Privacy Protection in Smart Grid using Blind Signature Method

K.Govinda, Abhigyan Singh, Somula Ramasubbareddy

Abstract*: *A grid (electrical) that is capable of being electronically controlled and that grid is used for connecting transmission, power generation, distribution (of electricity) as well as consumers using communication and or along with information technologies is called Smart Grid. Information flow that is Bi-directional in nature between the one that provide utility and the one that consumes electricity is one the key feature characteristic of the smart grid. This interaction that is two way in nature permits real time generation of electricity orin real-real--time period based on the demands of the consumer and requirement requests for power. The result of which is, privacy of the client becomes a vital importance and concern, when the usage data that is related to energy is collected with adoption as well as the deployment of smart grid technologies. For the protection of such sensitive data and information (related to consumer), it makes the use of mechanism that are used for privacy protection very much imperative or important for the protection the of smart grid user's privacy. This paper proposes an analysis related to the privacy mechanisms and solutions of the smart grid that are recently proposed and intern identifying their weaknesses as well as strengths in terms of their efficiency, complexity of implementation, simplicity and robustness.

Keywords: **Smart Grid, Security, Energy, networks, RSA.S.**

I. INTRODUCTION

The grid that is based on electric power is a system used for transmission or transmission system, are used for power and electricity transfers from systems like hydroelectric systems, nuclear systems ,wind farms, to substations used for distributing (as shown in Figure 1), and concluding with the delivery of electricity to house hold and industrial users

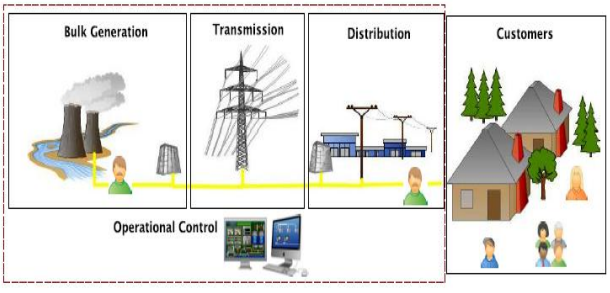

Fig1. Energy Distribution

The vitality creation and dispersion composition are directed by a brought together control framework, known as SCADA or Supervisory Control and Data Acquisition frameworks, responsible for envisioning and mapping any action that is operational or we can say functional action in this area just as capacity controlling and intensity request. Actually, SCADA (Supervisory Control and Data Acquisition frameworks) frameworks is capable of locally and remotely controlling the transmission of power and present interest dependent appropriation and pinnacle stacks along these lines limiting pointless power age as shown in figure2.

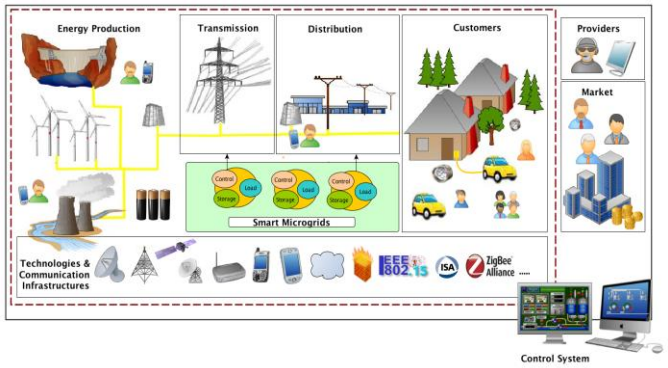

Fig 2: Architecture of the smart grid

Smart Meter (SM) is a critical and basic segment of the forthcoming vitality arrange, authored SG or the smart grid. Smart meter can be characterized as correspondence framework as well as related information the executive's framework which permit gathering, handling, and conveyance of data amongst the smart meters or the SM, clients as well as the service organizations. SM's importance is that it provides the ability of interconnecting various SG fragments as well as limiting inside a correspondence orchestrate that is two-way in nature. The objective or the aim is to help a financially compellingmonetary power system with security of supply andhigh gauge. To achieve or to accomplish this objective, pushed Smart meter or the SM limits may consolidate motorized meter readings (AMRs), coursed essentialness storing, circulated vitality asset the board (lfrom sustainable assets), just as vitality effectiveness instruments, for example, motivation based direct burden control and continuous enhancements for burden moving/planning. At last, SM or the smart meter will inturn help SG partners in advancing as well as improving lattice activities along with administrations.Data privacy usually concerns or deals with the security of the data linked with, or deals with inferring of information related to, individual's life. The issue related to security insurance is characteristic in the SG in light of the fact that visit information gathering from shrewd meters uncovers an abundance of data about private

Revised Manuscript Received on September 22, 2019.

K.Govinda,VIT Univeristy, Vellore, Tamilnadu.
Abhigyan Singh,VIT Univeristy, Vellore, Tamilnadu.
SomulaRamasubbareddy,,InformationTechnology,VNRVJIET, Hyderabad, Telangana.

apparatus use [4]. Data multiplication and remiss controls joined with granular savvy meter information accumulation make a danger of security attacks

The Smart Grid is intended to give the security in which has increased considerable consideration in the exploration network [1]. SG is a mix of various frameworks and subsystems and is helpless different assaults that may make diverse dimensions of damages the gadgets and even to the general public everywhere [2]. An essential issue which is related with brilliant lattice is the issue of security and protection. It is essential to verify the shrewd framework, from psychological militant assaults, yet additionally from clients and building specialists who can mess with different gadgets. The Key administration is one of the essential security prerequisites to accomplish information privacy and trustworthiness in brilliant lattice framework. The Smart Grid is intended to furnish purchasers with solid, productive, and safe electric vitality. Security in the Smart Grid isn't just imperative to verifying the new correspondences and frameworks on the Internet, yet in addition to guaranteeing wellbeing and unwavering quality for the basic utility of intensity. Giving a verification conspire and giving key administration conventions are necessary initial steps related to structuring as well as executing framework security in the smart grid or the SG.

In smart grid network, key inquiries in regards to setting the approaches on client information protection[17]. Data related to customer is owned by who? The access to as well as the use of data of the customer is regulated how? Ensuring the security as well as protection of client's information is done by whom? Indeed, opposition power suppliers can contend to the market overwhelming, and their entrance to clients' power use design and conduct data could be extremely significant. The power suppliers or supplier operators may utilize the client information to decide their business methodologies and exceptional bundles as well as offers. In a condition that is related to open market, these types of information can be somewhat gathered after opening of the offers and few data is accessible for all, however on the off chance that security is ruptured heretofore and explicit client information is accessible to a few gatherings, at that point these power suppliers may have out of line gains. Fitting protection arrangements may confine or relieve or resolve such utilization of out of line implies in setting business techniques. Every one of these issues clarify why the security of information of brilliant framework clients is a basic issue both for clients and the power suppliers.

Fig 2. A modern smart meter

II. PROTECTION

The popularity of SG technologies has led up the way to various issues related to security on different levels of the communication, the consumer, and the energy provider. NowSecurity perspectives, for example, privacy, verification, approval, uprightness, and non-revocation for keen framework advancements are presently being widely examined and different inventive arrangements are being proposed in the writing. The creators of [8] gave a portion of the early bits of knowledge into how to tidy power frameworks issues related to forgetting security. Also Lu et al. in [9] checked on the dangers related to security in the way of correspondence arranges in brilliant matrix environment as well as assessed effect of these dangers. Along with the authors stated above Steven et al. concentrated in a savvy network security territories, for example, correspondence, trust as well as gadget security. McDaniel et al. in [11] talked about a few issues coming about because of the organization of the savvy lattice framework and displayed different challenges related to protection as well as security challenges in the keen matrix. McDaniel et al. in their work recognize issues related to protection as well as security. They contend that arrangements related to security safeguard from different types of fakes as well as assaults to the framework while protection arrangements make information out of reach to unapproved parties. Despite the fact that crafted by McDaniel et al. given an exceptionally constrained commitment to the issue of keen framework security, it highlighted its significance in future brilliant network organization and appropriation. From that point forward, the investigation of protection in shrewd matrix has begun to produce a great deal of enthusiasm for the exploration network and industry especially with regards to the accumulation and the utilization of vitality utilization information gathered from homes that are utilizing the savvy lattice innovation. [22] stated that, a brilliant framework organized as 3 layers are considered by the creators, the 3 essential layers: at the most elevated layer or the upper, control focus is present kept up by the administrator of power, second layer comprises of various substations inside the circulation arrange thereby every SS(substation) is in charge of the region's power supply as well as the least layer has the shrewd meters that are deployed or set in clients' premises as appeared in Figure 4. i.e.the figure given below The proposed Anonymous Credential engineering [22] jelly clients' security data, including their day by day power utilization design from outsiders just as from the power administrator. The plan depends on visually impaired marks. Dazzle mark is a technique that permits the principal i.e the Party 1 to sign a message created by the second gathering i.e. Party 2, with its real substance unknown. The point when an outsider i.e. Party 3 gets the message that are marked, it can easily confirm that party 1 marked the message. The Anonymous Credential conspire utilizes visually impaired mark strategy to permit the control focus i.e. the party 1 to sign a certification created by a client i.e. the party 2 with its real substance unknown. Sometime in the not too distant future, the control focus itself i.e. Party 3 can confirm that the certification is to be sure marked by Party 1 without realizing who asked for the

mark or when the mark was produced.

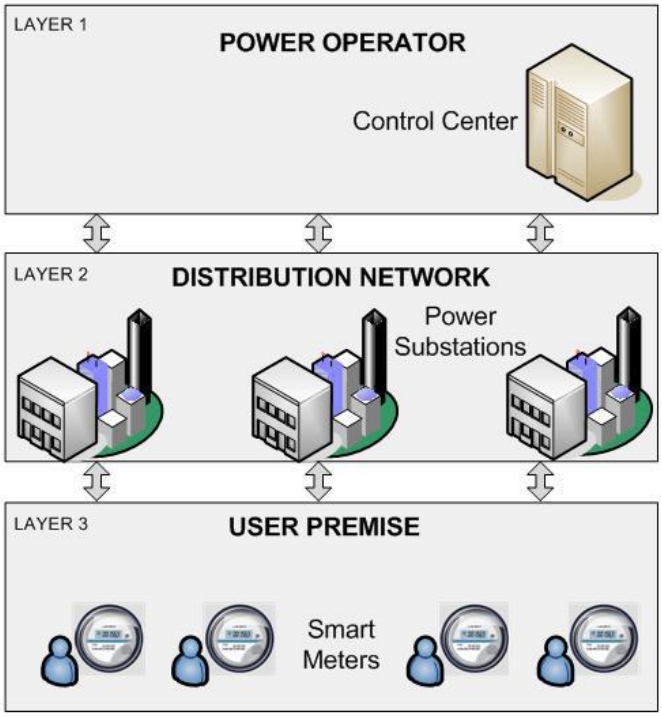

Fig 3. A 3-layer smart grid system

The use of the visually impaired mark strategy in this plan is as per the following: The clients set up a lot of certifications, each expressing the measure of power asked for, as well as request for the party1 to indiscriminately sign them with goal that the client can present any of these qualifications for the demand of power. Party 1 being unaware of the the actual content that comprises the message sent by Party 2, widely used e-cash scheme's special technique is used for the verification of the message is verified using a special technique. Various blinding factors are used to generate n messages by Party 2. n messages are then blinded as well as sent to the Party 1. After that,mmessagesis randomly chosen byParty 1 (m < n) and Party 2 is challenged to reveal them by providing or giving m blinding factors. If correct m blinding factors are provided, the signature request is accepted by Party 1 and remaining (m – n) messages are signed. The assumption of the scheme is that any type or kind of smart meter can be used for communication with the control center via a secure communication channel (such as in AES).

III. PROPOSED MATHOD

This proposes a method to solve the privacy issue in smart grids by using blind signature technique. During the presentation of a credential anonymously by a customer, the control center usually have a hard time telling or identifying the customer who made the request, yet the valid customer can be confirmed or verified by verifying the signature (since blind signatures can only be requested by valid customer). The 4 phases involved in the Anonymous Credential scheme follows:

Setup phase: RSA is assigned to a control center by itself i.e. private as well as public pair of keys for signing credentials.

Registration phase: Start of each month marks its starting and is carried out thereafter. The phase i.e. registration can be said as not anonymous. Authenticated channel are used through which customers using their real identity are required to be authenticated.

Power requesting phase: The moment need for more power is identified by the smart meter of the customer so as to support the electric appliances the execution of this phase can take place at any time of the month. This phase is anonymous.

Reconciliation phase: The end of every month marks this phase. The phase can be consideredanonymous. The unused credentials are sent back by the smart meter so as to the CC (control center) thereby evaluating the total amount of requested power.RSA is considered to be amongst primary sensible and effective public-key cryptosystems as well as transmission of data securely. In this type of cryptosystem, the key used for encryption is public in nature. In RSA, the asymmetry found is based upon the issue regarding that is quite practical about the factorization of 2 big prime numbers product, i.e. factoring problem. RSA came from the surnameRivest, Shamir, and Adleman, who in 1977 publicly described and detailed the algorithm. Amathematician, i.e. Clifford Cocks in 1973developed a same type of system, not declassified until 1997. A person who uses RSA creates, thereby publishes a key that is public that are 2 big numbers that are prime based, alongside auxiliary value. The prime numbers are supposed to be a secret. Any person will be able to make use of the key that is generally public for encryption ofthe message, but according tomethods that are currently published, if the key that is public is bigenough, only and only a persons with idea and knowledge of numbers that are prime will be able to feasibly decipher the message.[2]RSA problem is the term given to breaking of encryption done in accordance with RSA.

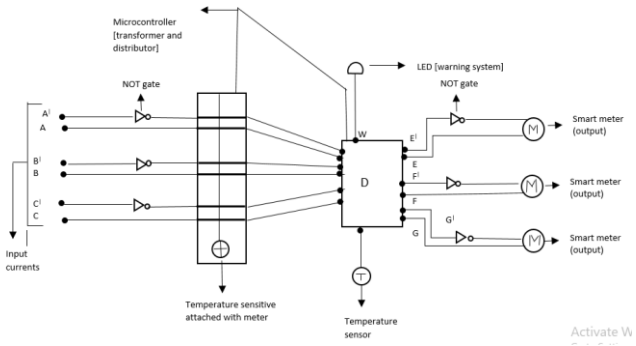

Fig4. Proposed Circuit Diagram

Upon As seen in the proposed architecture above, the input sources will have one extra path for each current carrying line but the difference is that the alternative line will be NOT Gates. These lines are then connected to a Micro controller which is inturn connected to another Micro Controller. The Distributor will have various Output lines same as the input lines I.E. having alternative paths installed with NOT gates. The output lines are connected to SMART Meters which are installed in households and various other buildings.Now under normal condition the micro

controller will be programmed in such a way that the current will only flow from normal lines (lines without NOT gates). Now suppose the output requirement is increasing but input current is stationary, this will cause a serious damage. To prevent this SMART meter will automatically signal, the distributor about increase in demand, thus distributor programmed in such a way that it will increase the current drawn from the transformer thereby satisfying the demand.SMART meter also prevent damages to household as it will report the distributor about any short circuit and the distributor will take the alternative path consisting of NOT gate which will intern nullify the current flowing through it thereby preventing damage. The TRANSFORMER will also work in the same way, it'll consist of a temperature sensor. In case the input current increases, the resistance will increase, increasing the temperature. The Transformer being programmed in such a way that after a particular temp. it will automatically switch to the alternative path for input current with a NOT gate. The Same Temperature sensor will be there in Distributor for the same function also initializing the warning system.

IV. RESULT AND CONCLUSION

A framework that is secure and related to the field of smart grids is presented in this paper which is capable of providingauthentication that is mutual as well as mechanisms related to key management by using anonymous identity modules and blind signatures. The security aspects that are required by a SG system are addressed by the proposed mechanism as well as, along with that, efficient process management. The paper also discusses about the anonymous credential technique which we can say isauthentication with low-cost mechanism as well as intuitive for the SG (Smart Grid) through RSA credential technique. SG because of big key sizes along with distribution of big key overhead endures resource utilization that is very inefficient so as to get the security benefits provided by PKI. Our mechanism as a final result saves quiet the consumption of resources that can be efficiently used for securing the system with higher security by refreshing keys or data delivery handling, bringing the utilization of smaller sizes key as an opportunity to SG, thereby reducing the resource consumption in system even further.

REFERENCES

1) R. McClanahan, "SCADA and IP: Is Network Convergence Really Here?", IEEE Industry Applications Magazine,Vol. 9, Issue 2, pages 29-36, 2003.
2) J. Fan and S. Borlase, "The Evolution of Distribution", IEEE Power and Energy Magazine, Vol. 7, Issue 2, pages:63-68, 2009.
3) H. Farhangi, "The Path of the Smart Grid", IEEE Power and Energy Magazine, Vol. 8, Issue 1, pages 18 –28,2010.
4) NIST, "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0.", NIST SpecialPublication 1108R2, February 2012.
5) J. Mark, "New Electricity Grids May Be Smart, but Not so Private - The Denver Post", 18 May 2010. Available at:http://www.denverpost.com/business/ci_15106430 (last accessed October 2, 2012).
6) U.S. Department of Energy, "Advanced Metering Infrastructure", White paper, NETL Modern Grid Strategy Powering our 21st-Century Economy,February2008.http://www.netl.doe.gov/smartgrid/referenceshelf/whitepapers/AMI%20White%20paper%20final%20021108%20%282%29%20 APPROVED_2008_02_12.pdf (last accessed October 2, 2012).
7) Federal Energy Regulatory Commission, "Assessment of Demand Response & Advanced Metering", Staff Report ,December 2008. Availableat:http://www.ferc.gov/legal/staff-reports/demand-response.pdf (last accessed October 2,2012).
8) A. Massoud and B. Wollenberg, "Toward a smart grid: power delivery for the 21st century", IEEE Power andEnergy Magazine, Vol. 3, No. 5, pages: 34-41, 2005.
9) Z. Lu, X. Lu, W. Wang, C. Wang, "Review and Evaluation of Security Threats on the Communication Networksin the Smart Grid", in Proceedings of IEEE Military ommunications conference, pages: 1830-1835, 2010.
10) J. Steven, G. Peterson, D. Frincke, "Smart-Grid Security Issues", IEEE Security and Privacy, pages: 81-85, 2010.
11) P. McDaniel, S. McLaughlin, "Security and Privacy Challenges in the Smart Grid", IEEE Security and Privacy,Vol. 7, No. 3, pages: 75-77, May-June 2009.
12) A. Westin, "Privacy and Freedom", New York: Atheneum, page 7, 1967.
13) J. Miller, "Who Are You? The Trade-Off between Information Utility and Privacy", IEEE Internet Computing,Vol. 12, No. 4, pages: 93-96, 2008.
14) J. Miller, "Who Are You, Part II: More on the Trade-Off between Information Utility and Privacy", IEEE InternetComputing, Vol. 12, No. 6, pages: 91-93, 2008.
15) D. Pedersen, "Personality correlates of privacy", Journal of Psychology, Vol. 112, pages: 11-14, 1982.
16) N. Brierley, "The meaning and use of privacy: A study of young adults", Ph.D. dissertation, The University ofArizona, USA, 1992.
17) International Energy Agency, "Technology Roadmap: Smart Grids", International Energy Agency, April 2011.Available at: http://www.iea.org/papers/2011/smartgrids_roadmap.pdf (last accessed October 2, 2012).
18) D. Kindy and A. Pathan, "A Detailed Survey on Various Aspects of SQL Injection: Vulnerabilities, InnovativeAttacks, and Remedies", Information Journal, Japan, 2012, to appear.
19) M. Singh, "Privacy for Telecom Services", IEEE Internet Computing, Vol. 6, No. 1, pages: 4-5, 2002.
20) C. Efthymiou, G. Kalogridis, "Smart Grid Privacy via Anonymization of Smart Metering Data", 1st IEEEInternational Conference on Smart Grid Communications, 2010, pages: 238-243.
21) F. Siddiqui, S. Zeadally, C. Alcaraz, S. Galvao, "Smart Grid Privacy: Issues and Solutions", in Proceedings ofSecond International Workshop on Privacy, Security, an Trust in Mobile and Wireless Systems (MobiPST 2012),Munich, Germany, July 30, 2012.
22) J. Cheung, T. Chim, S. Yiu, V. Li, "Credential-based Privacy –Preserving Power Request Scheme for SmartGrid Network", IEEE Global Telecommunications Conference, 2011, pages: 1-5.
23) S. Das, K. Kant, and N, Zhang, "Security and Privacy in the Smart Grid", Handbook on Security Cyber-Physical Critical Infrastructure, Morgan Kaufmann, Chapter 25, February 2012. .