Fortified-Grid 3.0: Security by Design for Smart Grid through Hardware Security Primitives

Giriraj Sharma
Dept. of Electronics & communication
Malaviya National Institute of Technology
Jaipur, India
2019rec9564@mnit.ac.in

Amit M. Joshi
Dept. of Electronics &communication
Malaviya National Institute of Technology
Jaipur, India
amjoshi.ece@mnit.ac.in

Saraju P. Mohanty
Dept. of comp science & Engg
University of North Texas
Texas, USA
Saraju.mohanty@unt.edu

***Abstract*—Traditional approaches to adding security measures and retrofitting them onto existing smart grid systems, have security flaw and vulnerability. Considering security from the beginning, potential vulnerabilities and risks can be identified and addressed early in the smart grid design process, leading to more robust and secure solutions. SbD involves incorporating security considerations and features into the design and architecture of a system rather than adding them as an afterthought. This paper provides an extensive overview of hardware security and trust, examining threats, countermeasures, and design tools. Fortified-Grid 3.0 introduces the latest advancements in hardware security research, aiming to inspire hardware designers and smart grid developers to embrace the challenges and opportunities of integrating additional security measures into robust hardware design, testing, and verification. This paper also discusses security by design in smart grids, focusing on primitives like PUF and TPM. Our paper addresses various challenges, presents solutions, and conducts comparative analyses of prevalent Security-by-Design approaches.**

***Index Terms*—Smart Grid, Security-by-Design (SbD), Physical unclonable function (PUF), Trusted platform module (TPM).**

I. Introduction

The Smart Grid is a network of interconnected devices and systems designed to manage electricity generation, distribution, and consumption efficiently. It leverages advanced technologies to collect and exchange data, transforming it into valuable insights for optimizing energy usage and grid operations. The integration of digital technologies within the physical infrastructure of the power grid brings about significant benefits and challenges related to security. As the Smart Grid ecosystem generates and exchanges substantial amounts of data, it becomes an attractive target for adversaries. The interconnected nature of the Smart Grid introduces various potential risks and vulnerabilities that need to be addressed to ensure information security. Security assurance within the Smart Grid ecosystem is a critical challenge that requires careful consideration [1].

Embedded security is a key issue when securing Smart Grid devices, which often operate with limited processing capabilities, power constraints, and bandwidth limitations. Design considerations for securing constrained Smart Grid devices are of utmost importance to achieve security by default. It is essential to incorporate established protocols and best practices during the design and development stages to address security challenges in the Smart Grid. By adhering to recommended security measures, many of the security concerns can be mitigated. Implementing robust security mechanisms and considering the unique requirements of constrained Smart Grid devices are fundamental steps in enhancing the overall security and resilience of the system [2].

By proactively integrating security measures into the design and operation of Smart Grid devices and systems, it becomes possible to mitigate risks, protect against cyber threats, and ensure the reliable and secure functioning of the grid. This includes safeguarding critical infrastructure, protecting sensitive data, and maintaining the trust and confidence of stakeholders in the Smart Grid ecosystem. [3]. Some important security primitive are Physical unclonable function (PUF), Trusted platform module (TPM) and Hardware security module (HSM) and SGX etc.

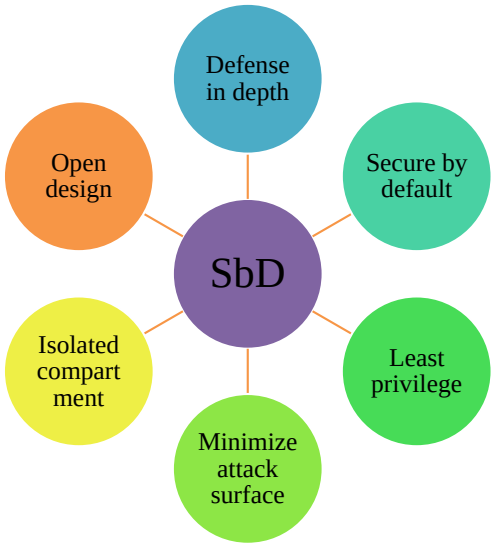

Fig. 1. Security-by-Design principle

Remainder of paper are as follow: Section II describes the research contribution. Section III describes the background of

smart grid while section IV explain about the need of security by design. Section V describes about the different security by design primitives while section VII describes about various challenges in SbD implementation. Section VIII concludes the paper.

II. Research contributions

The main contributions of this paper can be summarize as follows.

- We provide a complete overview of Security-by-Design for smart grid network. We have discussed latest advancements in hardware security research, aiming to inspire hardware designers and smart grid developers to embrace the challenges and opportunities of integrating additional security measures into robust hardware design, testing, and verification.
- We review the Security-by-Design methods and discussed various hardware primitives. The comparison of each method in terms of its advantages and disadvantages is summarised and tabulated.
- We review the various security constraints and their solutions in smart grid.

III. Background

A smart grid is an advanced electrical grid system that utilizes digital technologies, communication networks, and automation to manage electricity generation, distribution, and consumption efficiently. It incorporates smart meters, sensors, and control systems to enable two-way communication and real-time monitoring. This allows for improved energy management, optimized grid operations, better integration of renewable energy sources, and enhanced responsiveness to changing demand and grid conditions. The smart grid aims to increase energy efficiency, reliability, and sustainability while empowering consumers with more control over their energy usage and facilitating the transition towards a greener and smarter energy future [9].

A. Smart Grid component

- **AMI**: The Advanced Metering Infrastructure (AMI) employs a communication system and modern solid-state meters that have the capability to remotely relay detailed information about each customer's electricity consumption to the utility. This data is transmitted at intervals of either 15 minutes or hourly. Furthermore, AMI systems can offer information such as peak electricity consumption, voltage levels, and other power-related characteristics. Various communication methods are available for transmitting data from individual meters back to utility operations. Some of these options encompass public WiFi, private radio systems, and power line carrier systems, which use the electric distribution network to transmit information. In addition, smart meters can also function as radio gateways, allowing control and data collection for individual appliances within premises.
- **SCADA**: A robust SCADA system should encompass the infrastructure to support distribution automation and advanced applications in a DMS. Its role in a smart grid includes aiding distributed generation, alarms, telemetry, event logging, and remote control. It should facilitate power system data access for engineering planning without requiring operational workstations. SCADA's historical strength in data import/export remains relevant, but the evolving power system needs to demand decentralized, adaptable, and integrated control centres. Current SCADA technologies enabling decentralization are briefly assessed. With the Internet era, technology trends are moving towards microgrid/grid computing and web services, shaping the concept of future microgrid service-based control centres [10].

B. Different types of attack in Smart Grid

The Fortified-Grid 3.0 has to consider various types of attacks before implementation:

- Impersonation attack : A type of cyber attack on smart grid systems where an unauthorized entity masquerades as a legitimate user or device to gain unauthorized access, manipulate data, disrupt operations, or compromise the integrity and security of the grid infrastructure.
- Denial of service attack : A disruptive cyber attack targeting a smart grid system where an attacker overwhelms the grid's resources or communication channels, causing a significant degradation in service, potential power outages, or rendering the grid inoperable, impacting the reliability and availability of electricity distribution [11].
- Reverse engineering attack: A reverse engineering attack in the context of a smart grid refers to the process of analyzing and understanding the underlying technologies, protocols, or systems used in the grid to discover vulnerabilities or extract sensitive information. This attack aims to exploit weaknesses and potentially compromise the security and integrity of the smart grid infrastructure [12].
- Dictionary and brute force attack : A dictionary and brute force attack on a smart grid involves systematically trying different combinations of passwords or encryption keys, using precomputed dictionaries or exhaustive search methods, to gain unauthorized access to the grid's systems, control centres, or communication channels, compromising their security and potentially disrupting operations [13].

IV. Fortified-Grid 3.0: Need of Security-by-Design (SbD) in Smart Grid

The need for SbD in smart grid security arises since grids are placed in at open network. Smart grids are a critical component of modern energy systems, controlling and managing the flow of electricity across vast networks. Ensuring the security of smart grids is crucial to protecting the integrity and reliability of the entire energy infrastructure. By incorporating

TABLE I
A COMPARATIVE ANALYSIS OF DIFFERENT SBD SCHEMES

Research works	Application	Primitive used	Features
Yanambaka et al. 2019 [4]	IoMT (Device)	Arbiter PUF	Provide hardware security usig SbD
Mohanty et al. 2020 [5]	IoMT	Ring Oscillator PUF	Provide hardware security
Das, et al. 2022 [6]	IoT	PUF	Smart meter hardware security
Khurshid, et al. 2023 [7]	IoT Device	TPM, X.509	Supports Hardware-assisted security and firmware integrity
Bathalapalli, et al. 2023 [8]	IoT, Smart Grid	PUF and TPM both	TPM integrated PUF SbD

security measures from the design stage, potential vulnerabilities and risks can be identified and addressed proactively. Smart grids generate and process large amounts of sensitive data, including consumer information, energy usage patterns, and operational details. Security by design ensures that appropriate measures, such as encryption, access control, and secure communication protocols, are implemented to protect this data from unauthorized access, tampering, or misuse. Smart grids are increasingly becoming targets for cybercriminals, who may attempt to disrupt operations, steal data, or gain unauthorized control over the grid infrastructure. By integrating security measures from the design phase, potential vulnerabilities can be identified and mitigated, reducing the risk of successful cyber attacks.

Smart grids involve collecting and analyzing detailed energy consumption data from consumers. Security-by-Design helps protect the privacy of individuals by implementing robust privacy controls, anonymization techniques, and secure data handling practices [14]. The energy sector is subject to various regulations and standards related to security and privacy. Security-by-Design ensures that smart grid systems meet these requirements, reducing legal and regulatory risks for utilities and energy providers. Incorporating security measures from the design phase helps to avoid costly retrofitting or patching of vulnerabilities discovered after deployment. Building security into the system's foundation makes it more resilient, reducing the potential impact of security incidents and minimizing associated costs.

Overall, security by design is crucial for smart grids to protect critical infrastructure, safeguard sensitive data, mitigate cyber threats, ensure privacy, comply with regulations, and achieve long-term cost savings. It helps create a robust and secure energy infrastructure that can meet the evolving challenges of the digital age.

V. SECURITY-BY-DESIGN(SBD) PRIMITIVE

The popular primitives for Security-by-Design are PUF and TPM.

A. Physical Unclonable Function (PUF)

Hardware-assisted security using Physical Unclonable Functions (PUFs) leverages the unique physical properties of semiconductor devices to enhance security measures. PUFs provide a reliable and tamper-resistant means of generating unique identifiers or cryptographic keys, which can be utilized in various security applications. PUFs are discussed in details for hardware-assisted security.

Physical Unclonable Functions (PUFs) rely on the distinct

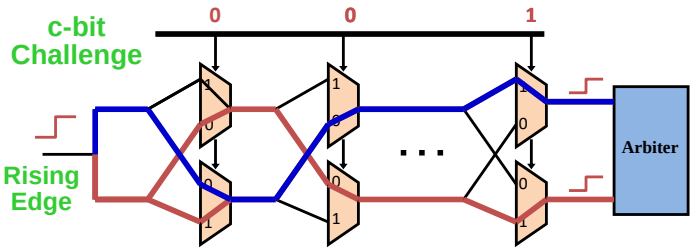

Fig. 2. Physical Unclonable Function

irregularities introduced during device fabrication to extract a unique fingerprint for each device [15]. Specific device parameters, such as threshold voltage or critical dimensions, are measured when external stimuli are applied. The initial measurement for a particular input stimulus or address in memory is termed the "original response," and both this response and the corresponding challenge are stored on a server. When the same parameter is remeasured with the same external stimulus, it's referred to as a response [16]. These challenge-response pairs (CRPs) are compared to validate device identity, and the disparity during registration and authentication is the challenge-response pair error (CRP error) [17].

PUFs can be broadly classified based on their number of possible CRPs: "strong PUFs" and "weak PUFs." Weak PUFs utilize manufacturing variability, yielding a limited number of stable responses tied to the number of components generating CRPs. These stable responses are suitable for secret key generation due to their consistency. In contrast, strong PUFs encompass a large CRP set. Their unique CRPs prevent brute force attacks even if temporary access is gained. As such, strong PUFs excel in authentication, potentially resulting in longer cryptographic keys.

B. Trusted Platform Module (TPM)

A Trusted Platform Module (TPM) is a specialized hardware chip developed by the Trusted Computing Group, designed to serve as a cryptographic co-processor in smart grid IoT devices, smart vehicle ECU and other security applications. The TPM consists of several key components that make it suitable for hardware security.The TPM houses multiple PCR, accessible via index values. PCR stores firmware hexadecimal values for smart vehicles and plays a role in measuring integrity. NVRAM permanent memory stores essential keys such as the Storage Root Key (SRK) and Endorsement Key (EK), contributing to the security of smart vehicular technology. To prevent security breaches arising from inadequate key generation, the RNG is employed to generate random keys and nonce. The TPM employs the RSA algorithm for tasks such as asymmetric encryption/decryption and digital signing, bolstering intelligent vehicular security.

TPM is very useful hardware security primitives used in

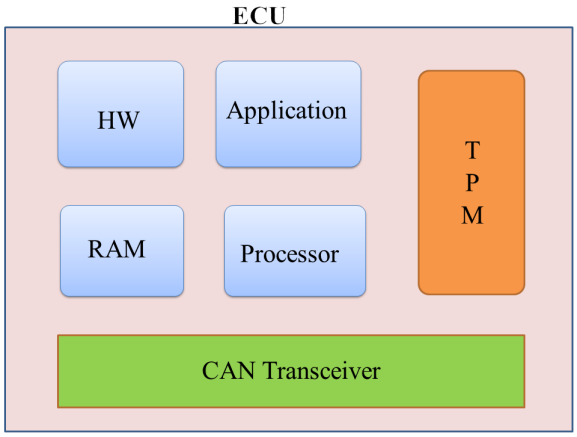

Fig. 3. Integration of TPM in ECU

SbD. It is helpful in device identification in network. Before TPM, devices were identified using less secure identifiers like MAC or IP addresses, which TPM improves upon. TPM's hardware-based random number generator enhances key generation security, countering vulnerabilities in vehicular communication security. The hardware-based nature of TPM key storage thwarts software attacks in the realm of smart vehicle technology. TPM counters previous vulnerabilities by enabling trustworthy health attestation of a system, avoiding false reports of compromised systems being deemed healthy. Recently implemented TPM 2.0 introduces greater flexibility in employing various algorithms, departing from the limitations of previous versions. This agility supports encryption algorithms that ensure secure communication within intelligent vehicular systems. The specification's adaptability mitigates the need for alterations in case of future algorithm vulnerabilities. By incorporating TPM into a hardware security architecture, organizations can enhance the security of their computing platforms and protect against a range of threats, including unauthorized access, tampering, and system-level attacks. TPM provides a trusted and secure foundation for various security functions, enabling hardware-assisted security measures.

VI. Comparison of Results of various SbD primitives

A comparison of various popular hardware primitives are shown in table II. Overhead of various schemes are compared in smart gird environment. We have compared results of PUF and TPM based popular schemes. PUF based schemes are Kaveh, et al. 2020 [18], Sharma, et al. 2021 [1], Jiang, et al. 2022 [19] and Reddy, et al. 2023 [20].

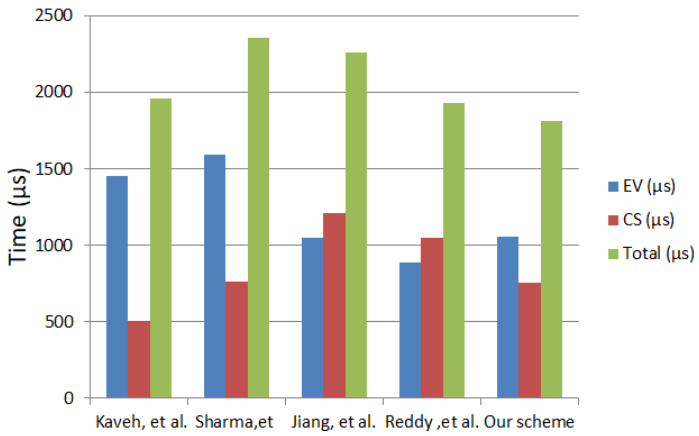

Fig. 4. Computational overhead analysis at EV and CS

VII. Challenges and Application

A. Smart Grid Security Constraints

- Transactions Latency: One of the key constraints in smart grid security is the impact on transaction latency. Security measures, such as authentication, encryption, and intrusion detection, introduce additional computational overhead and communication delays, leading to an increase in transaction latency within the smart grid system. These latency constraints can affect real-time grid operations and applications that rely on timely data exchange, such as fault detection, load balancing, and demand response. [21].
- Communication Latency: Communication latency is a significant security constraint in a smart grid. Security measures such as authentication, encryption, and data integrity checks introduce additional processing and transmission delays. These delays can impact the responsiveness of grid communication, affecting real-time monitoring, control, and decision-making.
- Transactions Computational Overhead: The computational overhead associated with transactions is a key security constraint in the smart grid. Security measures like authentication, encryption, and integrity checks require additional computational resources, impacting the processing capacity of devices and systems involved in transaction handling.

TABLE II
CRYPTOGRAPHER OPERATION AND COMPUTATIONAL COST

Schemes	Electric Vehicle	Charging Station	Computational Overhead Time (μs)
Kaveh, et al. 2020 [18]	8Th+4Tpuf+4Txor	8Th+4Txor	1960.8
Sharma, et al. 2021 [1]	6Th+2Tpuf+1Tadd+2Txor	6Th+2Tpuf+1Tadd+2Txor	2356.6
Jiang, et al. 2022 [19]	4Th+4Tpuf+2Txor	4Th+4Tpuf+6Txor	2259.2
Reddy, et al. 2023 [20]	8Th+2Tpuf+2Txor	8Th+4Tpuf+4Txor	1933.2

B. Application of SbD

The SbD applies to any software and hardware. SbD motivates to include cyber security strategies and technique during manufacturing and design process. These design ensures the implementation of the necessary security protocol. These protocol includes

- Authorization and accountability : Only authorized users can access certain parts of the system, making accountability clearer.
- Authentication : Users, regardless of privileges, undergo the necessary authentication process [21].
- Data confidentiality and availability: Data remain secure ,private and accessible only to authorised user .
- System integrity: Data and system can not be modified by intruder.

VIII. Conclusion

The article explores Security-by-Design as a proactive approach to integrating security measures during development. It surveys recent advancements in Security-by-Design, particularly within the context of hardware security. The paper covers various aspects, including an overview of Security-by-Design, its benefits, and its application in IoT, smart grids, and privacy considerations. Prioritizing security in the design phase aids in early risk identification and resource conservation, fostering user trust. In the realm of smart grids, PUF and TPM are popular primitives for Security-by-Design. Hardware security primitives encompass the integration of emerging technologies like AI and machine learning, along with the adoption of threat intelligence, ensuring continual adaptation of security measures. The paper aims to alert hardware designers and tool developers to address significant security gaps that conventional hardware design and verification methods may not adequately cover.

References

[1] G. Sharma, A. M. Joshi, and S. P. Mohanty, "An efficient physically unclonable function based authentication scheme for V2G network," in *Proc. IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 421–425.

[2] D. He, H. Wang, M. K. Khan, and L. Wang, "Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography," *IET Communications*, vol. 10, no. 14, pp. 1795–1802, 2016.

[3] H. Zhang, B. Liu, and H. Wu, "Smart grid cyber-physical attack and defense: A review," *IEEE Access*, vol. 9, pp. 29 641–29 659, 2021.

[4] V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical unclonable function-based robust and lightweight authentication in the internet of medical things," *IEEE Transactions on Consumer Electronics*, vol. 65, no. 3, pp. 388–397, 2019.

[5] S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUF chain: A hardware-assisted blockchain for sustainable simultaneous device and data security in the internet of everything (IoE)," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 8–16, 2020.

[6] R. Das, G. Karmakar, J. Kamruzzaman, and A. Chowdhury, "Measuring trustworthiness of smart meters leveraging household energy consumption profile," *IEEE Journal of Emerging and Selected Topics in Industrial Electronics*, vol. 3, no. 2, pp. 289–297, 2022.

[7] A. Khurshid and S. Raza, "Autocert: Automated TOCTOU-secure digital certification for iot with combined authentication and assurance," *Computers & Security*, vol. 124, p. 102952, 2023.

[8] V. K. Bathalapalli, S. P. Mohanty, E. Kougianos, V. Iyer, and B. Rout, "PUFchain 4.0: Integrating PUF-based TPM in distributed ledger for security-by-design of IoT," in *Proceedings of the Great Lakes Symposium on VLSI 2023*, 2023, pp. 231–236.

[9] H. Aranha, M. Masi, T. Pavleska, and G. P. Sellitto, "Enabling security-by-Design in smart grids: An architecture-based approach," in *15th European Dependable Computing Conference (EDCC)*. IEEE, 2019, pp. 177–179.

[10] J. Xia and Y. Wang, "Secure key distribution for the smart grid," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1437–1443, 2012.

[11] N. Saxena and B. J. Choi, "Authentication scheme for flexible charging and discharging of mobile vehicles in the V2G networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, pp. 1438–1452, 2016.

[12] S. P. Mohanty, "Security and privacy by design is key in the internet of everything (IoE) era." *IEEE Consumer Electron. Mag.*, vol. 9, no. 2, pp. 4–5, 2020.

[13] A. Jain and A. M. Joshi, "Device authentication in IoT using reconfigurable PUF," in *Proc. 2nd Middle East and North Africa COMMunications Conference (MENACOMM)*. IEEE, 2019, pp. 1–4.

[14] P. Gope and B. Sikdar, "An efficient privacy-preserving authentication scheme for energy internet-based vehicle-to-grid communication," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6607–6618, 2019.

[15] G. Sharma, A. M. Joshi, and S. P. Mohanty, "Fortified-Grid 2.: Fortifying Smart Grid through Integration of Physical Unclonable Function in Industrial IoT," *MDPI Information*, vol. 3, no. 2, pp. 289–297, 2023.

[16] S. K. Agarwal and A. M. Joshi, "Device authentication with FPGA based self-correcting physical unclonable function for internet of things," *Microprocessors and Microsystems*, vol. 95, p. 104717, 2022.

[17] A. Kumari, M. Trivedi, S. Tanwar, G. Sharma, and R. Sharma, "SV2G-ET: A secure vehicle-to-grid energy trading scheme using deep reinforcement learning," *International Transactions on Electrical Energy Systems*, vol. 15, 2022.

[18] M. Kaveh, D. Martín, and M. R. Mosavi, "A lightweight authentication scheme for V2G communications: A PUF-based approach ensuring cyber/physical security and identity/location privacy," *Electronics*, vol. 9, no. 9, p. 1479, 2020.

[19] Z. Jiang, Z. Zhou, L. Xiong, and L. Zhou, "An efficient lightweight anonymous authentication scheme for V2G using physical unclonable function," in *Proc. 94th Vehicular Technology Conference (VTC2021-Fall)*. IEEE, 2021, pp. 1–5.

[20] A. G. Reddy, P. R. Babu, V. Odelu, L. Wang, and S. A. Kumar, "V2G-Auth: lightweight authentication and key agreement protocol for V2G environment leveraging physically unclonable functions," *IEEE Transactions on Industrial Cyber-Physical Systems*, 2023.

[21] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably secure authenticated key agreement scheme for smart grid," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1900–1910, 2016.