Bulletin of Electrical Engineering and Informatics
Vol. 10, No. 1, February 2021, pp. 412~418
ISSN: 2302-9285, DOI: 10.11591/eei.v10i1.2024

Data falsification attacks in advanced metering infrastructure

Hasventhran Baskaran[1], Abbas M. Al-Ghaili[2], Zul-Azri Ibrahim[3], Fiza Abdul Rahim[4], Saravanan Muthaiyah[5], Hairoladenan Kasim[6]
[1,6] College of Computing & Informatics (CCI), UNITEN, Malaysia
[2,3,4] Institute of Informatics and Computing in Energy (IICE), Universiti Tenaga Nasional (UNITEN), Malaysia
[5] Department of Computer Science, Faculty of Computer Science & Information Technology, University Putra Malaysia**,** Malaysia

Article Info

Article history:

Received Dec 4, 2019
Revised Mar 31, 2020
Accepted May 4, 2020

Keywords:

Additive
Data falsification
Deductive
Smart meter
Use case

ABSTRACT

Smart grids are the cutting-edge electric power systems that make use of the latest digital communication technologies to supply end-user electricity, but with more effective control and can completely fill end user supply and demand. Advanced metering infrastructure (AMI), the backbone of smart grids, can be used to provide a range of power applications and services based on AMI data. The increased deployment of smart meters and AMI have attracted attackers to exploit smart grid vulnerabilities and try to take advantage of the AMI and smart meter's weakness. One of the possible major attacks in the AMI environment is false data injection attack (FDIA). FDIA will try to manipulate the user's electric consumption by falsified the data supplied by the smart meter value in a smart grid system using additive and deductive attack methods to cause loss to both customers and utility providers. This paper will explore two possible attacks, the additive and deductive data falsification attack and illustrate the taxonomy of attack behaviors that results in additive and deductive attacks. This paper contributes to real smart meter datasets in order to come up with a financial impact to both energy provider and end-user.

Corresponding Author:

Abbas M. Al-Ghaili,
Institute of Informatics and Computing in Energy (IICE),
Universiti Tenaga Nasional (UNITEN),
43000 Kajang, Selangor, Malaysia.
Email: abbas@uniten.edu.my

1. INTRODUCTION

Data falsification was a term well-known for research or scientific misconduct until the dawn of the big data era. As commercial sectors are venturing into big data to improve their competitiveness and profits, data falsification issues creep into these sectors too. Most large-scale industries demand an accurate and precise data received from their database and customers to keep track of the user preferences and forecast the company's economic growth. By having a predictive or prescriptive analysis of their big data, they tend to get clearer information to strategize their next move. These datasets also can be used to monitor the product they produce is defect-free. Many data falsification cases happened around the world and it can cause serious consequences. For example, in 2017, a Japanese company, Kobe Steel, a joint venture of Mitsubishi Materials has admitted of their data falsification for aluminum and copper products, which were supplied to 600 over companies and used in aircraft, cars, rocket and defense equipment [1]. The prospect of having a substandard material on the mentioned mode of transport and defense equipment due to data falsification is quite worrying. As these misconducts are spreading across industrial sectors,

it can cause large scale damage to the consumers and the manufacturers. The energy sector is one of the most important sectors that run the world. It is now being revolutionized by the introduction of smart grids in the United States of America, the United Kingdom, China, India, and other European countries. A smart meter is one of the important components in the smart grid architecture. It is a device that digitally sends meter reading to the utility provider for more accurate bills. The device is used to send electricity usage from a house back to the utility service provider remotely at a frequent rate [2]. Due to the smart meter's continuous collection and transmission of energy consumption data, users have a concern about the privacy and security risks of their data being transmitted [3]. Performance of such a task is usually monitored in order to keep the data secure and true [4].

Any architecture that needs to transmit data across many nodes or levels is vulnerable to cyber-attacks without adequate security measures. Smart meters are connected on wireless networks can be attacked easily if the gateway board is compromised by opening a network port to inject malicious code on the memory of the device [5]. Compared to traditional meters, smart meters have access to reach the utility providers remotely with the access of the Internet and causes the smart meter data to fall victim to cyber-attacks [6-9]. Smart meters can provide highly accurate measurements with automatic data reading and integration to a wider area [10-14]. Hence, smart meter data hold commercial value and can identify someone's activities by analyzing the energy consumption pattern if it is exploited. A data falsification attack on these smart meters can negatively affect both customers and utility providers. Bhattacharjee *et al.* [5] proposed four taxonomy of data falsification attacks in AMI micro-grids as additive, deductive, camouflage and conflict. In this paper, we will discuss further on the taxonomy of additive and deductive attacks that can inflict serious damage on smart meters. These attacks enable the attackers to sabotage the user and also to cause loss of revenue for the utility provider. The attack also can result in creating fake internal user data or the time synchronization function. The main objective of the additive attack is to increase the actual value of energy consumption in smart reading to increase the total bill consumption, while in the deductive attack, the false data injection in the smart meter reading reduces the total bill report to the energy utility provider. These attacks can be conducted by false data injection which is a rapidly growing problem in AMI [15].

2. ATTACKS ON SMART GRID

Smart grids are vulnerable to attacks in both physical and logical layers [16]. Theft, sabotage, and vandalism can occur at the physical layer whereas the data confidentiality can be compromised at the logical layer. This applies to the smart meter which is a component of a smart grid. Smart meters might suffer the most compared to other components of the smart grid due to their dependency on the wireless network. Smart meter works on few types of networks, wide area network (WAN), business area network (BAN), industrial area network (IAN) and home area network (HAN) [17]**.** Smart devices installed in a house, company building or industrial area are connected to the smart meter through HAN, BAN, and IAN respectively, whereas the WAN establishes connections between smart meters and the service providers. There is a real concern over the potential of a compromised smart meter. Cyber-attacks can occur at both WAN and HAN as smart meters are usually endpoints of smart grid [17] and the utility providers have limited control over it from a remote distance.

By infiltrating the smart meter through these wireless networks, the device can be compromised through additive or deductive attacks to cause loss or other negative effects to both users and utility providers [8]. These attacks can damage the confidentiality and integrity of the data being transmitted from smart meter. On a larger scale, it might damage the utility providers by conducting distributed denial-of-service (DDoS) attack [18, 19]. The data usage shown in Figure 1 shows the reading of electricity usage of a London based smart meter and it is based on half-hourly usage per block residents. London's average rate for electric is 14.5 pence [20]. The total electricity consumption for the smart meter and the month mentioned in Figure 1 is 414.62 kW/h. Hence, the electricity bill for that month should be 60.12 pound sterling.

2.1. Additive attack

Additive attacks in smart grid are the types of attacks that can add an arbitrary fixed value in an arithmetic circuit. This attack can modify the information sent from the smart meter by adding the amount of electric consumption from a user's smart meter which can affect the user's trust in a particular utility provider. In developing countries like India, metering and billing are not well-structured [21]. Hence, the attackers have a better chance of manipulating customers' electric bills. Figure 2 shows the use case of an attacker performing additive attacks to the smart meter consumption database. Different motivations will require different techniques to inject the falsified data in smart meter consumption. The output of this additive attack will be the dependent variable (Y_A) which results in a new meter reading with false power consumption data.

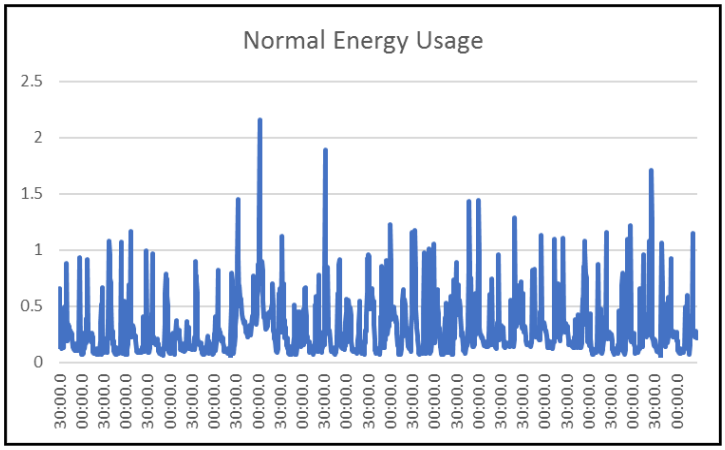

Figure 1. Readings of normal usage of a smart meter

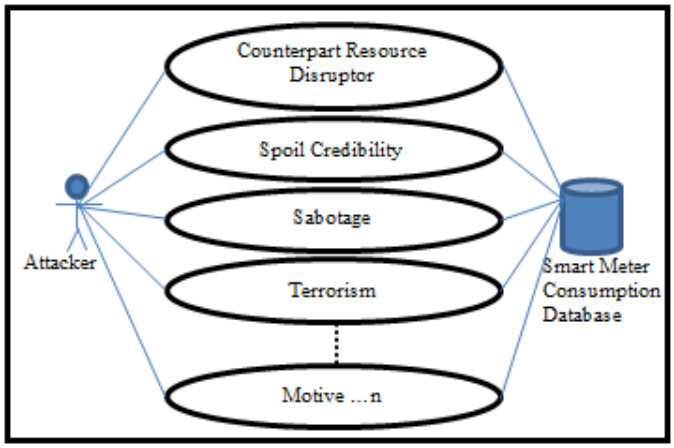

Figure 2. Use case for additive attack motivation

All the motivation for the attacker to do the additive attack will be the Independent Variable (X) and the average data consumption in the smart meter that affected by the additive attack will be represented as A_1, A_2, A_3…… A_n. As it can manipulate the smart meter reading to generate the output of the additive attack. The equation in (1) represents the additive attack in the smart meter:

$$Y_A = X_{A1} + X_{A2} + X_{A3} \ldots\ldots + X_{An} \quad (1)$$

From this equation, we generate the synthetic data from the original smart meter reading in Figure 1. The result of the attack is discussed and the result from Figure 3 can give different reading patterns from the original data and also affected the billing consumption for the end-user. Figure 3 shows the difference between a London based smart meter reading of normal usage and the reading of usage after randomly adding energy consumption rate. The readings of electrical usage are unusual after the tampering and it is evident on the graph as there are some gaps between the normal usage's line and added usage's line on the graph.

We have conducted this test from the original smart meter reading in Figure 1 where for every 24 data entries in the dataset, the data was changed manually by following the condition below. The variable for electricity usage is denoted by d. The consequent 24 data reading entries were unchanged and the cycle repeated for a total of 1440 meter reading. For example, the condition for additive attack will be applied for data entries, d_1 to d_{24} and the data entries starting from d_{25} to d_{48} will be unchanged. Then, the cycle continues back from d_{49} to d_{72} and the process goes on until the last data. The equation in (2) was used to manually change the meter reading: *IF* $(d_n<0.2)$

$$THEN\ d_n = d_n + 0.2 \quad (2)$$

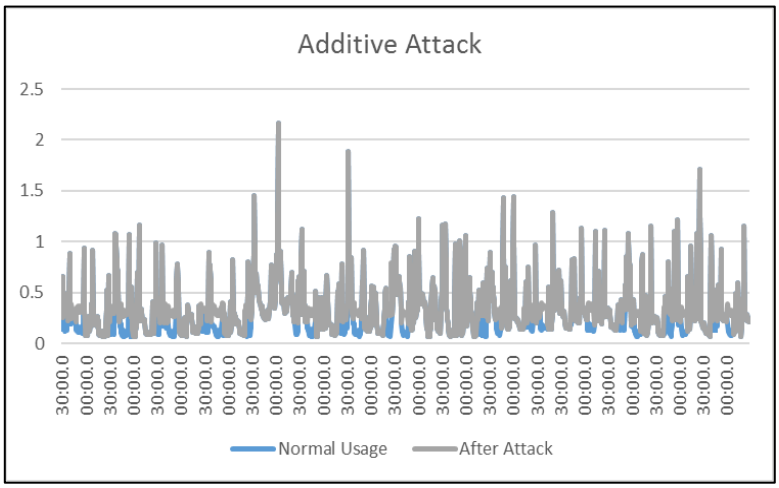

Figure 3. Readings of normal usage and updated usage after additive attack

Due to this additive attack, the customers might get an irrelevant bill for their low consumption. For example, despite the customers not being at their home for a certain number of weeks, the electric bill issued to him might be calculated on heavy usage of electricity for the whole month. In the sample case above, electrical usage is 482.82 kW/h. Hence, the electricity bill for that month is 70.01 pound sterling. This amount is 10 pound sterling higher than the actual bill which is 60.12 pound sterling. An attacker also could change the behavior or functions of smart meter by injecting malicious codes into it. The extra lines of malicious code might act as a transmitter of the smart meter data to the attacker or even worse as a carrier of a different set of malware to collapse the smart grid network [22]. However, the actual purposes for attackers to perform additive attack can be diverse. A rival could perform this attack for personal benefits, to disrupt the resource of counterpart or even to spoil the credibility of the victim, which in this case the utility providers. Utility providers' main concern in AMI is to avoid the manipulation of smart meters caused by the injection of false power consumption data into their network [23]. However, by using the smart meter as a vector for entry in the smart grid infrastructure, attackers could disrupt millions of households. Insider attacks where the unhappy employees sabotage the system to express their hatred can be equally damaging to the utility provider. For example, in 2015, a false data injection attack caused three Ukrainian regional power distribution companies to be compromised and affected 225,000 customers approximately due to a power outage [24, 25].

2.2. Deductive attack

As much as smart meters are being developed to be more user-friendly and concerned in protecting data privacy by granting more user control, it also might result in the potential occurrence of deductive attacks. Deductive attacks are the type of attack which modifies a certain set of data by reducing the value being sent over from a device. A tech-savvy user with good knowledge in systems and networking could perform this attack to benefit him/her illegally. The bills could be contrarily low to the actual energy consumption of the user. This will cause a loss in revenue for utility providers as they will not get the money for the actual usage. Attacking groups could perform this deductive attack to a devastating effect by using a logic bomb which is a preprogrammed malicious code that is activated when it reaches the time that was set by the attacker. This code can be injected into the Smart Meter to cut down a nation's crucial infrastructure (electricity) or to retrieve crucial information by breaking the security barriers.

Figure 4 shows the use case for the deductive attack. Like additive attack, in the deductive attack, the motivation will be different but it will generate different outputs from the original smart meter consumption which will represent as Y_D. X will be the motivation and technique to do FDIA to tamper the smart meter reading and D_n will be the average smart data in the smart grid environment. The equation in (3) represents the deductive attack in the smart grid environment:

$$Y_D = X_{D1} + X_{D2} + X_{D3} \ldots\ldots + X_{Dn} \quad (3)$$

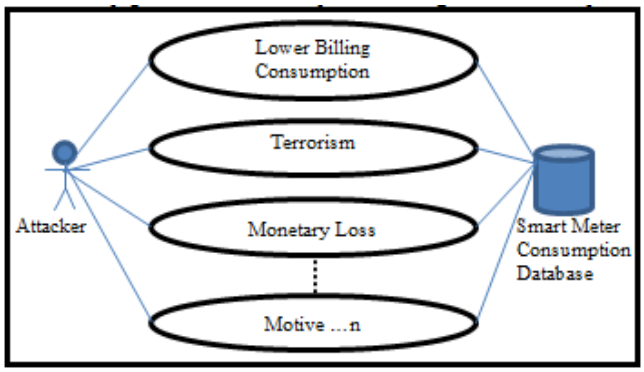

Figure 4. Use case for deductive attack motivation

We have generated the synthetic data for the deductive attack from the original smart meter reading in Figure 1 which demonstrates how this attack could produce different reading patterns as shown in Figure 5. The figure shows the difference between the same smart meter reading of normal usage and the reading of usage after randomly reducing the energy consumption rate. The readings of electrical usage are irregular after the tampering and it is visible on the graph as there are some discrepancies between the line of normal usage and the line on the graph of deducted use. The equation in (4) was used to manually change the meter reading: *IF* $(d_n>0.2)$

THEN $d_n=d_n - 0.2$ (4)

Due to this deductive attack, the attacker might get a lower electricity bill compared to the actual usage. In the sample case above, the electrical usage was 381.84 kW/h. Hence, the electricity bill for that month is 55.37 pound sterling. This amount is 4.75 pound sterling lower than the actual bill which was 60.12 pound sterling. The example above shows how deductive attacks can cause large scale monetary losses as much as distributed denial of service (DDoS) attacks if this attack involves a large number of smart meters. In DDoS, the attack will cut off the service availability and there will be no charge of bill due to the unavailability of electricity, whereas deductive attacks work on ongoing electricity supply and prevent the utility providers to get the correct amount that should have been charged for the actual usage. When this deductive attack occurs on a large scale like the state or national level, the monetary loss could be devastating to utility providers.

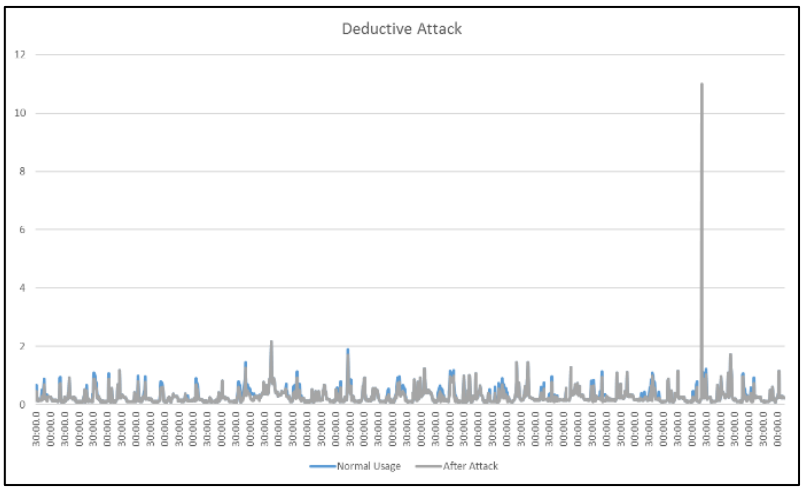

Figure 5. Readings of normal usage and updated usage after deductive attack

3. DISCUSSION

From the previous review, it is known that an additive attack is an attack that happens when an attacker tampered the user's electricity consumption by adding the end-user original smart meter reading

while the deductive attack will reduce it. Both attacks have different purposes and motivations for the attacker to execute it in the smart meter environment. Figure 3 and Figure 5 have shown that how the falsified data can produce a different pattern in the end-user smart meter reading consumption graph. It is important to understand how these attacks can change the original pattern of smart meter reading if a predictive analysis of these attacks needs to be conducted.

To produce an analytics model that can predict the additive attack in smart meter consumption, the verification of dependent and independent variables involved in addictive and deductive attacks must be done. Two use cases were developed from the review to further understand these attacks and from the use case, an equation will be generated to assist in generating the falsified data when predicting the additive and deductive attacks in smart meter consumption. The objective of the predictive analysis is to support the assumption that when there is an attack happen in smart meter consumption it will change the original pattern of the end-user smart meter reading or to answers the main analytics question on is there any statistically significantly different in smart meter consumption when additive or deductive attack tampering the smart meter data reading.

For this case, the output or the result of the predictive analysis data will be the Dependent Variable (DV), as the output can be either an additive or deductive attack that occurred in the smart meter reading. The motivation and techniques to initiate the additive or deductive attack will be the Independent Variable (IV) as this variable can affect the average reading of the meter reading which will determine whether the original data of the smart meter has tampered or not. The equation in (5) is generated and will further explain using additive (A) and deductive (D) use case:

$$\begin{aligned} DV &= IV\ (A1\ +\ A2\ +\ A3\ \ldots\ldots\ldots\ +\ An) \\ &\quad Or \\ DDV &= IV\ (D1\ +\ D2\ +\ D3\ \ldots\ldots\ldots\ +\ Dn) \end{aligned} \tag{5}$$

4. POTENTIAL SOLUTIONS

While smart meters making its way into millions of households in first-world countries, it is still a work in progress globally. There is a lack of sufficient smart meter data protection as the smart meter's has become a victim to data falsification due to its existence vulnerabilities makes a strong case for the need of proper security measures. Researchers around the world had tried to solve this problem with their proposed solutions. End-to-end encryption between a customer and utility provider can be a good solution. Both parties can share a key to encrypt and decrypt the data. Without the shared key, outsiders cannot have access to the data. A strong encryption algorithm will be efficient enough to halt the malicious acts of a hacker. Authors in [26] have proposed an encryption algorithm named as Spritz. It is claimed that this algorithm can be implemented on a microchip and installed in a smart meter. Spritz replaces RC4 by eliminating the major weaknesses of RC4. It is stream cipher that encrypts data byte by byte. Spritz takes 3 times longer than RC4 to break by brute force. Authors in [27] have proposed a scheme where users can combine a certified tariff policy with smart meter readings to produce their electricity bill.

The bill will be sent to the utility provider with zero-knowledge proof which shows that the calculation is correct. This ensures the transmission of data without being leaked and the prevention of data falsification eventhough a time-based attacking schemes are attempting to [28]. Authors in [29] have proposed a blockchain-based smart home architecture. A local private blockchain is created to keep track of transactions and enforce users' access control policy for incoming and outgoing transactions. A local miner authenticates and authorizes all the incoming and outgoing transactions. Since blockchain is immutable, any data going through IoT devices connected to the blockchain network will be tamper-proof. Since the smart meter is an IoT device, this architecture will fit the requirements to be tamper-proof. The solutions to address the data falsification issue is still a work in progress due to the focus being directed more in preserving smart meter's privacy issues. Current solutions can be improvised to tackle both privacy and data falsification issues.

5. CONCLUSION AND FUTURE WORKS

In this paper, we presented a taxonomy of additive and deductive attack in AMI, as may be conducted by attackers. We illustrated both techniques and explained how this attack could give a financial impact to the end-user and utility provider. We have shown that the method is generic and can be used across various real smart meter datasets. For future works, we will propose a method for classifying the smart meters that have been injected with false power consumption that will be driven by the falsified datasets from this paper. The wider impact of data falsification techniques and security properties also will be outlined.

ACKNOWLEDGMENTS

The authors would like to thank the Ministry of Higher Education Malaysia (MoHE) and Universiti Tenaga Nasional (UNITEN) for funding this study under the Fundamental Research Grant Scheme (FRGS) of Grant No. FRGS/1/2017/ICT03/UNITEN/03/1.

REFERENCES

[1] L. Li, H. Yang, Y. Xia, and H. Yang, "Event-based distributed state estimation for linear systems under unknown input and false data injection attack," *Signal Processing*, vol. 170, p. 107423, May 2020.
[2] F. Halim, S. Yussof, and M. E. Rusli, "Cyber security issues in smart meter and their solutions," *International Journal of Computer Science and Network Security*, vol. 18, no. 3, pp. 99-109, 2018.
[3] M. Wigan, "User Issues for Smart Meter Technology," in *IEEE Technology and Society Magazine*, vol. 33, no. 1, pp. 49-53, 2014.
[4] K. Khalid, A. Mohamed, R. Mohamed, and H. Shareef, "Performance Comparison of Artificial Intelligence Techniques for Non-intrusive Electrical Load Monitoring," *Bulletin of Electrical Engineering and Informatics*, vol. 7, no. 2, pp. 143-152, 2018.
[5] S. Bhattacharjee, A. Thakur, S. Silvestri, and S. K. Das, "Statistical Security Incident Forensics against Data Falsification in Smart Grid Advanced Metering Infrastructure," *Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy*, USA, pp. 35-45, 2017.
[6] P. Van Aubel and E. Poll, "Smart metering in the Netherlands: What, how, and why," *International Journal of Electrical Power & Energy Systems*, vol. 109, pp. 719-725, July 2019.
[7] S. -Z. Liu, Y. -F. Li, and Z. Yang, "Modelling of Cyber-Attacks and Defenses in Local Metering System," *Energy Procedia*, vol. 145, pp. 421-426, July 2018.
[8] W. Mesbah, "Securing Smart Electricity Meters Against Customer Attacks," in *IEEE Transactions on Smart Grid*, vol. 9, no. 1, pp. 101-110, Jan 2018.
[9] Y. Wu, et al., "False Load Attack to Smart Meters by Synchronously Switching Power Circuits," *in IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2641-2649, May 2019.
[10] F. D. Garcia, F. P. Marafão, W. A. de Souza and L. C. Pereira da Silva, "Power Metering: History and Future Trends," *2017 Ninth Annual IEEE Green Technologies Conference (GreenTech)*, Denver, CO, pp. 26-33, 2017.
[11] S. Wang, H. Chen, L. Wu, and J. Wang, "A novel smart meter data compression method via stacked convolutional sparse auto-encoder," *International Journal of Electrical Power & Energy Systems*, vol. 118, p. 105761, June 2020.
[12] D. B. Avancini, J. J. P. C. Rodrigues, S. G. B. Martins, R. A. L. Rabêlo, J. Al-Muhtadi, and P. Solic, "Energy meters evolution in smart grids: A review," *Journal of Cleaner Production*, vol. 217, pp. 702-715, April 2019.
[13] T. Sirojan, S. Lu, B. T. Phung and E. Ambikairajah, "Embedded Edge Computing for Real-time Smart Meter Data Analytics," *International Conference on Smart Energy Systems and Technologies (SEST)*, Porto, Portugal, pp. 1-5, 2019.
[14] A. M. Al-Ghaili, et al., "A Dynamical Behavior Measurement Algorithm for Smart Meter Data: An Analytical Study," *IEEE Conference on Application, Information and Network Security*, Pulau Pinang, Malaysia, pp. 66-70, 2019.
[15] Z. Guan, N. Sun, Y. Xu, and T. Yang, "A comprehensive survey of false data injection in smart grid," *International Journal of Wireless and Mobile Computing*, vol. 8, no. 1, pp. 27-33, 2015.
[16] C. Lopez, A. Sargolzaei, H. Santana, and C. Huerta, "Smart Grid cyber security: An overview of threats and countermeasures," *Journal of Energy and Power Engineering*, vol. 9, no. 7, pp. 632-647, 2015.
[17] G. R. Barai, S. Krishnan and B. Venkatesh, "Smart metering and functionalities of smart meters in smart grid - a review," *2015 IEEE Electrical Power and Energy Conference (EPEC)*, London, ON, pp. 138-145, 2015.
[18] P. Yi, T. Zhu, Q. Zhang, Y. Wu and J. Li, "A denial of service attack in advanced metering infrastructure network," *2014 IEEE International Conference on Communications (ICC)*, Sydney, NSW, pp. 1029-1034, 2014.
[19] R. C. Diovu and J. T. Agee, "A cloud-based openflow firewall for mitigation against DDoS attacks in smart grid AMI networks," *2017 IEEE PES PowerAfrica*, Accra, pp. 28-33, 2017.
[20] Jean-Michel D. "Smart meters in London - Smart meter data from London area." *kaggle*, 2019
[21] E. Yurday. "Average Unit Cost of Electricity in the UK 2020." *NimbleFin*s, 2019.
[22] G. Liang, J. Zhao, F. Luo, S. R. Weller and Z. Y. Dong, "A Review of False Data Injection Attacks Against Modern Power Systems," in *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630-1638, July 2017.
[23] F. Skopik and Z. Ma, "Attack Vectors to Metering Data in Smart Grids under Security Constraints," *2012 IEEE 36th Annual Computer Software and Applications Conference Workshops*, Izmir, pp. 134-139, 2012.
[24] G. Liang, S. R. Weller, J. Zhao, F. Luo and Z. Y. Dong, "The 2015 Ukraine Blackout: Implications for False Data Injection Attacks," in *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317-3318, July 2017.
[25] Y. Hua, F. Chen, S. Deng, S. Duan, and L. Wang, "Secure distributed estimation against false data injection attack," *Information Sciences*, vol. 515, pp. 248-262, April 2020.
[26] L. K. Kiarie, P. K. Langat, and C. M. Muriithi, "Application of Spritz Encryption in Smart Meters to Protect Consumer Data," *Journal of Computer Networks and Communications*, vol. 2019, p. 5910528, March 2019.
[27] A. Rial and G. Danezis, "Privacy-preserving smart metering," Proceedings of the 10th annual ACM workshop on Privacy in the electronic society, pp. 49-60, Oct 2011.
[28] S. S. Reza, A. Ayob, M. M. Arifeen, N. Amin, M. H. M. Saad, and A. Hussain, "A lightweight security scheme for advanced metering infrastructures in smart grid," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 2, pp. 777-784, 2020.
[29] A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," *IEEE International Conference on Pervasive Computing and Communications Workshops*, Kona, pp. 618-623, 2017.