Authentication Technique for Safeguarding Privacy in Smart Grid Settings

B. Pragathi[1], and P. Ramu[2]
[1]Associate Professor, Department of Electronics and Communication engineering, DVR & Dr.HS MIC college of Technology, NTR district, India.
[2]Research Scholar, Department of Electronics and Communication, GIET University, Gunupur, Orissa, India.
Email: drbpragathi@mictech.ac.in, podili.ramu@giet.edu

Abstract. As a way to address issues like the depletion of energy sources and efficient energy management through the convergence of multiple fields, interest in green energy has been growing recently. As a result, the intelligent electrical grid, or "smart grid," projects are being completed quickly in order to achieve low-carbon, green growth. But because IT is primarily focused on the electrical grid, there is a shortage of IT in smart grids as well, and the complexity of convergence is making the issue worse. There is also a growing concern about this issue because different personal data and payment information within the smart grid are progressively turning into big data and becoming a target for external intrusion and attack.

1 Introduction

The intelligent electrical grid, also known as the smart grid, is the subject of ongoing research dependent on recent merging technologies, and it is regarded as a key technology for achieving low-carbon, green growth. By integrating IT into the current electrical grid and transferring real-time data back and forth between suppliers and consumers, smart grid technology connects smart energy demand requirement and renewable energy resources management. By integrating IT technologies with the current electrical grid systems, power providers and consumers can increase the system energy efficiency of the entire electrical utility grid system by exchanging valuable information in real-time. in particular, a system for bidirectional information exchanged between power supply providers and customers[1-3].As of the recent trend, the government intends to provide AMI to more than 50% of all consumers in the country through 2016. For KEPCO's (Korea Electric Power Corporation) high voltage consumer, the AMI supply has already been finished.
The switch from mechanical watt-hour meters to smarter meters is crucial for the variety of rate plans, increased consumer choice, and the development of new services that arise from the use of AMI. With the replacement, real-time confirmation of an individual's own electricity use and rate, along with automated remote device control, can set up the foundation for energy use optimization [4].

Corresponding Author: drbpragathi@mictech.ac.in

There are benefits that additional installation costs can be minimized once the interworking between the home network and the AMI system, which is currently being studied with a power supplier serving as its sponsor, is finished. Additionally, a smart grid environment can make use of the broadband internet telecommunications infrastructure that is currently available to millions of households. A "home network" is an external internet network that connects to information appliances inside the home and allows users to control those appliances from anywhere in the house. Nonetheless, because a home network has a variety of wired medium and wireless medium with the protocols coexisting in it, it has security vulnerabilities similar to those of legacy mediums and protocols.

Another issue is that home networks can be targeted by previously employed network-based cyberattack technologies via the internet.

Thus, dependable security frameworks and technologies are required in a secure smart grid environment in order to combine different devices with novel concepts and wired medium and wireless network telecommunication terminals. In smart utility grid environments in particular, breif personal data will be gathered, processed, and stored occasionally disclosed illegally. As a result, there is a growing need for a privacy protection framework that includes device security, privacy intrusion detection, effective home device access control mechanisms, and other measures [5-8]. Like other modern communication networks, the AMI of a smart grid should use a variety of security measures, such as secure access control mechanisms, to defend its various services from outside attackers. A key area of research for creating a safe smart grid environment is the protection of private information during access to, from, and within homes networks [9–14].

Thus, the goal of this study is to suggest an authentication mechanism for protecting home devices' private information in a smart grid setting.

2 Literature Review

2.1 Smart utility Grid: A smart grid is made up of several infrastructures, including smart devices like smart meters, software, and hardware, as well as monitoring and control systems deployed in facilities for the production, transmission, and supply of electricity. The main technologies of the smart grid are information technology, smart devices (smart meters, for example), distributed system technology for energy management, technology based on energy quality and reliability, technology for energy production, storage, and transmission, whole system monitoring technology, and core system—security technology that guarantees system stability.

Additionally, two-way communication serves as the foundation for the more dependable smart grid through the main telecommunications infrastructure, or AMI. AMI's telecommunication infrastructure can be made up of both wired and wireless technologies, including 3GPP, Wi-Fi, and ZigBee, as well as PLC (power line communication) and Ethernet. It comprises a hierarchical structure wherein several smart meters in an AMI communication environment can establish a connection with a DCU (data aggregate unit), acting as a gateway; additional DCUs can establish a WAN connection with the power supplier's AMI server. Since AMI acts as a point of contact for power users' internal and external telecommunication networks, it can be the target of threats such as worm, virus, malicious code, and firmware circulation, as well as meter bots and DDoS attacks.[15, 16]. Figure 1 depicts the AMI communication network, which facilitates communication between the power and control systems that make up the smart utility grid.

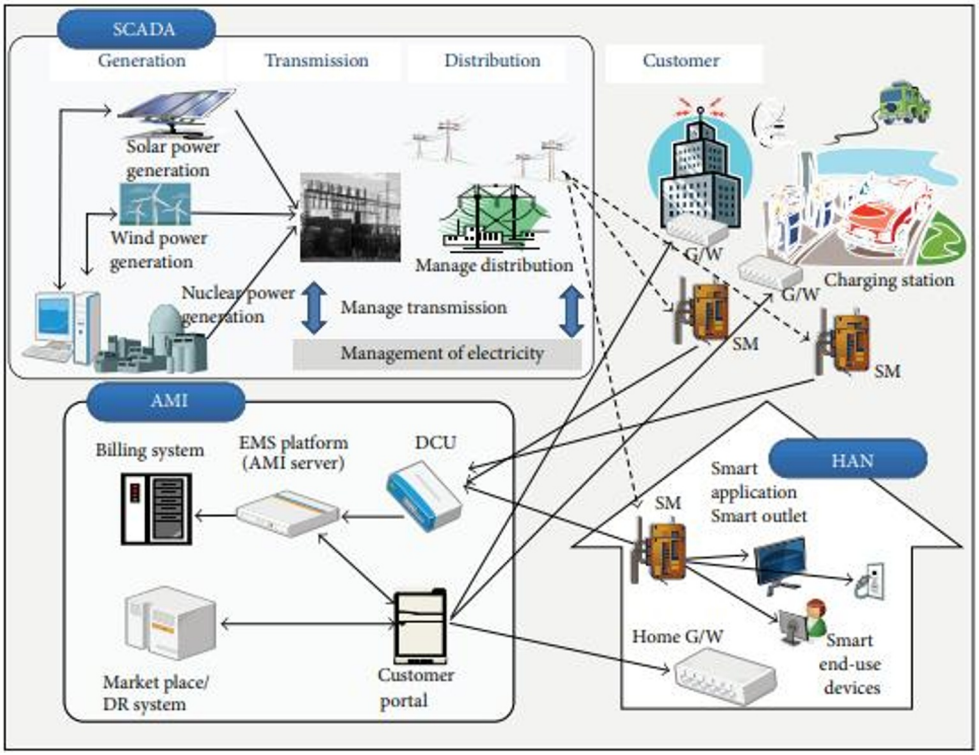

Figure 1: Communication infrastructure of smart utility grid

.

2.2 Smart Grid Security Risks and Vulnerabilities

Smart grid environments are not immune to cyberattacks like the current electrical grid is. First off, because a smart grid environment necessitates two-way data transmission, various data must be collected in order to automatically perform system operation and provide an adequate power supply. Because of this, the reliability of the smart grid cannot be assured, and if false or counterfeit data is presented in any node, it could pose a cyber danger. Additionally, smart devices that can serve as a point of contact for information exchange at the consumer's terminal, like smart meters, home gateways, sensors, and others, can be used as a cyberattack vector. Furthermore, the computing capacity of home network information appliances is relatively low, making it challenging to install robust security features and While there are a number of home networking technologies available, a home network lacks the correspondence technology required to resolve the medium's inherent security vulnerability. Furthermore, middleware lacks a security infrastructure that can meet each middleware's specific security needs and Provide security in an integrated middleware environment with flexibility— the location of the middleware fusion. It is hence susceptible to security lapses brought about by malware, worms, viruses, DDoS attacks, hacking, and wiretapping of communication networks. To combat these cyberattacks, the security of the home gateway—which serves as the door connecting the private network within the home to the public network outside—as well as the security of wired and wireless networks are crucial. The user-based information security in the user environment and device access are the two categories into which In smart grid contexts, AMI-based security threat aspects can

be divided. Figure 2 lists the components of the security threat in AMI and provides a detailed explanation of each one as follows.

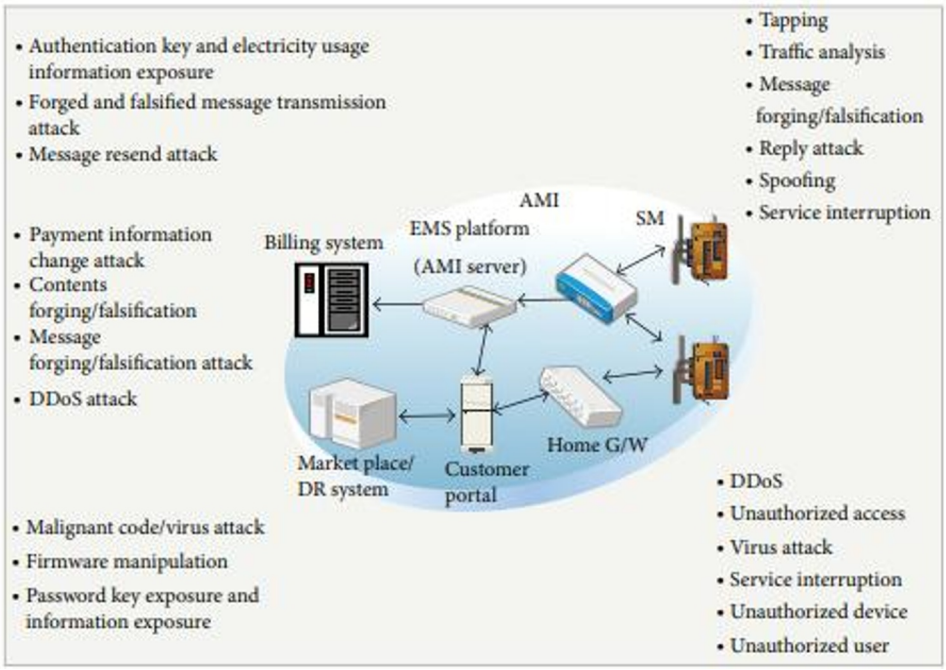

Figure 2: Security alerts/threats in AMI network

(i) Firmware Design Manipulation: There is a threat component because the device's password could be discovered, which leads to the disclosure of all information through firmware manipulation in devices that aren't protected, like smart meters.

(ii) DDoS deign Attack: This is a threat component that includes distributed denial of service attacks and service denial attacks using traffic spikes to target smart meters while they are providing different services. The attack exploits the fact that the embedded device-based AMI's field device delivers service via a CPU.

(iii) Malicious design Code and Virus Attack: Installing harmful and virus-ridden code on smart devices, including smart meters, is a threat factor. This assault exploits the device's weakness in AMI, where capacity constraints make it difficult to deploy a viral vaccination.

(iv) User Information Exchange and Disclosure Attack: It is a threat component to both the electrical grid and e-commerce. This type of attack entails changing payment details via forging and fabricating utility bills, user profiles, payment information, and other user data within the user environment.

(v) Authentication Key and User Information:This is a threat factor since it comprises the revelation of the authentication key created during encrypted communication between all of the AMI's devices as well as the subsequent disclosure of customer power usage data.

(vi) Message Resender: This is a threat component that involves the forging and deception of messages since continuous two-way telecommunication is used

to transmit and receive data about network status,power usage demand, electricity usage and bills, and user information within AMI.

2.3 Security Necessities of Smart Utility Grid

Secrecy, integrity, availability, and general network security are the main objectives of the smart grid's security requirements. Furthermore, a number of additional security requirements should be taken into account in order to mitigate the security threats that are typical in a smart grid environment.

i) Confidentiality: Data stored on systems and devices, as well as data transmitted over networks, must have their confidentiality protected. Important information, including privacy information like usage and rate-related data, is transmitted through networks when data is gathered from local and remote smart devices in a smart grid environment. As a result, it is necessary to protect important information by utilizing mechanisms like encryption to prevent unauthorized users from accessing it.

ii) Data Integrity: It should be ensured that no data was altered by unauthorized users while it was being created, transmitted, and stored. Regarding the smart grid environment, a man-in-the-middle attack can be used to forge and falsify the message sent between the server and smart device. Thus, a solution that can protect the integrity of data transferred between media is required in order to counter such a security threat.

iii) Device Integrity: Intelligent devices, like smart meters in smart grid environments, are typically installed in unmonitored areas and process critical data necessary for service delivery. These devices are typically used on platforms with open interfaces due to factors like ease of use and lower implementation costs. When a device's integrity is compromised, malicious software can be installed on it or its function can be altered, contaminating the network or affecting the device's availability. As a result, additional verification of the device's integrity is needed.

iv) Availability: It is important to ensure that all networks and services are available. DDoS attacks are a type of attack that compromise system availability and productivity, making it more difficult to provide services related to system resources and information. Thus, sufficient security measures that ensure availability are needed in a smart grid environment in order to protect subjects' or devices' ability to access information.

3 Method of Access Authentication for Home Device

This study suggests an access control and authentication mechanism to safeguard privacy so that remote users can operate in a home network-based smart grid environment and securely access HAN.

The NIST privacy subgroup of the CSWG (cyber security working group) splits privacy into four key categories: privacy of personal communications, privacy of personal information, privacy of person, and privacy of behavior [1]. Among these, the privileges to control and access personalised information are referred to as privacy. the private data that makes it possible to identify a specific person and others. The right to privacy encompasses the ability to manage one's physical integrity, including matters that are medically required. The right to keep some aspects of one's personal behavior private from other people includes the right to maintain the facts about those behaviors private. Therefore, the right to communicate without interference, such as unfair monitoring, is referred to as the privacy of personal communications. All four of the aforementioned factors need to be taken into

account for smart grid privacy. This can only be accomplished with an authentication method that controls remote users' access to services and the encryption of critical data. This study offers privacy within the smart grid by using a secure access service and an authentication procedure.

3.1 System Structure of AM

An essential component of the smart grid is the AMI, which connects smart devices to data regarding user consumption patterns and electricity consumption that is created within the home network is received and transmitted by the electrical grid. The entire architecture of the home server, authentication server, and MDMS that make up the home network-based AMI (meter data management system), is shown in Figure 3. Energy management data can be efficiently shared between home server and MDMS via web service. In addition to other services, MDMS offers meter data resource management and electricity consumption monitoring.

Meter data is sent to a web service-based MDMS and integrated into the home server. The home server, which is an addition to the current home gateway's service module for electricity management, offers control over household appliances, data and network device sharing, and multimedia services. Home installed server data is processed to the database access controlling module section, allowing access to be controlled based on user access levels. This offers access control for the system and services for every user as well as access control that is tailored according to the user's service access environment. The general layout of the suggested mechanism of authentication for residential networks is shown in Figure 3.

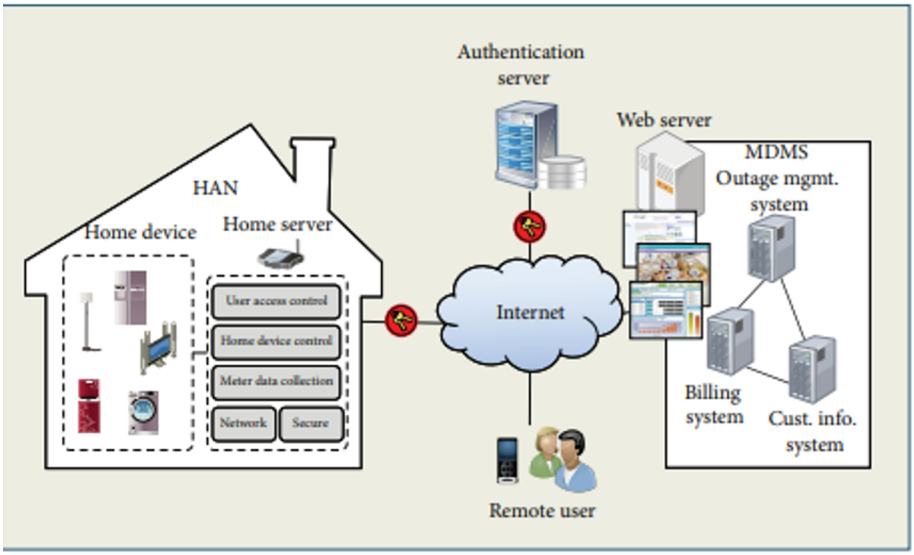

Figure 3: Structure of the proposed authentication system

3.2 Phase of Shared Secret Key Update:

Token required for home device access approval is demanded by the remote user from the authenticated server. After verifying the remote user's information, the authentication server sends the token to the user. The token is transmitted to the home device by the remote user receives it in order to establish a session key and perform mutual authentication with the device.

The process of mutual authentication and session key creation between the home device and the distant user is depicted in Figure 4.

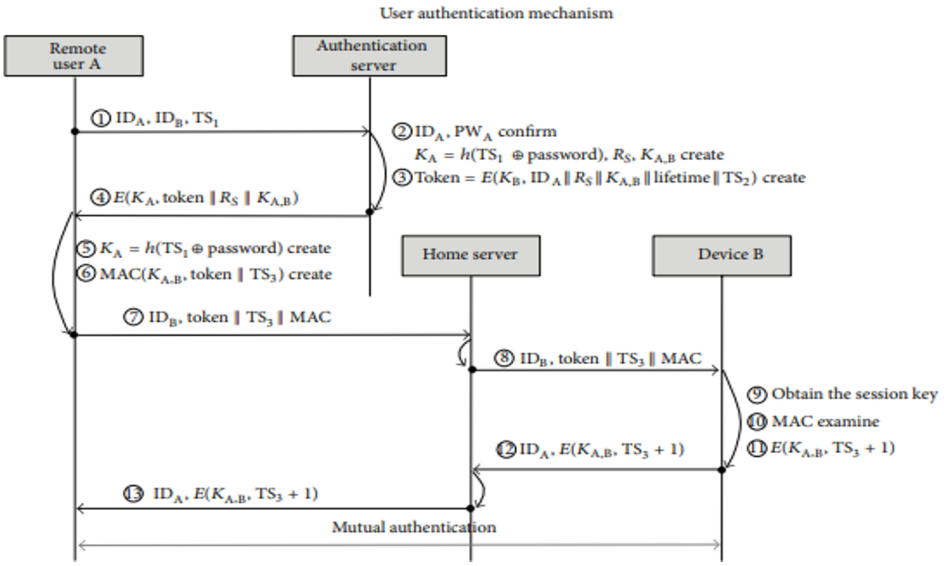

Figure 4: mutual authentication and session key creation between the home device and the distant user

3.3 Module for Authentication in Home Device Access Control:

After the user authentication process is finished, access to every device is achieved through the home server, as seen in Figure 5. Upon a remote user's access to the home device, the home server authenticates the service and data access authentication procedure is started by the user, who also has access authority for the device. Access to a home device is managed for each user through an authentication process and through a home device's access control, personal information created within is restricted from being accessed. The access authority betweenusers or consumers inside and users outside the house, as well as between administrators and regular users, was distinguished by the proposed access control module. As a result, certain authority was restricted to administrator level users, including the ability to register user, smart meter, and home device.

.

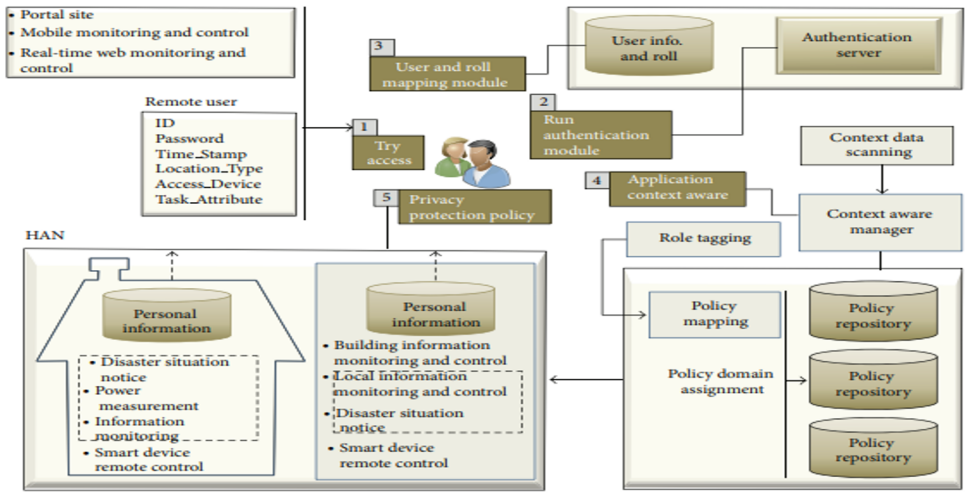

Figure 5: Access controllable design flow chart

4. Security Design Analyses

In addition to data misuse and abuse, immoral usage, malevolent internal users, technical challenges connected to sharing, data loss or spill, and account or service hijacking, a smart grid environment requires security against unknown threat profiles.
To protect user privacy in smart grids, management and technical countermeasures must be put in place. These include internal management plans for privacy information, procedures to prevent authorized access records and access control from being forged or falsified, and encryption processes for user personal information and electricity consumption data.

Within HAN telecommunications, there is a security concern associated with the interception of communication data between AMI and home appliances. The telecommunication protocol's supported encryption algorithm and key management system must be implemented. as well as to set up technical countermeasures like entity authentication and the encryption of HAN telecommunication data. Important personal data is kept private within the home network thanks to the authentication mechanism suggested in Section 3 that regulates service access via remote user access authentication within HAN.
Different service authorization should be given to users within a home network based on their roles as part of a privacy information management plan. Consequently, access control procedures and security policies pertaining to role-based service authority grant

The weakest link in the ID/password based authentication system that the home network is currently using is the attacker's dictionary assault. Therefore, the attacker shouldn't be able to gain any password information using passive attack methods like wiretapping while the proper user authentication protocol is being followed. The recommended method uses the password and time stamp to create a one-time key, and previous registration information of the user along with a random number for the remote user's authentication. As a result, access is not possible even after obtaining the user's registered password.

Furthermore, each registered device needs to have its session value since in the event of an impersonation assault, the authentication process uses the authorized MAC value. From this angle, access.

i) Replay Attack: The proposed method employs a one-way hash function to generate a one-time secret key based on a time stamp and password. As a result, the attacker is unable to use intercepted ID and carry out a replay attack. For these reasons, the access is refused appropriately by applying the time stamp value, even in the event that the attacker tries to use the session to reuse it.

ii) Impersonation Attack: An authorized MAC value is required by the attacker when they try to remotely spoof a home device. Currently, in order to generate an authorized MAC value, the registered device's session value is necessary. The secret key of the device that was provided by the authentication server must be entered in order to obtain the session value at this time. Consequently, it is impossible for an unauthorized user to access.

iii) Mutual Authentication:It is safe from illegal piracy, access, and invasion of unauthorized user space since By examining the device's reason for access using the MAC value, random value, session value, and registered device ID, the mutual authentication process between the home device and remote user is carried out.

iv) Access Control: When accessing a database system and device within a home network, Only authorized members receive the appropriate application of the access level with context-aware data.; consequently, By varying the level of access for the same service, it reduces access to devices and personal data. Access control and authentication mechanisms are implemented to prevent users or administrators from accessing devices situated in remote areas within smart grid environments. These mechanisms are designed to

prevent users from exceeding authorized authority and to protect against improper application activity and access.

v) Man-in-the-Middle Attack:In the event of an attack where the attacker intercepts the data transmitted from the communication channel and poses as the sender for the receiver and the receiver for the attacker, the behavior of the middle attacker, including data forging and message modification, is blocked with the creation of an appropriate key value applied during the session creation. Since the device's secret key, which was supplied by the authentication server, is required to retrieve the session value at the start of each session, spoofing is not permitted.

The aforementioned security evaluation analyses prevented unauthorized outside users from accessing home appliances in a home network-based smart grid setting and enabling authorized users to safely access them from a distance. Additionally, it made a number of services possible, such as confirmation of the amount of electricity utilized in the home network and remote device control. In terms of the power provider, it can offer information checks on users' electricity consumption, monitoring for irregular use, and services for detecting illegal invasions. By doing this, it will be possible to maximize the energy efficiency of users of home networks.

5. Conclusion

The security of smart grids faces more challenges than those of simple networks. This is because it necessitates the security of the telecommunications system, IT, and power. Apart from the security of confidentiality, integrity, and availability, it also needs privacy protection, defense against cyber-physical attacks, and dependability. The smart grid is the next generation of intelligent electrical grids that maximize energy efficiency by allowing providers and customers to communicate real-time information by integrating IT technology into the existing electrical infrastructure. But in a smart grid setting like this, there's a good chance that there will be a number of security risks, like data leaks and data theft through two-way communication with smart devices like AMI and smart meters.Research on the user's service access authentication process is especially important in light of the numerous privacy-compromising smart grid attacks. Data security is becoming more and more of a concern as personal, payment, and living information progressively merge into big data. This study proposed a secure authentication method to protect user privacy in a environment for smart grid based on home networks. The recommended authentication approach protects against replay attacks, impersonation attacks, entity mutual authentication, and other risks by requiring users to complete the authentication procedure before they can access personal data created and sent from home networks and AMI.

The access control authentication approach in this study prevents unauthorized access from the outside and enables secure remote control of access to personal information in the home network by producing a one-time key using a random value and password. Message authentication is then carried out using this key. Once a session has been established with them, Regardless of key value spillage, the time stamp value and one-time key cannot be utilized again in the authentication process.In a smart grid setting, such a service offers additional functions that allow users to actively contribute to reducing their energy use in addition to consulting information on reducing energy consumption, such as managing their usage history and analyzing their usage patterns.In comparison to the suggested security module, a more lightweight security system ought to be put into place, and further research into more varied applications should be done.

References

[1]. E. W. Gunther, A. Snyder, G. Gilchrist, and D. R. Highfill, "Smart Grid Standards Assessment and Recommendations for Adoption and Development (Draft v0. 82)," Enernex for California Energy Commission, 2009.
[2] U.S. Department of Commerce, "NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1. 0 (Draft)," 2009.
[3] S.-S. Yeo, D.-J. Kang, and J. H. Park, "Intelligent decisionmaking system with green pervasive computing for renewable energy business in electricity markets on smart grid," Eurasip Journal on Wireless Communications and Networking, vol. 2009, Article ID 247483, 2009.
[4] K. Geun-Young and K. Young-Myoung, "Implemen-tation of Telco Home Network-based AMI," Journal of the Korean Institute of Information Scientists and Engineers, vol. 27, no. 11, pp. 93–97, 2009.
[5] D.-S. Wang and J.-P. Li, "A novel mutual authentication scheme based on fingerprint biometric and nonce using smart cards," International Journal of Security and Its Applications, vol. 5, no. 4, pp. 1–12, 2011.
[6] H. Jin-Bum and H. Jong-Wook, "A security model for home networks with authority delegation," in Proceedings of the International Conference on Computational Science and Its Applications (ICCSA '4), pp. 360–369, 2006.
[7] S. Sun, Z. Yan, and J. Zambreno, "Demonstrable differential power analysis attacks on real-world FPGA-based embedded systems," Integrated Computer-Aided Engineering, vol. 16, no. 2, pp. 119–130, 2009.
[8] D.-E. Cho, B.-S. Koh, and S.-S. Yeo, "Secure D-CAS system for digital contents downloading services," Journal of Supercomputing, vol. 64, no. 26, pp. 477–491, 2011.
[9] T. A. L. Pham, N. Le-Thanh, and P. Sander, "Decompositionbased reasoning for large knowledge bases in description logics," Integrated Computer-Aided Engineering, vol. 15, no. 1, pp. 53–70, 2008.
[10]. X. Tao, Y. Li, and R. Nayak, "A knowledge retrieval model using ontology mining and user profiling," Integrated Computer-Aided Engineering, vol. 15, no. 4, pp. 313–329, 2008. [11] Q. Chen, S. Zhang, and Y.-P. P. Chen, "Rule-based dependency models for security protocol analysis," Integrated ComputerAided Engineering, vol. 15, no. 4, pp. 369–380, 2008.
[12] H. Ko, G. Marreiros, H. Morais, Z. Vale, and C. Ramos, "Intelligent supervisory control system for home devices using a cyber physical approach," Integrated Computer-Aided Engineering, vol. 19, no. 1, pp. 67–79, 2012.
[13] S.-C. Kim, S.-S. Yeo, and S. K. Kim, "A hybrid user authentication protocol for mobile IPTV service," Multimedia Tools and Applications, pp. 1–14, 2011.
[14] A. Sanchez, E. O. Nunes, and A. Conci, "Using adaptive ´ background subtraction into a multi-level model for traffic surveillance," Integrated Computer-Aided Engineering, vol. 19, no. 3, pp. 239–256, 2012.
[15] L. Tan and S. Xu, "A model-checking-based approach to risk analysis in supply chain consolidations," Integrated ComputerAided Engineering, vol. 16, no. 3, pp. 243–257, 2009.
[16] https://sites.google.com/a/itrconline.net/itrc/projectinfo/2012 semina.
[17] J. Kim, H. Jeon, and J. Lee, "Network management framework and lifetime evaluation method for wireless sensor networks," Integrated Computer-Aided Engineering, vol. 19, no. 2, pp. 165– 178, 2012.

[18] D.-E. Cho and S.-J. Kim, “Study on safe remote control method of home device under environment of smart grid,” Lecture Notes in Electrical Engineering, vol. 179, no. 2, pp. 281–286, 2012.
[19] Z. Bankovic, J. M. Moya, ´ A. Araujo, D. Fraga, J. C. Vallejo, and ´ J.-M. de Goyeneche, “Distributed intrusion detection system for wireless sensor networks based on a reputation system coupled with kernel self-organizing maps,” Integrated Computer-Aided Engineering, vol. 17, no. 2, pp. 87–102, 2010.
[20] D.-E. Cho, H.-J. Shin, and S.-J. Kim, “The personal information protection technique in smart grid environment,” Information B, vol. 16, no. 3, pp. 2179–2184, 2013.
[21] NIST, “Smart Grid Cyber Security Strategy and Requirements,” DRAFT NISTIR, 7628, 2010.
[22] P. McDaniel and S. McLaughlin, “Security and privacy challenges in the smart grid,” IEEE Security and Privacy, vol. 7, no. 3, pp. 75–77, 2009