INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 1753 – 1757
RECEIVED: 08-03-17 PUBLISHED: 22-03-17

March 22, 2017

EB CHECK: SYSTEMATIC ROLE CHECK WITH HUMANLESS AUTO METER READING USING LIFI

S.Baby[1], S.Hemamalini[2], N.Pavithra[3], V.Suganya[4], T.Karthikeyan[5],
[1,2,3,4]UG Scholar, Department of Computer Science and Engineering, Sri Balaji Chockalingam Engineering college, Arni.
[5]HOD, Department of Computer Science and Engineering, Sri Balaji Chockalingam Engineering college, Arni.

Abstract

In manual process, there is growing demand to protect the user credentials privacy. The insider attacker can get access to modify meter readings and can view private information of the customer at the customer endpoint. Similarly, insider attacker may be able to access the electricity price information, network infrastructure information, and other information communicated by protocols, so it is less security. To propose a technique of LIFI, where in EB meter when transmit the electricity consumption reading details to server. Electricity consumption reading sensor is connected to the device to verify the switching state of the device. Reading details transmit to server through LIFI. Server calculates the cost of remaining units and send EB bill to user mobile phone via SMS. User view SMS and pay their EB bills through remotely. Android Application is deployed to the customer for Payment System.

Intex terms: LIFI,Digital Meter,SMS,Android application

1. INTRODUCTION

Only manual process of taking EB meter reading. We are proposed to automatic meter reading. Security challenges have focused on protecting the system against various forms of external (outsider) cyber-attacks, including man-in-the-middle attacks, intrusion-based attacks, malware-based attacks, denial of service attacks, isolated attacks, and coordinated attacks. An insider threat is a user who has appropriate permissions to access required resources of the system and misuses its privileges. For smart grid having many integrated components and user groups, insider threats can influence the system massively. They can compromise integrity by modifying data without authorization, availability by creating delays where low latency is required ,relaying, few seconds for feeding data to supervisory control and data acquisition, data transmission to substations and wide area monitoring messages, few minutes for monitoring equipment and market pricing information, and few hours for smart meter confidentiality by exposing privacy of customer information and some parts of electric market information, and accountability by avoiding liability and responsibility.

Hence, the countermeasures must address outsider as well as insider attacks. Similarly, insider attacker may be able to access the electricity price information, network infrastructure information, and other information communicated by protocols. Some of these systems and protocols are energy management system distributed network protocol, inter control center communications protocol and open smart grid protocol. The EMS enables transmission of real-time information, such as grid's status, remote automation of grid functionalities, and etc. The OSGP provides reliable and efficient

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 1753 – 1757
RECEIVED: 08-03-17 PUBLISHED: 22-03-17
March 22, 2017

delivery of command and control information among various smart grid devices, including smart meters, control modules, and gateways.

2. RELATED WORK

The Smart Grid, generally referred to as the next-generation power system, is considered as a revolutionary and evolutionary regime of existing power grids. More importantly, with the integration of advanced computing and communication technologies, the Smart Grid is expected to greatly enhance efficiency and reliability of future power systems with renewable energy resources, as well as distributed intelligence and demand response. In this paper, we present a comprehensive survey of cyber security issues for the Smart Grid. Specifically, we focus on reviewing and discussing security requirements in the Smart Grid. We aim to provide a deep understanding of security vulnerabilities and solutions in the Smart Grid and shed light on future research directions for Smart Grid security.
Cloud computing is emerging as a powerful architecture to perform large-scale and complex computing. It widens the information technology (IT) capability by giving on-demand admittance to work out resources for dedicated use. The security information and privacy are the main concerns over the cloud from user viewpoint. In cloud computing cloud users and cloud severs are not present in the same domain. Due to this problem of data security and privacy, access control is required. In centralized cloud system is given only with single key distribution Centre and makes use of symmetric key approach algorithm. The proposed scheme is to hide the user's attributes using Attribute Based Encryption algorithm for providing any control. In this system the cloud confirm the authenticity of the user with no knowing the users identity before storing the data.

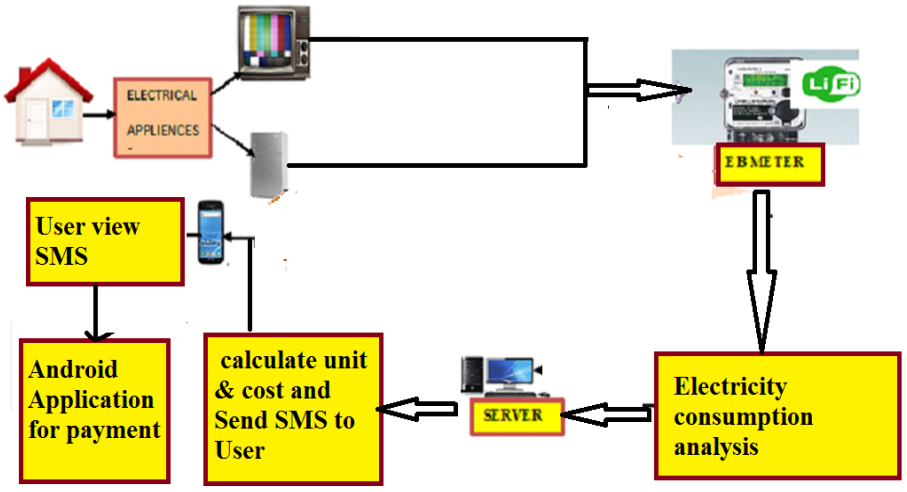

Figure 1 EB Meter consisting home appliances and EB Server calculate unit & cost automatically

This method contains an added feature of access control in which only the valid users are able to decrypt the stored information from cloud sever. Entity authentication and related key managements an active research topic in smart grid security. But existing works seem to have overlooked the significance that the smart grid is a cyber-physical system, which entails more considerations in the integration of its cyber and physical domains. This paper proposes a two-factor cyber-physical device authentication protocol to defend against coordinated cyber-physical attacks in the smart grid. The resulting protocol provides assurance on not only the digital identity of a device, but also the device's controllability in the physical domain. While the design is for the electric vehicle ecosystem, the framework could be readily extended to other smart grid subsystems.A smart grid is a modern electric power grid infrastructure for enhancing efficiency and reliability using modern communication and control technologies. Smart grid can be considered as an outcome of a developmental electricity networks towards an optimized and sustainable energy system. The current power systems are based on solid communication whereas, smart grid technology is based on grid-integrated communications between various grid elements, transmission and distribution using sensing and metering technologies and modern energy management techniques. This paper describes various smart grid concept sand details. The smart grid (SG) is a promising platform for providing more reliable, efficient, and cost effective electricity to the consumers in a secure manner. Therefore, this paper addresses the required objectives of an authentication protocol in the smart grid network along with the focus on mutual authentication, access control, and secure integration among different SG components. We review the existing authentication protocols, and analyse mutual authentication, privacy, trust, integrity, and confidentiality of communicating information in the smart grid network. We also review the existing authentication schemes for the vehicle-to-grid (V2G) communication network along with various available secure integration and access control schemes.

3. IMPLEMENTATION

3.1 USER REGISTRATION

User registration module every user will be register with the Server. So user has to give user name, password, address, mobile number and other details. Once the user create an account, they are to be login into their account and requested job and respond to them. In the Login module mobile user can login by their user Id and password and make request for their home, office or firm electric bill details. This request will send to the central server mobile and collect data from it and response to the end user. All the user data will be stored in the database.

3.2 POWER CONSUMPTION MONITOR

In this module we monitor the behavior of the user, the usage of the current monitoring, TV programming monitoring and if the current charge go beyond the limit it will charged double.

3.3 LIFI COMMUNICATION

In this module we use advance technology LIFI, we can able to transfer the file through by light and in this project we deployed a LIFI communication for data communication between the EB meter and Server.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 1753 – 1757
RECEIVED: 08-03-17 PUBLISHED: 22-03-17
March 22, 2017

3.4 EB SERVER

In the Main EB Server all the details of the user are stored. LIFI boards are connected with the RS 232 Serial Port of the EB Server. Real time mobile phone is connected with the EB Server for sending SMS to the customers regarding the amount information. This server will have the entire data of all the customers' information. The server can be created using java programming languages.

3.5 ANDROID PAYMENT SYSTEM

User once receives the sms alert regarding the payment; user can give the payment through online itself. Mobile client is an android application which created and installed in the User's mobile phone. So that we can give the payment through online itself. The application first page consist of the user registration process. Well create the user login page by button and text field class in the android. Once we create the full mobile application, it will generated as android platform kit(APK) file. This APK file will be installed in the user's mobile phone an application. This process reduces customers going directly standing in the queue to pay money.

4. FUNCTION RIDE

As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). We develop a new cryptosystem for ¯ne-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE).In our cryptosystem, cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. We demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption. Our construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).

5. CONCLUSION

In this paper, we proposed a user authentication and authorization scheme for accessing many different types of devices in the SG. Our scheme can be easily applied to different user roles, such as auditors, operators, and etc., who access different devices in the SG system, as each user-role is computed dynamically based on attribute-based access control using a SHA256 hash function with (mode of access, department, location, SDP) attributes provided by each user. Our scheme enables two-factor authentication so that a rogue device could not re-use the previous captured information of a legitimate user. A bilinear pairing cryptography-based shared secret key is generated between the user and the device for further secure communications within a session. The proposed scheme is efficient in terms of both, communication and computation overheads in comparison with the existing schemes, and is able to defeat many well-known outsider attacks as well as insider attacks.

FUTURE WORK

In future we can extend the LI-FI up to long range distances using an hub for an each range area. And the billing details are sends in the form of voice messages instead of using SMS or through E-Mails.

REFERENCE

[1] N. M. Pindoriya, D. Dasgupta, D. Srinivasan, and M. Carvalho, "Infrastructure security for smart electric grids: A survey," Optimization an Security challenges in smart power grids(Energy systems), V.Zpappu, M.Carvalho, and P. Pardalos, Eds. Berlin, Germany: Springer, 2013, pp. 161–180.

[2] C.-H. Lo and N. Ansari, "Decentralized controls and communications for autonomous distribution networks in smart grid," IEEE Trans. Smart Grid, vol. 4, no. 1, pp. 66–77, Mar. 2013."

[3] N. Saxena and B. J. Choi, "State of the art authentication, access control, and secure integration in smart grid," Energies, vol. 8, pp. 11883–11915, Oct. 2015.

[4]Guidelines for smart grid cybersecurity: Supportive analyses and references," NISTIR, Tech. Rep. 7628, Aug. 2010. [Online].Available:http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf

[5] Smart grid information assurance and security technology assessment," Energy Res. Develop. Division, Final Project Rep. CEC-500-2013-056, 2010. [Online]. Available:http://www.energy.ca.gov/2013publications/CEC5002013056/CEC5002013056.pdf

[6]AndroidDeveloper2015.[Online].Available:http://developer.android.com/reference/android/hardware/SensorEventListener.html.

[7] J. Clark and P. van Oorschot, "Sok: Ssl and https: Revisiting past challenges and evaluating certificate trust modelenhancements," in Security and Privacy (SP), 2013 IEEE Symposium on, May 2013, pp. 511–525.

[8]Smartgrid,"PowerSyst.Eng.Res.Center,Tech.Rep.Feb.2012,p.29.[Online].Available:http://pserc.wisc.edu/documents/publications/papers/fgwhitepapers/govindarasu_future_grid_white_paper_cps_feb2012.pdf

[9] Tropos Wireless Communication Systems, ABB. (2012). A Secure Distribution Area Network Architecture for SmartGrids.

[10] Smart grid cyber security potential threats, vulnerabilities and risks," Public Interest Energy Res. (PIER) Prog. Interim Rep., California State Univ., Sacramento, Sacramento, CA, USA, Tech. Rep. CEC-500-2012-047,May 2012, p. 83. [Online]. Available:http://www.energy.ca.gov//2012