Blockchain-IoT Enabled Smart Metering System

Mariam AlHawamdeh
Informatics Department/Graduate Studies College
Palestine Polytechnic University)
Hebron, Palestine
malhawamdeh@ppu.edu

Radwan Tahboub
Informatics Department/Graduate Studies College
Palestine Polytechnic University)
Hebron, Palestine
radwant@ppu.edu

***Abstract*—Smart Metering System is a trending technology that is known widely in recent years as one of the topics related to Smart Grids (SG). It refers to the usage of a smart meter with a pre-defined and designed architecture to measure, collect, and analyze the energy consumption of customers in real time. The smart metering system contains some components that are connected to provide the desired application. The basic component is the smart meter that is related to energy customers and connected by a gateway to the utility supplier database. Which allows system measuring and monitoring of energy consumption remotely. One of the important aspects of a smart metering system is data security, where a smart metering system is providing service for a large number of customers and it collects very sensitive data of a customer's energy consumption and other private information that mustbe secured. To address this, researchers improved different security solutions to preserve the security of smart metering systems taking in mind protecting customers' data and utility network depending on the architecture of the system and desired application. Internet of Things (IoT), Blockchain, Lightweight algorithms, machine learning, and others are used as security-providing solutions for smart metering systems. Therefore, in thisstudy, we presented a review of the recent solutions that provide security for smart metering applications by integrating the smart metering system with different technologies, we also propose a new smart metering system that enables Blockchain technologyin order to provide system monitoring and security preserving.**

***Keywords* —Smart Metering, Advanced Metering Infrastructure (AMI), Smart Grid, Internet of Things (IoT), Security, Blockchain, Ethereum, Machine Learning (ML)**

I. INTRODUCTION

In recent decades, the energy distribution process was dependent on transmitting energy from the supplier to the end customers using a traditional grid system that relies on traditional electricity meters to measure the energy consumption depending on accumulative measurement [1]. And after a pre-agreed time period like a month, a worker from the energy supplier company came to read the energy consumptionmanually to produce the energy consumption bill. However, with the huge increase of energy customers and rapid progress of human civilization, the traditional energy distribution systems no longer sufficed. In order to follow the growth, the energy grids have become more automated and developed. The automatic Meter Reading (AMR) technique was proposed to solve the problem of manually reading and monitoring. AMR is a one-way directional communication technique be- tween the energy supplier utility and an advanced energy meter to read the energy consumption of each connected meter in a predefined period of time over a pre-configured communication network. This technology helped in energy consumption management and analysis. [2].

Fourth Industrial Revolution (Industry 4.0) affected energy grids by developing the energy meters and the whole network to be more reliable, interactive, secure, and smart [3]. A smart energy grid is an energy network that enables two-way communication technology to transmit and receive data through communication media between the components of the grid. The main components of the smart energy grid are a smart meter(SM), data concentrator unit (DCU), and meter database management system (MDMS). Smart meters are used to measure energy consumption and collect data related to the home that is connected. Then, it transmits this data at the requested time or at a pre-defined time period to the DCU that is related depending on the grid subdivision areas. The DCU is connected to many smart meters in the same area. And, the main aim of the DCU existence is to connect the smart meters with the MDMS and transmit received data to MDMS. MDMS is responsible for data management and control as supplier utility systems, it also can take action depending on the data received. The action can be a token transmitted to one or more smart meters through the communication network [4].Data in a smart grid system is highly sensitive, it can be a customer's personal information, energy consumption, consumption bill, customer debts, or other data. So, one of the important challenges facing the smart grid is preserving security and providing a reliable, scalable, and secure system [5]. The researchers have proposed many solutions to preserve the security of the smart energy grid. The solutions dependon enabling trending technologies like IoT, Blockchain [1][6], and Machine Learning [7] [8] in addition to Lightweight Encryption Algorithms.

In this paper, we will take an overview of the recent solutions and proposed systems that are concerned to preserve the security of the smart energy grids. After that, a new Blockchained IoT Smart Metering System is proposed. The proposed system is employing Blockchain and IoT in the smart metering system architecture in order to provide full system monitoring and security preservation. The rest of the paper is organized as follows; An overview of the recent smart energy grid solutions is provided in section 2, and

section 3 presents the proposed Blockchain smart metering system model. Simulation notes and expected results are provided in section 4. Finally, the conclusions and future works are summarized in section 5.

II. An Overview of Recent Solutions

In this section, an overview of some of the recently proposed solutions to preserve the security of different smart metering systems is presented.

A. Framework for Security Automatic Meter Reading Using Blockchain Technology

In this paper [9], the authors proposed a new automated meter reading framework that enables Blockchain technology to provide security for the proposed framework.
The proposed framework takes into mind the benefits of Blockchain technology to create a hybrid model of the smart metering system that consists of two components. First, smart meters are distributed in an area and related to customers. The second is the Blockchain network which consists of a cluster of servers Blockchain-enabled, and each server is connected to a group of smart meters. The cluster of servers is responsible for maintaining and reading the energy consumption of the connected smart meters. The servers receive data from the smart meters, then the data is considered input for the Blockchain network. The proposed solution utilizes the decentralized nature of the Blockchain to secure the data transmission in the network.
The proposed framework also includes a set of processes that ensure the security of the proposed AMR system, including data encryption, access control, and transaction validation using a predefined smart contract. The smart contract is a set of rules that are agreed upon between the system components and used to create a valid and authorized transaction to be recorded to the ledger of the Blockchain. The proposed framework ensures data integrity, confidentiality, and availability. The framework also can provide a secure and reliable solution against different attacks like reply and DoS attacks.

The proposed framework has been implemented by configuring the Ethereum Blockchain platform [10] as a Blockchain network. It also has been evaluated in terms of response time and latency on transaction creation. In addition, the proposed framework has experimented against DDoS attacks using LoIC [11] tool. The proposed framework provides safety and security for the system data and network.

B. Implementation of a smart energy meter using Blockchain and Internet of Things: A step toward energy conservation

In this article [12], the authors proposed a smart metering system that combines IoT and Blockchain technologies in order to make efficient control of renewable energy. The proposed system allows users connected to the same smart energy grid to use energy generated by neighborhood users in order to conserve local energy and mitigate energy loss. In this proposal, IoT and Blockchain are integrated to design an IoT-enabled energy meter that uses the Ethereum Blockchain to control and manage the authentication and authorization of the transactions between users, which followed a smart contract to make an authenticated and secure transaction for the Blockchain. One of the basic transactions is energy transferring between smart meters through an Android application. Any registered user in the smart grid database can download the Android application to be able to read its smart meter energy consumption and energy conserved in real time. Also, the user can sell extra conserved power to other users in the smart grid and each buy and sell transaction will be recorded in the Blockchain after being authenticated by the smart contract. The proposed system has been designed using Arduino Nano and ESP8266 for IoT network implementation and Ethereum Blockchain for Blockchain and smart contracts. The proposed system works effectively compared with other previous work [13].

C. Blockchain and Secure Element, a Hybrid Approach for Secure Energy Smart Meter Gateways

In the proposed work [14], the authors proposed a hybrid approach that combines Blockchain with Secure Element [15] technologies in order to secure data stored and transferred through the system. The proposed approach uses Blockchain for securing data immutability and Secure Element for ensuring data security at the point of generation which leads to building a trusted node at the device level before data transmission. The proposed approach aims to deliver effective and secure communication between smart meters and external market participants by relaying smart gateways in between to provide the security needed for the data exchanged.
The proposed approach delivered three case studies for different three solutions, which were designed and improved to achieve the desired goal. The First is an end-to-end implementation using the Bigchain database [16] as a Blockchain database in addition to Riddle&Code Secure Element at the device level as a robust root. The designed case uses Wi-Fi as communication technology. The second uses Helium Blockchain [17] as a Blockchain database to store data and Multos Trust Core [18] as a Secure Element. In the last case, the author used UBIRCH Blockchain with 1NCE SIMs [19] and classic IoT at the robust root.

The proposed three scenarios have been implemented and tested to be used as a P2P energy trading Platform. In addition, they provided a secure solution to safeguard IoT networks from cyberattacks. The three solutions are feasible, end-to-end secure, and trusted over different challenges of IoT platforms.

D. A Blockchain-Enabled Distributed Advanced Metering Infrastructure Secure Communication (BC-AMI)

In this paper [6], the authors proposed a secure communication scheme that uses Blockchain to secure data transactions of the Advanced Metering Infrastructure (AMI) system. The proposed scheme uses a smart contract to substitute the trusted

The third-party in order to avoid the single point of failure in the traditional (AMI). Hyperledger Fabric Blockchain [20] is used to provide network distribution integrated with Practical Byzantine fault tolerance (PBFT) to ensure Blockchain transactions [21]. While users in Blockchain are able to communicate with each other without needing a trusted third party in a way that preserves the privacy of the communication of AMI components. The proposed scheme model is working in four main phases, the first is system initialization, which aims to pre-load the main values of the system initiators of the Blockchain database. Second, is system registration and key generation, which aims to identify and register smart meters and MDMS to the defined Blockchain. In addition, generate the private and public keys f each component which are derived from the ECC curve based on the smart contract. The third phase is to start data transactions and validate each transaction depending on the smart contract. The smart meter creates a transaction that contains electricity usage with a time of reading as a time stamp. The transaction is encrypted by the public key of MDMS then the transaction is verified by the smart contract. The fourth and last phase is to release the Blockchain. After a predefined period, the Blockchain data are transformed into the MDMS to be stored there. The proposed system has been implemented and the performance has been analyzed in terms of communication cost and time cost in comparison with other related studies.

E. Secure and resilient demand side management engine using machine learning for IoT-enabled smart grid

In [8], the authors proposed a secure demand-side management (DSM) engine that integrates machine learning with an IoT-enabled smart grid to maintain system security and optimize energy utilization. The proposed system has a new design of Home Area Network (HAN) to be associated with the secure demand side management and connected to a fixed WiFi network. Secure demand-side management performs authentication to secure all received data. Then, the data is processed into a resilient agent for the decision-making process. The resilient agent is responsible for maintaining the system's security from attacks and intrusions by applying data classification using machine learning models. The system can predict the authorized and unauthorized entities using a machine learning classifier. The proposed system has been implemented and analyzed, the results showed that the proposed systemis effective and reliable in securing the smart grid system in addition to reducing the power utilization of DSM in smart grid and HAN devices.

F. Privacy-Preserving Electricity Theft Detection Scheme with Load Monitoring and Billing for AMI Networks

In [22], the authors proposed a privacy-preserving electricity theft detection scheme for the AMI grid and called it PPETD. PPETED aims to monitor system loads, compute bills, pre-serve customers' privacy, and identify electricity thefts using a machine learning model. The proposed model depends on the system operator (SO) which receives the periodic report of customers' energy consumption in the AMI grid where each customer has its smart meter. SO aims to learn the activities of fine-grained power consumption of smart meters in order to detect malicious customers in the network, which are tampering with their reports or trying to attack others. PPETED uses 4 techniques and protocols to preserve data security in the network: secret sharing cryptographic technique [23], SPDZ protocol [24], garbled circuits [25], and convolution neural networks (CNN) [26]. The proposed system has been mathematically modeled and implemented. The training and the privacy-preserving models have been implemented using Python 3 libraries and the OblivC framework on real smart meter data from Irish intelligent energy Trials [27]. The simulation results indicate that the proposed system detects malicious users in acceptable computation and communication overhead with privacy-preserving of the users of the network.

III. Proposed Model Design

In this section, we provide an overview of the proposed system. The proposed system focuses on applying Blockchain technology to the IoT-enabled smart metering architecture. The proposed system aims to monitor the smart metering system by achieving privacy preservation and preventing any unauthorized party from tampering with data transmitted or received by the smart meters. In addition, the proposed system aims to detect the energy losses at the layers of smart devices and smart meters and allows the MDMS to take action for the detected problem.

The proposed system combines the IoT-enabled Smart Grid system and Blockchain technology by taking the advantage of decentralized nature of the Blockchain network for avoiding any single point of failure.

Blockchain in this system is used to preserve the security of data transmitted and received by the network components and ensure confidentiality, integrity, and availability of the components' data. Applying Blockchain on the decentralized network is crucial in preventing data manipulation on several levels by unauthorized parties.

In addition, the system is consisting of four layers: LAN, HAN, NAN, and WAN. Each layer is applying the Blockchain network in a way to take advantage of it. And take advantage of the available devices to work as Blockchain nodes. For proposing this system, we assume the Smart Grid is located in a two-dimensional area of Am that is divided into N neighborhoods. Each neighborhood is connected to the smart grid by a Data Concentrator Unit (DCU) that is connected to the main Meter Data Management System (MDMS). Each DCU is connected to the other DCUs. In addition, each DCU is responsible for neighborhood smart meters. Each smart meter is connected to the neighborhood DCU and the other smart meters in the neighborhood. Also, the smart meter is connected to a smart home that has all appliances connected to the internet as embedded systems. As shown in Figure 1.

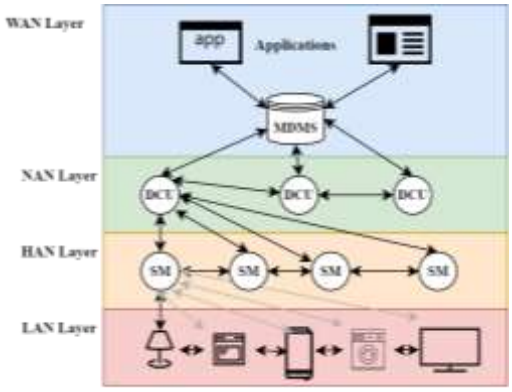

Figure 1:Proposed System Architecture Layers

For connections, we assume that all smart grid units are connected to the internet by predefined connections using wireless e.g.: Wi-Fi, or wired connections e.g.: Fiber optic connections. Each

component in this system can transmit and receive data from the upper and lower components in a two-communication way. The system network is decentralized, so there is no single point of failure because all components in the same layer are connected to each other.

A. Proposed System Architecture

The proposed system has four main layers: LAN, HAN, NAN, and WAN as shown in Figure 4.2. The system architecture has been inspired by IoT architecture [28] combined with AMI system architecture [29] and modified to meet the objectives of the proposed model.

1) LAN Layer: The first is the lower layer of the system architecture which is the Local Area Network layer (LAN). The LAN layer is the smart home network that consists of the electrical appliances in the home that are connected to the home network. This layer is connected by a two-way communication connection to the smart meter of that home.

$$LANi = \{SMi, D1, D2, \ldots, Dn\}$$

2) HAN Layer: The upper is the Home Area Network layer (HAN) that is consists of the neighborhood smart meters that are two-way connected to the same DCU as well they are connected to each other.

$$HANi = \{DCUi, SM1, SM2, \ldots, SMn\}$$

3) NAN Layer: The third is the Neighborhood Area Network layer (NAN). NAN consists of the DCUs that are connected to each other in a two-way connection. In addition, DCUs are two-way connected to the Fourth layer.

$$NANi = \{MDMS, DCU1, DCU2, \ldots, DCUn\}$$

4) WAN Layer: The fourth layer is the Wide Area Network layer (WAN). WAN is mainly composed of MDMS in the energy server of the Power Supply Company Data Center. WAN transmits and receives data from the lower layers through two-way communication technologies.

B. System Layers Data and Communication

Each component in each layer collects data, processes it, and then transmits it to the upper layer.

In the LAN layer, any home Di can read its energy consumption in kWh and sends the reading to the smart meter SMi. So, the smart meter SMi in the LAN layer can have an instant reading of the energy consumed by each connected device. Also, the smart meter can read the whole energy consumed by the home devices which is the energy that comes out of it. The DCUi in the HAN layer can read the neighborhood energy consumption coming from the smart meters. So, all these readings will be received by the MDMS. After that the collected data can be processed by MDMS, it can take any action depending on the data readings. Also, the readings will be stored in the system database.

Utility system users will use MDMS to transmit instructions to the system's lower layers, e.g.: settings changing of a specific meter or DCU depending on a map that is defined in MDMS. Therefore, DCU will receive the instructions transmitted by the MDMS and take action depending on it, e.g., re-transmit the instructions to the required smart meter.

For enabling IoT in the proposed system, we suppose that all devices in the system are connected to the internet, and transmit and receive data through an internet connection using an IP address. Each device has an embedded IoT controller [30] to enable using it as a small computer like the Raspberry Pi [31]. After implementing the controller of the device to be accessible using the internet, we need to implement internet security measures to protect the device from cyber-attacks and insure system connectivity and availability. To insuring data security, Blockchain technology will be integrated with system architecture.

The use of Blockchain technology within the proposed system is to achieve more advanced connectivity in addition to security preservation of the system data by preventing different attacks, especially data tampering attacks. In addition, Blockchain is used to detect energy losses. In a simple sense, Blockchain is used as a database to record transactions between system components. So, each component in the system should participate in a Blockchain network in order to validate and preserve data transmitted and received.

C. Blockchained Proposed Model

To create the Blockchain network, first, we define smart contracts between components in the system. A smart contract is a digital programmable contract that defines the rules and basic agreements between system components, in order to force the decentralized network components to adhere to these rules [10].

Each layer in the proposed system has its smart contract and Blockchain ledger that enable communication between layer components. In addition, each component in the system has its own key pair (public and private keys), that is generated by a pseudorandom generator system at the system construction. The public key is shared between the system components. But the private key must be secret. The key pair of each component will be used to encrypt and decrypt data transmitted or received in order to preserve data confidentiality. In addition, the system components know each other depending on the IP address and the public key.

Smart contracts will be created at the creation of the network

for each layer and stay immutable. And the read and write functions are predefined in the smart contract. Each component has a copy of the smart contract of the layer in addition to a copy of the Blockchain ledger, the verification process is shown in Figure 2.

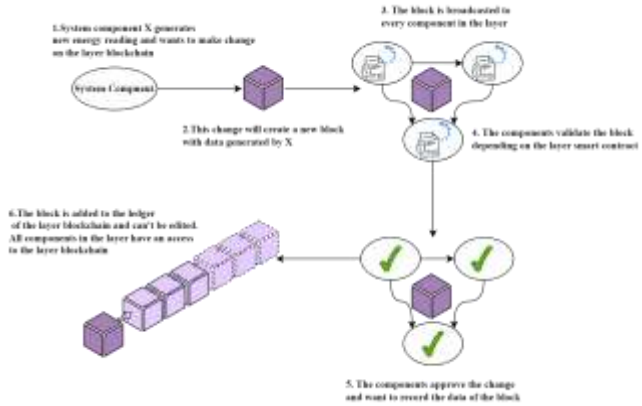

Figure 2: Transaction Verification in Each Layer

1) LAN Layer: The LAN layer has its own Blockchain that consists of the LAN components. Each component in the LANlayer has a copy of the smart contract and the ledger of this layer. The smart contract of the LAN layer is executed to validate any message sent by a component in the layer to be stored as a transaction in the Blockchain ledger. The message in this case is an energy consumption reading at a specific time. To read the energy consumed by a device Di connected

to smart meter SMi in LANi, Di transmits the reading to other connected devices and smart meter SMi. Each component sends the reading to the smart contract function to validate the public key an IP of the device and validate the reading, then each device votes, if 51% of the devices vote true, the data will be stored as a transaction in the Blockchain ledger of LANi. So, each component has two operating modes, oneis the device mode which makes it act as a normal electrical device, and the other is Blockchain node mode, which enables it to act as a Blockchain node to validate transactions of other nodes in the same layer.

2) HAN Layer: For HAN Layer, the process is not different but instead of home devices the read is given by the smart meter SMi. The SMi transmits its energy consumption reading to other connected smart meters and to the DCUi. All connected components of the HAN layer validate the reading of the smart meter depending on the smart contract of the HAN layer. If the reading is validated it will be stored as a transaction in the HANBlockchain ledger.

3) NAN Layer: For NAN, the process is working in the same steps by taking the reading of DCUi, validating it using other DCUs and MDMS, and storing the transaction in the NAN Blockchain ledger.

4) WAN Layer: For the WAN layer the process is somehow different because the message that will be validated is not an energy reading, it's a token that will be sent from the MDMS to a specific DCU, smart meter, or group of smart meters. This token must be validated and the DCUi will receive the data transmitted by SMi and they must validate this data to store it in the Blockchain. So, they firstly should ensure that the public key of SMi is valid in the smart contract. If it is valid, then the components will decrypt the encrypted data using their private keys. After that, each component will ensure from the previous Blockchain transactions that SMi's previous reading was equal to or less than the received energy reading. If the current reading is not equal or greater than the previous, then the data is false and there is a problem in SMi. So DCUi transmits a message to the MDMS that is there a problem in SMi, which will alert the company workers to take action for this meter. But if the current SMi reading is valid, the system components will note whether this data is valid or not. If and only if more than 51% of the system components voted that this data is valid then it will be stored as a transaction in the Blockchain of each component.

IV. Simulation and Implementation

The main work in this section is to show briefly the steps that will be followed to simulate and implement the proposed system model using Ethereum Blockchain.

- *Smart Contract Writing:* In the proposed system, four layers of smart contracts will be implemented using solidity language. Solidity is a high-level programming language that is similar to JavaScript [32]. Each layer will have its own smart contract with related member variables and functions in order to validate and record transactions in the layer Blockchain. Then, the Truffle framework [33] will be used to compile, test and deploy the smart contracts on a local Ethereum network.
- *Energy Consumption Readings Generation:* To generate energy consumption readings for devices in The LAN layer, we implement a Python code that generates random energy consumption readings at periodic intervals based on time of day, weather conditions, and device historical consumption. Then the implemented code will be integrated with the smart contracts to trigger the execution of certain functions based on the generated readings.
- *Smart Metering Network Architecture:* The proposed system architecture is designed to include communication protocols, data exchange mechanisms, and security measures using the Python web framework web3.py [34]. The system architecture is depending on Ethereum Blockchain [10]. A user interface or API that allows users to interact with smart contracts, view energy consumption data, and initiate transactions will be implemented to integrate the system parts. Blockchain framework Ganache [35] will be used to set up the local Ethereum network for testing and development purposes. Finally, the smart contracts will be deployed on the localnetwork to test their functionality and ensure that they meet the requirements.
- *Expected Results:* The simulation results will be studied and analyzed. In addition to applying security tests to test the proposed system performance against security attacks like DoS, MinM, replay, and EVD attacks [9]. We expect the Proposed system will

achieve two-way communication security against these attacks. In addition to higher speed with real-time two-way communication and full energy consumption monitoring at each layer. The proposed system is expected to provide high scalability and reliability as a smart metering system.

V. Conclusion and Future Work

Through the research carried out in the paper, we have provided a review of the recent works and studies in the field of smart metering, advanced metering infrastructure, and securitypreservation techniques for these systems. In addition, we have proposed a smart metering system architecture that enables IoT and Blockchain in order to provide system connectivity, scalability, and security. The proposed system has four layers that are integrated and work together to provide full energy consumption monitoring for every single device of the system. Each device is connected to the internet and will have a copy of the Blockchain and the smart contract of the layer thatit's related to. That ensures system and data availability, in addition to providing validation and authentication of each transaction before it is recorded in the Blockchain. For Future work, first, we are intended to complete the system simulation to provide a full scientific contribution. Moreover, Artificial Intelligence (AI) algorithms will be used to provide smartactions depending on the data received by MDMS. In addition to providing energy loss detection at each layer level.

References

[1] A. A. G. Agung and R. Handayani, "Blockchain for smart grid," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 3, pp. 666–675, 2022.

[2] F. E. Abrahamsen, Y. Ai, and M. Cheffena, "Communication technologies for smart grid: A comprehensive survey," *Sensors*, vol. 21, no. 23, 2021.

[3] M. Faheem, S. Shah, R. Butt, B. Raza, M. Anwar, M. Ashraf, M. Ngadi, and V. Gungor, "Smart grid communication and information technologies in the perspective of industry 4.0: Opportunities and challenges," *Computer Science Review*, vol. 30, pp. 1–30, 2018.

[4] R. Rashed Mohassel, A. Fung, F. Mohammadi, and K. Raahemifar, "A survey on advanced metering infrastructure," *International Journal of Electrical Power Energy Systems*, vol. 63, pp. 473–484, 2014.

[5] H. Tian, Y. Jian, and X. Ge, "Blockchain-based ami framework for data security and privacy protection," *Sustainable Energy, Grids and Networks*, vol. 32, p. 100807, 2022.

[6] N. Islam, M. S. Rahman, I. Mahmud, M. N. A. Sifat, and Y.-Z. Cho, "A Blockchain-enabled distributed advanced metering infrastructure secure communication (bc-ami)," *Applied Sciences*, vol. 12, no. 14, 2022.

[7] A. S. M. Tayeen, M. Biswal, and S. Misra, "Dp-ami-fl: Secure framework for machine learning-based ami applications," in *2023 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, pp. 1–5, 2023.

[8] M. Babar, M. U. Tariq, and M. A. Jan, "Secure and resilient demand side management engine using machine learning for iot-enabled smart grid," *Sustainable Cities and Society*, vol. 62, p. 102370, 2020.

[9] E. Dbabseh and R. Tahboub, "Framework for securing automatic meter reading using Blockchain technology," in *ITNG 2021 18th International Conference on Information Technology-New Generations*, IEEE, 2021.

[10] E. Foundation, "What is ethereum?." https://ethereum.org/en/what-is-ethereum/, Accessed on 2023-01-13.

[11] Imperva, "What is low orbit ion cannon (loic)?." https://www.imperva.com/learn/ddos/low-orbit-ion-cannon/, Accessed on 2023-01-13.

[12] M. Tahir, N. Ismat, H. H. Rizvi, A. Zaffar, S. M. Nabeel Mustafa, and A. A. Khan, "Implementation of a smart energy meter using Blockchain and internet of things: A step toward energy conservation," *Frontiers in Energy Research*, vol. 10, 2022.

[13] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, and M. Bertoncini, "Blockchain based decentralized management of demand response programs in smart energy grids," *Sensors*, vol. 18, no. 1, 2018.

[14] C. Zakaret, N. Peladarinos, V. Cheimaras, E. Tserepas, P. Papageorgas, M. Aillerie, D. Piromalis, and K. Agavanakis, "Blockchain and secure element, a hybrid approach for secure energy smart meter gateways," *Sensors*, vol. 22, no. 24, 2022.

[15] T. Schläpfer and A. Rüst, "Security on iot devices with secure elements," in *Embedded World Conference 2019 - Proceedings*, 2019.

[16] BigchainDB, "Features of BigchainDB." https://www.bigchaindb.com/features/, Accessed on 2023-02-27.

[17] Helium, "Helium Technology." https://www.helium.com/technology, Accessed on 2023-03-06.

[18] MULTOS, "MULTOS Trust Core Developer Boards." https://multos.com/support/multos-trust-anchor/developer-boards/trust-core-details/, Accessed on 2023-03-06.

[19] U. GmbH, "Ubirch SIM Tutorial." https://ubirch.com/digital-corona-lab-certificate-1/ubirch-sim-tutorial/, Accessed on 2023-04-06.

[20] M. Graf, R. Küsters, and D. Rausch, "Accountability in a permissioned Blockchain: Formal analysis of hyperledger fabric," in *2020 IEEE European Symposium on Security and Privacy (EuroSP)*, pp. 236–255, 2020.

[21] O. Onireti, L. Zhang, and M. A. Imran, "On the viable area of wireless practical byzantine fault tolerance (pbft) Blockchain networks," in *2019 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, 2019.

[22] M. Nabil, M. Ismail, M. M. E. A. Mahmoud, W. Alasmary, and E. Serpedin, "Ppetd: Privacy-preserving electricity theft detection scheme with load monitoring and billing for ami networks," *IEEE Access*, vol. 7, pp. 96334–96348, 2019.

[23] J. C. Choon and J. Hee Cheon, "An identity-based signature from gap diffie-hellman groups," in *Public Key Cryptography — PKC 2003* (Y. G. Desmedt, ed.), (Berlin, Heidelberg), pp. 18–30, Springer Berlin Heidelberg, 2002.R. Livni, S. Shalev-Shwartz, and O. Shamir, "On the computational efficiency of training neural networks," in *Advances in Neural Infor- mation Processing Systems* (Z. Ghahramani, M. Welling, C. Cortes, N. Lawrence, and K. Weinberger, eds.), vol. 27, Curran Associates, Inc., 2014.

[24] Y. Huang, D. Evans, J. Katz, and L. Malka, "Faster secure two-party computation using garbled circuits," in *Proceedings of the 17th ACM conference on Computer and communications security*, pp. 124–133, ACM, 2010.

[25] Y. LeCun, Y. Bengio, *et al.*, "Convolutional networks for images, speech, and time series," *The handbook of brain theory and neural networks*, vol. 3361, no. 10, p. 1995, 1995.

[26] A. Alsharif, M. Nabil, M. Mahmoud, and M. Abdallah, "Privacy-preserving collection of power consumption data for enhanced ami networks," in *2018 25th International Conference on Telecommunications (ICT)*, pp. 196–201, IEEE, 2018.

[27] G. Kanagachidambaresan, R. Anand, E. Balasubramanian, and V. Mahima, *Internet of things for industry 4.0: Design, challenges and solutions*. Springer, 2020.

[28] I. Petruševski, M. Živanović, A. Rakić, and I. Popović, "Novel ami architecture for real-time smart metering," in *2014 22nd Telecommunications Forum Telfor (TELFOR)*, pp. 664–667, 2014.

[29] T.-A. Chen, S.-C. Chen, W. Tang, and B.-T. Chen, "Internet of things: Development intelligent programmable iot controller for emerging industry applications," *Sensors*, vol. 22, no. 14, 2022.

[30] R. P. Foundation, "Raspberry Pi 3 Model B+." Available online, Accessed 08-04-2023.

[31] Solidity Documentation, "Solidity v0.8.20 documentation," 2021.

[32] Truffle Suite, "Truffle documentation," 2021.

[33] Web3.py Contributors, "Web3.py documentation," 2021.

[34] Truffle Suite, "Ganache documentation," 2021.