ISSN 1870-4069

Cybersecurity on Transactions in Smart Metering Systems Using Blockchain

Juan C. Olivares-Rojas, Enrique Reyes-Archundia,
José A. Gutierrez-Gnecchi

Tecnológico Nacional de México / Instituto Tecnológico de Morelia,
México

{juan.or, enrique.ra, jose.gg3}@morelia.tecnm.mx

Abstract. Smart Metering Systems (SMS) provide real-time monitoring of energy consumption and production, enabling advanced services such as automatic connection and disconnection, demand-response events, and dynamic pricing. The most widely implemented SMS is the Advanced Metering Infrastructure (AMI). Despite their advantages, SMS face significant challenges, particularly in cybersecurity, including data manipulation, false information injection, and communication interruptions. Furthermore, SMS data is not fully exploited for advanced analytics, which could support applications such as energy theft detection, power quality monitoring, and fault prediction.This work proposes an extended AMI architecture that integrates a multi-tier blockchain framework with embedded data analytics capabilities. The proposed approach ensures secure and reliable energy transactions while enabling intelligent services directly at the smart meter and edge level. The research introduces a novel blockchain consensus algorithm, Proof-of-Efficiency (PoEf), combined with time-series forecasting, statistical methods, and reinforcement learning for anomaly detection and energy efficiency optimization. Experimental progress includes prototype development, security enhancements, and initial data analytics implementations to support fraud prevention, energy quality assessment, and failure detection in electrical networks.

Keywords: Smart metering systems, advanced metering infrastructure, cybersecurity, blockchain, proof-of-efficiency, data analytics, machine learning, energy theft detection, fog-edge-cloud computing.

1 Introduction

The Smart Metering Systems (SMS) allow the final-user, real-time monitoring of their energy consumption through Smart Meter (SM). The SM measures the energy consumption and energy production, and reports this data to the utilities. Also, SMS allows the automatic connection and disconnection, demand-response events and dynamic electrical price according to offer and demand [1]. The most implemented SMS is the Advanced Metering Infrastructure (AMI) [2].

Despite the enormous advantages of SMS, it has a lot of challenges and opportunities; one of them, it is related with the data cybersecurity. There are a lot of threats on cyber security in SMS: the interruption of the measurement (disconnection of the meter, deletion of the event log), investment of the meter (for less consumption data record), the deletion of records, the alteration of stored data, the interruption of communications to prevent data from being reported, the tamper of consumption data "on the fly" when they are reported, as well as the injection of false information (for example, alteration of dynamic energy prices), and the retransmission of packets (duplicate packets), among others [3].

On the other hand, SMS is not used actually for data analytic applications inside of SMs. The data reported by the SMs could be used for diverse applications such as fraud energy prevent, power quality prediction, fault detection, among others.

2 Previous Work in the Area

The main security mechanisms implemented to solve this problem lie in the use of cryptographic techniques [4]. Other techniques used are digital signature schemes and public-key schemes (PKI), Preventing and Intrusive Detection Systems (IPS and IDS), among others [5]. Recently, blockchain techniques (Blockchains) have been used because it is the combination of multiple cybersecurity techniques [6].

On the other hand, there are works related to data analytics, machine learning, and artificial intelligence with data in SMS [7, 8], in specific fields such as energy thief [9]. The most related works are presented in [9-15].

3 Research Objectives

The general objective of this work is develop a new architecture for AMI that in addition to the basic services related to measurement and billing can provide additional services to improve energy efficiency and contribute to better respond to the demand of electricity, through the use of data analytics directly in the measuring devices that allow to measure and control the quality of the energy as well as the detection of faults in the electrical network considering for all these services the security and privacy of the data.

4 Methodology

For the development of the proposed work, it is necessary to carry out the following steps:

1. Study and evaluation of AMI infrastructure that allows knowing the best way to implement AMI.
2. Implementation of a functional AMI prototype for testing.
3. Implementation of a multi-tier blockchain architecture for AMI that guarantees security and confidence in electricity transactions.

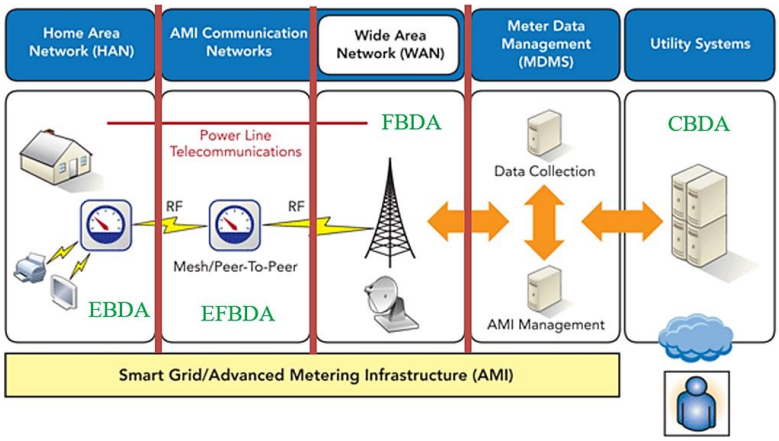

Fig. 1. AMI General Architecture with the inclusion of a Multi-Tier Blockchain and Data Analytic Platform.

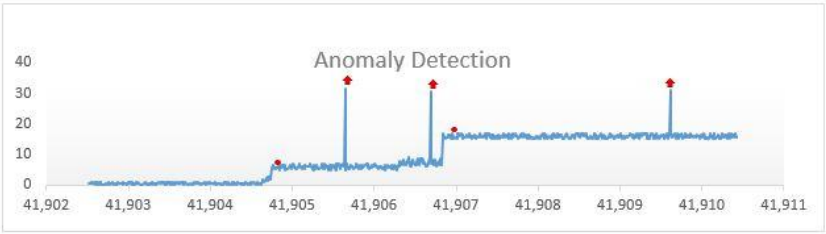

Fig. 2. Anomaly Detection consider as Energy Theft.

4. Strengthening of security and infrastructure in AMI.
5. Development of data analysis and machine learning techniques to improve energy efficiency and failure detection in electrical networks.

5 State of the Research

The authors are developing a new consensus algorithm for blockchain named Proof-of-Efficiency (PoEf) in their first version works with Moving Average (MA) and a basic Heuristic for data analytic based on Time Series Approaches like ARIMA. Right now, the authors are improving the algorithm to predict possible energy theft, check the quality of energy and determines the most efficient household. Each data analytic application has a different algorithm to process data. The analytic platform works with a reinforcement learning approach [16] with the idea of improving the results of estimations in each iteration.

Figure 1 shows the general AMI architecture extended with a multi-tier architecture of blockchain and data analytics platform. The readers can note that exist 4 main areas: CBDA (Cloud Blockchain and Data Analytics) represented with the utility's data center

servers, FBDA (Fog Blockchain and Data Analytics) represented with Data Concentrators (DC) in Substations, EFBDA (Edge-Fog Blockchain and Data Analytics) represented with DC in Neighbor Area Network (NAN) and SM, and the last tier EBDA (Edge Blockchain Data Analytics) represented with SM and Smart Appliances (SA). Figure 2 shows the main idea of detecting anomaly consumption/production inside SM. The techniques used are a hybrid approach between inferential statistics with machine learning classifiers.

6 Conclusions

There are some advances in the cybersecurity field programming a multi-tier blockchain in SMS. There is work in progress developing a new consensus algorithm using data analytics to rewarding energy transactions. Right now, we are working on improving a fog-edge-cloud computing architecture for secure data analytic application in SMS.

References

1. Coelho, P., Gomes, M., Moreira, C.: Smart metering technology. Microgrids Design and Implementation, pp. 97–137 (2018)
2. Weranga, K.S.K., Kumarawasu, S., Chandima, D.P.: Smart metering design and applications. Springer (2014)
3. Knapp, E.D., Samani, R.: Applied cyber security and the smart grid: Implementing security controls into the modern power infrastructure. Syngress (2013)
4. Borges de Oliveira, F.: On privacy-preserving protocols for smart metering systems: security and privacy in smart grids. Science Direct (2017)
5. Song, H., Flick, G.A., Jeschke, S.: Security and privacy in cyber-physical systems: foundations, principles, and applications. John Wiley & Sons (2018)
6. Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P.: Blockchain for IoT security and privacy: The case study of a smart home. In: IEEE International Conference on Pervasive Computing and Communications Workshops, pp. 618–623 (2017)
7. Ye, F., Qian, Y., Qingyang-Hu, R.: Smart grid communication infrastructures: Big data, cloud computing, and security. In: Communication, Networking and Broadcast Technologies; Components, Circuits, Devices and Systems; Computing and Processing; Photonics and Electrooptics; Power, Energy and Industry Applications; Geoscience, pp. 304, Wiley–IEEE Press (2017)
8. Al-Shaer, E., Rahman, M.A.: Security and resiliency analytics for smart grids: Static and dynamic approaches. Springer (2017)
9. Badrinath-Krishna, V., Lee, K., Weaver, G.A., Iyer, R.K., Sanders, W.H.: F-DETA: A framework for detecting electricity thef attacks in smart grids. In: 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (2016)
10. Aitzhan, N.Z., Svetinovic, D.: Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. In: IEEE Transaction on Dependable and Secure Computing (2016)

11. Gao, J., Omono-Asamoah, K., Boateng-Sifah, E., Smahi, A., Xia, Q., Xia, H., Zhang, X., Dong, G.: Gridmonitoring: Secured sovereign blockchain based monitoring on smart grid. In: IEEE Access, 6, pp. 9917–9925 (2018)
12. Sompolinsky, Y., Wyborski, S., Zohar, A.: PHANTOM: A scalable BlockDAG protocol. School of Engineering and Computer Science (2018)
13. Cebe, M., Akkaya, K., Aksu, H., Uluagac, S.: Block4Forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles. In: IEEE Communications Magazine, 56(10), pp. 50–57 (2018)
14. Sharmar, P.K., Chen, M.Y., Hyuk-Park, J.: A software defined fog node based distributed blockchain cloud architecture for IoT. In: IEEE Access, 6, pp. 115–124 (2018)
15. Gu, J., Sun, B., Du, X., Wang, J., Zhuang, Y., Wang, Z.: Consortium blockchain-based malware detection in mobile devices. In: IEEE Access, 6, pp. 12118–12128 (2018)
16. Rayati, M., Sheikhi, A., Ranjbar, A.M.: Applying reinforcement learning method to optimize an energy Hub operation in the smart grid. In: IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), pp. 1–5 (2015)