SMART METER SECURITY ISSUES: A REVIEW PAPER

Osama Alshannaq [1], Mohd Rizuan Baharon [1], Shekh Faisal Abdul Latip [1],
Hairol Nizam Mohd Shah [2] and Áine MacDermott [3]

[1] Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia.
[2] Fakulti Teknologi & Kejuruteraan Elektrik, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia.
[3] School of Computer Science and Mathematics, Liverpool John Moores University, Liverpool, L3 3AF, United Kingdom.

ABSTRACT

In recent decades, conventional electric power systems have seen escalating issues due to rising electrical consumption, leading to voltage instability, recurrent blackouts, and heightened carbon emissions. These challenges highlight the pressing necessity for a more efficient and sustainable energy infrastructure. The smart grid has emerged as a disruptive solution, providing improved energy distribution, real-time monitoring, and facilitating renewable integration. Central to this evolution are smart meters, which are essential elements of the Advanced Metering Infrastructure (AMI), facilitating precise energy monitoring, bidirectional connectivity, and remote oversight within smart households and grids. Nonetheless, despite their functionalities, smart meters provide potential security threats, including susceptibility to cyberattacks and physical interference. This review article seeks to examine the fundamental characteristics and functionalities of smart meters, identify significant security and implementation difficulties, and emphasise their role within the larger smart grid ecosystem. This paper conducts a thorough analysis of existing literature to analyse the communication technologies utilized, the possible threat landscape, and the significance of strong security frameworks. The results underscore the necessity for secure communication protocols, sophisticated encryption, and physical protections to guarantee the reliability and integrity of smart meter implementations in contemporary power systems.

KEYWORDS

Smart grid; Secure smart meter; Attacks on data; network attacks; Physical hardware attacks.

1. INTRODUCTION

The global electricity sector is undergoing a radical transformation, with smart grids replacing aging power grids. The need to reduce carbon emissions, meet growing energy demands, and make electricity distribution more reliable and efficient are the primary drivers of this transformation. Smart meters are a key part of advanced metering infrastructure (AMI) and are essential to this transformation. They enable real-time monitoring, two-way communication, and remote management of energy consumption [1][2]. Smart meters have changed the way we use and manage energy by facilitating demand regulation, dynamic pricing, and communication with home energy management systems (HEMS). While smart meters offer certain operational advantages, they also pose serious privacy and security threats that must be addressed to maintain the stability and reliability of smart grid systems [3], [4]. Smart meter security can be divided into three main categories: data security, network security, and physical security. Data security is the process of ensuring the availability, privacy, and accuracy of the data collected and transmitted by smart meters. Because these devices often handle sensitive user data, such as complex

DOI: 10.5121/ijnsa.2025.17401

consumption patterns [5], they are easy targets for data theft, tampering, or the creation of unauthorized profiles.

Network security aims to protect the communication channels used by smart meters, which often rely on radio frequency (RF) or power line communications (PLC). Many different types of attacks can occur on these channels, such as man-in-the-middle (MITM) attacks, replay attacks, spoofing, and eavesdropping [6], [7]. Smart meters are typically placed in locations easily accessible to the public, making them easy to tamper with, access unauthorized devices, or replace. For this reason, physical security is critical. People with malicious intent can exploit physical access to manipulate the meter's operation or install malware [8].

Alongside these issues, there is growing concern about user privacy. Smart meters collect extensive information about how people use their devices, how often they are at home, and how they behave there. If this information is shared without authorization, it could be monitored or exploited by third parties [9], [10]. Given these complex risks, protecting smart meters is not just a technological need, but also an ethical imperative. To address these threats, recent research has proposed a number of intrusion detection systems, lightweight encryption methods, and privacy-protecting protocols. However, challenges remain, particularly in finding the right balance between robust security and the limited processing power of smart meters [11], [12]. This review paper aims to provide a focused look at the privacy and security issues that arise with smart meters. It begins by explaining how smart meters work and their purpose in the smart grid. It then addresses three types of threats and vulnerabilities: physical, network, and data. This is achieved with the help of real-world case studies and research findings. Finally, it explores new approaches and areas of research that could lead to reliable smart metering systems that respect individual privacy.

However, underscores the dual characteristics of this technology. While smart meters provide operational benefits, they also have significant vulnerabilities. These vulnerabilities are categorised into three main areas: data security, network security, and physical security. Each of these domains is specific to threats such as data breaches, channel attacks, and physical tampering. Another key issue raised is privacy, especially in relation to the extensive user data collected by smart meters. The threat of unauthorised profiling or surveillance presents both ethical and technical challenges. Therefore, securing smart meters is framed not only as a technical requirement but also as an ethical responsibility.

Unlike prior reviews that often focus on a single aspect of smart meter security, such as encryption methods, communication protocols, or individual threat categories, this paper offers a unified and multidimensional assessment of security risks in smart metering systems. It contributes a comparative analysis across network, data, and physical attack vectors, and maps these to corresponding security properties such as confidentiality, integrity, and authentication. Furthermore, this review critically evaluates the suitability of proposed solutions in the context of real-world constraints, such as computational limitations and deployment scalability. It also uniquely emphasizes the intersection of security and privacy, a dimension frequently underrepresented in earlier surveys. By consolidating these perspectives, the paper provides a comprehensive reference point for researchers and practitioners seeking holistic and implementable smart meter security strategies.

By outlining the aim of this paper: to provide an organized review of current threats and solutions, supported by case studies and emerging research. It paves the way for an in-depth discussion on the development of secure and privacy-preserving smart metering systems that are compatible with the resource constraints of these devices.The remaining sectionsare described as follows. Section 2 explains the Literature Review, Section 3 Architecture of Smart Grid, Section 4 Smart Meter Security Issues, and Section 5 the Conclusion.

2. LITERATURE REVIEW

Several studies have addressed threats to smart meters. Since many electric utilities plan to integrate the smart grid, installing smart meters in every household is crucial. These devices enable remote load monitoring, transparent communication between consumers and providers, and even remote disconnection of power. We categorize commonly reported security vulnerabilities to inform strategies

2.1. Smart Meter Advantages

Smart meters offer multiple benefits from three perspectives as illustrated in Figure 1.

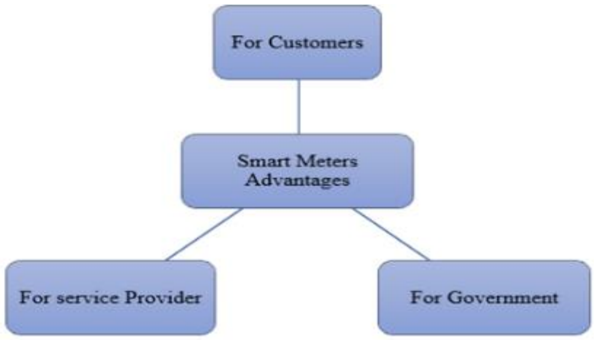

Figure 1. Beneficiary categories of smart meters

2.1.1. Advantage Experienced by Customers through the Use of Smart Meters

Cost Savings: Consumers can track real-time usage, shifting heavy-load tasks to off-peak hours, and reducing electricity bills[13], [14], [15].

More Accurate Billing: Detailed daily or hourly reports eliminate estimation errors.
Improved Supply Quality:Faster diagnosis and resolution of maintenance issues lead to fewer power interruptions [16], [17]. This is possible because the smart meter allows for the remote collection of data and minor maintenance, eliminating the need to wait for scheduled maintenance. Consequently, several challenges can be addressed more promptly.

2.1.2. Advantages Realized by Service Providers through the Utilization of Smart Meters

Automated Meter Reading: Reduces manual labor, thereby saving costs.
Better Demand Management: Smart meters help track overall energy consumption in real time, aiding faster fault detection.

Enhances Customer Engagement: More precise consumption data can guide users toward efficient energy use. [13], [14], [15],[16].

2.1.3. Benefits Experienced by the Government through the Implementation of Smart Meters

Environmental Gains: Lower consumption means reduced CO_2 emissions[13][15]

Economic Stimulation: Large-scale deployments create opportunities in meter production, IT infrastructure, and other sectors[16].

2.2. Drawbacks of Existing Studies and Limitations of Prior Techniques

Although numerous studies have proposed security improvements for smart meters, most suffer from critical shortcomings that limit their practical application in real-world smart grid environments. For example, schemes such as "Secure Query Processing of Smart Grid Data Using Searchable Symmetric Encryption" and "A Practical Searchable Symmetric Encryption Scheme for Smart Grid Data" rely heavily on centralised key management and impose computational burdens unsuitable for resource-constrained devices. Other schemes, like "Searchable Multi-Keyword Encryption for Smart Grid Edge Computing," allow for flexible searching but come with high communication costs and complicated key distribution, assuming that edge servers can be trusted, something that's not realistic because edge nodes can be physically attacked. Furthermore, many existing technologies fail to adequately preserve user privacy, often leaking access patterns or metadata, and rarely incorporate privacy-preserving methods such as ORAM due to their complexity. Real-time performance is another common limitation, as many proposed models exhibit high latency and are only evaluated through simulations without hardware validation. Furthermore, these solutions typically lack standardisation and compatibility with existing AMI infrastructure, complicating their deployment across diverse utility systems. Finally, physical and firmware security vulnerabilities, including hardware tampering and malware injection, as well as the risk of insider threats, are often overlooked, resulting in incomplete security models that must be addressed in future research [86].

The latest comparison of searchable symmetric encryption (SSE) systems for smart grid data reveals major issues with performance, scalability, and privacy. The system suggested by Wang et al. in "Secure Query Processing of Smart Grid Data Using Searchable Symmetric Encryption" aims to keep queries private and lower computing costs by using keyword matching, but it has trouble handling changes to data, like updating or deleting records. In contrast, the solution presented by Zhang et al. in "A Practical Searchable Symmetric Encryption System for Smart Grid Data" enhances ease of use by supporting simple operations designed for smart meter constraints; however, it still relies on centralised key distribution and lacks resistance to the statistical leakage of query patterns. Meanwhile, Liu et al.'s approach in "Searchable Multi-Keyword Encryption for Smart Grid Edge Computing" supports complex multi-keyword queries and enhances the flexibility of edge processing. However, this increased expressiveness results in increased storage and communication costs, making it less suitable for large-scale AMI deployments. In general, although these systems contribute significantly to securing data access in smart grids, they are hampered by issues such as poor forward privacy, poor update efficiency, reliance on trusted servers, and partial protection against inference attacks. So, future efforts should focus on creating simpler, privacy-protecting SSE models that can handle changing queries, cost less to run, and work well for real-time smart meter uses [87].

When comparing the reviewed schemes, notable methodological differences emerge. For example, solutions like Wang et al.'s keyword-matching SSE are lightweight but limited in dynamic query handling, while Liu et al.'s multi-keyword scheme improves flexibility at the cost of increased storage and communication overhead. In terms of effectiveness, centralised key management approaches may simplify control but present a single point of failure, reducing resilience to targeted attacks. On the other hand, distributed models often assume a high-trust edge environment, which may not hold in real-world deployments. Furthermore, while some methods prioritise performance through hardware-efficient encryption, they tend to sacrifice privacy protections such as forward secrecy or access pattern confidentiality. This comparative perspective reveals a trade-off landscape where achieving security, privacy, scalability, and efficiency simultaneously remains an unresolved challenge.

2.3. Literature Gap

The shift to smart grids and the widespread deployment of smart meters significantly enhances energy management capabilities. However, existing literature predominantly addresses smart meter security threats individually and lacks a comprehensive analysis integrating network, data, and physical security dimensions. Furthermore, previous studies frequently overlook the practical constraints of resource-limited smart meter devices and fail to adequately discuss the ethical and privacy implications associated with large-scale deployments.

This review addresses these gaps by providing an integrated and holistic evaluation of smart meter security threats, emphasizing the interconnectivity of these vulnerabilities. Additionally, it highlights the importance of developing scalable, lightweight, and robust security solutions tailored to resource-constrained environments, identifying new directions for future research.

3. Architecture of Smart Grid

Figure 2 and 3 illustrate the typical smart grid metering system that uses sensors, meters, and actuators connected to a central station. Customers and relevant agencies can access the collected data. The central head-end system (HES) retrieves data from terminal nodes (smart meters, gateways, data concentrators), relaying information via wired or wireless connections[17] , [18], [19].

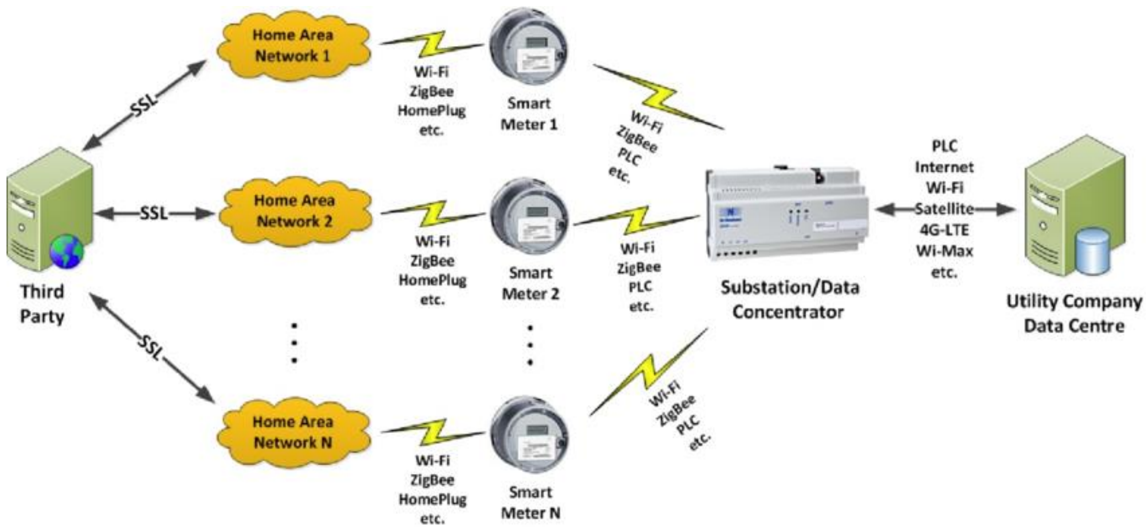

Figure 2. Architecture of Smart Grid[17]

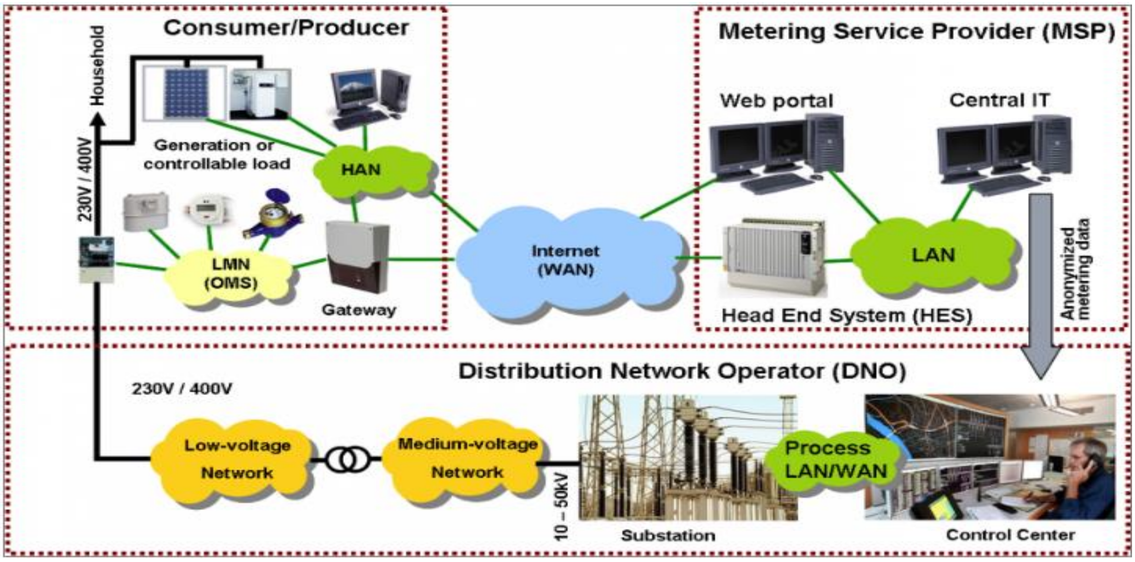

Figure 3.Architecture of a Smart Meter[18]

4. Smart Meter Security Issues

4.1.Network Attacks

Wireless communication (e.g., ZigBee, RF) can be exploited by attackers through eavesdropping, replay attacks, and network interruptions [37].In wired setups, open ports may also expose vulnerabilities where malicious data or code is injected. Ensuring secure routing is a common protective measure [20]– [24], Figure 4 highlights the security issues on smart meter.

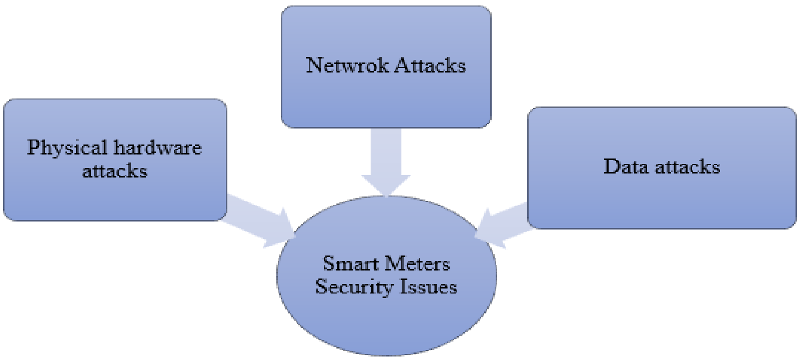

Figure 4. Research structure and security issues on Smart Meter

Many studies, as outlined in Table 1, have emphasized the growing security risks associated with network attacks across various digital environments, particularly in software-defined networks (SDNs), big data systems, and energy infrastructures. SDNs are especially vulnerable due to their centralized control mechanisms, which can be exploited for denial-of-service and spoofing attacks. In big data environments, attackers can misuse advanced analytics to extract sensitive information and conduct targeted intrusions, raising serious concerns about privacy and data integrity. Some researchers have proposed proactive frameworks that utilize behavioural analytics and threat modelling to monitor security states and predict potential attacks. Additionally, real-world cyber incidents have shown that threats now extend across domains, impacting both critical energy infrastructures and social media platforms, highlighting the convergence of cyber risks in interconnected digital ecosystems.

Table 1. Security issues (network attacks) with a smart meter.

Author	Security issue	Implemented Solution	Disadvantages and weaknesses
(Karmakar et al.,2019)	Attacks in SDN	Policy-based security application framework.	Lacks real-world efficacy validation.
(Liu et al., 2023)	Pre-emptive overflow attacks on SDN	POA Guard: specialized defence mechanism.	It addresses POA, but the scalability of large networks is unclear.
(Li and Min, 2019)	Big data-driven attacks	Data fusion tracking recognition.	Privacy compliance must be ensured
(Zhan et al., 2020)	security state and predict an attack	Semi-CRF-based event extraction.	Limited generalizability beyond tested datasets.
Kumar et al.,2019)	Real cyberattacks on SM networks	Threat taxonomy & classification.	Relies on trust in third-party data aggregators.

4.2.Security Attack on Physical Hardware

Attackers can leverage network access to cause actual physical damage, such as draining nodes' batteries or shutting down meters [15]. Direct meter tampering (e.g., via JTAG interfaces) is also a concern, as it can reveal sensitive cryptographic keys [53]. Table 2 presents examples of hardware-targeted attacks.

Table 2. Security issues (physical attacks) with a smart meter.

Author	Security issue	Implemented Solution	Disadvantages and weaknesses
(Guha et al., 2019)	Hardware Trojan attacks on reconfigurable hardware.	Ensuring reliability for periodic & non-periodic tasks.	Practical, full-scale prevention strategy lacking.
(Zou et al., 2020)	Cyber-physical attacks on the smart grid.	Parameter correction via Jacobian matrix & Taylor approximation.	Limited testing scope on IEEE 14 & 118 bus systems.
(Attia et al., 2018)	Price manipulation attack.	Lightweight detection algorithm	Assumes the control center is fully trusted.
(Gunduz et al., 2020)	Malware-based physical tampering	Cyber-attack model & detection mechanisms.	Hardware spoofing & physical tampering are still possible.
(Shao et al., 2021)	Cooling load injection (thermal attack)	Monitoring & detection algorithms for behind-the-meter threats.	Need complex equipment for detection.

4.3. Attacks on Data

Smart meter data contains personal and billing information, making them a valuable target. Attackers can modify readings to affect billing, pricing calculations (LMP), or glean user behaviour [58], [59].

Methods like false data injection or ciphertext-only attacks can compromise the integrity and confidentiality of real-time consumption data [30][36]. Table 3 offers notable examples.

Table 3. Security issues (data attacks) with a smart meter.

Author	Security issue	Implemented Solution	Disadvantages and weaknesses
(Shen et al., 2020)	Malicious data mining attack.	Data aggregation scheme for verifying malicious activity	Slightly higher communication costs
(Li et al., 2022)	False data injection (FDIA)	Secure federated learning with Paillier cryptosystem.	Lacks discussion on real-world integration.
(Chen et al., 2019)	Dynamic states under data injection attacks.	Online detection for dynamic state estimation vulnerabilities.	Damage impact analysis is limited.
(Eltayieb et al., 2019)	Cloud-based data storage & searching	Attribute-based encryption scheme (online/offline).	Large data volumes require robust storage strategies.

Core security properties, integrity, availability, confidentiality, and non-repudiation, must be upheld [34]. Attackers may impersonate legitimate systems (compromising confidentiality or integrity) or disrupt signals (violating availability) [35]. Encryption, digital signatures, and secure channel protocols are vital to prevent data theft [36].

Table 4 provides an overview of the main security concerns identified across various studies in the context of smart meters. Specifically, it summarizes which core security properties, namely data integrity, data privacy, data confidentiality, data availability, and data authentication, have been addressed or highlighted as areas of concern by different authors. This comparative analysis includes contributions from recent literature spanning multiple years, reflecting the evolving focus and priorities in smart meter security research. The presence or absence of attention to each security property is indicated for each referenced work, thereby enabling a clear understanding of the current research landscape and revealing potential gaps that warrant further investigation. This table serves as a valuable reference for identifying trends and directing future efforts toward more comprehensive and balanced security frameworks in smart metering systems.

Table 4. Some of the concerns in terms of security properties in smart meters.

Author, year	Data integrity	Data privacy	Data Confidentiality	Data Availability	Data Authentication
(Khattak et al.,2019)	No ☒	Yes☑	No ☒	Yes☑	No ☒
(P. Kumar et al. 2019)	Yes☑	No ☒	No ☒	No ☒	No ☒
(Abdalzaher, et al.,2022)	Yes☑	Yes☑	Yes☑	No ☒	Yes☑
(Garg et al. 2020)	Yes☑	Yes☑	Yes☑	Yes☑	No ☒
(Orlando et al. 2022)	Yes☑	Yes☑	Yes☑	Yes☑	Yes☑
(Y. Wanget al.2019)	Yes☑	Yes☑	No ☒	No ☒	Yes☑
(Islam, Baig, 2019)	Yes☑	Yes☑	No ☒	No ☒	Yes☑
(Mood et al. 2020)	Yes☑	Yes☑	No ☒	No ☒	Yes☑
(Kamal ,2019)	No ☒	No ☒	No ☒	Yes☑	Yes☑
(Harishma et al. 2022)	No ☒	Yes☑	No ☒	Yes☑	Yes☑

Author, year	Data integrity	Data privacy	Data Confidentiality	Data Availability	Data Authentication
(Avancini et al. 2021)	No ☒	Yes☑	Yes☑	Yes☑	Yes☑
(Sun et al. 2021)	Yes☑	Yes☑	Yes☑	Yes☑	Yes☑
(Sureshkumar et al. 2020)	No ☒	Yes☑	No ☒	No ☒	No ☒
(Farokhi 2020)	Yes☑	No ☒	Yes☑	No ☒	Yes☑
(Zhang, Rong, 2020)	No ☒	Yes☑	Yes☑	Yes☑	Yes☑
(Shrestha et al. 2020)	No ☒	Yes☑	No ☒	No ☒	Yes☑
(Chakraborty et al. 2021)	Yes☑	Yes☑	No ☒	Yes☑	Yes☑

The results reveal that data privacy and authentication/identification were the most commonly addressed features, each appearing in 87% of the reviewed works. This trend underscores the increasing emphasis on protecting consumer data and verifying user identity in modern metering systems.

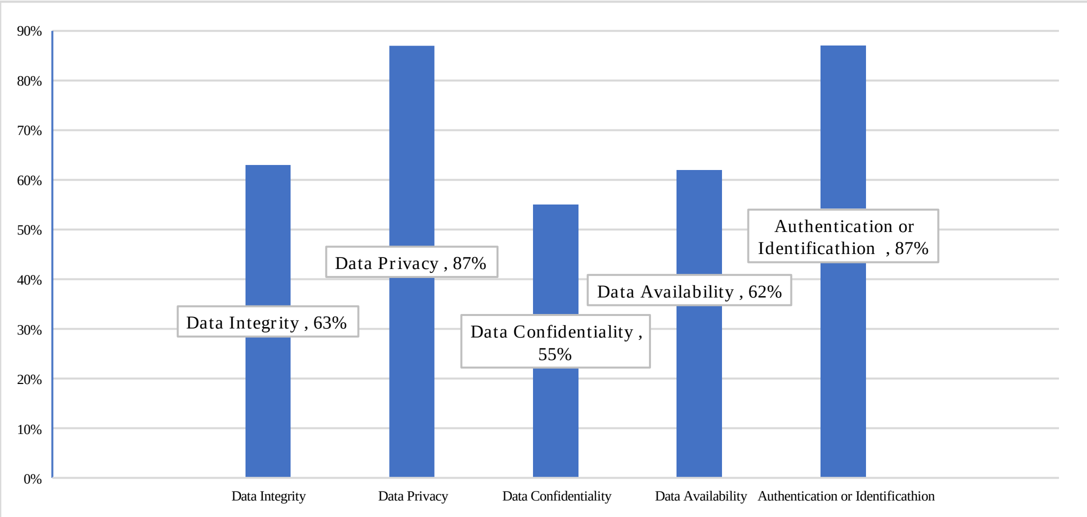

Figure 5. Security properties of smart meter systems.

Figure 5 shows that data privacy and authentication/identification are the most frequently addressed security concerns in smart metering literature, each covered in 87% of the reviewed studies. Data integrity 63% and data availability 62% receive moderate attention, while data confidentiality is less explored, appearing in only 55% of studies. These findings underscore the need for continued focus on data privacy and authentication as primary security priorities in future smart metering research and applications.

Table 5 discusses the most famous and most frequent types of attackson smart meter systems and networks, which have been studied in the literature and past studies: Denial of Service (DoS) attacks, Man-in-the-middle (MITM)attacks, False data injection attacks (FDIA), Data replay attacks, Impersonation attacks, and Malicious attacks, as shown in Figure 6.

Table 5: Contributions to the Type of Attack on Smart Meters.

Type of attacks	Issue	Proposed solution
Attacks on the network	Focus on communication technologies (e.g., ZigBee with IEEE 802.15.4), vulnerable to network interruptions, sniffing, black hole attacks, etc..	Strengthen the network's routing mechanism to counter wireless-based threats.
Attacks on physical hardware	Cyber-physical exploits can drain nodes' batteries, crash networks, and cause physical damage.	Adopt a four-dimensional approach, time, breadth, depth, and actor, to safeguard all data layers and curb physical tampering.
Attacks on data	Stored meter data may be targeted for manipulation (e.g., altering consumption records). Attackers range from criminals to corrupt officials	Implement a security index to detect manipulated data [61].

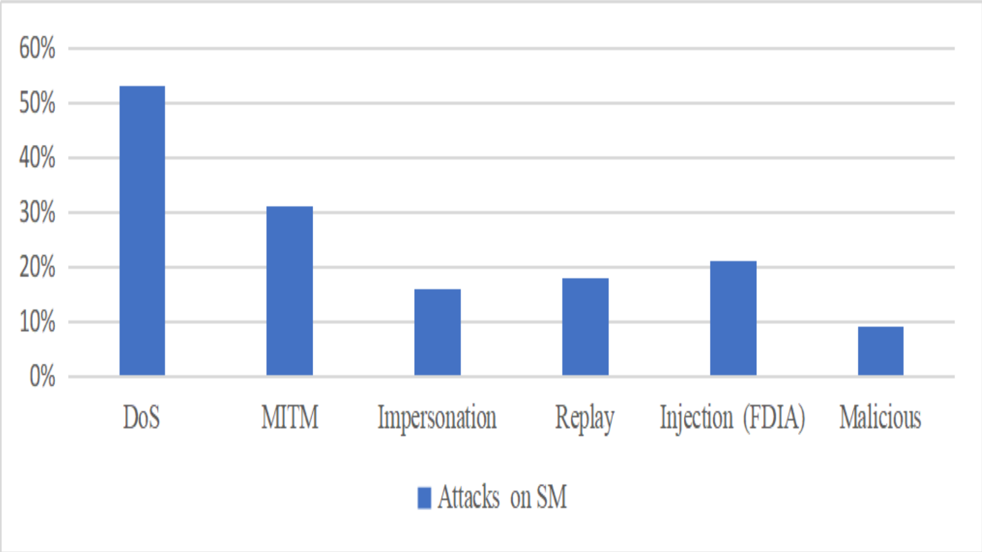

Figure 6. The most frequent types of attacks on smart meter systems.

Table 6 provides a comprehensive overview of the security properties and their associated vulnerabilities within the Smart Meter network. It examines five key security properties, data integrity, data privacy, data confidentiality, data availability, and authentication, against five common types of cyberattacks: Denial of Service (DoS), Man-in-the-Middle (MITM), Impersonation Attack, Replay Attack, and False Data Injection Attack (FDIA). The analysis indicates that data integrity is particularly vulnerable to MITM, replay, and FDIA attacks, while data privacy and data confidentiality are primarily compromised by MITM attacks. Data availability is notably affected by DoS attacks, reflecting its susceptibility to disruptions in service. Authentication is shown to be at risk from both impersonation and replay attacks. This classification highlights the specific threats posed by different attack vectors and emphasizes the need for targeted security mechanisms to protect the critical properties of smart metering systems.

Table 6. Security properties and vulnerability in the Smart Meter.

Attacks Properties	**(DoS)**	**(MITM)**	**Impersonation attack**	**Replay attack**	**(FDIA)**
Data integrity	☒ No	☑ Yes	☒ No	☑ Yes	☑ Yes
Data privacy	☒ No	☒ No	☒ No	☒ No	☒ No
Data Confidentiality	☒ No	☑ Yes	☒ No	☒ No	☒ No
Data Availability	☑ Yes	☒ No	☒ No	☒ No	☒ No
Authentication	☒ No	☒ No	☑ Yes	☑ Yes	☒ No

5. CONCLUSION

In conclusion, this paper highlights the growing importance of smart meters in modern energy systems, given their vital role in enabling real-time energy monitoring and communication in smart grids. While they offer numerous operational benefits to consumers, service providers, and governments, their use poses significant security and privacy risks that cannot be ignored. Our main thesis has emphasised that smart meter vulnerabilities fall into three main categories: data, network, and physical attacks, all of which pose threats to the integrity, availability, and confidentiality of the system. While some studies indicate the adequacy of current encryption methods and communication protocols, this review has highlighted their shortcomings in addressing real-time threats, user privacy concerns, and scalability in resource-constrained environments. Therefore, we call for continued innovation in lightweight cryptographic protocols, intrusion detection systems, and privacy-preserving models tailored to the unique constraints of smart meters.

Looking ahead, future research should prioritize the development of lightweight cryptographic protocols that maintain strong security guarantees while minimizing computational and energy overhead. This is especially critical for deployment in resource-constrained environments. Additionally, there is a pressing need for standardized frameworks that ensure interoperability across heterogeneous smart grid infrastructures. Real-world implementation also faces challenges such as key distribution at scale, firmware-level vulnerabilities, secure integration with legacy grid components, and the threat of insider attacks. Emerging directions include privacy-preserving machine learning for anomaly detection, blockchain-based decentralized authentication, and integration of physically unclonable functions (PUFs) for tamper-resistant hardware. Addressing these challenges will be essential for translating theoretical models into resilient, real-world smart metering systems.Future research should also focus on practical applications and standardisation to ensure robust and secure smart metering systems that are in line with the evolving smart grid landscape.

ACKNOWLEDGEMENTS

This work has been supported by UniversitiTeknikal Malaysia Melaka. The authors gratefully acknowledge the continuous support from the Center for Research and Innovation Management (CRIM) UTeM.

REFERENCES

[1] Khan, R., et al., "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," Proc. 10th Int. Conf. Frontiers of Information Technology, 2021.

[2] Gungor, V. C., et al., "Smart Grid Technologies: Communication Technologies and Standards," IEEE Transactions on Industrial Informatics, vol. 7, no. 4, pp. 529–539, 2021.

[3] C. Alcaraz and J. Lopez, "A security analysis for wireless sensor mesh networks in highly critical systems," IEEE Trans. Syst., Man, Cybern., vol. 42, no. 4, pp. 939–950, 2022.

[4] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," Comput. Netw., vol. 57, no. 5, pp. 1344–1371, 2023.

[5] Z. Tan et al., "Privacy-aware smart metering: Challenges and opportunities," IEEE Commun. Surveys Tuts., vol. 25, no. 1, pp. 108–134, 2023.

[6] Y. Zou et al., "A survey on wireless security: Technical challenges, recent advances, and future trends," Proc. IEEE, vol. 104, no. 9, pp. 1727–1765, 2022.

[7] N. Saxena and S. Grijalva, "Security and privacy issues in smart grid metering and control," IEEE Commun. Mag., vol. 50, no. 5, pp. 38–45, 2023.

[8] H. Mohsenian-Rad and A. Leon-Garcia, "Distributed Internet-based load altering attacks against smart power grids," IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 667–674, 2021.

[9] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in Proc. IEEE SmartGridComm, 2022.

[10] A. Molina-Markham et al., "Private memoirs of a smart meter," in Proc. ACM BuildSys, 2023.

[11] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," Sensors, vol. 12, no. 1, pp. 55–91, 2022.

[12] A. Elmaghraby and M. Losavio, "Cyber security challenges in smart grid systems," Comput. Netw., vol. 57, no. 5, pp. 1344–1371, 2023.

[13] W. Elmenreich and D. Egarter, "Design guidelines for smart appliances," in WISES 2012 – Proc. Workshop Intell. Solutions Embedded Syst., pp. 76–82, May 2012.

[14] F. Molazem, "Security and privacy of smart meters: A survey," Working Paper, pp. 1–11, 2012.

[15] J. Zheng, D. W. Gao, and L. Lin, "Smart meters in smart grid: An overview," in IEEE Green Technol. Conf., pp. 57–64, 2013.

[16] F. Benzi, N. Anglani, E. Bassi, and L. Frosini, "Electricity smart meters interfacing the households," IEEE Trans. Ind. Electron., vol. 58, no. 10, pp. 4487–4494, Oct. 2011.

[17] X. Fan and G. Gong, "Security challenges in smart-grid metering and control systems," Technol. Innov. Manag. Rev., vol. 3, no. 7, pp. 12–18, 2013.

[18] D. von Oheimb, "IT security architecture approaches for smart metering and smart grid," in Int. Workshop Smart Grid Security, Springer, pp. 1–25, 2012.

[19] S. Kaplantzis and Y. A. Şekercioğlu, "Security and smart metering," in Proc. Eur. Wireless Conf., pp. 1–8, 2012.

[20] Z. Fan et al., "Smart grid communications: Overview of research challenges, solutions, and standardization activities," IEEE Commun. Surveys Tuts., vol. 15, no. 1, pp. 21–38, 2013.

[21] C. A. F. Lima and J. R. P. Navas, "Smart metering and systems to support a conscious use of water and electricity," in Proc. 24th Int. Conf. ECOS, pp. 961–973, 2011.

[22] K. K. Karmakar, V. Varadharajan, and U. Tupakula, "Mitigating attacks in software defined networks," Clust. Comput., vol. 22, pp. 1143–1157, 2019.

[23] Y. Liu, Y. Wang, and H. Feng, "POAGuard: A defense mechanism against preemptive table overflow attack in software-defined networks," IEEE Access, vol. 11, pp. 123659–123676, 2023.

[24] P. Kumar et al., "Smart grid metering networks: A survey on security, privacy and open research issues," IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2886–2927, 2019.

[25] T. Zou et al., "Smart grids cyber-physical security: Parameter correction model against unbalanced false data injection attacks," Electr. Power Syst. Res., vol. 187, p. 106490, 2020.

[26] R. Chen, X. Li, H. Zhong, and M. Fei, "A novel online detection method of data injection attack against dynamic state estimation in smart grid," Neurocomputing, vol. 344, pp. 73–81, 2019.

[27] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," Comput. Netw., vol. 169, p. 107094, 2020.

[28] Y. Li et al., "Detection of false data injection attacks in smart grid: A secure federated deep learning approach," IEEE Trans. Smart Grid, vol. 13, no. 6, pp. 4862–4872, Nov. 2022.

[29] S. Kim et al., "A secure smart-metering protocol over power-line communication," IEEE Trans. Power Del., vol. 26, no. 4, pp. 2370–2379, Oct. 2011.

[30] M. N. Al-Mhiqani et al., "Cyber-security incidents: A review of cases in cyber-physical systems," Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 1, pp. 499–508, 2018.

[31] Y. Liu, Y. Wang, Y. Zhang, and J. Zhou, "Privacy-preserving multi-keyword searchable encryption for smart grid edge computing," IEEE Trans. Ind. Informat., vol. 16, no. 3, pp. 2134–2144, 2020.

[32] A. Souror, M. M. Hassan, A. Alamri, and M. S. Hossain, "Efficient and privacy-preserving searchable symmetric encryption for smart grid data," J. Supercomput., 2024. doi: 10.1007/s11227-024-06326-z.

[33] H. Shen, Y. Liu, Z. Xia, and M. Zhang, "An efficient aggregation scheme resisting on malicious data mining attacks for smart grid," Inf. Sci., vol. 526, pp. 289–300, 2020.

[34] S. Zhang, J. Rong, and B. Wang, "A privacy protection scheme of smart meter for decentralized smart home environment based on consortium blockchain," Int. J. Electr. Power Energy Syst., vol. 121, p. 106140, 2020.

[35] M. Shrestha et al., "A methodology for security classification applied to smart grid infrastructures," Int. J. Crit. Infrastruct. Prot., vol. 28, p. 100342, 2020.

[36] M. Erol-Kantarci and H. T. Mouftah, "Management of PHEV batteries in the smart grid: Towards a cyber-physical power infrastructure," in Proc. IWCMC, pp. 795–800, 2011.

[37] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in Proc. IEEE SmartGridComm, pp. 327–332, 2010.

[38] J. Liu et al., "Cyber security and privacy issues in smart grids," IEEE Commun. Surveys Tuts., vol. 14, no. 4, pp. 981–997, 2012.

[39] M. Attia et al., "An efficient intrusion detection system against cyber-physical attacks in the smart grid," Comput. Electr. Eng., vol. 68, pp. 499–512, 2018.

[40] O. Alshannaq et al., "Analysis of the lowest memory consumption through running different cryptography techniques for different types of images," J. Phys. Conf. Ser., vol. 2319, no. 1, p. 012027, 2022.

[41] Fedorchenko, I., Oliinyk, A., Stepanenko, A., Zaiko, T., Korniienko, S., Burtsev, N. "Development of a genetic algorithm for placing power supply sources in a distributed electric network". European Journal of Enterprise Technologies, issue 5/101, 6–16 (2019).

[42] B. Stelte and G. D. Rodosek, “Thwarting attacks on ZigBee - Removal of the KillerBee stinger,” 2013 9th International Conference on Network and Service Management, CNSM 2013 and its three collocated Workshops - ICQT 2013, SVM 2013 and SETM 2013. pp. 219–226, 2013, doi: 10.1109/CNSM.2013.6727840.

[43] T. M. Chen, J. C. Sanchez-Aarnoutse, and J. Buford, “Petri Net Modeling of Cyber-Physical Attacks on Smart Grid.” IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 741-749, Dec. 2011, doi 10.1109/TSG.2011.2160000, 2011.

[44] Vigo R, Yüksel E, Ramli CD. Smart grid security a smart meter-centric perspective. In2012 20th Telecommunications forum (TELFOR) 2012 Nov 20 (pp. 127-130). IEEE.

[45] Haq EU, Pei C, Zhang R, Jianjun H, Ahmad F. Electricity-theft detection for smart grid security using smart meter data: A deep-CNN based approach. Energy Reports. 2023 Mar 1;9:634-43.

[46] Win, Lae Lae, and Samet Tonyalı. "Security and privacy challenges, solutions, and open issues in smart metering: A review." 2021 6th International Conference on Computer Science and Engineering (UBMK). IEEE, 2021.

[47] T. Goodspeed, S. Bratus, R. Melgares, R. Speers, and S. W. Smith, “Tools for exploring the wireless attack surface in smart meters.” 2012 45th Hawaii International Conference on System Sciences, 2012.

[48] C. Bennett and S. B. Wicker, “Decreased time delay and security enhancement recommendations for AMI smart meter networks,” Innovative Smart Grid Technologies Conference, ISGT 2010. 2010, doi: 10.1109/ISGT.2010.5434780.

[49] Oliinyk, A., Fedorchenko, I., Stepanenko, A., Katschan, A., Fedorchenko, Y., Kharchenko, A., Goncharenko, D. "Development of genetic methods for predicting the incidence of volumes of emissions of pollutants in air". 2019 2nd International Workshop on Informatics and Data-Driven Medicine, IDDM, CEUR Workshop Proceedings, 2019, Vol.2488, pp. 340–353.

[50] P. Singh et al., "Blockchain and homomorphic encryption-based privacy-preserving data aggregation model in smart grid," Computers & Electrical Engineering, vol. 93, p. 107209, 2021.

[51] F. Naseri et al., "Cyber-physical cloud battery management systems: Review of security aspects," Batteries, vol. 9, no. 7, p. 382, 2023.

[52] L. Alabdulkarim and Z. Lukszo, “Information security assurance in critical infrastructures: Smart Metering case,” 2008 1st International Conference on Infrastructure Systems and Services: Building Networks for a Brighter Future, INFRA 2008. 2008, doi: 10.1109/INFRA.2008.5439670.

[53] Oliinyk, A., Fedorchenko, I., Stepanenko, .Rud M., Goncharenko, D. Implementation of evolutionary methods of solving the traveling salesman problem in a robotic warehouse // Lecture Notes on Data Engineering and Communications Technologies, 2021, 48, P. 263–292.

[54] W. Duo, M. Zhou, and A. Abusorrah, "A survey of cyber attacks on cyber physical systems: Recent advances and challenges," IEEE/CAA J. Autom. Sinica, vol. 9, no. 5, pp. 784–800, 2022.

[55] M. H. Yaghmaee, Q. A. Frugh, and M. Bahekmat, “Monitoring approach for detection compromise attacks in smart meter,” IET Conference Publications, vol. 2013, no. 615 CP. 2013, doi: 10.1049/cp.2013.0962.

[56] Govindarasu, Manimaran, Adam Hann, and Peter Sauer. "Cyber-physical systems security for smart grid." Power Systems Engineering Research Center, Feb (2012).

[57] Phang, F. A., Pusppanathan, J., Nawi, N. D., Zulkifli, N. A., Zulkapri, I., Che Harun, F. K., Wong, A. Y. K., Alsayaydeh, J. A., & Sek, T. K. (2021). Integrating Drone Technology in Service Learning for Engineering Students. International Journal of Emerging Technologies in Learning (iJET), 16(15), pp. 78–90.

[58] M. N. Al-Mhiqani, R. Ahmad, K. H. Abdulkareem, and N. S. Ali, “Investigation study of Cyber-Physical Systems: Characteristics, application domains, and security challenges,” ARPN J. Eng. Appl. Sci., vol. 12, no. 22, pp. 6557–6567, 2017.

[59] M. N. Al-Mhiqani, R. Ahmad, Z. Z. Abidin, N. S. Ali, and K. H. Abdulkareem, “Review of cyber attacks classifications and threats analysis in cyber-physical systems,” Int. J. Internet Technol. Secure. Trans., vol. 9, no. 3, pp. 282–298, 2019.

[60] Y. Niu, X. Tan, S. Chen, H. Wang, K. Yu, and Z. Bu, “A security privacy protection scheme for data collection of smart meters based on homomorphic encryption,” IEEE EuroCon 2013. pp. 1401–1405, 2013.

[61] A K M Zakir Hossain, Nurulhalim Bin Hassim, Jamil Abedalrahim Jamil Alsayaydeh, Mohammad Kamrul Hasan and Md. Rafiqul Islam, “A Tree-profile Shape Ultra Wide Band Antenna for Chipless RFID Tags” International Journal of Advanced Computer Science and Applications(IJACSA), 12(4), 2021.

[62] L. Jia, R. J. Thomas, and L. Tong, “MALICIOUS DATA ATTACK ON REAL-TIME ELECTRICITY MARKET.” 2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2011.

[63] K. Song, D. Seo, H. Park, H. Lee, and A. Perrig, “OMAP: One-way memory attestation protocol for smart meters,” Proc. - 9th IEEE Int. Symp. Parallel Distrib. Process. with Appl. Work. ISPAW 2011 - ICASE 2011, SGH 2011, GSDP 2011, pp. 111–118, 2011, doi: 10.1109/ISPAW.2011.37.

[64] Indha, W.A., Zamzam, N.S., Saptari, A., Alsayaydeh, J.A., Hassim, N.B. Development of Security Systems Using Motion Sensor Powered by RF Energy Harvesting, 2020. IEEE Student Conference on Research and Development, SCOReD 2020, 2020, pp. 254–258, 9250984.

[65] Alshannaq O, Baharon MR, Alsayaydeh JA, Hammouda MB, Hammouda K, Nawafleh MM, Rahman AI. Analysis of the Lowest Memory Consumption (Memory Usage) Through Running Different Cryptography Techniques for Different Types of Images. InJournal of Physics: Conference Series 2022 Aug 1 (Vol. 2319, No. 1, p. 012027). IOP Publishing.

[66] Fedorchenko, I., Oliinyk, A., Stepanenko, Zaiko, T., Korniienko S., Kharchenko, A. Construction of a genetic method to forecast the population health indicators based on neural network models // Eastern-European Journal of Enterprise Technologies, 2020, 1 (4-103), P. 52–63. DOI: 10.15587/1729-4061.2020.197319.

[67] Alshannaq O, Alsayaydeh JA, Hammouda MB, Ali MF, Alkhashaab MA, Zainon M, Jaya AS. Particle swarm optimization algorithm to enhance the roughness of thin film in TiN coatings. ARPN Journal of Engineering and Applied Sciences. 2022;17(22):186-93.

[68] I. Fedorchenko, A. Oliinyk, Jamil Abedalrahim Jamil Alsayaydeh, A. Kharchenko, A. Stepanenko and V. Shkarupylo. MODIFIED GENETIC ALGORITHM TO DETERMINE THE LOCATION OF THE DISTRIBUTION POWER SUPPLY NETWORKS IN THE CITY. ARPN Journal of Engineering and Applied Sciences, 2020, 15(23), pp. 2850–2867.

[69] Khattak, A.M., Khanji, S.I. and Khan, W.A., 2019. Smart meter security: Vulnerabilities, threat impacts, and countermeasures. In Proceedings of the 13th International Conference on Ubiquitous Information Management and Communication (IMCOM) 2019 13 (pp. 554-562). Springer International Publishing.

[70] Kumar, P., Lin, Y., Bai, G., Paverd, A., Dong, J.S. and Martin, A., 2019. Smart grid metering networks: A survey on security, privacy and open research issues. IEEE Communications Surveys & Tutorials, 21(3), pp.2886-2927.

[71] Abdalzaher, Mohamed S., Mostafa M. Fouda, and Mohamed I. Ibrahem. "Data privacy preservation and security in smart metering systems." Energies 15, no. 19 (2022): 7419..

[72] Garg, Sahil, Kuljeet Kaur, Georges Kaddoum, Joel JPC Rodrigues, and Mohsen Guizani. "Secure and lightweight authentication scheme for smart metering infrastructure in smart grid." IEEE Transactions on Industrial Informatics 16, no. 5 (2019): 3548-3557.

[73] Orlando M, Estebsari A, Pons E, Pau M, Quer S, Poncino M, Bottaccioli L, Patti E. A smart meter infrastructure for smart grid IoT applications. IEEE Internet of Things Journal. 2021 Dec 22;9(14):12529-41.

[74] Wang, Yi, Qixin Chen, Tao Hong, and Chongqing Kang. "Review of smart meter data analytics: Applications, methodologies, and challenges." IEEE Transactions on Smart Grid 10, no. 3 (2018): 3125-3148.

[75] Islam, Shama Naz, Zubair Baig, and Sherali Zeadally. "Physical layer security for the smart grid: Vulnerabilities, threats, and countermeasures." IEEE Transactions on Industrial Informatics 15, no. 12 (2019): 6522-6530..

[76] Abbasinezhad-Mood, Dariush, Arezou Ostad-Sharif, Morteza Nikooghadam, and Sayyed Majid Mazinani. "A secure and efficient key establishment scheme for communications of smart meters and service providers in smart grid." IEEE Transactions on Industrial Informatics 16, no. 3 (2019): 1495-1502.

[77] Kamal, Mohsin, and Muhammad Tariq. "Light-weight security and blockchain-based provenance for advanced metering infrastructure." IEEE Access 7 (2019): 87345-87356

[78] Harishma, Boyapally, Paulson Mathew, Sikhar Patranabis, Urbi Chatterjee, Umang Agarwal, Manu Maheshwari, Soumyajit Dey, and Debdeep Mukhopadhyay. "Safe is the new smart: PUF-based authentication for load modification-resistant smart meters." IEEE Transactions on Dependable and Secure Computing 19, no. 1 (2020): 663-680.

[79] Avancini, Danielly B., Joel JPC Rodrigues, Ricardo AL Rabêlo, Ashok Kumar Das, Sergey Kozlov, and Petar Solic. "A new IoT-based smart energy meter for smart grids." International Journal of Energy Research 45, no. 1 (2021): 189-202.

[80] Sun, Chih-Che, D. Jonathan Sebastian Cardenas, Adam Hahn, and Chen-Ching Liu. "Intrusion detection for cybersecurity of smart meters." IEEE Transactions on Smart Grid 12, no. 1 (2020): 612-622.

[81] Sureshkumar, Venkatasamy, S. Anandhi, Ruhul Amin, N. Selvarajan, and R. Madhumathi. "Design of robust mutual authentication and key establishment security protocol for cloud-enabled smart grid communication." IEEE Systems Journal 15, no. 3 (2020): 3565-3572.

[82] Farokhi, Farhad. "Review of results on smart-meter privacy by data manipulation, demand shaping, and load scheduling." IET Smart Grid 3, no. 5 (2020): 605-613..

[83] Zhang, Shaomin, Jieqi Rong, and Baoyi Wang. "A privacy protection scheme of smart meter for decentralized smart home environment based on consortium blockchain." International Journal of Electrical Power & Energy Systems 121 (2020): 106140.

[84] Shrestha, Manish, Christian Johansen, Josef Noll, and Davide Roverso. "A methodology for security classification applied to smart grid infrastructures." International Journal of Critical Infrastructure Protection 28 (2020): 100342.

[85] Chakraborty, Soham, Sarasij Das, Tarlochan Sidhu, and A. K. Siva. "Smart meters for enhancing protection and monitoring functions in emerging distribution systems." International Journal of Electrical Power & Energy Systems 127 (2021): 106626.

[86] Zhang, Xun, et al. "A Privacy-Preserving Searchable Encryption Scheme for Data Protection in Smart Grid." International Artificial Intelligence Conference. Singapore: Springer Nature Singapore, 2023.

[87] K. Fan et al., "MSIAP: A dynamic searchable encryption for privacy-protection on smart grid with cloud-edge-end," IEEE Trans. Cloud Comput., vol. 11, no. 2, pp. 1170–1181, 2021.

AUTHORS

Osama Alshannaq received his Bachelor's degree in Computer Science at the Faculty of Computer Science in Jordan at Jadara University in 2016. He did his Master's degree in Computer Science (Internetworking technology) at the Faculty of Information and Communication Technology, UniversitiTeknikal Malaysia Melaka (UTeM) in 2019. He is a Lecturer at the Department of information technology and security, Toledo College, Jordan. He started his career as a lecturer at this college in May 2021. He has experience in teaching Computer Science and cryptography. His research interests are in the areas of Computer Networks, Computer Science, Network Security, Data Security, Data Privacy and Integrity, and Cryptography. Currently, he is doing his Ph.D. in the network security department at UniversitiTeknikal Malaysia Melaka (UTeM). He can be contacted at email: osamaalshannaq99@gmail.com.

Mohd Rizuan Baharon received the PhD degree in Computer Science from Liverpool John Moores University, Liverpool, United Kingdom, in 2017. He completed his master degree in Mathematics in 2006 and his undergraduate studies in 2004 at UniversitiTeknologi Malaysia, Malaysia. Currently, he is a Senior Lecturer at the Department of Computer System and Communication, Faculty of Information and Communication Technology, UniversitiTeknikal Malaysia Melaka, Malaysia. He started his career as a lecturer at this university since June 2006. He has vast experience in teaching Computer Science, Cryptography and Mathematics subjects. His research interests are mainly in the area of Mobile Network Security, Cloud Computing Security, Data Privacy and Integrity, Mobile Users Accountability and Cryptography. He is a lifetime member of Mathematical and Sciences Association Malaysia (PERSAMA, Malaysia). He has produced a number of journal and conference papers at national and international levels. He can be contacted at email: mohd.rizuan@utem.edu.my

Shekh Faisal Abdul Latip is currently working at the Faculty of Information and Communication Technology, UniversitiTeknikal Malaysia Melaka (UTeM). He received his PhD in 2012 from the University of Wollongong, Australia, in the field of Cryptography. Prior to his PhD studies, he obtained an M.Sc in Information Security from Royal Holloway, University of London, in 2003. He earned both a B.Sc (Hons) in Computer Science (2000) and a Diploma in Electronic Engineering (1994) from UniversitiTeknologi Malaysia (UTM). His main research interest focuses on symmetric-key cryptography, specifically the design and cryptanalysis of block ciphers, stream ciphers, hash functions, and MACs. He is currently a member of a focus group and one of the evaluation panel experts for the MySEAL project, which aims to recommend a list of trusted cryptographic algorithms for use by public and private sectors in Malaysia. To promote new ideas and activities in cryptology-related areas in Malaysia, he joined and became a member of the executive committee of the Malaysian Society for Cryptology Research (MSCR).

Hairol Nizam Mohd Shah received the Diploma (Electric-Electronic) from UniversitiTeknologi Malaysia in 2000, B.Eng. (Electric-Electronic) from Universiti Malaysia Sabah in 2004. He received the M. Eng. (Mechatronics) and PhD (Mechatronics) at UniversitiTeknikal Malaysia Melaka in 2008 and 2018. Currently he is a senior lecturer at the UniversitiTeknikal Malaysia Melaka, Ayer Keroh Melaka. His primary interests related to vision systems, robotics and computer-integrated and image processing.

Dr Áine MacDermott is a Senior Lecturer in the School of Computer Science and Mathematics at Liverpool John Moores University (LJMU) in the UK. She obtained her PhD in Network Security from LJMU in 2017, and a BSc (Hons) in Computer Forensics in 2011. Áine is a member of Research Centre for Critical Infrastructure Computer Technology and Protection (PROTECT) at LJMU, with research interests including the Internet of Things, collaborative intrusion detection in interconnected networks, digital forensics, and machine learning.