National College of Ireland

Cybersecurity Challenges and Data Protection in Smart Grids: Providing Blockchain & Cryptographic Countermeasures

MSc Research Project
MSc. In Cyber Security

Ishaan Singh
Student ID: x20233485

School of Computing
National College of Ireland

Supervisor: Mr. Niall Heffernan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Ishaan Singh		
Student ID:	x20233485		
Programme:	Msc. In Cyber Security	**Year:**	2021-2022
Module:	Msc. Research Project		
Supervisor:	Mr. Niall Heffernan		
Submission Due Date:	19/09/2022		
Project Title:	Cybersecurity Challenges and Data Protection in Smart Grids: Providing Blockchain & Cryptographic Countermeasures		
Word Count:	6863	**Page Count:**	21

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Ishaan Singh

Date: 19/09/2022

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Cybersecurity Challenges and Data Protection in Smart Grids: Providing Blockchain & Cryptographic Countermeasures

Ishaan Singh
x20233485

Abstract

Smart grids have a higher chance of security breach because of the complex coupling between communication and electrical infrastructure. A smart grid operator will be able to manage the system more efficiently if the state estimation accuracy is improved. This paper describes cryptographic impacts in smart grids from the perspective of security objectives, requirements, and challenges. In particular, the study examined current cryptographic countermeasure research work that can help in producing security threats. Our goal is to shed light on the role of cryptographic aspects in smart grids and guide future research directions for the security of smart grids against malicious attacks. Using blockchain technology to aggregate data efficiently can reduce the risks associated with grid privacy and security. A blockchain-based communication platform is integrated with distributed state estimation in this research study. In conclusion, we will analyze the work of blockchain in distributed state estimation in detail.

1 Introduction

Today, a paradigm shift is taking place in the electric power grid. New challenges are posed to the static grid, which requires a transformation into one that is more flexible, intelligent, and modern in order to meet them. By establishing a decentralized energy distribution system, distributed renewable energy sources can be integrated in a huge way, resulting in more efficient energy use. As part of the future energy system, advanced sensing is integrated into the power system, billing is provided efficiently and effectively (Real time: 15 - 20-minute intervals). And, in addition it provides two-way communications between consumers and service providers. The platform will also facilitate a time-to-time exchange of computations and communications between the customer and the energy supplier. A working smart metering infrastructure is a key component of a smart grid. Among the many uses of this feature are implementing efficient energy distribution algorithms, dynamic pricing models, and flexible load management, among others. [1]

Smart grids have a large number of components, devices and sensors that interact in a secure or insecure channel where the transmission of data is kept private between two parties.

Additionally, it is critical to understand the real identity of both parties when making any kind of request or response. From the security perspective of smart grids, authentication and encryption are of the utmost importance. Recently, cryptographic aspects known as authentication have been used to fill security holes in the last few years to identify parties and to communicate with them. An encryption mechanism has been proposed for securely sending data between them using key agreement techniques that have been used in smart meters and utility servers. Cyber security in smart grid infrastructure refers to maintaining the core cyber security standards, namely the CIA triads which are confidentiality, integrity, and availability, as well as mitigating the cyber threats. Z. El Mrabet. et al., [4].

In addition, the decentralized smart grid system, however, is also a security, privacy, and trust nightmare due to its large number of components and complex connections, requiring new and innovative technologies to solve. Meanwhile, blockchain presents new possibilities for building decentralized systems as a promising and emerging technology. As this blockchain technology is decentralized, there is no central trusted authority needed to manage it; rather, multiple entities can store, create, and maintain a chain of blocks among themselves. In this decentralized system, any system becomes unnecessary and tough to system failures and cyber-attacks and solves many problems associated with centralized systems. Every entity can verify that chain order and data have not been tampered with. Due to its excellent properties, the blockchain is being increasingly used in non-monetary applications as well, despite the fact that it was initially introduced and populated as digital currencies. As well as digital currencies, blockchain is facilitating the development of secure, privacy-preserving, and trusted smart grids towards decentralization as well. Andoni M., et al., [5]

This paper, however, contributes a number of important findings that are not contained in the related survey papers.

- ✓ Our discussion focuses on the various aspects of privacy challenges in the smart grid and explains why addressing them is a priority.
- ✓ The purpose of this study is to provide a theoretical framework for how smart grid security requirements will be satisfied with the achievement of security objectives through an analysis of the current situation and possible research guidance on cryptography.
- ✓ In this paper, we will also see the effective side of cryptographic aspect of protecting, security and privacy from cyber threats in smart grids. On the other hand, how the countermeasure practices show the advantages and disadvantages as well as potential directions for future research in smart grid technologies.
- ✓ In order to understand why blockchain is relevant, and how blockchain can contribute to solving these challenges, we discuss the key research challenges of smart grid parts and scenarios. The opportunities for blockchain research in smart grid are discussed.
- ✓ In this paper, we also provide detailed information about our proposed solution of blockchain framework which concludes, blockchain block structure, blockchain architecture, samples of block structure, and the technologies related to BC that can

be used in smart grids. Furthermore, we identify some future research directions for integrating blockchain into the smart grid and discuss existing challenges.

The reminder of this paper is organized as follows; in **Section 2** we presented discussion about the related work on smart grids security. **Section 3** discusses the research methodology related to smart grid. **Section 4** we will be describing the design specifications, formulation and approach for the blockchain framework and cryptographic countermeasures. The implementation of the proposed solution for the research problem is explained in **Section 5**. **Section 6** evaluates the overall analysis and findings of the study. Last, **Section 7** will conclude the whole study and discusses the future work for the blockchain and cryptography countermeasures for smart grid security.

2 Related Work

2.1 Smart Grid Security with Cryptographic Countermeasures.

The advanced metering infrastructure (AMI) involves a kind of intelligent technology applied to smart grid technology to ensure service providers and users of facilities are related or correspondent to each other. AMI has a number of advantages, but it needs to be faster, low power, and require less processing time. Garg, S., et al. [2] There are four main parts to the architecture of AMI: the customer premises, the service provider, the intelligent device, the server, and the smart meter and the last is communication channel. The National Institute of Standard and Technology (NIST) identifies the six major components of a smart grid, including bulk generators, distribution and transmission systems, markets, operations, service providers, and customers. With the help of Internet networking technologies like IP technology, advanced metering components can be incorporated into smart grid components FitzPatrick, J., [3].

Smart grids can also transmit, distribute, and communicate efficiently with all the components. Using communication channels connected between smart meters, sensors, meter data management systems, advanced metering infrastructure and utility servers, the customer and service provider interact with each other. For information protection, authentication, identification, and encryption of data must be performed between each entity. Many of the cryptographic aspects of the recently proposed cryptographic mechanism served to mitigate a known cyber-attack while overcoming privacy and security concerns. Cryptography is primarily used to accommodate the cryptography aspect, while some previous works have used multiple cryptographic aspects or only one cryptographic aspect to achieve cyber security goals. We can define the effective prospects of protecting smart grid infrastructure from malicious attacks with encryption, authentication, and key agreements.

Security Goal	Attack Types
Confidentiality	Eavesdropping, MITM, Traffic Analysis, Replay, Password Pilfering, Masquerading, Sniffing, Data Injection, Forward Secrecy, Impersonates.
Integrity	Data Tempering, Message Injection, Data Modification, Wormhole, Spoofing, Phishing, Man-In-The-Middle, Time Synchronization, Insider Attack, Anonymity.
Availability	Jamming Attack, Distributed Denial of Service Attack, Low-rate Dos Attack, Spoofing Attack, Masquerading, MITM.

Figure 1: CIA (Confidentiality, Integrity, Availability) Triad Based Attacks

The CIA triad based cyber-attack mentioned above in **Figure. 1** poses a threat to smart grid components, as well as customers and service providers. All parts of a smart grid infrastructure should be protected by a cyber security solution. In a cryptography context, there are three major operations that are implemented: encryption to protect data integrity, confidentiality and authentication to ensure identity, and key agreement to ensure efficiency. Most recent solutions based on the cryptographic parameter used in smart grids have been discussed in the next section (**Table. 1)**. These include encryption intents for data protection, authentication for validating identity among the different components of smart grid, and key agreements for generating the keys of configuration and distributing them. We all know that cryptography provides privacy and security for both private and operational data.

Proposed Solutions	Research Goal	Cryptographic Aspect	Security Objectives	Description
[6]	The authors establish a stable cloud approach for big data frameworks and secure data management.	Encryption and Authentication is used, and Key Management is not used.	Confidentiality and Integrity are present but no Availability.	**Pros:** Identity between the two components has been achieved. **Cons:** - Increased communication costs. - Key management device was used as an extra hardware device.
[7]	A protocol for authentication and key agreement is proposed in order to mitigate known attacks.	Only Authentication is used, Encryption and Key Management is not used.	Confidentiality and Integrity are present but no Availability.	**Pros:** Ensured the privacy and security of smart meters. **Cons:** In order to increase security, an additional authentication system is used.
[8]	A primary goal of this author is to enhance the security of message integrity and data privacy, as well as the availability of data.	Encryption and Authentication is used, and Key Management is not used.	Confidentiality, Integrity and Availability all three are present.	**Pros:** - A proposed solution can mitigate the threat of CIA triad attack. - The smart meter and server were able to make a reliable connection.

				Cons: It will increase the computation time.
[9]	Data transmission between smart meters and utility servers can be made secure with an authentication-based scheme proposed in this study.	Encryption, Authentication and Key Management all three are used.	Confidentiality, Integrity and Availability all three are present.	**Pros:** - Authentication of the smart meter with the utility provider has been achieved. - Results from this scheme were better than those from RSA. **Cons:** Verification of session keys will take more time.
[10]	For the smart gird security, privacy and paper protection are key topics which are focused.	Encryption, Authentication and Key Management all three are used.	Confidentiality and Integrity are present but no Availability.	**Pros:** - Computation and communication cost are reduced. - Many threats are mitigated. **Cons:** Scheme is vulnerable to DoS attack.
[11]	A PKI based cryptoanalysis mechanism is proposed in order to increase security and reliability.	Authentication and Key Management are used, and Encryption is not used.	Confidentiality, Integrity and Availability all three are present.	**Pros:** - Several attacks can be mitigated. - Lightweight mechanism can be easily achieved. **Cons:** Network technology has a high dependency.

Table 2: Research Work based on Cryptographic Aspect

2.2 Smart Grid Security with Blockchain.

Essentially, blockchains are decentralized ledgers which keep records of every transaction carried out through a network from its very beginning. Each peer has a copy of the ledger, which is shared between the nodes (also known as peers) in the network. The system is secure because it uses cryptography to ensure that each block is connected to the previous one, making it resistant to malicious attacks and malpractice.

Using the help of Wireless Sensor Networks (WSNs) and the Internet of Things (IoT), smart grids are advancing technologically at an accelerated rate. Through the adoption of intelligent systems, energy production and consumption can be optimized by monitoring and communicating with each other. Advanced Metering Devices (AMI) automate smart sensor-based metering systems, reducing manpower requirements and improving accuracy. As a result, energy can be efficiently utilized by building the grid more smart. Furthermore, smart grids can facilitate the transfer of energy between local energy producers and consumers, thus enhancing the efficiency of tapping renewable sources of energy.

Producers-cum-consumers (prosumers) can gather renewable energy sources such as light of sun using the solar panels which are at rooftop and can be sold to neighboring consumers or the grid when surplus energy is available. Using renewable energy sources also promotes consumer behavior. There is a requirement for a energy management system which is decentralized due to the ever-growing energy demand and the different sources of energy. Li, Jianan et al., [12] There should be no tampering with data or loss of information between users or between users and the grid, so that the system can manage individual transactions between both. It is very demanding for utilities to approximate the state of a system when distributed resources of renewable energy whose power generation is highly flickering are integrated. A third party's requirement for energy distribution and supply is another obstacle to an efficient grid management system. This is where blockchain enters and offers an encouraging solution to some of these existing issues of the smart grid by drastically increasing the cost of operations and facilitating incorrect transactions, intentionally or otherwise. Jokar, P., et al., [14]

To get the services such as monitoring, billing, bidding and energy trading, smart grid components depend on either centralized platforms or inter-mediaries currently available in technology. The current smart grid system faces a number of challenges even though it has matured solutions and is functioning properly. In addition, we discussed previously that the smart grid facilitates the combination of a large number of electric vehicles, distributed energy resources, prosumers, and cyber-physical systems. In addition, the grid topology is the whole itself undergoing an adaptation and a shift from a centralized to a decentralized, fully automated network so the components will be able to interact more effectively. Moreover, the smart grid market is evolving from a centralized producer-governing network to a decentralized prosumers-interactive network through the utilization of EI concept. Because blockchain has the following characteristics, it is a suitable tool for facilitating this shift towards decentralized systems.; Decentralization, Scalability, Trustless but Secure, Immutability, Transparency and Auditability, Resiliency, and Secure Script Deployment Andoni M., et al., [5]. With its features as discussed above and the cutting-edge cryptographic security benefits, blockchain can be a promising substitute to conventional centralized systems in terms of improving security, privacy, and trust, as well as removing barriers to achieving a decentralized and resilient system.

AMI is an advanced metering infrastructure that uses smart meters to support automated and two-way communication between utility companies, consumers, and producers within smart grid networks. Energy use and production, as well as the status and diagnostics of advanced smart meters are recorded in greater detail than those of conventional or traditional meters. Billing, appliance control, monitoring, and troubleshooting are often carried out with the help of this data. Nevertheless, in traditional centralized storage systems or cloud computing environments, this diverse data is transferred over wide area networks. There are inherent risks associated with centralized systems, such as privacy leaks and single points of failure. Gai, K, et al., [16]

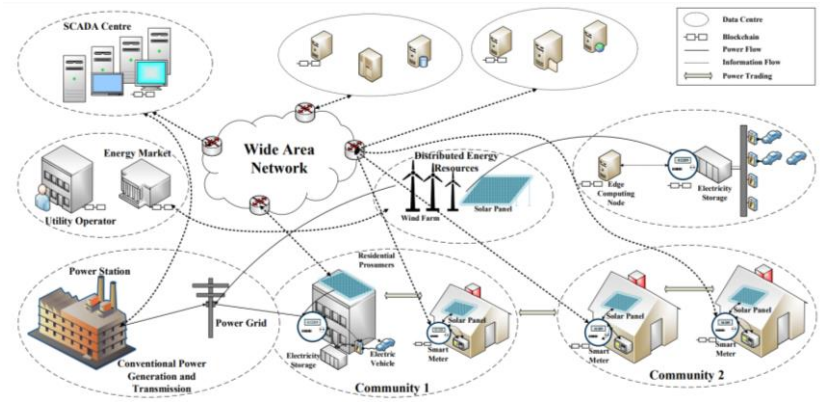

Figure 3: This is an illustration of a future smart grid based on blockchain technology.

The following section **(Table. 2)** summarizes all of the blockchain-based solutions for smart grids we have discussed. Yet, many of these solutions are still being developed or in the development stage. Based on the limitations of these solutions, we can conclude that if a blockchain-based solution is to be designed for the smart grid applications, and the following factors should be considered, namely (i) security requirements and trust levels, (ii) practical validation, (iii) scalability, privacy, security and decentralization and efficiency, (iv) energy efficiency (v) application scenarios and (vi) specific targets/needs.

Proposed Solutions	Research Goal	Practical Approach	Focused Approach
[15]	By using blockchain-based AMI, DER energy exchange can be made secure and fast.	Smart contracts and the public blockchain.	Energy applications based on transactive energy.
[16]	For smart grids, this study develops a permissioned blockchain ensures energy security and privacy (tracking and transparency of energy consumption).	Smart contracts, permissioned blockchains, voting-based consensus, pseudo names, and edge computing, consensus are some of the techniques used for group signature and covert channel authorization.	Transparency and traceability of energy consumption.
[17]	Providing energy service companies with a blockchain-based energy scheduling model that preserves privacy.	Algorithms for relaxation of Lagrange, smart contracts, and consensus-based PoS (Proof of Stake).	Information of supply and demand in Energy.
[18]	Using blockchain technology to facilitate secure energy transactions and to maintain privacy in energy pricing negotiations as a proof-of-concept is deployed.	Digital Signature Algorithm (ECDSA) with Elliptic Curve, Multi-signature, Anonymous Messaging Streams, Proof of Work.	The pricing and trading of energy are decentralized.
[19]	In order to ensure real-time data transparency between electricity companies and consumers, blockchain can be applied to smart grid monitoring.	Side-chains and smart contracts.	Smart Grid Monitoring.

Table 2: Research Work based on Blockchain for Smart Girds

In Sakurama, K., Miura, M., [20], an incentive-based, communication-based decentralized pricing scheme is presented by the authors as a mechanism for deciding the incentive signals in a smart grid technology. DR events are computed using a price signal computed from the Lagrangian multiplier using a decentralized method defined and implemented by the proposed mechanism. Despite this, data privacy remains a major drawback. In Aitzhan, N.Z., Svetinovic, [18] an energy trading platform based on blockchain is proposed called PriWatt, which enables producers and consumers to exchange energy. In this case, the DSO acts as a mediator between energy demand and production. It is assumed that the system allows dynamic price negotiation of energy, but how this is accomplished is still unclear. Cryptography and consensus algorithms (Proof-of-Work) are the fundamental components of any system based on blockchain technology.

A cyberattack that degrades such properties, like a denial-of-service (DoS) attack or false data injection (FDI). It is important to note that when a central control unit is compromised, all data can either be lost or controlled by the hackers (as happened in the recent cyberattack on Ukraine [23]). A distributed control scheme may be one of the solutions. The distributed grid, however, can also be attacked by cybercriminals, for instance attacking the control centers, the measurement units, the communication lines between the control centers and the measurement units, and the communication lines among the control centers itself (i.e. between the areas).

3 Research Methodology

3.1 Research Questions.

Over the course of this research paper, we will be analyzing and answering the following research questions;

(i) What are the security and privacy issues in smart grids?
(ii) An important question associated with today's smart grids is that how the data which is being exchanged in these smart grids is transferred and maintained and how to secure this data?
(iii) A further question that arrives is that this data is encrypted or not?
(iv) How cryptographic countermeasures can help in providing data protection for smart grid infrastructure?
(v) Does blockchain can be useful for data protection?
(vi) Can the blockchain framework be enhanced to strengthen the security in smart grids?

3.2 Review Protocol.

It is possible to follow the specific protocol of the procedures during the study. In addition, assessment of review issues, search strategy, quality assessment, data synthesis, inclusion criteria, data extraction, research collection, and dissemination plans need to be carried out. We considered only fully published English-language conferences and journals between 2010 and 2022. A review protocol involves the identification of data sources, extracting data, collecting data, and selecting research strategies.

3.3 Data Sources.

We selected research papers related to smart grids, smart grid security, cyber security challenges in smart grids, cryptography in smart grids, smart grid future, privacy issues in smart grids, blockchain, IoT, and big data to assist in answering the research questions. Articles related to the research questions which don't even address or endorse the questions had to be rejected. We use the following libraries to find published research publications:

S. No.	Libraries
1.	Google Scholar
2.	IEEE Xplore Digital Library
3.	ACM Digital Library
4.	Science Direct
5.	MDPI
6.	Elsevier
7.	Research Gate
8.	Springer Open

Table 3: Libraries for Research Publications

3.4 Search Process.

As part of the research methodology, we investigated data privacy, cryptographic countermeasures, Cyber-Security challenges, IoT and blockchain-based keyword patterns to identify any research queries related to Smart Grids (SG). To find out the following keywords, we use Boolean operators and symbols such as "AND", "OR": (data privacy OR (privacy issues in SG), (cryptographic countermeasures for SG OR (cryptographic aspect), (cyber-security challenges AND issues in SG), (block chain for SG OR (block chain technology for Smart Grids) OR (block chain with security in SG AND block chain issues within Smart Grids) OR (IoT security for Smart Grids)) OR (big data in Smart Grids) AND (requirements of blockchain in SG AND solution for SG).

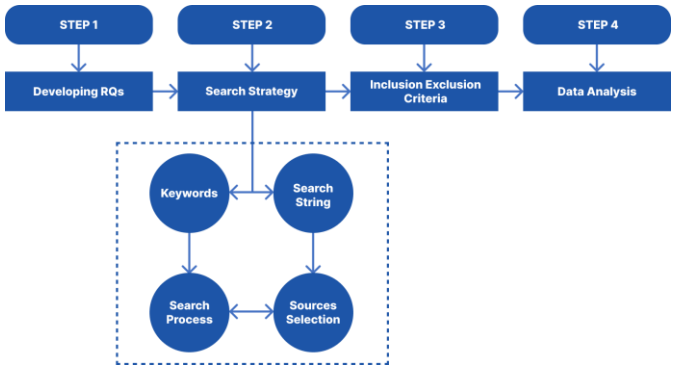

Figure 4: Overall Search Process followed for the study.

3.5 Data Selection.

Data collection refers to the process of deciding which data sources and types are appropriate and which methods will be most effective in collecting the data. In order to repeat data collection, it is necessary to select the data first. The following criteria were used to select data:

(i) Was the study published between 2010 and July 2022?
(ii) Does the research paper come from reputable/recommended data sources?
(iii) Does the paper or study mention any of the following: Smart Grids (SG)/Cryptographic Countermeasures/Data Privacy/BC/IoT/big data?
(iv) Does the research paper discuss security, requirements, or practices?

3.6 Data Extraction.

Data Extraction: We discovered almost 100 publications and websites in July 2022 after completing the search process. In addition to achieving the rejection and collection criteria, related research papers were carefully extracted as part of the search process. In total, 60 abstract studies and around 40 full-length reviews, journals and research papers were found to have preliminary results.

3.7 Implementation, Evaluation and Results.

Cyber-Security challenges and issues in Smart Grids. There are several problems and risks associated with the smart grid. Inefficient cryptographic premises and lack of identification present a variety of cyber security challenges.

(i) ***Communication***. As the smart grid integrates numerous interoperating devices, sensors, gateways, servers, monitoring tools, and it is utmost important that data privacy is maintained during service delivery, the network architecture is sophisticated in smart grids. The systems need to be highly secure against attacks and security flaws despite the decentralized nature of the smart grid setting. Blackouts, loss of performance, and serious harm can result from attacks. The reason for this is that attackers are controlling the system.
(ii) ***Trustworthy.*** Currently, customer service is not considered trustworthy because of the reachability of the power systems that influenced the decisions described by design. There are many customers who violate laws and agreements, such as deliberately damaging the smart meter for the purpose of producing duplicate reports.
(iii) ***Consumer Privacy***. Smart grid schemes must ensure customer privacy during information transmission and ensure that it is well protected and secured. There are many components in a smart grid that use unsecured channels for data transmission, making it an extremely sensitive infrastructure. In order to prevent unauthorized access to user information, it is important to protect user privacy during the transmission of information. Every day, smart meters transfer information to the power service provider's server in routine intervals, which will be protected from unauthorized access or parties.

Advanced metering infrastructure (AMI), which is a revolutionary technology, can be thought of as a type of middleware between consumers and service providers. They provide connectivity between a neighborhood network on a wide-area network and a service provider system on a known local or home area network. Several unknown nodes are included in the

network due to the inconsistent technologies used, making it very difficult to identify the source from the destination via encrypted data exchange. Additionally, the high dependency on communication creates the possibility of malicious intruders interfering with the transmission of data over the grid. A number of security vulnerabilities were raised as a result of the above issues. The purpose of this section is to discuss well-known security breaches that occur in smart grid infrastructure based on device attacks, data attacks, privacy attacks, and network attacks.

Device Attacks: This is the initial step in a sophisticated attack, in which the device is exploited and controlled.
Data Attacks: Data attack is intended to create false information and deceive the smart grid into making bad decisions by inserting, modifying, or deleting data or monitoring commands within the movement of the communication network.
Network Attacks: An attack aimed at overloading or using a smart grid's communication and computing resources as well as resulting in a pause or loss of communication.
Privacy Attacks: This attack attempts to infer or collect private information from electricity consumption data about users.

Network security, *cryptography for data security and privacy*, and *device safety* are typically the three categories of smart grid security precautions.

Cryptographic Countermeasures for Data Privacy in Smart Grids. To protect smart grid infrastructure against malicious attacks, encryption, authentication, and key agreements can be defined as effective security measures.

(i) *Encryption.* Encryption is one of the most basic and useful tools for securing information and ensuring secure communications for the entire information system. The smart grid relies on encryption systems to protect data confidentiality and integrity. Sensors, smart devices, smart meters, and network gateways that are part of the smart grid gather data through a wide span of smart grid systems. Insecure channels created an insecure environment for data collection without encryption. By using the advanced encryption standard of quantum key distribution, the author R.C. Diovu and J.T. Agee [8], proposes to enhance the security of smart grid AMI which is cloud-based in order to maintain data confidentiality, integrity, while avoiding network-based cyber-attacks.
(ii) *Authentication.* In the field of security, authentication refers to the process of proving the true identity of two objects. There are many customers in a smart grid, along with smart meters, sensors, meter data management systems, advanced metering infrastructure, and utility servers, etc. Authentication consists of three fundamentals known as Cipher text which is used as an authentication method, message authentication code (message digest) and hash code as a decryption method or an Authenticator.
(iii) *Key Management.* An important aspect of encryption and authentication is key management. In order to maintain data privacy, it represents a crucial cryptographic mechanism. In addition, cryptographic countermeasures don't only rely on authentication or encryption, but also on the key management. Having inadequate key management could lead to attackers gaining access to the smart grid's keys, even putting the whole purpose of safe communication at risk. To make a secure smart grid, key management uses a cryptographic primitive procedure definite from any other process. The author Garg, S., et al., [2], proposed a lightweight secure scheme for smart grid using elliptic curve cryptography to protect data and hash functions suggested by the authenticators to transmit data over insecure channels.

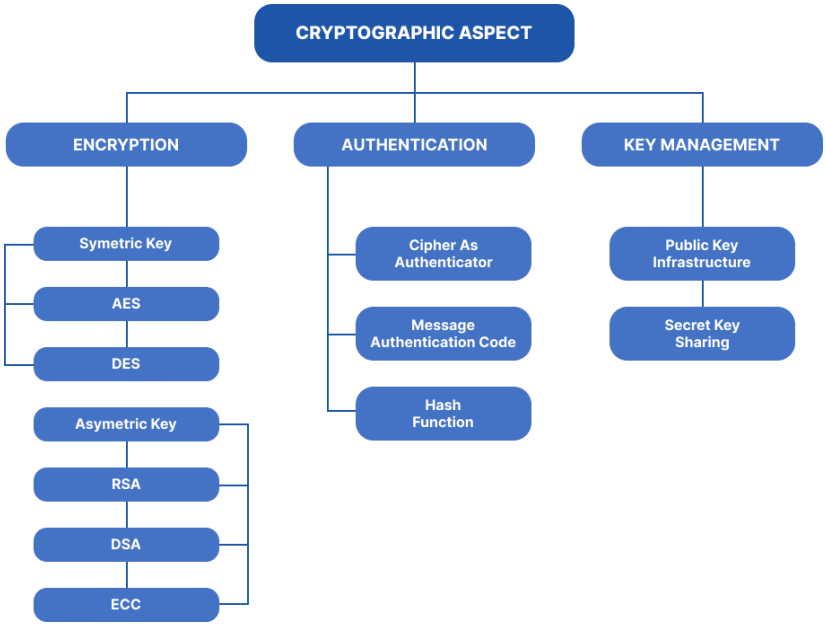

Figure 2: Cryptographic Aspects in Smart Grids.

Despite the fact that blockchain technology in no way directly guarantees privacy preservation, data privacy can be achieved using advanced cryptographic mechanisms. A number of techniques are available that protect the privacy of the involved devices, including the **Elliptic Curve Digital Signature Algorithm (ECDSA)** [9], **zero knowledge proof (ZKP)**, and **linkable ring signatures**.

Applications based on blockchain for Smart Grids. There can be many blockchain applications for the Smart Grid security, but our main focus will be on Security and Privacy Preserving Blockchain Techniques which can used for securing the data in Smart Grids and helpful in maintaining the data privacy.

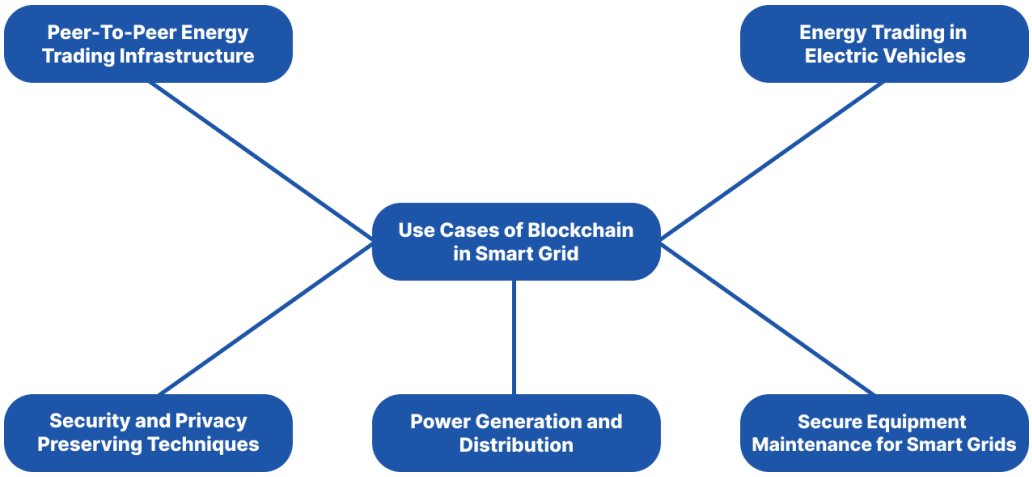

Figure 5: Applications based on blockchain for Smart Grids.

Using smart meters, utilities can get real-time information about electricity consumption at every house, which can then be used for a wide variety of purposes [21]. When malicious

entities analyze the electricity consumption profiles of the consumers or users, they are able to reveal the private information of the users [24]. Guan, Z., et al., [22] In their study, the authors developed a blockchain-based model for aggregating the data and privacy preservation. Each group used a blockchain to record the data of the users. The scheme uses a bloom filter for fast authentication, enabling users to check the legality of their user IDs in the scheme at a glance. In order to maintain privacy within the group, users use pseudonyms.

We have integrated Distributed state estimation (DSE) along with the Blockchain (BC) has been proposed and the purpose of this is to prevent attackers from exploiting such an opportunity while information is being transferred between areas.

4 Design Specification

An architecture for the aggregation of data and the preservation of privacy scheme; Users are split up into several groups/neighborhood area networks (NANs) based on their electricity consumption. The key management center (KMC) generates multiple public key pairs and private key pairs for each and every user who is using the RSA, a popular cryptography (public-key) algorithm, with the user's pseudonym as the public key. For each group, the KMC creates a bloom filter based on the pseudonyms collected, and it sends it out to all the members of that group. Zero-knowledge proof, a theoretic method of cryptography verification, can be used to verify the authenticity of the user pseudonym. Among the group's members, a mining node is selected for each time slot based on the group's average electricity consumption. Using the help of wide-area networks (WANs), the mining node accumulates the data of electricity consumed and records it on a private blockchain before sending it to the central unit. On the billing date, the billing center calculates and records the users' electricity bills. The central unit can take out electricity consumption profiles for energy planning in the real-time and dynamic pricing.

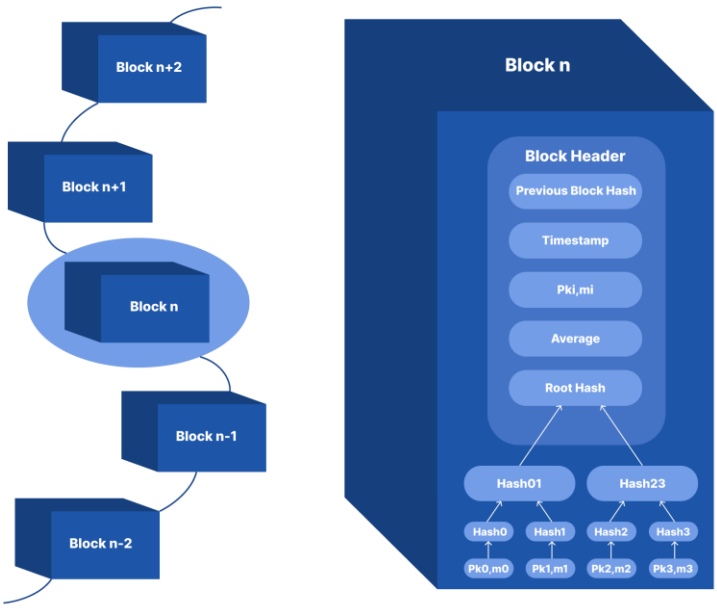

Figure 6: Block Structure for the privacy preservation scheme and data aggregation in Smart Grids

As shown in **Figure 6**, the Proof of work (PoW) consensus algorithm is used to select mining nodes among the users based on their electricity consumption data [22]. The mining nodes use a Merkle tree to record electricity consumption data. Block headers contain the hash value of the earlier block, a pseudonym, the timestamp, the Merkle tree root hash value, and the average value. Pseudonyms are generated by the KMC and represent the public keys for each user. Average is the value of average electricity consumption for each user. A timestamp indicates when each transaction takes place on the BC (blockchain) and what and when happened on the blockchain.

Ethereum Architecture; Computers (nodes) can run an instance of the Ethereum Blockchain (BC) in full nodes or in light nodes [25]. A full node can store the entire BC data. If a light node is running the Ethereum BC in a light mode, it can only serve light requests. A new block can be proposed to add to the ongoing chain by verifying all blocks and states. State roots' data in a block header can be verified by the light node, which only stores the header of the chain. When interacting with the DApp (Decentralized App), clients should run a full node themselves and interact with the network using Ethereum clients like OpenEthereum. Due to Ethereum BC's growth and storage requirements, running a full node can be challenging. The application programming interfaces (APIs) provided by third-party platforms like Infura make accessing Ethereum BC feasible. Ethereum consists of two of the main parts; the code and the database.

Gas is the fee associated with the Ethereum BC for executing each transaction. Upon adding a transaction to a block, the transaction fee is paid to the miner as a reward for using computational resources. The gas unit of Ethereum Virtual Machine (EVM) measures the difficulty of performing computations. The BC charges gas only when data is modified; accessing and reading data are not charged.

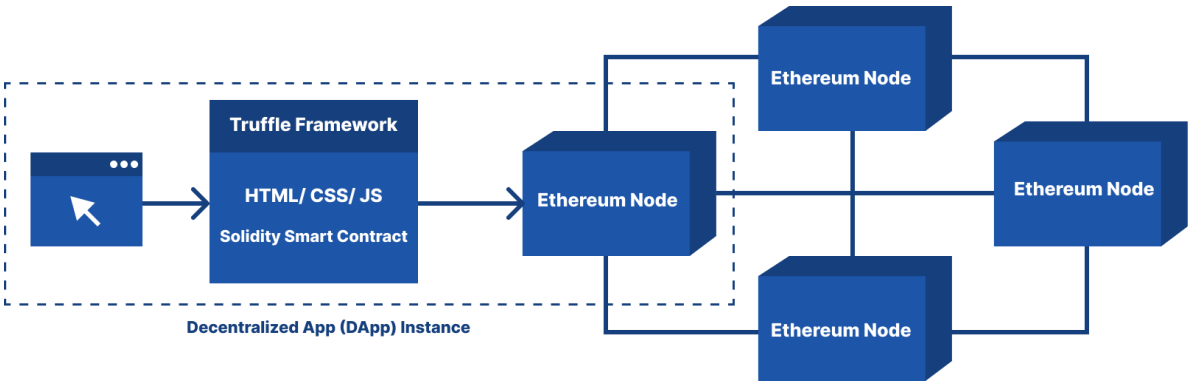

Figure 7: Overall Structure of Ethereum Network.

Data Verification; A private key should be used to sign data that represents the formation of a transaction before it can be broadcast to other nodes in the network. An imposter who signed the message without the private key can't prove that the sender is genuine without a signature. Public key infrastructure is used by BC for asymmetric cryptography. Documents like pdfs, emails, etc. are authenticated electronically with digital signatures, just like physical signatures [26]. BC nodes share their public keys with each other, and each pair of public and private keys is unique to each. An owner of a private key owns or controls the node associated with its public key, allowing them to gain access to that node's restricted activities.

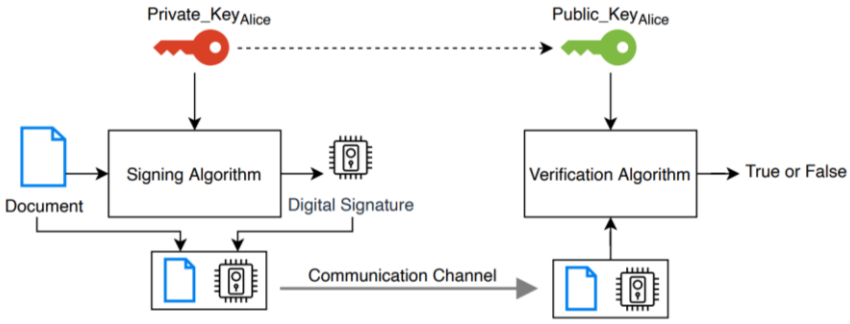

Figure 8: Using Public and Private Keys for the verification of data.

Data which is transferred is Asynchronous or Asynchronous Data Transfer; When renewable energy sources are coupled with information and communication technologies (ICT), the power system becomes a cyber-physical power system (CPPS) [27] rather than a physical one. Power grids represent the physical part, while control and computation layers represent the cyber part. Generators, transformers, transmission lines, etc., are part of the physical layer. Meanwhile, the cyber layer includes elements like sensors, communication mediums, control systems, and is responsible for computing, analyzing, and assessing the power grid.

5 Implementation

The Truffle framework and Ganache are used to deploy a Proof of concept (PoC) on the Ethereum test network. Decentralized applications and smart contracts can be built on Ethereum without any downtime or interference from third parties. The Truffle Suite combines a BC developer environment, a testing framework, and an asset management pipeline that uses the Ethereum Virtual Machine (EVM). With Ganache (a personal Blockchain), you can develop distributed applications based on Ethereum and Corda. Through Ganache and Truffle, a deterministic and safe development environment can be created for the DApp.

The DApp code is written and developed in *python programming language*. Kali Linux is used to run the python scripts. As it is easy to run these scripts in Linux command terminal and external libraries can be installed easily with simple and one-line commands. For doing experiments with Truffle, *Jupyter* Notebook is used to understand easily the data with graphs. Some extra libraries like Web3Py (There is a requirement for this library to be connected to an Ethereum node. These connections are referred to as Providers, and they can be configured in a variety of ways.) is installed and some are preinstalled like pandas (Statistical analysis and data manipulation are possible with Pandas. It is a programming library which is written in the Python programming language.) and numpy (Mathematical functions to operate on large, multidimensional arrays and matrices are available using NumPy, a library for Python that supports large, multi-dimensional arrays and matrices). Data connections samples are used for both the connections established/destablished between the GRID. Real data has been sent in these connections. Some arbitrary values have been sent among the GRIDS, by importing values from .csv files.

In the smart contract GridConnections, the connections can only be established by the Auditor. In addition, a new contract *GRIDdataCommunication* is deployed by the auditor, which keeps track of new connections and disconnections between the Grid Areas and

communicates with *GRIDconnections*. A function can only be executed by the sender *passingValues(_sender,_to,_iteration,_value*) of the data (let's say Area_1) based on the connection status between the sender and receiver (let's say Area_2).

Parameter	Type	Attack Types
_sender	address	Transaction executor and sender of data (Area computaion values)
_to	address	Recipient (Area computation values)
_iteration	unit	Incrementing round of data transfer
_value	array	Payload of data that is transfered, with each iteration different data of size transfered

Table 4: Output Evaluation

IEEE 14 bus transmission systems has been considered in this research as the GRID test case. [28]

6 Evaluation

The aim or the main focus of the proposed solution is that an application of blockchain is trying to secure the whole transmission of data in a distributed state estimation (DSV). The final result which comes out is quite good and can somehow increase the system's reliability. The data is encrypted and can only read with the help of a private key which can been seen in Ganache. We recommend do not use this private key as ganache is a public blockchain application. The connection among the GRIDs is secured as the data which is transmitted over the connection is encrypted and save from attackers.

Table 4. will help in understanding the final output which is coming after running the python script in the terminal.

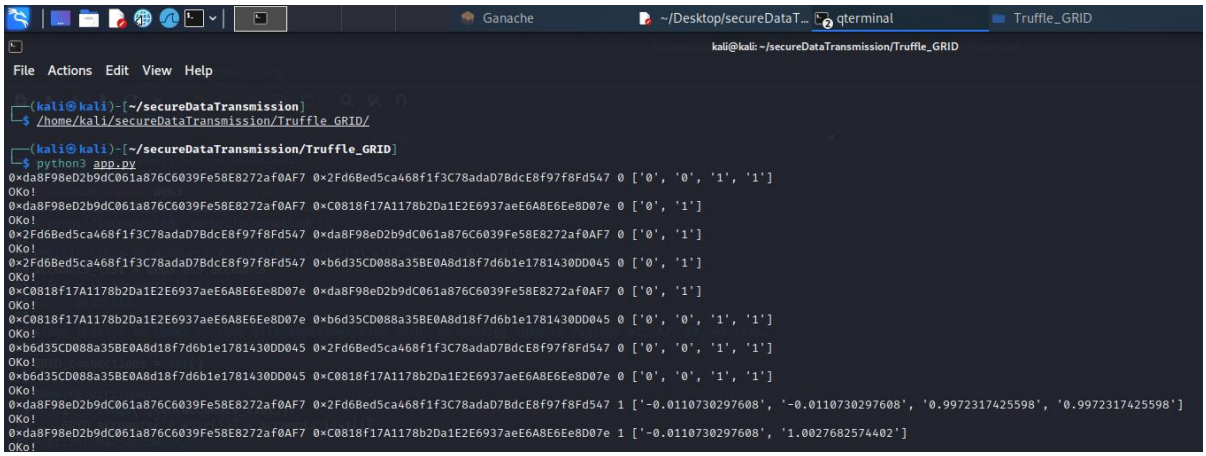

Figure 9: Final Encrypted Output.

6.1 Experiment / Case Study

Experiment has been conducted on the Jupyter Notebook for understanding the data which is being transmitted over the Smart Grid connection. In the Jupyter Notebook, first we check the amount of Gas used on deploying the whole contract and how much Gas is spent on making the transactions. After that we will check for the per transaction also. And, we will also see the gas consumption of payloads in bytes.

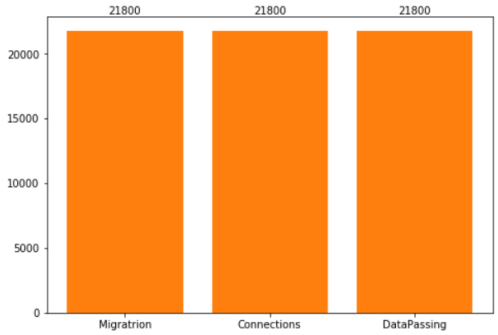

Figure 10: Gas spent on deploying contract.

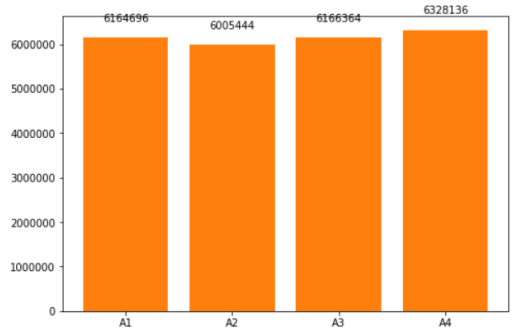

Figure 11. Gas spent on making transactions

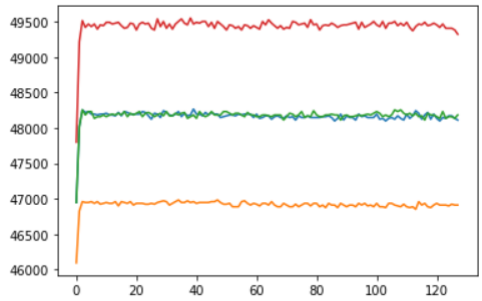

Figure 12: Gas spent on making one single transaction.

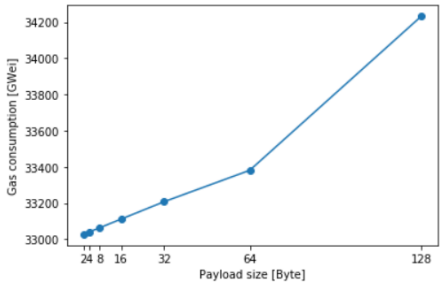

Figure 13. Gas consumption of Payloads

Now, we will see that we send the real data without sending arbitrary values what will happen with that data, we have also shared the key in this plot for making it understandable.

Figure 14. When working with real data for the experiment

6.2 Discussion

In the previous research papers, we have many solutions and techniques, some are very useful with respect to the data privacy like homomorphic algorithm but is very complex and expensive also. ECDSA is a very good and useful approach for the privacy in smart grids. Some researchers applied blockchain in smart grid technology for different use cases as shown in **Figure 5.** Our proposed solution is a combination of blockchain and cryptographic countermeasures which comes data encryption, data authentication and key agreement. As a result of the overall analysis, this method offers high security and reliability for distributed state estimation, while meeting real-world performance requirements.

In order to increase the system's reliability, we've combined distributed state estimation (DSE) with a blockchain-designed communication platform as our proposed solution for secure data transmission. The solution showed some good experimental results as discussed and the developed solution is not much complex. The final results demonstrates that the data which is sent and the received is different and encrypted and locked with the key.

The characteristics of the proposed solution are as follows;

(i) The transmitted data is much more secure than the regular data transmission which is done over smart girds, as it is encrypted and can only be seen or decrypt with the help of the private key which is unique and unknown to both the parties.

(ii) This solution is not complex and can explained to anyone easily; We have done this experiment on the public blockchain but others or companies can do this on private blockchains which is much safer from this public BC.

(iii) It will make the whole system much more secure and reliable. Attackers find it difficult to get the data from these connections because of the three cryptographic countermeasures which applied in this solution with security which comes with blockchain also.

Limitations: There also some major challenges which can be faced while implementing blockchain in smart grids; like scalability issues (sometime require heavy storage capabilities), chances of centralization, overall development and the infrastructure cost is more than some of the other solutions, Legal and Regulatory support (current legal system does not support any changes in the grid network or in the main power grid).

7 Conclusion and Future Work

The aim of the research is that to explain the cyber security challenges related to data privacy which comes in smart grids when the data is transmitted over one network to another. Attackers can perform an attack while the data is being transmitting to collect the individual's private information. We have concluded the main security challenges in this research. Next, we clarify that the data is not secured while in transit and there can be many attacks which an attacker can perform. After the we get to know that the data is not encrypted and can be easily readable or extracted. Cryptographic aspects or countermeasures plays a very important role in securing the data and maintaining the user's privacy. We can easily implement these countermeasures and secure the whole power grid. We also gain knowledge about the various characteristics of the blockchain technology and it can be very useful when implement on smart grids. Our proposed blockchain framework is very secure and reliable as

compared to other blockchain solutions because we use the cryptographic aspects in such a way that the transmitted data is encrypted and only who has a private key can decrypt this data. The purpose of this study is to develop a communication platform based on blockchain technology for secure data transfer while increasing the system's reliability in combination with distributed state estimation. By implementing the smart contracts concept, overall system security would be improved. Additionally, the method has been evaluated for robustness to latency in data transmission.

Future Work: A distributed transmission system combining state estimation with blockchain was presented. As renewable energy sources are gaining exponentially in popularity, implementing a combination of this distributed system that combines these two sources could be a future direction. Our work can be potentially enhanced by doing the changes in our architecture by making it more secure by introducing multi-signature in it. Research and the industrial community may also find the efficient analysis of BC's implementation in the power system interesting and could contribute to this study's future direction. Telemetry is a more mature, cost-effective method of grid communication today than blockchain, which is still in its beginning stage and can be done in future.

References

[1] Energy.gov, 2008. The Smart Grid: An Introduction, n.d. Office of Electricity. URL https://www.energy.gov/oe/downloads/smart-grid-introduction-0. [Accessed 31 July 2022].

[2] Garg, S., Kaur, K., Kaddoum, G., Rodrigues, J.J.P.C., Guizani, M., 2020. Secure and Lightweight Authentication Scheme for Smart Metering Infrastructure in Smart Grid. IEEE Transactions on Industrial Informatics 16, 3548–3557. https://doi.org/10.1109/TII.2019.2944880.

[3] FitzPatrick, J., 2012. n.d. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0 227. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1108r2.pdf.

[4] Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. El Ghazi, 2018. Cyber-security in smart grid: Survey and challenges, Comput. Electr. Eng., vol. 67, pp. 469–482, https://arxiv.org/abs/1809.02609.

[5] Andoni M., Robu V., Flynn D., Abram S., Geach D., Jenkins D., McCallum P., Peacock, (2018). Blockchain technology in the energy sector, A systematic review of challenges and opportunities | Elsevier Enhanced Reader, n.d. https://doi.org/10.1016/j.rser.2018.10.014.

[6] Brito, A., Fetzer, C., (2019). Köpsell, S. *et al.* Secure end-to-end processing of smart metering data. *J Cloud Comp* **8,** 19 https://doi.org/10.1186/s13677-019-0141-z.

[7] Odelu, V., Das, A.K., Wazid, M., Conti, M., 2018. Provably Secure Authenticated Key Agreement Scheme for Smart Grid. IEEE Transactions on Smart Grid 9, 1900–1910. https://doi.org/10.1109/TSG.2016.2602282.

[8] R.C. Diovu and J.T. Agee. 2019. Enhancing the security of a cloud-based smart grid AMI network by leveraging on the features of quantum key distribution. Trans. Emerg. Telecommun. Technol. 30, https://doi.org/10.1002/ett.3587.

[9] Farooq, S.M., Suhail Hussain, S.M., Ustun, T.S., 2019. Elliptic Curve Digital Signature Algorithm (ECDSA) Certificate Based Authentication Scheme for Advanced Metering Infrastructure, Innovations in Power and Advanced Computing Technologies (i-PACT). pp. 1–6. https://doi.org/10.1109/i-PACT44901.2019.8959967.

[10] Khan, AA., Kumar V., Ahmad, M., 2019. An elliptic curve cryptography based mutual authentication scheme for smart grid communications using biometric approach | Elsevier Enhanced Reader, n.d. https://doi.org/10.1016/j.jksuci.2019.04.013.

[11] Ali, W., Din, I.U., Almogren, A., Kim, B.-S., 2022. A Novel Privacy Preserving Scheme for Smart Grid-Based Home Area Networks. Sensors 22, 2269. https://doi.org/10.3390/s22062269.

[12] Li, Jianan, Zhou, Z., Wu, J., Li, Jianhua, Mumtaz, S., Lin, X., Gacanin, H., Alotaibi, S., 2019. Decentralized On-Demand Energy Supply for Blockchain in Internet of Things: A Microgrids Approach. IEEE Transactions on Computational Social Systems 6, 1395–1406. https://doi.org/10.1109/TCSS.2019.2917335.

[13] Jokar, P., Arianpoo, N. and Leung, V.C.M. (2016), A survey on security issues in smart grids. Security Comm. Networks, 9: 262-273. https://doi.org/10.1002/sec.559.

[14] Musleh, A.S., Yao, G., Muyeen, S.M., 2019. Blockchain Applications in Smart Grid–Review and Frameworks. IEEE Access 7, 86746–86757. https://doi.org/10.1109/ACCESS.2019.2920682.

[15] Mylrea, M., Gourisetti, S.N.G., 2017. Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security, in: 2017 Resilience Week (RWS). pp. 18–23. https://doi.org/10.1109/RWEEK.2017.8088642.

[16] Gai, K., Wu, Y., Zhu, L., Xu, L., Zhang, Y., 2019. Permissioned Blockchain and Edge Computing Empowered Privacy-Preserving Smart Grid Networks. IEEE Internet of Things Journal 6, 7992–8004. https://doi.org/10.1109/JIOT.2019.2904303.

[17] Tan, S., Wang, X., Jiang, C., 2019. Privacy-Preserving Energy Scheduling for ESCOs Based on Energy Blockchain Network. Energies 12, 1530. https://doi.org/10.3390/en12081530.

[18] Aitzhan, N.Z., Svetinovic, D., 2018. Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams. IEEE Transactions on Dependable and Secure Computing 15, 840–852. https://doi.org/10.1109/TDSC.2016.2616861.

[19] Gao, J., Asamoah, K., Sifah, E., Smahi, A., Xia, Q., 2018. GridMonitoring: Secured Sovereign Blockchain Based Monitoring on Smart Grid. IEEE Access PP, 1–1. https://doi.org/10.1109/ACCESS.2018.2806303.

[20] Sakurama, K., Miura, M., 2017. Communication-Based Decentralized Demand Response for Smart Microgrids. IEEE Transactions on Industrial Electronics 64, 5192–5202. https://doi.org/10.1109/TIE.2016.2631133.

[21] Avancini D.B., Rodrigues J.J., Martins S.G., Rabêlo R.A., Al-Muhtadi J., Solic P., 2019. Energy meters evolution in smart grids: A review | Elsevier Enhanced Reader, n.d. https://doi.org/10.1016/j.jclepro.2019.01.229.

[22] Guan, Z., Si, G., Zhang, X., Wu, L., Guizani, N., Du, X., Ma, Y., 2018. Privacy-Preserving and Efficient Aggregation Based on Blockchain for Power Grid Communications in Smart Communities. IEEE Communications Magazine 56, 82–88. https://doi.org/10.1109/MCOM.2018.1700401.

[23] D. U. Case, 2016, Analysis of the cyber attack on the ukrainian power grid, Electricity Information Sharing and Analysis Center (E-ISAC), vol. 388, 2016. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf.

[24] Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C., 2016. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts, in: 2016 IEEE Symposium on Security and Privacy (SP). IEEE, San Jose, CA, pp. 839–858. https://doi.org/10.1109/SP.2016.55.

[25] Nodes and clients, 2022, n.d. ethereum.org. URL https://ethereum.org/en/developers/docs/nodes-and-clients/ (Accessed 01 August 2022).

[26] Q. ShenTu and J. Yu., 2015. A Blind-Mixing Scheme for Bitcoin based on an Elliptic Curve Cryptography Blind Digital Signature Algorithm, arxiv., https://arxiv.org/ftp/arxiv/papers/1510/1510.05833.pdf.

[27] Yohanandhan, R.V., Elavarasan, R.M., Manoharan, P., Mihet-Popa, L., 2020. Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications. IEEE Access 8, 151019–151064. https://doi.org/10.1109/ACCESS.2020.3016826.

[28] R. Christie, 1993. Power systems test case archive. 14 bus power flow test case, https://digital.wpi.edu/downloads/qz20ss63v.