Letters in High Energy Physics
ISSN: 2632-2714
Volume 2024

Enhancing Security of Smart Energy Meter Data Using Blockchain Technology

[1]Lina Aziz Swadi, [2]Haider M. Al-Mashhadi

[1]Department of Computer Science, College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq
Email: linaswadi01@gmail.com

[2]Department of Cybersecurity, College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq
Email:
haider.abdulnabi@uobasrah.edu.iq

Abstract

People recognize the Internet of Things (IoT) as a transformative innovation. That facilitates the connection of numerous things to the Internet. However, this interconnectivity also gives rise to apprehensions over the security and confidentiality of delicate information, requiring enhanced precautions. The networks have weaknesses that might be applied to initiate assaults and gain unauthorized access. Blockchain is a cryptographic protocol that ensures secure storage and transmission of data across a decentralized network. It preserves an impervious and immutable ledger of information that is distributed among several network nodes. This study proposes a prototype that combines blockchain and IoT technologies to address security issues in the realm of IoT efficiently. The data is securely delivered in an encrypted format from smart meters daily at consistent intervals to blockchain nodes. Thereafter, these transactions are recorded in a ledger, whereby a proof-of- work technique is used to generate a new block. The data is generated from smart meters then provided to blockchain nodes daily, and subsequently documented in a ledger. Every day, the monthly bill values for a specific meter are determined by calculating the total energy consumed each day using the smart meter readings retrieved from the blockchain blocks.

Keywords: smart meter, blockchain, IoT, security, sustainability.

1. INTRODUCTION

The advanced metering infrastructure (AMI) comprises of smart meters, a network of interconnected devices for communication, and a system for organizing and controlling data. Advanced metering infrastructure (AMI) is crucial in Power delivery systems that utilize load pattern recording and bi-directional information exchange. Simultaneously, the process of deregulating the electricity business, namely in terms of the delivery aspect, is steadily progressing in numerous countries across the globe. [1] The existence of numerous electricity consumers in large cities poses challenges in terms of measuring and designing the electrical network. Trust difficulties may arise due to these system's lack of transparency and centralization. On the other hand, customers are unaware that their data might be susceptible to assaults or exploitation without their knowledge. [2] The combination of the IoT with mobile sensor networks in smart grid development has been prompted by the need to deal with the challenges associated with electricity distribution. Nevertheless, deploying the smart grid encounters substantial challenges because of privacy and security concerns regarding the exchange and usage of electrical data. [3] Blockchain is a suitable solution when there is a need for a comprehensive and transparent record of assets. Monitoring and safeguarding digital interactions, along with maintaining a distributed and decentralized ledger of records, are crucial in applications related to electricity generation, distribution, transmission, and consumption. As well as those employed for data exchange and conducting safe transactions. These challenges can be efficiently addressed by utilizing blockchain technology in such applications. [4] An innovative concept in the energy field that transforms from a traditional centralized structure to a decentralized system. The energy sector is incorporating sources of renewable power into the energy network to fulfill

sustainability objectives. This requires a modification that combines prominent conventional energy producers with diverse small- and large-scale electricity producers inside a single structure. Despite its complexities, substantial transformation can be achieved through the utilization of contemporary advancements in technologies for communication and information, digitization of the industry 4.0 structure, and IoT technology. [5] In [6] Approaches have been proposed to implement IoT in smart energy meters. This methodology integrates IoT devices, cloud-based data management, artificial intelligence, machine learning predictions, and real-time user engagement to develop an advanced smart metering system focused on optimizing energy usage and improving the smart grid infrastructure. The limitations encompass scalability challenges and data privacy concerns.

This paper presents a method that aims to enhance the transparency, security, and effectiveness of smart metering systems through leveraging blockchain and Internet of Things technologies. IoT devices provide a cost-effective and efficient means of collecting and transmitting real-time data. The project involves creating a secure database for meter data storage and billing information, integrating blockchain technology to create a reliable log of transactions, and improving transparency and confidence in the metering system. It also includes bill calculations considering energy use and data analysis for users. [7] In general, this method seeks to address issues about the security, confidentiality, and reliability of smart metering systems, by presenting a solution that is more robust, transparent, and user-friendly.

2. BACKGROUND

2.1 Internet of Things (IoT)

Internet of Things (IoT) is an upcoming technology that enhances existing connections by facilitating the integration of any device with the Internet. The widespread adoption of IoT devices is experiencing huge expansion. The number of smart devices purchased through both offline and online channels has experienced a substantial surge in recent years. [8] as presented in Fig. [9]

Fig. 1: IoT Utilization

IoT is a complex network of disparate objects. Sensors play a crucial role in IoT applications as they collect information from the environment and send it through a connection to the Internet gateway. These sensors frequently carry out tasks autonomously. [10] The principal objective of IoT is to improve the quality of living by closely monitoring and managing various activities, such as energy use. Therefore, conserving and overseeing energy is a crucial factor, given that the majority of energy is derived from non-renewable sources. [11]

2.2 Cloud Computing

Cloud computing Facilitates the distribution of diverse services and information via the Internet. Users can utilize software applications, store data,

and do computations on far-off servers preserved by providers of cloud service instead of on local PCs or personal devices. The internet is the essential foundation of cloud computing. It links users to distant servers where data and applications are stored. Cloud computing architectures are structured to offer services as needed. The services are adaptable and versatile, enabling resources to be modified based on the user's requirements. The components consist of hardware, such as servers and storage devices, and software, such as databases and applications. [12] Cloud Computing is a proficient platform for IoT applications that store and analyze data on remote servers located in data centers. The extensive utilization of IoT in critical applications that cannot tolerate delays requires prompt reactions from the service providers. [13]

2.3 Data Security

The data is heavily influenced by the paramount concerns of privacy and security. Recently, numerous research initiatives have been conducted to address the issue of privacy protection of data. These initiatives mostly focus on access control, attribute-based encryption (ABE), confidence, and reputation. However, these efforts are fragmented and lack a cohesive framework. [14] Cloud computing has attracted significant interest due to its numerous advantages. The benefits encompass favorable costs, time efficiency, and optimal utilization of computing resources. However, concerns around security and privacy have contributed to the suspicion surrounding this phenomenon. Cloud computing necessitates customers to migrate their data to servers hosted by cloud service providers. There are methods available for consumers to monitor and assess the features of their data security and apply cryptographic algorithms to ensure the sustained privacy and security of the data. [15] Services provided by the cloud are commonly regarded as the fundamental infrastructure of IoT that facilitates the storage of data, data processing, and data transmission. Cybercriminals are specifically focusing on IoT computer equipment and nodes that store or transmit confidential information. [16]

2.4 Blockchain

Decentralized cryptocurrency systems have surfaced in recent years. Bitcoin was the inaugural example of these systems, which employ blockchain technology. Bitcoin allows users to safely carry conduct payments and transfer a digital currency (bitcoins) among other people, reducing the need to depend on a third party for trust. Blockchain serves as an immutable ledger of blocks which includes timestamps, and this ledger is spread across all the network nodes. This decentralized approach removes the need for a single controlling authority. This technology facilitates the exchange and storage of data over a decentralized peer-to-peer network. It has a significant effect on enabling financial transactions. Furthermore, it can serve as an enabler in diverse fields. It has an enormous effect on enabling transactions in finance. Decentralized applications encompass several domains such as IoT, supply chains, proof of document existence, and energy smart meters. [17] The blockchain is a group of linked blocks that store and transmit data. Every block has a reference to the block that directly precedes it. This pointer functions as a hash value for the previous block. As presented in Fig. 2 [18]

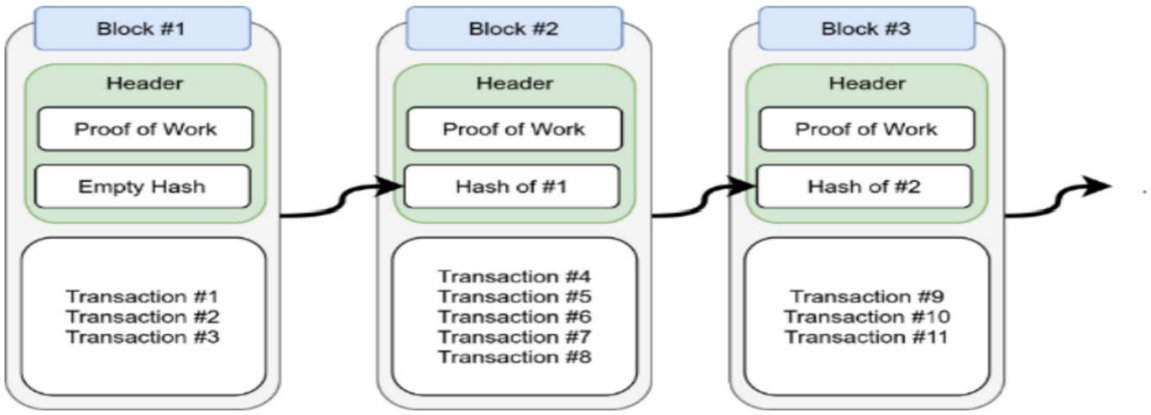

Fig. 2: Blockchain Structure

At its core, a blockchain is a chronologically ordered collection of immutable data entries managed by a decentralized network of computers. Each data block is protected using cryptographic techniques and linked to the others. Blockchains are digital systems that utilize encryption, networking, incentive structures, and distributed ledger technology to simplify the procedures of validating, executing, and documenting transactions across numerous participants. [19] Blockchain's inherent features of security, authenticity, confidentiality, and data integrity make it a viable solution for smart metering. [20] The primary encryption methods utilized in blockchain technology involve both symmetric and asymmetric encryption techniques. A symmetric encryption algorithm consists of both the transmitter and receiver using the same key to encrypt and decrypt massive volumes of data, which is then transported over the network. As part of an asymmetric encryption process, the sender initially employs a public key to encrypt the data. Next, the recipient employs the appropriate private key to decipher the ciphertext. [21] A Digital Signature is a technique used to confirm and authenticate the originality of a message or document, while also ensuring its integrity and preventing denial of its origin. Authenticity is the primary characteristic in cryptography for verifying the user's identity. Digital signatures operate using the merging of public and private keys, as well as hash algorithms. [22] Common consensus algorithms employed in Blockchains encompass proof-of-stake (PoS) and also proof- of-work (PoW). In Blockchains (PoW) participants in the network attempt to resolve a highly computational mathematical problem. Each peer in the network must use their computation capacity to resolve mathematical problems. The individual who devises the answer emerges as the victor in the block race and successfully mines a new block. After a block is sent to the network, every peer validates the solution and adds the block to their Blockchain. (PoS) was implemented as a solution to the power inefficiency problem associated with (PoW). In the (PoS) consensus algorithm, a user's mining power is defined by the aggregate quantity of coins they possess. An auction is conducted for each new block to determine the chosen miner. Users submit bids for the block, and the individual with the highest bid is chosen as the miner. [23]

Table 1: Comparison of Blockchain Algorithms for Smart Metering

Algorithm	Description	Strengths	Weaknesses	Use Case in Smart Meters
Proof-of-Work (PoW)	A consensus algorithm that requires nodes to solve complex mathematical puzzles.	High security, widely used	High energy consumption, slow transactions	Used in validating transactions in smart meters
Proof-of-Stake (PoS)	Nodes validate transactions based on the number of coins they hold.	Energy-efficient, faster than PoW	Potential for centralization	Potential use in energy-efficient smart meters

2.5 Smart Energy Meters

Smart energy meters are essential components of grid innovation, capable of capturing customer usage at frequent intervals using communication networks. By implementing advanced metering infrastructure (AMI), an abundance of new energy consumption data becomes available. Energy consumption can be monitored periodically using IoT technology, allowing the user to efficiently manage their usage. [24] Smart meters are devices that measure several electricity parameters for every prosumer, including power consumption and power export. They locally record this data and then transmit it to a central server via connection networks for operational purposes. The smart meter's ability to carry out tasks such as recording current and voltage measurements and storing

information is facilitated by the metering infrastructure. The transmission infrastructures facilitate two-way communication between consumers and energy suppliers through electricity line connections or wireless communication networks. The smart energy meters can establish connections with remote centers to facilitate control and management functions. This connection constitutes what is known as an advanced metering infrastructure (AMI). [25]

2.6 Attacks on Smart Meters

The information often consists of log data that is utilized to quantify specific factors to determine suitable solutions for the applications. Due to the sensitivity of this information, there is a risk of the device being captured and the data being tampered with, which might result in significant performance deterioration of the network. [26] There are various categories of potential attacks such as data integrity, when an external attacker compromises the communication channel and gains unauthorized access to the protection and control algorithms of a digital relay, a replay attack is a deceptive tactic in which genuine data is intentionally and dishonestly duplicated or replicated. During replay assaults, assailants can duplicate the data that has been obtained from a hacked database or data recorder and use it repeatedly for a specific time. An attacker initiates a Denial of Service (DoS) attack to disrupt or exploit the relay's critical services. [27] Data transmission throughout the network creates vulnerabilities for cyberattacks. Encompass malicious software and eavesdropping attacks. [28]

3. RELATED WORKS

The study in [29] investigates how the combination of blockchain technology and IoT can improve the monitoring of energy consumption, specifically in urban areas. The system emphasizes the importance of user privacy by enabling individuals to keep their personal data on their own devices, sharing it only as needed, and using encryption to safeguard sensitive information. However, these devices are susceptible to cyberattacks that could potentially jeopardize the entire system if they are not properly safeguarded.

The paper in [30] intends to demonstrate the impact and utilization of blockchain technology with an intelligent power management system integrated onto the SealedGRID platform. The technology allows users to instantly monitor power use in a smart grid system. The platform is being constructed with a focus on protection and resistance against potential threats. The methodology may face challenges in guaranteeing seamless compatibility across various blockchain platforms and pre-existing energy management systems. This can impede the smooth integration of many technologies and devices inside the smart grid.

The work in [31] Proposed El DApp, an application for monitoring power use that integrates IoT and blockchain technologies to establish a system that is both decentralized and secure to collect data, enhancing the design of smart meters. The DApp utilizes a Raspberry Pi-powered Ethereum network to offer a safe and cost-efficient decentralized real-time power usage log for users. The solution does not encompass the physical safeguarding of the Raspberry Pi components, so leaving the system vulnerable to potential harm or unauthorized manipulation of the hardware, which could endanger its overall integrity. However, they are only capable of mining the network once every hour. This process necessitates the presence of online peers and a dedicated internet connection. Additionally, Raspberry Pi nodes lack physical security measures.

Utilization of IoT devices in [32] to collect real-time data from smart meters and utilize blockchain technology for secure data storage and transaction management. Energy consumption data gathered by IoT devices are encrypted and saved into a blockchain to guarantee the integrity as well as the security of the data. The automation of billing and transactions conducted by smart contracts creates an efficient, transparent, and tamper-proof system. The method improves data security and privacy, while also permitting precise tracking and billing of energy usage. The proposed design effectively updates the configuration in the middleware. However, it takes somewhat longer, by a few milliseconds, compared to alternative servers such as SSH and FTP.

The methodology in [33] integrates both IoT and blockchain techniques for establishing a reliable decentralized network for smart energy metering and billing. The system employs smart contracts for trust-based interactions and transparency, for real-time power usage recording a Raspberry Pi-based

Ethereum network is used, and certificates aggregated ring decryption for confidentiality protection. A secure private blockchain for direct communication between consumers and energy producers is utilized. Even though the paper assumes that there is minimal energy loss when transferring between nearby users, in practice, there might be some energy loss, particularly over greater distances or in systems that are less efficient. This could impact the true number of energy that the buyer receives compared to what the seller aimed to transfer.

Creating a blockchain-based smart meter for microgrids that facilitates a peer-to-peer energy market in [34]. When the project involves creating the hardware component of a smart power meter with a focus on achieving high levels of security, trustworthiness, and measurement precision. The design integrates precision, cybersecurity, communication, and engagement within the Smart Energy Administration System. The research suggests that additional testing and refinement are necessary, namely in relation to the hashing methods and cybersecurity prerequisites. This implies that the existing methodology may not be completely proven and necessitates further investigation to verify its reliability.

The proposal in [35] suggests a Privacy-Preserving Monitoring and Billing scheme (PMBFE) for AMI networks, utilizing Functional Encryption. The authors have defined the data aggregation privacy issue and created the PMBFE scheme While ensuring user data privacy, the suggested PMBFE shows a notable improvement in speed with respect to computation and communication overheads. However, the paper does not thoroughly examine other potential vulnerabilities; instead, it focuses exclusively on collusion and eavesdropping attacks. As well as Smart meters computing and storage capacities may still be a constraint.

The study in [36] examines a multitier blockchain architecture that employs a proof-of-efficiency mechanism to enhance privacy and data safety, particularly for smart metering applications. The layout of this structure suggests the utilization of a large-scale database for storing and managing massive data in smart meters. However, this approach is complex and expensive, and the network may be exposed to new vulnerabilities, such as the attacks of man-in-the-middle due to multitier of blockchain.

The paper in [37] a sophisticated energy meter is suggested, which will accurately gauge power consumption and store the readings securely on the blockchain. This measure aims to prevent fraudulent activities and facilitate direct payments without the involvement of intermediaries such as banks. In blockchain approach, transactions can be conducted peer-to-peer, without the need for third parties, utilizing cryptocurrencies like bitcoin, ether, and others. The user will have the capability to verify the invoices stored in the blockchain and make payments. Implementing blockchain technology enhances the security of user data and provides solutions to IoT security concerns. However, to enhance the efficiency of the task, it is highly beneficial to automate the process of uploading energy meter readings. This not only proves to be highly advantageous but also ensures that the security measures are effectively implemented.

The proposed architecture in [38] was put into practice to create the BSEMS, which uses smart meters and Hyperledger technology to securely and accurately record energy consumption data. Its main goal is to effectively measure and manage energy consumption using a specific blockchain architecture. However, smart contracts depend on precise information provided by smart meters. If the data gathered is inaccurate or tampered with, it may result in incorrect execution of contracts, impacting billing and energy management operations.

Table 2: Comparison of Blockchain-Based Approaches in Smart Grids

Study	Methodology	Strengths	Weaknesses	Relevance to Smart Meters
Study A	Combines blockchain with IoT for secure energy monitoring.	High security, decentralized	Requires extensive computational resources	Applicable to decentralized smart meter networks

Study B	Uses smart contracts for automated energy billing.	Transparency, automation	Compatibility issues with existing systems	Relevant for automated billing in smart meters
Study C	Blockchain-based energy management with PoW consensus.	Secure, tamper-proof	Energy-intensive	Useful in energy-sensitive environments

4. METHODOLOGY

Security concerns are increasing with using centralized electrical networks. External opposed assaults, third-party dependencies, and privacy breaches have led to significant economic losses in electricity grids. The conventional centralized electricity grid has restricted options. Many scenarios depend on human oversight. Managing a significant number of smart appliances in a centralized way for grid control, status monitoring, and metering is a difficult undertaking. Conversely, many intelligent sensors produce vast quantities of data that are difficult to store and analyze using a central server. Additionally, the management of security by the control center is inefficient and results in unnecessary waste for several smart gadgets in the event of criminal attacks. [39] This study introduces a model that leverages a decentralized system of servers, represented by blockchain nodes. The blockchain is a decentralized, transparent, and distributed organization of data specifically built as digital records for recording transactions into the blockchain nodes that are distributed among several servers. It can improve cybersecurity by making it very difficult to tamper with any block once it has been chained to the Blockchain. [40] Utilizing the Proof-of-work (PoW) technique as a consensus algorithm ensures the integrity of the data by validating the transactions from smart energy meters. The framework focuses on managing, maintaining authenticity, and ensuring uniformity of the public ledger across all nodes of the blockchain. It also aims to protect the system from attacks such as 51% of the computing power and instances of double spending assaults. The fundamental concept involves distributing accounting costs and incentives by nodes that are vying for the processing capacity of the hash by competing with each other, using a specific set of information. Nodes of the network compute the specified answer for an issue in mathematics. The most efficient node for resolving the issue is responsible for generating the subsequent block and receiving the mining reward. [41] Daily Meter Data is collected daily for each meter. Including location and values for different metrics such as timestamp, energy consumption, current, voltage, humidity, temperature, and a unique ID consisting of nine digits to each meter by combining three fixed digits for zone code with randomly generated three digits for building as well as three digits for meter number. This step guarantees that each data point can be traced back to its original meter.

Table 3: Structure of Smart Meter Data Collected Daily

Meter ID	Location	Timestamp	Energy Consumption (kWh)	Current (A)	Voltage (V)	Temperature (°C)	Humidity (%)
352522395	37.4217636 - 122.084614	2024-01-01 00:00:00	10.47	47.88	194.90	3.72	28.52
352522395	37.4217636 - 122.084614	2024-01-02 00:00:00	27.48	54.14	177.22	8.01	68.25
352522395	37.4217636 - 122.084614	2024-01-03 00:00:00	27.43	73.83	48.31	26.54	65.90

352522395	37.4217636 - 122.084614	2024-01-04 00:00:00	18.19	21.16	25.34	23.18	69.37

The data is encrypted using a hybrid encryption method that combines asymmetric cryptography with elliptic curve cryptography (ECC) for key generation and symmetric encryption using advanced encryption standards (AES) for encrypting the data. A key generation involves the creation of a private key using Elliptic Curve Cryptography (ECC). From this private key, the corresponding public key is derived. AES operates on data blocks that must be a multiple of the block size. To comply with AES block size criteria, the data blocks are padded. An initialization vector (IV) is created randomly for the AES cipher in Cipher Block Chaining (CBC) mode to guarantee that encrypting identical plaintext blocks will produce distinct ciphertext blocks. [42] The combination of techniques enables a smaller key length and a more efficient security system for data protection. One of the fundamental characteristics of (ECC) is its small key size. When (AES) is implemented for encryption using (ECC), the size of the encryption key is reduced, leading to enhanced performance. Elliptic Curve Cryptography (ECC) employs standardized keys for both decryption and encryption to minimize key size and establish a safe key system. Employing (ECC) in conjunction with (AES) is the optimal approach for safeguarding data against unwanted access. After the key size is determined, the ciphertext will be generated to perform the data encryption and decryption. The private key generated by the Elliptic Curve Cryptography (ECC) algorithm is used by the Advanced Encryption Standard (AES). [43] As presented in Fig. 5.

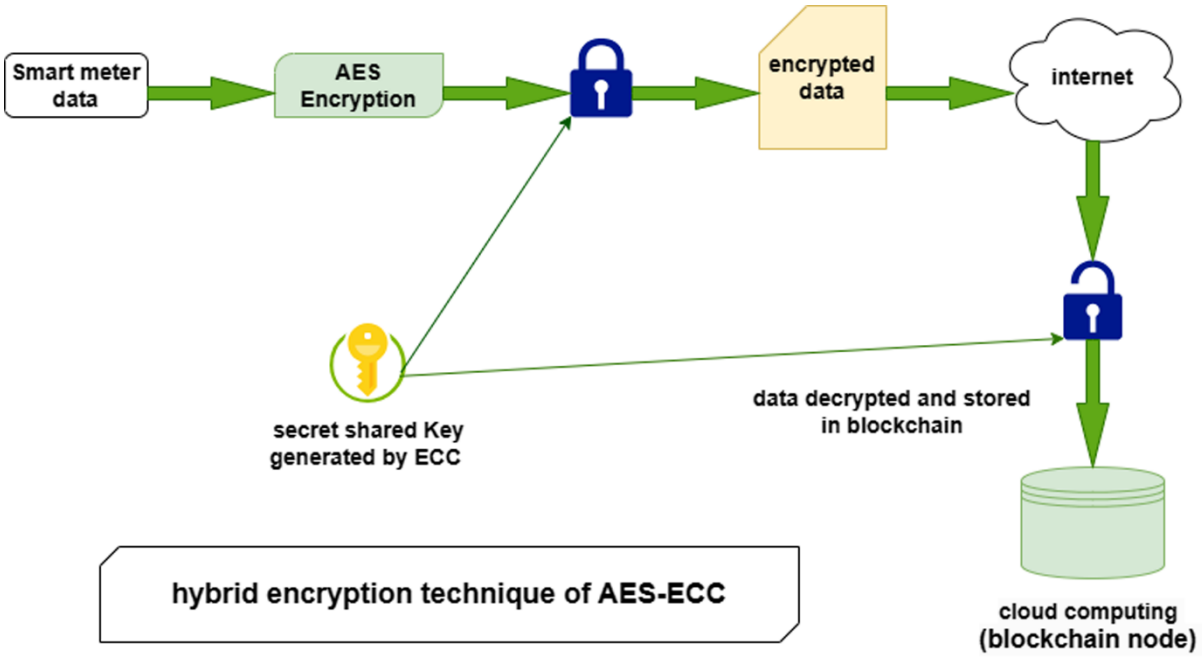

Fig. 5: Hybrid Approach of AES and ECC Algorithms

Every smart meter employs a hybrid approach of AES and ECC cryptography algorithms to encrypt smart meter data, guaranteeing the security and confidentiality of data. Once encrypted, these readings are transmitted to a utility server where the blockchain system is implemented. The server then decrypts the data to verify its integrity and authenticity, followed by a validation process to ensure it was not tampered with during transmission. This validation is carried out using a Proof of Work (PoW) consensus mechanism, then used in creating a new block. Once a block is validated, it is appended to the blockchain. This method enables effective data handling by ensuring safe storage,

convenient retrieval, and analysis of smart meter data in a decentralized system. The data from the server is structured using an HTML file and can be remotely accessed in its formatted state. This characteristic improves the ease of access and functionality of the information for both utility providers and consumers. [44] As presented in Fig. 6.

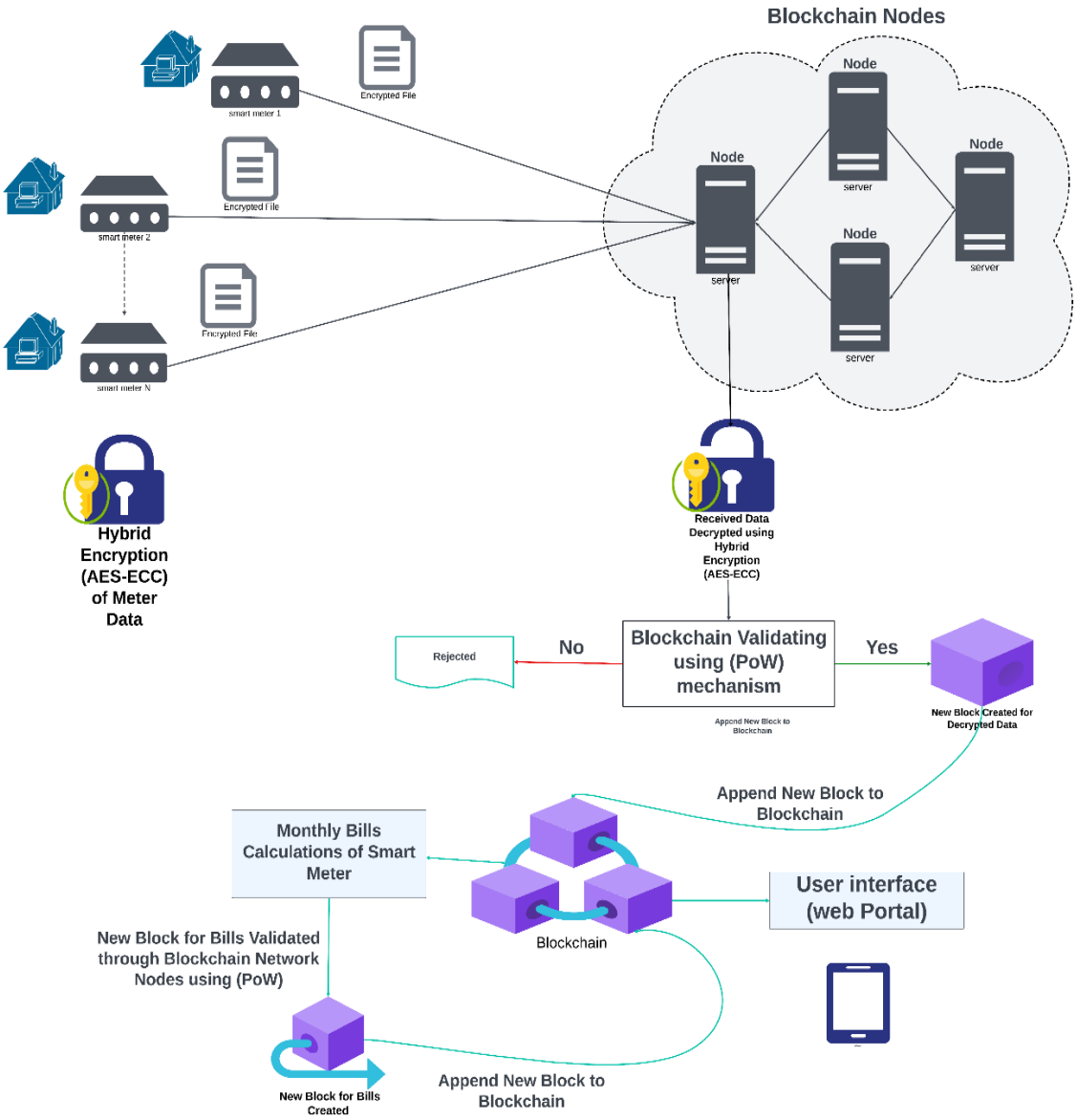

Fig. 6: The Proposed System

The blockchain stores data, with the initial block being generated and its content hash calculated. The mining process involves modifying the nonce value until the block's hash fulfills particular criteria, such as a required number of leading zeros. The proof-of-work technique serves to safeguard the blockchain against manipulation and guarantees consensus in distributed networks. [45] Monthly bills are calculated using the electricity usage of a particular smart meter during a specific period. The process involves iterating through each block in the blockchain, except the genesis block, calculating the total energy usage, and determining the bill according to the overall monthly consumption. The monthly bills are saved in a new block generated and chained to the blockchain. As presented in Fig. 7.

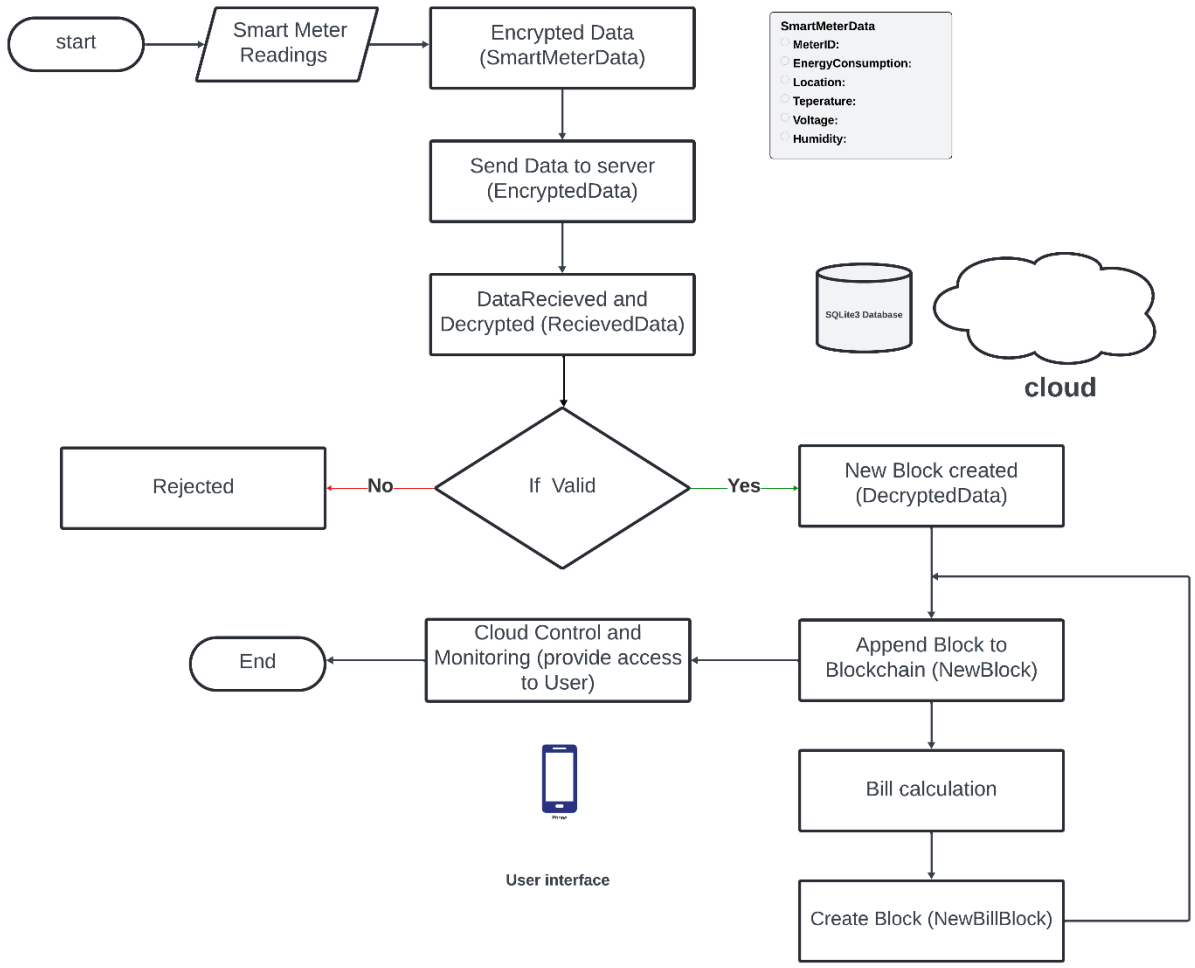

Fig. 7: Flowchart of Methodology

The list of bills is retrieved in the SQLite 3 database for easy access control, the bills can be executed on a daily or monthly basis. To guarantee dependability and safety, particularly with encryption and blockchain technology. Collecting data from smart meters, where data are sent to the blockchain every day at midnight. The data is verified, and a new block is created every day. This operation entails the blockchain's consensus mechanism utilization to authenticate data from the meters, organizing this data into blocks, and subsequently chaining these blocks to the blockchain. A cloud application has been developed. As presented in Fig. 8. The application serves as an interface for managing and visualizing smart meter data practically. As presented in Table. 4.

Table 4. Smart Meter Data

Meter ID	Location	Timestamp	Energy consumption	Current	Voltage	Temperature	Humidity
352522395	37.4217636, -122.084614	2024-01-01 00:00:00	10.47	47.88	194.90	3.72	28.52
352522395	37.4217636, -122.084614	2024-01-02 00:00:00	27.48	54.14	177.22	8.01	68.25
352522395	37.4217636, -122.084614	2024-01-03 00:00:00	27.43	73.83	48.31	26.54	65.90

352522395	37.4217636, -122.084614n	2024-01-04 00:00:00	18.19	21.16	25.34	23.18	69.37

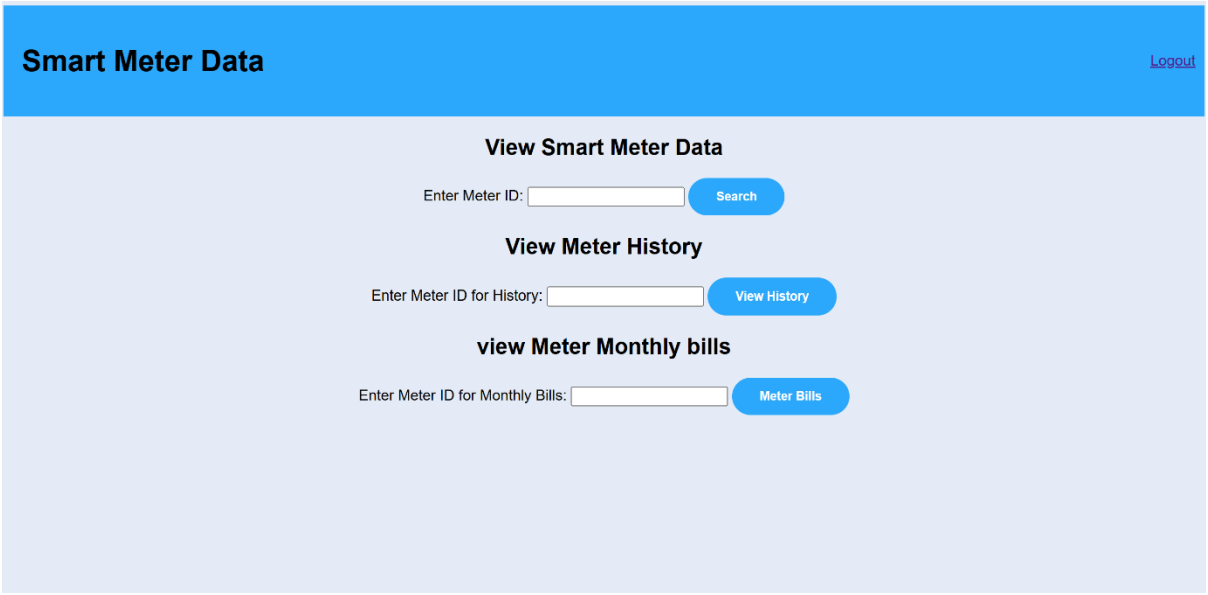

Fig. 8: Cloud Application

The project's backend is developed using Python and Flask for server-side procedures, and for managing the database SQLite3 is used, which stores billing and meter reading data. Specialized utility functions have been created to handle and present blockchain data in a user-friendly format. The project extracts smart energy meter data from the blockchain network and displays it on a user-friendly web interface. Real-time data visualization, accessing historical data, and obtaining billing information are features included in the project. as presented in Fig. 9.

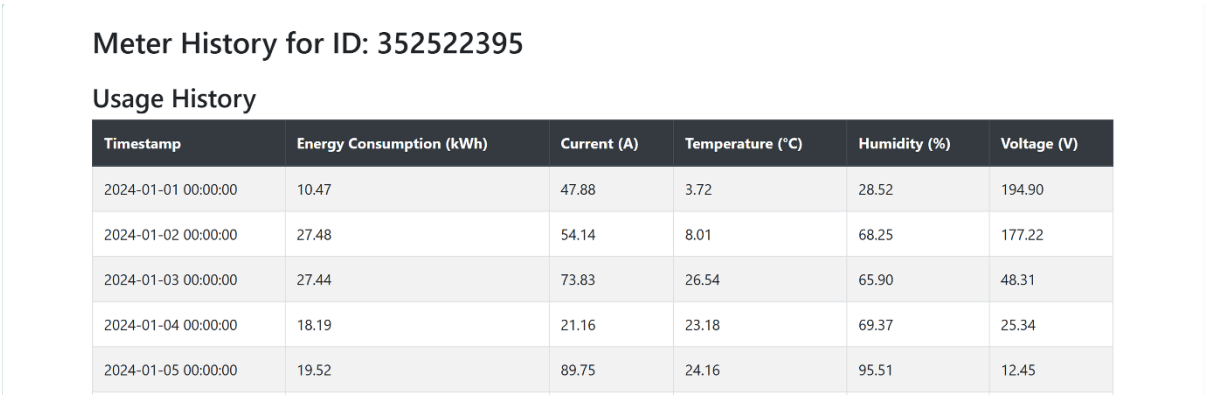

Fig. 9: Meter Data History

Monthly bills are calculated using the total daily consumption of energy for each month. The billing calculation relies on the data retrieved from the blockchain and subsequently stored in the SQLite database. The bills are calculated and subsequently inserted into the database to display them on a web portal page. As presented in Fig 10.

Monthly Bills

Meter ID: 352522395

Bill Month	Bill Amount ($)	Bill Date
January	$9.31	2024-01-31
February	$9.05	2024-02-29
March	$9.36	2024-03-31
April	$9.47	2024-04-30
May	$8.90	2024-05-31
June	$9.17	2024-06-30
July	$9.71	2024-07-31
August	$9.46	2024-08-31
September	$8.74	2024-09-30
October	$9.23	2024-10-31
November	$8.93	2024-11-30
December	$9.43	2024-12-31

Fig. 10: Meter Monthly Bills

The methodology has been implemented by deploying an application to mimic real-world situations and evaluating the scalability, security, and efficiency of the blockchain system. Illustrating the possibility of safely handling smart meter data on a decentralized network using the application, addressing issues related to transparency, data integrity, and user privacy. The application demonstrates how blockchain technology may be used in smart grids and suggests the possibility of combining IoT devices with blockchain to improve energy management systems.

5. RESULTS AND DISCUSSIONS

The blockchain securely stores data in several blocks, where the POW mechanism automates the verification of transactions. Ensuring its integrity and protection from tampering and unlawful access. The implementation of hybrid encryption provides both the integration and privacy of data during its transfer to the server (blockchain node). It offers a remedy for the vulnerabilities and ineffectiveness of conventional electrical networks. The primary objective of SealedGRID is to provide compatibility between various blockchain platforms and pre-existing energy management systems, which may result in integration complexities. The paper's methodology prioritizes a particular use case that involves collecting real-time data from IoT devices and utilizing advanced encryption techniques. This approach has the potential to provide enhanced security and efficiency.

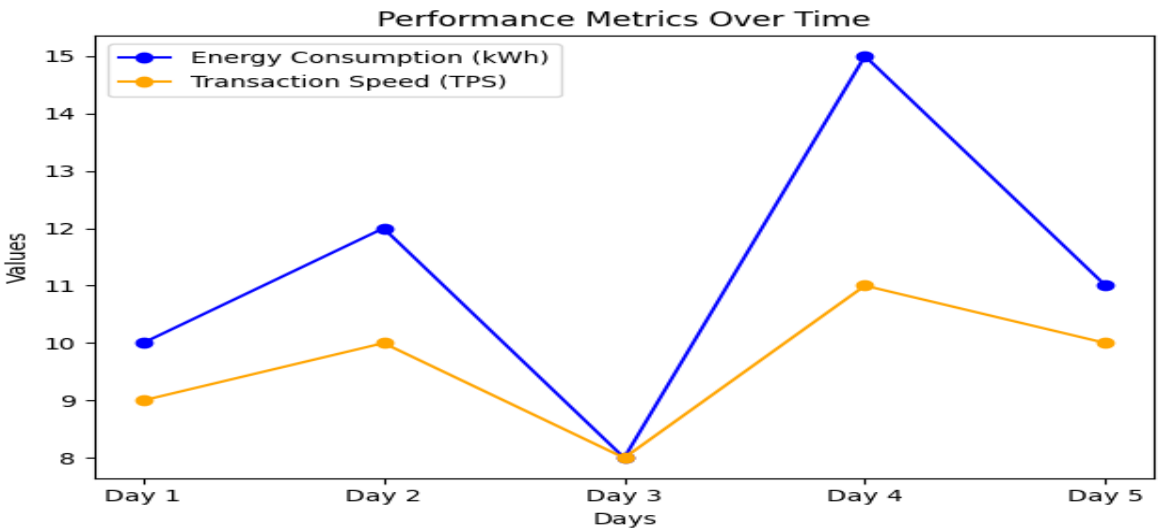

Fig. 11: Line Chart for Performance Metrics Over Time

The multitier technique emphasizes the utilization of a proof-of-efficiency mechanism to manage extensive amounts of data, which may lead to intricacy and possible susceptibilities. The paper's approach utilizes a straightforward, single-tier blockchain structure with a well-established proof-of-work technology, which could provide enhanced stability and less intricacy.

The focus of the system is on ensuring the security of data and processing it in real-time, an automated data gathering system. whereas BSEMS prioritizes the effective measurement and management of energy consumption.

The final result is a setting demonstrating the blockchain's abilities to manage transaction volumes, guarantee data integrity via encryption, and uphold a secure ledger of meter readings, when each single node in the network preserves a comprehensive record of all transactions. For monthly cost calculation utilizing daily recorded consumption data minimizes inaccuracies that may arise in conventional systems. The project illustrates a decentralized method for monitoring distributed energy resources through blockchain technology. This provides transparency, decreases fraud, and simplifies operations in smart grid ecosystems, emphasizing the security and efficiency significance in contemporary energy systems. It enhances its worth by specifically addressing the needs of the business and providing a detailed experimental setup that can be easily duplicated or expanded upon in future study, distinguishing it from more theoretical or generalized approaches.

However, limited scalability and speed could impede its ability to perform well in high-demand situations. There is a requirement for comprehensive real-world testing to confirm the effectiveness of the system and to uncover any potential problems that may not be noticeable in smaller trials.

6. CONCLUSIONS

It is essential in the altering of digital security and intelligent facilities management environment the utilization of combined cryptography method with (AMI). This paper describes a detailed approach to building a program that combines encryption, database management, and blockchain technology to securely and efficiently handle smart meter data. The system's objective is to address security issues through the utilization of decentralized networks. This proposal attempts to improve the transparency, security, and efficiency of monitoring electricity usage and billing in smart grids. While (ECC) cryptography improves data privacy. An unchangeable record that guarantees the data submitted cannot be modified, the suggested approach is suitable for use in smart city applications because of its strong data security, real-time processing, decentralization, and compatibility. Whereas maintaining privacy and allowing for data correction. Consistent monitoring, routine security evaluations, and keeping updated on current security protocols and weaknesses are essential for sustaining the system's security status in the long term.

References

[1] Y. Wang, Q. Chen, T. Hong, and C. Kang, "Review of Smart Meter Data Analytics: Applications, Methodologies, and Challenges," *IEEE Trans Smart Grid*, vol. 10, no. 3, pp. 3125–3148, May 2019, doi: 10.1109/TSG.2018.2818167.

[2] A. Althobaiti, A. Jindal, A. K. Marnerides, and U. Roedig, "Energy Theft in Smart Grids: A Survey on Data-Driven Attack Strategies and Detection Methods," *IEEE Access*, vol. 9, pp. 159291–159312, 2021, doi: 10.1109/ACCESS.2021.3131220.

[3] T. Alladi, V. Chamola, J. J. P. C. Rodrigues, and S. A. Kozlov, "Blockchain in smart grids: A review on different use cases," Nov. 02, 2019, *MDPI AG*. doi: 10.3390/s19224862.

[4] M. Güçyetmez and H. S. Farhan, "Enhancing smart grids with a new IOT and cloud-based smart meter to predict the energy consumption with time series," *Alexandria Engineering Journal*, vol. 79, pp. 44–55, Sep. 2023, doi: 10.1016/j.aej.2023.07.071.

[5] M. Biegańska, "IoT-Based Decentralized Energy Systems," Nov. 01, 2022, *MDPI*. doi: 10.3390/en15217830.

[6] A. D. John William *et al.*, "Blockchain Technologies: Smart Contracts for Consumer Electronics Data Sharing and Secure Payment," *Electronics (Switzerland)*, vol. 12, no. 1, Jan. 2023, doi: 10.3390/electronics12010208.

[7] M. Gerardi, F. Fallucchi, and F. Orecchini, “Blockchain Technology for Monitoring Energy Production for Reliable and Secure Big Data,” *Electronics (Switzerland)*, vol. 12, no. 22, Nov. 2023, doi: 10.3390/electronics12224660.

[8] T. Suman, S. Kaliappan, L. Natrayan, and D. C. Dobhal, “IoT based Social Device Network with Cloud Computing Architecture,” in *Proceedings of the 2023 2nd International Conference on Electronics and Renewable Systems, ICEARS 2023*, 2023. doi: 10.1109/ICEARS56392.2023.10085574.

[9] H. M. Al-Mashhadi and K. R. Hassan, “西南交通大学学报 DESIGN AND IMPLEMENTATION OF A SMART INTEGRATED FRAMEWORK TO MONITOR AND CONTROL THE SMART CITY USING THE INTERNET OF THINGS,” *Journal of Southwest Jiaotong University*, vol. 54, no. 6, 2019, doi: 10.35741/issn.0258-2724.54.6.61.

[10] B. N. Rao and R. Sudheer, “Energy Monitoring using IOT,” in *Proceedings of the 5th International Conference on Inventive Computation Technologies, ICICT 2020*, Institute of Electrical and Electronics Engineers Inc., Feb. 2020, pp. 868–872. doi: 10.1109/ICICT48043.2020.9112426.

[11] S. Meisami, S. Meisami, M. Yousefi, and M. R. Aref, “Combining Blockchain and IoT for Decentralized Healthcare Data Management,” *International Journal on Cryptography and Information Security*, vol. 13, no. 1, pp. 35–50, Mar. 2023, doi: 10.5121/ijcis.2023.13102.

[12] M. Joshi, S. Budhani, N. Tewari, and S. Prakash, “Analytical Review of Data Security in Cloud Computing,” in *Proceedings of 2021 2nd International Conference on Intelligent Engineering and Management, ICIEM 2021*, Institute of Electrical and Electronics Engineers Inc., Apr. 2021, pp. 362–366. doi: 10.1109/ICIEM51511.2021.9445355.

[13] M. Shahzad, J. Panneerselvam, L. Liu, and X. Zhai, “Data aggregation challenges in fog computing,” in *Proceedings - 2019 IEEE SmartWorld, Ubiquitous Intelligence and Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Internet of People and Smart City Innovation, SmartWorld/UIC/ATC/SCALCOM/IOP/SCI 2019*, Institute of Electrical and Electronics Engineers Inc., Aug. 2019, pp. 1717–1721. doi: 10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00306.

[14] V. Tayal, H. K. Meena, R. Bhakar, and C. P. Barala, “Blockchain Enabled Smart Metering Solutions: Challenges and Opportunities,” in *2022 22nd National Power Systems Conference, NPSC 2022*, 2022. doi: 10.1109/NPSC57038.2022.10069901.

[15] Q. He and H. He, “A novel method to enhance sustainable systems security in cloud computing based on the combination of encryption and data mining,” *Sustainability (Switzerland)*, vol. 13, no. 1, pp. 1–17, Jan. 2021, doi: 10.3390/su13010101.

[16] P. J. Sun, “Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions,” *IEEE Access*, vol. 7, pp. 147420–147452, 2019, doi: 10.1109/ACCESS.2019.2946185.

[17] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, “IoT privacy and security: Challenges and solutions,” *Applied Sciences (Switzerland)*, vol. 10, no. 12, Jun. 2020, doi: 10.3390/APP10124102.

[18] M. M. Ashor and H. M. Al-Mashhadi, “Enhanced Security of Iraqi National Card Based on Blockchain Technique,” *Iraqi Journal of Intelligent Computing and Informatics (IJICI)*, vol. 2, no. 2, pp. 58–67, 2023, doi: 10.52940/ijici.v2i2.26.

[19] M. S. Mohammed and A. N. Hashim, “Blockchain technology, methodology behind it, and its most extensively used encryption techniques.,” *Al-Salam Journal for Engineering and Technology*, vol. 2, no. 2, pp. 140–151, May 2023, doi: 10.55145/ajest.2023.02.02.017.

[20] S. Abolhassani Khajeh, M. Saberikamarposhti, and A. M. Rahmani, “Real-Time Scheduling in IoT Applications: A Systematic Review,” Jan. 01, 2023, *MDPI*. doi: 10.3390/s23010232.

[21] Y. Chen, H. Chen, Y. Zhang, M. Han, M. Siddula, and Z. Cai, "A survey on blockchain systems: Attacks, defenses, and privacy preservation," *High-Confidence Computing*, vol. 2, no. 2, Jun. 2022, doi: 10.1016/j.hcc.2021.100048.

[22] S. J. Basha, V. S. Veesam, T. Ammannamma, S. Navudu, and M. V. V. S. Subrahmanyam, "Security enhancement of digital signatures for blockchain using EdDSA algorithm," in *Proceedings of the 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks, ICICV 2021*, Institute of Electrical and Electronics Engineers Inc., Feb. 2021, pp. 274–278. doi: 10.1109/ICICV50876.2021.9388411.

[23] M. Saad *et al.*, "Exploring the Attack Surface of Blockchain: A Comprehensive Survey," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 3, pp. 1977–2008, Jul. 2020, doi: 10.1109/COMST.2020.2975999.

[24] R. Aswini and V. Keerthihaa, "IoT Based Smart Energy Theft Detection and Monitoring System for Smart Home," in *2020 International Conference on System, Computation, Automation and Networking, ICSCAN 2020*, Institute of Electrical and Electronics Engineers Inc., Jul. 2020. doi: 10.1109/ICSCAN49426.2020.9262411.

[25] Z. Chen, A. M. Amani, X. Yu, and M. Jalili, "Control and Optimisation of Power Grids Using Smart Meter Data: A Review," *Sensors*, vol. 23, no. 4, Feb. 2023, doi: 10.3390/s23042118.

[26] P. Subhash, G. R. Chandra, and K. Samrat Surya, "Power Trust: Energy Auditing Aware Trust-Based System to Detect Security Attacks in IoT," in *2021 International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2021*, Institute of Electrical and Electronics Engineers Inc., Mar. 2021, pp. 265–269. doi: 10.1109/WiSPNET51692.2021.9419474.

[27] M. Ghiasi, M. Dehghani, T. Niknam, A. Kavousi-Fard, P. Siano, and H. H. Alhelou, "Cyber-Attack Detection and Cyber-Security Enhancement in Smart DC-Microgrid Based on Blockchain Technology and Hilbert Huang Transform," *IEEE Access*, vol. 9, pp. 29429–29440, 2021, doi: 10.1109/ACCESS.2021.3059042.

[28] B. M. R. Amin, S. Taghizadeh, M. S. Rahman, M. J. Hossain, V. Varadharajan, and Z. Chen, "Cyber attacks in smart grid - Dynamic impacts, analyses and recommendations," *IET Cyber-Physical Systems: Theory and Applications*, vol. 5, no. 4, pp. 321–329, Dec. 2020, doi: 10.1049/iet-cps.2019.0103.

[29] A. Ö. Gür, Ş. Öksüzer, and E. Karaarslan, "Blockchain Based Metering and Billing System Proposal with Privacy Protection for the Electric Network," in *7th International Istanbul Smart Grids and Cities Congress and Fair, ICSG 2019 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., Apr. 2019, pp. 204–208. doi: 10.1109/SGCF.2019.8782375.

[30] G. Suciu *et al.*, "Securing the Smart Grid: A Blockchain-based Secure Smart Energy System," in *2019 54th International Universities Power Engineering Conference, UPEC 2019 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., Sep. 2019. doi: 10.1109/UPEC.2019.8893484.

[31] Dr. B. N. and S. S. Vinayak E, "EL DAPP – An Electrıcıty Meter Trackıng Decentralızed Applıcatıon," *Journal of Electronics and Informatics*, vol. 2, no. 1, pp. 49–71, Mar. 2020, doi: 10.36548/jei.2020.1.006.

[32] M. .S and T. Raj L, "A Secure Protocol for Smart Meters using IoT Enabled Distribution Networks and Blockchain Security Mechanism," *Journal of Ubiquitous Computing and Communication Technologies*, vol. 2, no. 1, pp. 48–58, Mar. 2020, doi: 10.36548/jucct.2020.1.006.

[33] 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," *Front Energy Res*, vol. 10, Dec. 2022, doi: 10.3389/fenrg.2022.1029113.

[34] O. Laayati, H. El Hadraoui, M. Bouzi, A. El-Alaoui, A. Kousta, and A. Chebak, "Smart Energy Management System: Blockchain-Based Smart Meters in Microgrids," in *Proceedings - 2022 IEEE 4th Global Power,*

Energy and Communication Conference, GPECOM 2022, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 580–585. doi: 10.1109/GPECOM55404.2022.9815559.

[35] M. I. Ibrahem, M. M. Badr, M. M. Fouda, M. Mahmoud, W. Alasmary, and Z. M. Fadlullah, "PMBFE: Efficient and privacy-preserving monitoring and billing using functional encryption for AMI networks," in *2020 International Symposium on Networks, Computers and Communications, ISNCC 2020*, Institute of Electrical and Electronics Engineers Inc., Oct. 2020. doi: 10.1109/ISNCC49221.2020.9297246.

[36] J. C. Olivares-Rojas, E. Reyes-Archundia, J. A. Gutierrez-Gnecchi, J. Cerda-Jacobo, and J. W. Gonzalez-Murueta, "A Novel Multitier Blockchain Architecture to Protect Data in Smart Metering Systems," *IEEE Trans Eng Manag*, vol. 67, no. 4, pp. 1271–1284, Nov. 2020, doi: 10.1109/TEM.2019.2950410.

[37] V. Vinay* and S. K. K S, "Enhancing IoT Security for Smart Energy Meter using Blockchain," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 6, pp. 506–510, Mar. 2020, doi: 10.35940/ijrte.F7410.038620.

[38] M. Singh, S. Ahmed, S. Sharma, S. Singh, and B. Yoon, "BSEMS—A Blockchain-Based Smart Energy Measurement System," *Sensors*, vol. 23, no. 19, Oct. 2023, doi: 10.3390/s23198086.

[39] Y. Guo, Z. Wan, and X. Cheng, "When blockchain meets smart grids: A comprehensive survey," *High-Confidence Computing*, vol. 2, no. 2, Jun. 2022, doi: 10.1016/j.hcc.2022.100059.

[40] L. Golightly, P. Modesti, R. Garcia, and V. Chang, "Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN," Dec. 01, 2023, *KeAi Communications Co.* doi: 10.1016/j.csa.2023.100015.

[41] A. J. Al-Musharaf, S. M. Al-Alak, and H. M. Al-Mashhadi, "Improving Blockchain Consensus Mechanism via Network Clusters," in *1st Babylon International Conference on Information Technology and Science 2021, BICITS 2021*, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 293–298. doi: 10.1109/BICITS51482.2021.9509882.

[42] A. Subashini and P. Kanaka Raju, "Hybrid AES model with elliptic curve and ID based key generation for IOT in telemedicine," *Measurement: Sensors*, vol. 28, Aug. 2023, doi: 10.1016/j.measen.2023.100824.

[43] S. Rehman, N. Talat Bajwa, M. A. Shah, A. O. Aseeri, and A. Anjum, "Hybrid aes-ecc model for the security of data over cloud storage," *Electronics (Switzerland)*, vol. 10, no. 21, Nov. 2021, doi: 10.3390/electronics10212673.

[44] R. K. Kodali and V. S. K. Gorantla, "Weather tracking system using MQTT and SQLite," in *Proceedings of the 2017 3rd International Conference on Applied and Theoretical Computing and Communication Technology, iCATccT 2017*, 2018. doi: 10.1109/ICATCCT.2017.8389134.

[45] A. A. Muslam, M. Joundy, M. Zrigui, A. Ali, J. Hazar, and M. Mabrouk, "Proposal of a Modified Hash Algorithm to Increase Blockchain Security," 2023, doi: 10.13140/RG.2.2.36352.40968.