A lightweight and safe method for authenticating and establishing keys in smart grid systems.

Julianto[1], Chika Dwiyana[2]
1 Department of computer science, Esa Unggul University, Indonesia; juliantochai@outlook.com

2 Department of computer science, Esa Unggul University, Indonesia; Chikadw09@gmail.com

ABSTRACT Authenticating and establishing keys in Smart Grid systems is crucial for ensuring secure communication and protecting against unauthorized access, thereby maintaining the integrity and reliability of the entire electrical grid infrastructure. This article addresses the essential role of security in Smart Grids, focusing on lightweight authentication and key agreement mechanisms to counteract security threats like unauthorized access and data alteration. It reviews Smart Grid communication protocols and their limitations, advocating for resource-efficient, lightweight cryptographic solutions. The article discusses how to safeguard Smart Grid safety and proposes easy, helpful methods using codes for devices with restricted power. It concludes by encouraging stakeholders to collaborate in adding these safety methods into Smart Grid plans. It is very important to make our energy systems more powerful and safe so we can have a better future with lots of power.

KEYWORDS Smart Grid Security, Lightweight Cryptography, Authentication Mechanisms, Energy Infrastructure Resilience

I. Introduction

The growth of power lines has led to the creation of the Smart Grid, a large and interconnected network for making electricity, sharing it around, and using up. Smart Grids use smart tools like sensors, networks, and data study to make energy systems work better, be more trustworthy and greener. This is contrast to conventional power grids [1].

It's very important to have safety in Smart Grids. They are a big part of our everyday lives. The Smart Grid enables the continuous monitoring and regulation of power distribution, making it vulnerable to many safety issues. These risks include a lot of malicious actions, such as going into systems without permission, altering data and stopping services. Safety in a Smart Grid is extremely important because any issue can lead to major issues, loss of money and even threats to public safety [2].

To manage these dangers, it is crucial to develop authentication and key agreement approaches made only for the special traits of Smart Grids. Unlike regular computer things, many parts of a Smart Grid like sensors and actuators often have less power to process information. This makes using complex security too hard or impossible. It's important to use lightweight solutions so that devices with resource-constrained devices can work properly [3,4].

This article aims to study lightweight methods of authentication for Smart Grids. Our aim is to look at the difficulties of creating safety systems that offer a good combination of protection, speed and without wasting resources. We also aim to share advice on creating tools and deployment of efficient and low-weight security solutions. This will help fix safety issues in power grids that are connected. We will closely examine the safety needs, issues, and potential answers in detail for smart grid system.

II. Smart Grid Communication Protocols

Smart power systems use many ways of talking to each other to make sure data can pass easily between different parts of the system. These rules are basic to how Smart Grid works, allowing machines to talk with each other, share information, and quickly respond when the grid changes [5]. Some of the prevalent communication protocols utilized in Smart Grids are:

- **Advanced Metering Infrastructure (AMI) Protocols**: AMI rules let the smart meters share information with the energy company. Some networks you might know are Zigbee, Wi-Fi and mobile networks [6].

- **Supervisory Control and Data Acquisition (SCADA):** SCADA systems use DNP3 and Modbus methods to watch over and control machines in stations for power or other important building work [7,8].

- **Wide Area Network (WAN) Protocols**: MPLS and LTE are types of big network rules. They help set up links between small power stations and main control places that sit in different parts of the land [9].

Current Authentication and Key Agreement Techniques

In recent times, the area of computer safety has come up with many ways for a range of authentication and key agreement mechanisms, these methods have been put in place to protect how our Smart Grids connect. These approaches cover both symmetric and asymmetric cryptography methods and consist of:

- **Public Key Infrastructure (PKI)**: PKI gives a solid base for handling digital certificates and public-private key pairs, assuring the honesty and hiddenness of messages [10].

- **Pre-shared Keys (PSK):** PSK ways are simpler to carry out but require sharing keys securely with the devices used [11].

- **Elliptic Curve Cryptography (ECC):** ECC gives strong protection with smaller keys, making it good for devices that don't have a lot of power or space [12].

- **The Diffie-Hellman Key Exchange is** allowing two parties to construct a shared secret key via communication channel that is not secure. But it may need a lot of computer power for some machines [13].

Constraints of Existing Methods

Although current authentication and key agreement methods have demonstrated their efficacy in many scenarios, they possess inherent drawbacks when employed in Smart Grids:

- **Resource Intensive:** Many secret code methods, like RSA, need a lot of computing power. This makes them not useful for systems with limited ability to process information and store it in memory [14].

- **Scalability Challenges**: Normal ways of keeping data safe might find it hard to quickly grow and fit the many devices and communication points in a Smart Grid [14].

- **Primary Challenges in Key Management**: Safe sharing and control of secret codes are hard to do, particularly in changing Smart Grid situations [15].

Rationale for Utilizing Lightweight Solutions

The rationale behind using lightweight authentication and key agreement systems in Smart Grids arises from the necessity to overcome the constraints. As Smart Grids grow and use more low-power devices, the need for good security ways that can work well, change to fit any size system become more evident. Lightweight solutions aim to achieve a balanced equilibrium between security and constraints on resources, guaranteeing the safeguarding of the essential infrastructure of Smart Grids while enabling effective and secure communication between devices and components. [16].

III. Security Requirements in Smart Grid

A. Data confidentiality

- Making sure no one can see your information is very important for safety in Smart Grids.

- It makes sure that important data, like customer info and the process will be kept private by stopping anyone from getting to it who shouldn't.

- Keeping data secret in Smart Grid communication needs us to use ways of turning it into code [17].

B. Data integrity talks about how true, steady, and trustable data is from start to end.

Data integrity makes sure that data stays the same and true when it's shared or saved.

- In the world of Smart Grids, changing data can lead to wrong decisions and might even cause problems in how the grid works.

- Hash functions and digital signatures are often used to check if data has been changed [18,19].

C. Device authentication

Making sure that only trusted devices can use and work with the Smart Grid is very important.

- Device verification helps to stop devices that are not allowed from giving wrong information or managing important grid systems.

- We use techniques like digital certificates and safe sign-in steps to make sure a device is real [20].

D. Management of cryptographic keys

- Key management is the safe way of making, sharing, and keeping secret codes used for locking up data, confirming who you are or talking about keys with others.

- Good management of keys is very important to make sure that the messages in Smart Grids are kept secret and unchanged.

- Changing keys and getting rid of old keys are important parts of good key control [21].

IV. Lightweight Authentication Techniques

A. Overview of Lightweight Cryptography

- Lightweight cryptography means a set of special ways to keep things secret. These ways are made for devices with very few supplies [22].

- These methods boost effectiveness, lowering the need for a lot of computer and memory use. This makes them right for Smart Grid tools.

- Simple methods and small keys are often used in easy-to-carry safety systems, while keeping a good level of protection.

B. The differences of Public Key and Symmetric Key Methods

Public key cryptography utilizes a set of public and private. Keys to provide safe encryption and authentication.

Symmetric key cryptography employs a mutually agreed secret key for both the encryption and decryption processes.

In the context of lightweight authentication, symmetric key techniques are preferred due to their computational efficiency and lower overhead [23].

C. Advantages of Lightweight Authentication

- **Minimized Resource Utilization**: Easy-to-use ways of authentication are great at using just a little bit of computer power. This makes them good for weak devices in the Smart Grid.

- **Enhanced Authentication Speed:** Using lightweight methods helps to speed up authentication, which is very important for smooth and quick live Smart Grid tasks.

- **Reduced Energy Consumption**: Using lightweight authentication uses less power, which makes battery-powered things last longer.

- **Scalability:** lightweight methods are great for handling the growing needs of Smart Grids [24].

Examples of Lightweight Authentication Algorithms

- **HMAC (Hash-based Message Authentication Code):** HMAC is a popular and effective way to check if something is real or not. It uses a secret key along with a math function that turns data into code bits, so messages can always be trusted and are not changed in any bad way [25].

- **AES-CCM (Advanced Encryption Standard in Counter with chaining mode):** AES-CCM is a way of coding that mixes checking if something is real and secret writing using the AES block code. It is made to work well and be good for small tasks. It gives hiddenness, honesty, and realness in a concise format [26].

- **SPECK: SPECK** is a compact cryptographic algorithm designed to achieve high efficiency on devices with limited resources. It may be used for encryption and authentication. [27].

- **LEAP (Lightweight and Efficient Authentication Protocol):** LEAP is a way to prove something is real that's designed for situations with few resources and abilities. It gives good and trustworthy proof [28].

- **Tiny JAMBU: Tiny JAMBU** is a simple and light way to hide information that also makes sure it's real, good for small devices with not much power [29-34].

These authentication mechanisms that have little weight are suitable for dealing with the security difficulties presented by devices with limited resources in the Smart Grid. They enable efficient and secure communication while protecting the integrity and confidentiality of data.

VI. CONCLUSIONS

In this article, we look closely at the important parts of safety in Smart Grids, mostly talking about why there should be easy to use ways for lightweight authentication and key agreement mechanisms. The main points are that devices for Smart Grid have limited resources, there is a need for good authentication processes, and the significance of energy-efficient security solutions. The special problems that Smart Grids face make it very important to have security measures that are not heavy. These security methods are key to balance the small resources of devices and keep strong protection. This points out why it's vital to use easy protection methods for keeping data safe, true, and quickly checked in the Smart Grid system.

The call to action for adopting lightweight authentication and key agreement methods is vital as Smart Grid technology evolves. Stakeholders such as utility companies, device manufacturers, and legislators are urged to prioritize the integration of lightweight security solutions in Smart Grid deployments. Collaboration between the cybersecurity community and Smart Grid experts is essential for developing, refining, and standardizing security procedures that are effective yet not resource heavy. The implementation of these lightweight security measures is key to enhancing the resilience of Smart Grids against various challenges, and in supporting the long-term, secure management of our electrical infrastructure. Ultimately, merging Smart Grids with lightweight security presents an optimistic future, ensuring reliable and protected operations of our energy

systems and paving the way for a more resilient, efficient, and secure energy future.

References

[1] Tuballa, M. L., & Abundo, M. L. (2016). A review of the development of Smart Grid technologies. Renewable and Sustainable Energy Reviews, 59, 710-725.

[2] Saxena, N., Choi, B. J., & Lu, R. (2015). Authentication and authorization scheme for various user roles and devices in smart grid. IEEE transactions on Information forensics and security, 11(5), 907-921.

[3] Tanveer, Muhammad, Habib Shah, Ahmed Alkhayyat, Shehzad Ashraf Chaudhry, and Musheer Ahmad. "ARAP-SG: Anonymous and reliable authentication protocol for smart grids." IEEE Access 9 (2021): 143366-143377.

[4] Nyangaresi, V. O., Abduljabbar, Z. A., Refish, S. H. A., Al Sibahee, M. A., Abood, E. W., & Lu, S. (2021, November). Anonymous Key Agreement and Mutual Authentication Protocol for Smart Grids. In International Conference on Cognitive Radio Oriented Wireless Networks (pp. 325-340). Cham: Springer International Publishing.

[5] Qays, M. O., Ahmad, I., Abu-Siada, A., Hossain, M. L., & Yasmin, F. (2023). Key communication technologies, applications, protocols and future guides for IoT-assisted smart grid systems: A review. Energy Reports, 9, 2440-2452.

[6] Abdullah, A. A., El-den, B. M., Abo-Al-Ez, K. M., & Hassan, T. M. (2023). Security Management for an Advanced Metering Infrastructure (AMI) System of Smart Electrical Grids. Applied Sciences, 13(15), 8990.

[7] Raghunandan, K. (2022). Supervisory Control and Data Acquisition (SCADA). In Introduction to Wireless Communications and Networks: A Practical Perspective (pp. 321-337). Cham: Springer International Publishing.

[8] Tang, B. (2014). New approaches to smart grid security with SCADA systems. Louisiana State University and Agricultural & Mechanical College.

[9] De Almeida, L. F. F., Pereira, L. A. M., Sodré, A. C., Mendes, L. L., Rodrigues, J. J., Rabelo, R. A., & Alberti, A. M. (2020). Control networks and smart grid teleprotection: Key aspects, technologies, protocols, and case-studies. IEEE Access, 8, 174049-174079.

[10] Choudhary, S., Kumar, A., & Kumar, K. (2023). PKIF-AKA: A Public Key Infrastructure Free Authenticated Key Agreement Protocol for Smart Grid Communication. IETE Journal of Research, 1-12.

[11] Höglund, J., Furuhed, M., & Raza, S. (2023). Lightweight certificate revocation for low-power IoT with end-to-end security. Journal of Information Security and Applications, 73, 103424.

[12] Prabakaran, B., Sumithira, T. R., & Nagaraj, V. (2023). Smart Grid Communication Under Elliptic Curve Cryptography. INTELLIGENT AUTOMATION AND SOFT COMPUTING, 36(2), 2333-2347.

[13] Xia, Z., Liu, T., Wang, J., & Chen, S. (2023). A Secure and Efficient Authenticated Key Exchange Scheme for Smart Grid. Heliyon.

[14] Mahmood, K., Chaudhry, S. A., Naqvi, H., Shon, T., & Ahmad, H. F. (2016). A lightweight message authentication scheme for smart grid communications in power sector. Computers & Electrical Engineering, 52, 114-124.

[15] Ghosal, A., & Conti, M. (2019). Key management systems for smart grid advanced metering infrastructure: A survey. IEEE Communications Surveys & Tutorials, 21(3), 2831-2848.

[16] Mahmood, K., Chaudhry, S. A., Naqvi, H., Shon, T., & Ahmad, H. F. (2016). A lightweight message authentication scheme for smart grid communications in power sector. Computers & Electrical Engineering, 52, 114-124.

[17] Jha, R. K. (2023). Cybersecurity and Confidentiality in Smart Grid for Enhancing Sustainability and Reliability. Recent Research Reviews Journal, 2(2), 215-241.

[18] Hu, C., Liu, Z., Li, R., Hu, P., Xiang, T., & Han, M. (2023). Smart contract assisted privacy-preserving data aggregation and management scheme for smart grid. IEEE Transactions on Dependable and Secure Computing.

[19] Zhu, F., Yi, X., Abuadbba, A., Luo, J., Nepal, S., & Huang, X. (2022, September). Efficient hash-based Redactable signature for smart grid applications. In European Symposium on Research in Computer Security (pp. 554-573). Cham: Springer Nature Switzerland.

[20] Li, Y., Zhang, D., Wang, Z., & Liu, G. (2023). A Blockchain-Based Cooperative Authentication Mechanism for Smart Grid. Applied Sciences, 13(11), 6831.

[21]Priyanka, C. N., & Ramachandran, N. (2023). Analysis on Secured Cryptography Models with Robust Authentication and Routing Models in Smart Grid. International Journal of Safety & Security Engineering, 13(1).

[22] Tanveer, M., & Alasmary, H. (2023). LACP-SG: Lightweight Authentication Protocol for Smart Grids. Sensors, 23(4), 2309.

[23] Yu, W., & Wang, S. (2023). Identity-Based Key Management Scheme for Smart Grid over Lattice. KSII Transactions on Internet & Information Systems, 17(1).

[24] Chen, C., Guo, H., Wu, Y., Shen, B., Ding, M., & Liu, J. (2023). A Lightweight Authentication and Key Agreement Protocol for IoT-Enabled Smart Grid System. Sensors, 23(8), 3991.

[25] Castellon, C. E., Roy, S., Kreidl, O. P., Dutta, A., & Bölöni, L. (2022, October). Towards an Energy-Efficient Hash-based Message Authentication Code (HMAC). In 2022 IEEE 13th International Green and Sustainable Computing Conference (IGSC) (pp. 1-7). IEEE.

[26] Pammu, A. A., Ho, W. G., Lwin, N. K. Z., Chong, K. S., & Gwee, B. H. (2018). A high throughput and secure authentication-encryption AES-CCM algorithm on asynchronous multicore processor. IEEE Transactions on Information Forensics and Security, 14(4), 1023-1036.

[27] Sleem, L., & Couturier, R. (2021). Speck-R: An ultra light-weight cryptographic scheme for Internet of Things. Multimedia Tools and Applications, 80, 17067-17102.

[28] Lu, Z., Wang, Q., Chen, X., Qu, G., Lyu, Y., & Liu, Z. (2019, October). LEAP: A lightweight encryption and authentication protocol for in-vehicle communications. In 2019 IEEE Intelligent Transportation Systems Conference (ITSC) (pp. 1158-1164). IEEE.

[29] Meent, T. (2022). A comparative study on lightweight authentication protocols in IoT (Bachelor's thesis, University of Twente).

[30] Gupta, B. B., & Sheng, Q. Z. (Eds.). (2019). Machine learning for computer and cyber security: principle, algorithms, and practices. CRC Press.

[31] Bhushan, K., & Gupta, B. B. (2017). Security challenges in cloud computing: state-of-art. International Journal of Big Data Intelligence, 4(2), 81-107.

[32] Singh, A., & Gupta, B. B. (2022). Distributed denial-of-service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms: issues, challenges, and future research directions. International Journal on Semantic Web and Information Systems (IJSWIS), 18(1), 1-43.

[33] Gupta, B. B., Perez, G. M., Agrawal, D. P., & Gupta, D. (2020). Handbook of computer networks and cyber security. Springer, 10, 978-3.

[34] Zhang, Q., Guo, Z., Zhu, Y., Vijayakumar, P., Castiglione, A., & Gupta, B. B. (2023). A deep learning-based fast fake news detection model for cyber-physical social services. Pattern Recognition Letters, 168, 31-38.