid. It goes beyond and means much more than even energy efficiency and demand response combined. Smart energy demand is what delivers the majority of smart meter and smart grid benefits. Smart energy demand is a broad concept. It includes any energy-user actions to: a) Enhancement of reliability b) reduce peak demand, c) shift usage to off-peak hours d) lower total energy consumption e) actively manage electric vehicle charging f) actively manage other usage to respond to solar wind and other renewable resources g) buy more efficient appliances and equipment over time based on a better understanding of how energy is used by each appliance or item of equipment. All of these actions minimize adverse impacts on electricity grids and maximize utility and, as a result, consumer savings.

## IV. FUNCTIONS OF SMART GRID

Before examining particular technologies, a proposal can be understood in terms of what it is being required to do. The governments and utilities funding development of grid modernization have defined the functions required for smart grids. Smart Grid Technology will have following functionalities [1] such as

### *A. Self-healing*

Using real-time information from embedded sensors and automated controls to anticipate, detect, and respond to system problems, a smart grid can automatically avoid or mitigate power outages, power quality problems, and service disruptions. Technology such as Fault Detection Isolation and Restoration can be used in conjunction with protective relays to automatically detect and isolate a fault, and then restore power to as many customers as possible. This will greatly improve the reliability of the electrical distribution network

### *B.Consumer Participation*

A smart grid is a means for consumers to change their behavior around variable electric rates or participate in pricing programs designed to ensure reliable electrical service during high-demand conditions. Historically, the intelligence of the grid in North America has been demonstrated by the utilities operating it in the spirit of public service and shared responsibility, ensuring constant availability of electricity at a constant price, day in and day out, in the face of any and all hazards and changing conditions. A smart grid incorporates consumer equipment and behavior in grid design, operation, and communication.

### *C. Resist Attack*

Smart grid technologies better identify and respond to man-made or natural disruptions. Real-time information enables grid operators to isolate affected areas and redirect power flows around damaged facilities.

### *D. High Quality Power and Generation options*

As smart grids continue to support traditional power loads they also seamlessly interconnect fuel cells, renewables, micro turbines, and other distributed generation technologies at local and regional levels. Integration of small-scale, localized, or on-site power generation allows residential, commercial, and industrial customers to self-generate and sell excess power to the grid with minimal technical or regulatory barriers.

### *E. Enable Electricity Market*

Significant increases in bulk transmission capacity will require construction of new transmission lines before improvements in transmission grid management proposed by smart grids can make a difference. Such improvements are aimed at creating an open marketplace where alternative energy sources from geographically distant locations can easily be sold to customers wherever they are located.

### *F. Optimize Assets*

A smart grid can optimize capital assets while minimizing operations and maintenance costs. Optimized power flows reduce waste and maximize use of lowest-cost generation resources. Harmonizing local distribution with inter-regional energy flows and transmission traffic improves use of existing grid assets and reduces grid congestion and bottlenecks, which can ultimately produce consumer savings. Smart Grid technologies will enable power systems to operate with larger amounts of such energy resources since they enable both the suppliers and consumers to compensate for such intermittency.

## V. SMART GRID DATA MANAGEMENT

In terms of the flow of smart grid data, we have identified five architectural stages that can be used to guide the design of the data management structure. As Figure 2 illustrates, data is initially generated by network devices such as meters and sensors, before being transported for storage and processing by various applications—the persistence phase. Then it is transformed into actionable operations-oriented information for network and technical analysis, requiring new visualization capabilities. Finally, the resulting analytics applicable for the non-real time operational consumption are integrated at the enterprise level to drive strategic decision making.

There are five separate classes of smart grid data, each with its own unique characteristics.

1. *Operational data*—represents the electrical behavior of the grid. It includes data such as voltage and current phasors, real and reactive power flows, demand response capacity, distributed energy capacity and power flows, and forecasts for any of these data items.

2. *Non-operational data*—represents the condition, health and behavior of assets. It includes master data, data on power quality and reliability, asset stressors, utilization, and telemetry from instruments not directly associated with grid power delivery.

3. *Meter usage data*—Includes data on total power usage and demand values such as average, peak and time of day. It does not include data items such as voltages, power flows, power factor or power quality data, which are sourced at meters but fall into other data classes.

4. *Event message data*—consists of asynchronous event messages from smart grid devices. It includes meter voltage loss/restoration messages, fault detection event messages and event outputs from various technical analytics. As this data is triggered by events, it tends to come in big bursts.

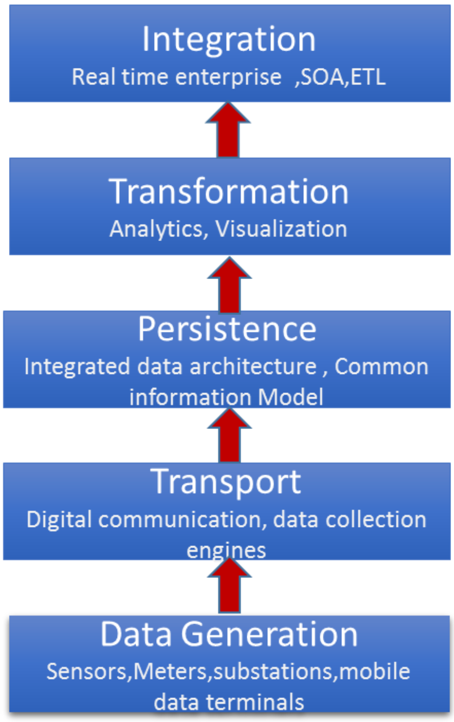
Integration
Real time enterprise ,SOA,ETL
Transformation
Analytics, Visualization
Persistence
Integrated data architecture , Common information Model
Transport
Digital communication, data collection engines
Data Generation
Sensors,Meters,substations,mobile data terminals

**Figure-2 Five architectural stages of smart grid data management**.

5. *Metadata*—is the overarching data needed to organize and interpret all the other data classes. It includes data on grid connectivity, network addresses, point lists, calibration constants, normalizing factors, element naming and network parameters and protocols. Given this scope, managing metadata for a smart grid is a highly challenging task. While the first three of these classes are relatively familiar to utilities, the last two have been less prominent to date—and are likely to present more problems as utilities adapt to the smart grid world

In our view, there are two prerequisites for overcoming the challenges of the smart grid data deluge. One is ensuring that the five data classes we previously highlighted are reflected in the data integration architecture. The other prerequisite is the effective use of the right analytics to turn the mass of data into usable information and business intelligence.

If designed properly, the data architecture will provide the capabilities utilities will need to deal with future change and evolution in their smart grids and business environment. To do this, the architecture will need to include more than just data stores, but also elements such as master data management, services and integration buses to effectively share data and information.

## VI. VULNERABILITIES IN SMART GRID DATA MANAGEMENT

Smart grid network which not only provides improved capabilities to the conventional power network making it more complex in terms of generating huge volume of data which leads to vulnerable to different types of attacks. These vulnerabilities might allow attackers to access the network, break the confidentiality and integrity of the transmitted data, and make the service unavailable [2][3]. The following are the vulnerabilities to be considered:

a) Network security of distributed systems across meters, substations, poles and In-home devices including authentication, detection, and monitoring

b) Identity & access management for managing customer information
c) Messaging and application security communications including data network communications, and transactions.

d) Security policy management and implementing web services security standards

e) Customer security: Smart meters autonomously collect massive amounts of data and transport it to the utility company, consumer, and service providers. This data includes private consumer information that might be used to infer consumer's activities, devices being used, and times when the home is vacant.

f) Greater number of intelligent devices: A smart grid has several intelligent devices that are involved in managing both the electricity supply and network demand. These intelligent devices may act as attack entry points into the network. Moreover, the massiveness of the smart grid network (100 to 1000 times larger than the internet) makes network monitoring and management extremely difficult.
g) Physical security: Unlike the traditional power system, smart grid network includes many components and most of them are out of the utility's premises. This fact increases the number of insecure physical locations and makes them vulnerable to physical access.

h) Implicit trust between traditional power devices: Device-to-device communication in control systems is vulnerable to data spoofing where the state of one device affects the actions of another. For instance, a device sending a false state makes other devices behave in an unwanted way.

i) Different Team's backgrounds: Inefficient and unorganized communication between teams might cause a lot of bad decisions leading to much vulnerability.

j) Using Internet Protocol (IP) and commercial off-the-shelf hardware and software: Using IP standards in smart grids offer a big advantage as it provides compatibility between the various components. However, devices using IP are inherently vulnerable to many IP-based network attacks such as IP spoofing, Tear Drop, Denial of Service, and others [7].

## VII. PROPOSED SECURITY MODEL TO SMART GRID DATA

Encryption is mechanism is used to address security or privacy concerns whether is it is a small or big data, or when data in data centres are shared between different types of consumers. The main aim is to secure every clients data so that it will remain inaccessible to unauthorized parties even if they come into possession of it. By above study we have proposed this model shown in figure-3 known as Smart Grid Secure Data Management Model [8].

In this proposed model we enhance the security of Smart Grid Data (SGD) stored data in cloud data centre by providing multi-level layered security solution for data at storage and at the client level. Cloud Service Provider(CSP) stores SGD stored at Data centre is monitored by Security Provider Service (SPS) which generates keys to ensure security by encrypting data stored at Data centre as well as data stored at Distributer site. In SPS module we have used MDET security algorithm which provides multiple keys to ensure security to customer data.

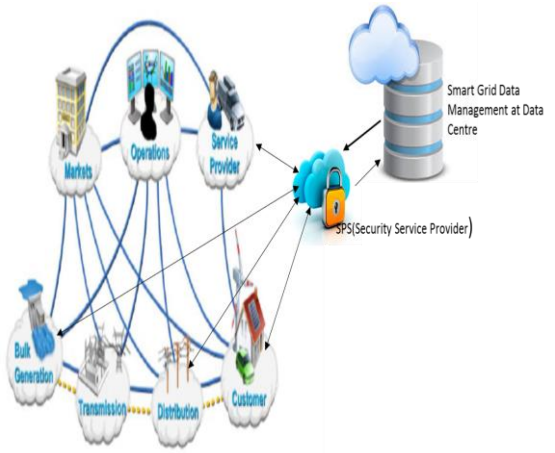

**Fig: 3 Smart Grid Data at Data centre Secured by SPS service**

The Proposed model mainly contains two Services controlled by CSP

*a) Registration Service* used for registration of Distribution Company Client/Customer which is using Smart Grid Services to store data in data centres in Cloud.

*b) Security Provider Service (SPS*) which authenticates client request and stores clients data securely which will be secured from attacks in networks. In this SPS we have used various MDET which uses cryptographic techniques for secure storage and transfer of data in communication networks.

## VIII. MULTIPLE DATA ENCRYPTION TECHNIQUE (MDET)

In this environment of Data Centres at Cloud terabytes of data generated by Smart Grid applications are stored which raises various concerns of security are raised. So to ensure security for data of each client , in this paper we are proposing Multiple Data Encryption Technique(MDET) in which each record in stored is encrypted two times by Security Provider Service (SPS) first by Data centres 's public key and by Clients, and decrypted only by Client. Since the record 'R' to be stored at data centre is encrypted by twice, Smart Grid Data SGD cannot be revealed. In this way the proposed

MDET technique is secure by not revealing the record to other client or Intruders at Data centres in Cloud.

In this technique, we assume $C_1,C_2,C_3….C_n$ are clients of Smart Grid Company who stores data in Data centres in cloud C. Let Cloud service provider (CSP) and Security Service Provider provides sharing of database securely to multiple clients In this algorithm the data is stored in encrypted format for security purpose, as the database is in cloud, to avoid unauthorized users to access data. The algorithm is given below

## A. MDET ALGORITHM

1. SPS generates a large Prime $T_p$ from credentials of Client user of Smart Grid Data stored in data centre in Cloud Service Provider.

2. SPS computes $N=2*T_p$

3. SPS generates Cyclic group $Z_N*$ of order $Ø(N)$(Euler Totient function)

4. A subgroup $Z_{Ø(N)}*$ subset of $Z_N*$ of order $Ø(Ø(N))$ is generated by SPS with generator $g \in Z_n*$

5. SPS picks randomly picks up two private keys $T_q$ and $T_r \in Z_N*$ $T_q\equiv g^{k1}$ mod N and $T_r\equiv g^{k2}$ mod N where $k1,k2 \in Z_{Ø(N)}^*$ where g is generator for $Z_N^*$

6. SPS computes $N= T_q* T_r$ for Smart Grid Client $C_i$

7. SPS chooses ‘e’ for $C_i$ such that gcd(e, Ø(N))=1

8. SPS determines ‘d’ for $C_i$ such that $ed\equiv 1 \bmod Ø(N)$

9. SPS computes $CP_r = e.rs_t$ such that $e.rs_t \equiv 1 \bmod Ø(N)$ and $CP_b =d.rs_d$ such that $d.rs_d \equiv 1 \bmod Ø(N)$ where $CP_r$ :Private key $<CP_r,d,e>$, $CP_b$: Client public key, Public key$<N,CP_b>$

10 SPS encrypts the data of each Client $C_i$ stored in data centre with First level key and obtains Clients encrypted record (CER) $CER= R^e \bmod n$

11. SPS stores CER in $C_i$ after encrypting CER another time to obtain Encrypted Smart Grid Data Record $ESGDR=CER^{CP_b} \bmod n$

12. When Clients data is used/requested at Distributor site other than data Centre SPS sends Security Key to Distributor Location separately.

14. When Client $C_i$ requests data from Cloud CSP sends encrypted record ESGDR to Distributor Site.

15. After receiving Client at distributor site $C_i$ computes Smart Grid Data $SGD=ESGDR^{rst} \bmod N$ to obtain original Record.

## IX. CONCLUSION

Smart Grid is required that combines Information Technology (IT) with renewable energy to significantly improve how electricity is generated, delivered, and consumed. Smart grids generates huge volumes of data which are stored in data centres in cloud which should be stored securely to avoid modification of data by unauthorized users which may lead to collapse of grid. So the Smart Grid Data (SGD) in data centres should be secured by cloud with an efficient cryptographic technique which we have proposed as Multi Data Encryption Technique (MDET). MDET technique is used by Security Provider Service which encrypts data twice for security. Smart grid data management will enable the information collected through smart grids will not only empower customers to manage their electricity consumption but will enable electricity system operators to better understand and meet users' needs. In this paper we have taken the issue of security to Smart Grid data and given a Model containing SPS which helps CSP to ensure security and in our future works we give practical results to above model.

## REFERENCES

[1] Sinha, A.; Neogi, S.; Lahiri, R.N.; Chowdhury, S.; Chowdhury, S.P.; Chakraborty, N, ”*Smart grid initiative for power distribution utility in India*”, Power and Energy Society General Meeting,IEEE,(2011).

[2] Pearson I. Smart grid cyber security for Europe. Energy Policy, 2011; 39(9):5211-5218.

[3] Clements S and Kirkham H. *Cyber-security considerations for the smart grid*. In: Proc of the IEEE Power and Energy Society General Meeting, 2010:1-5.

[4] Tariq Samada, Sila Kiliccote ,”*Smart grid technologies and applications for the industrial sector*”, Journal of Computers and Chemical Engineering,Elsevier,2012

[5] Wenye Wang,Yi Xu, Mohit Khanna,”*A survey on the communication architectures in smart grid*”, Journal of computer networks, Elsevier,pp 3604–3629,2011

[6] Fadi Aloula*, A. R. Al-Alia , Rami Al-Dalkya, Mamoun Al-Mardinia, , *Smart Grid Security:Threats, Vulnerabilities and Solutions*, International Journal of Smart Grid and Clean Energy vol. 1, no. 1, September 2012,

[7]. K.Venkataramana, Prof.M.Padmavathamma, *Multi- Tenant Data Storage Security In Cloud Using Data Partition Encryption Technique,* International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013, ISSN 2229-5518

[8]. Jason Deign,Carlos Márquez Salazar, *Data Management and Analytics For Uitlities*, Smart Grid Update, www.smartgridupdate.com

[9]. E. Hayden, "*There is No SMART in Smart Grid without secure and reliable communications*," Tech. Rep., Varizon, http://www.verizonenterprise.com/resources/whitepapers/wp_no-smart-in-smart-grid-without-secure-comms_en_xg.pdf.

[10]. X. Fan and G. Gong, "*Security challenges in smart-grid metering and control systems*," Technology Innovation Management Review. In press.

[11]. *Guidelines for Smart Grid Cyber Security*, The Smart Grid Interoperability Panel: Cyber Security Working Group, Gaithersburg, Md, USA, 2010.