Technological Approach towards Smart Grid Security: A Review

[*,1]Saish Kothawade, [2]Akshat Dubey, [3]Anush Shetty, [4]Kartik Chaudhari,
and [5]Rachana Yogesh Patil

[1,2,3,4,5]Department of Computer Engineering, Pimpri Chinchwad College of Engineering,
Pune, India
[*]saish.kothawade20@pccoepune.org

Abstract: The conventional power grid is a huge and intriguing infrastructure, but it can't accommodate our changing energy usage due to external influences. Smart Grid is needed to enhance efficiency, save costs, etc. The Smart Grid is a next gen energy grid that employs bidirectional power and information flows to establish an automated energy supply network and incorporate green and renewable technology. IoT, edge computing, AI, big data, 5G, etc. are smart grid technologies. The goal of smart grid is to create a two-way flow of information and electricity to create a large, efficient power supply chain, but to achieve this, we have a lot of sensor data to manage. Sending this huge volume of data directly to the cloud will cause issues with privacy, security, high bandwidth usage, and latency. This challenge might be handled with edge computing and smart embedded devices that can make intelligent judgments. We discuss the security of the Smart Grid using cloud computing, blockchain, and a methodology for securely integrating cloud services into the smart grid.

Keywords: Smart grid, security, privacy, cloud computing, edge computing, blockchain.

1. INTRODUCTION

The term "grid" has historically been used to refer to an electrical system that supports all or more of the following four functions: power production, transmission, distribution, and control [1]. In a conventional transmission system, energy is produced in real time, taking into account seasonal and tidal variations in electrical consumption. When demand is at its highest, electricity production, transmission, and distribution systems must be able to keep up with it [2]. In order to make our 20th-century energy system smarter and capable of making its own choices, it is urgently necessary to integrate IoT devices into the grid. However, since energy is created in real-time, we need quicker and more effective data interchange in order to take use of the massive quantity of data arriving from IoT devices.

The use of information and communication technology in the Smart Grid has raised the risk of cyberattacks and unauthorized data access. As cloud computing offers a platform for data collecting and analysis, it can improve Smart Grid security by gathering data from all network areas, detecting threats, and weaknesses, and exchanging information with relevant users such as utilities, governmental bodies, and research institutions. Cloud-based monitoring technologies can increase Smart Grid visibility and detect potential faults. Smart Grid security is essential as it is a critical infrastructure. Cloud computing can help

secure the Smart Grid by offering a platform for data gathering, analysis, and network visibility.
The main goal of these initiatives is to create a sustainable society, but the centralized grid struggles with many connections. As a consequence, the smart grid topology is becoming decentralized. On the other hand, the blockchain with its excellent security traits is suitable for this, with its immutable transactions and history for auditing and resolving transactional disputes between producers and consumers.

So what is Smart Grid? It's basically a contemporary electrical power network that employs two-way digital communication to provide energy to its users [4]. To increase efficiency, lower energy usage and costs, and encourage the openness and dependability of the energy supply chain, this system provides monitoring, analytics, control, and communications across the distribution chain [4]. It integrates various components such as sensors, automation systems, energy storage devices, renewable energy sources, and intelligent devices that communicate with each other to optimize the grid's performance.

The remainder of the paper is organized as follows: Section II focuses on the literature review, subdivided into three sections, it addresses the previous work undertaken on securing the Smart Grid using cloud computing, IoT-enabled edge computing, and blockchain technology. The existing privacy and security concerns applicable to electricity grids are addressed in Section III. The table in Section IV provides a comprehensive comparative study of all the three studied technologies. Section V includes illustrations of the conclusion and future scope

2. Related Work

In this section, we mainly describe the relevant work in three different areas of smart grid security using: cloud computing-based approach, edge computing-based approach and blockchain-based approach.

2.1 Security of Smart Grid Network using Cloud Computing

Role of Cloud Computing in Smart Grid

Cloud computing is a recent IT innovation that offers numerous advantages over traditional computer processing techniques. It provides scalable processing, storage, and network capabilities to any internet-connected device, making it user-friendly and flexible. Cloud computing can help experimental smart grid initiatives overcome cost-benefit hurdles and improve data management. It consumes less power, has low operating costs, and is more adaptable and agile. It is expected to become the computing standard soon. Additionally, cloud computing improves smart grid data management by reacting to changes in data volume and effectively utilizing computational resources. It helps utilities speed up network performance and problem resolution by collecting and analyzing smart grid data to improve system management [5]. A landscape for integrating the cloud and smart grid is shown in Figure 1.

Smart grids, with their interconnectedness, are vulnerable to cyberattacks and illegal power consumption. Manipulating data is also a security concern. A secure and reliable architecture is needed for complex grid systems.

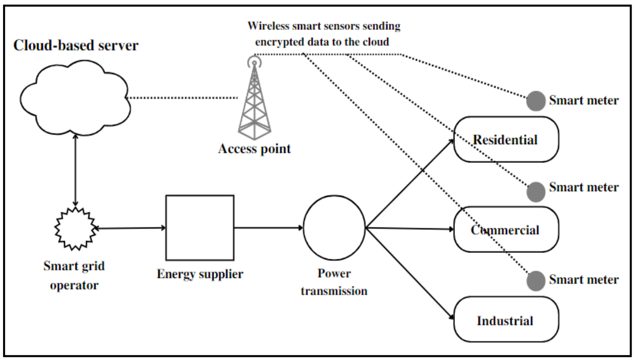

Fig. 1. Smart grid cloud integration landscape

Smart grids are more advanced than traditional ones due to intelligent sensor networks, wireless technologies, and smart meters, which complicate information security. With millions of smart meters in use, end-user protection is crucial as DoS attacks can disrupt smart grid apps. Utilities and other parties have access to users' personal data.

Various Smart Grid Security Technologies Using Cloud Computing

Electric power sector information protection solutions are insufficient for the continuously expanding complexity of security concerns [10]. In smart grid development, researchers have proposed numerous cloud-based application security techniques [10–15].

Yanliang et al.[10] present a cloud-based power transmission information safety and defence system. The authors split cloud security between server and client. Server data and outcomes drive client behaviour. Using the cloud services platform to build distributed storage, the server makes smart decisions. Customers get results through their selected web media.

Simmhan et al. [11] examined smart grid software designs deployed in different cloud environments for security and privacy vulnerabilities to address these issues. Private cloud systems manage enormous user data easily. Cloud computing can help electric utilities quickly and cheaply remove malware, improving network security and lowering maintenance costs.

Distributed verification protocols (DVPs) like Ugale et al. [12] protect cloud data storage. Cloud computing was recommended to smart grid clients to save money. Ugale et al. recommended DVP protocol implementation for smart grid energy management and storage [12].

Power cloud services for smart grid development address several security issues [13]. Cloud computing increases confidence and participation in traditional security procedures. A trusted administrator's access to sensitive data and the cloud platform provider's data centre are examples.

Maheshwari et al. [14] developed a cloud-based infrastructure for smart grid state estimation. PKI adoption overcomes failure tolerance and intrusion detection issues. Their state estimate technique maximizes cloud bandwidth for robust, safe, and failure-tolerant smart grid architecture. This platform's software handles cores similarly.

Wen et al. [15] propose a smart grid smart metering system that safeguards user data. The suggested method would transfer encrypted data from each smart meter to a cloud server. Thus, only authorized parties may access it. Data inquiries might be limited. The query is divided into two query tokens to collect the essential information while safeguarding users' identity. Table 1 displays a comparison of several smart grid cloud application security features. Cyber-physical, data security and privacy, and threat detection are some of the smart security aspects compared.

Table 1. Comparison of several smart grid cloud security features

Cloud Security Model Name	Cyber-Security	Data Security and Privacy	Threat Detection
Software platform for server and client security [10]	Yes	No	Yes
Software architecture for security and privacy [11]	Yes	Yes	Yes
Distributed verification protocol [12]	Yes	No	No
Power cloud computing [13]	No	Yes	Yes
State estimation method [14]	No	Yes	Yes
Privacy Preservation [15]	No	Yes	Yes

The authors of [10]-[15] offer a variety of security mechanisms for use in a cloud-based smart grid design; they are summarized and expanded upon in Table 2.

Table 2. Various security mechanisms for use in a cloud-based smart grid design

Cloud Security Model Name	Cloud Computing Applications	Future Scope
Electric power grid data security system [10]	Server plays role of cloud and gathers information from its clientele.	Potential for the development of cloud-based SaaS solutions to data privacy concerns raised.
SG software's data privacy concerns. [11]	Helps utilities rapidly and efficiently eliminate harmful programs.	Smart meter data can be supported with proper security and privacy regulations.

Cloud Security Model Name	Cloud Computing Applications	Future Scope
Distributed verification protocol [12]	Safety of data in cloud storage.	Prevent data leakage with a distributed verification protocol
Security technologies for cloud computing [13]	Cloud services increase the radius of trust.	Enhance QoS mechanisms and non-tech challenges via extended power cloud apps.
Real-time state estimation for smart grid [14]	Cloud-hosted system's current state estimation method.	Mission-oriented security solution assessment strategy for smart grid.
Guaranteeing Confidentiality range-query [15]	Cloud-based information privacy preserving scheme.	Incorporating a Ranked Range Query, while guaranteeing users' confidentiality.

Yangling et al. [10] proposed smart grid server-client protection. Cloud software as a service can protect client data and drive smart grid adoption. Simmhan et al. [11] created a cloud-based security and privacy framework to resist harmful software attacks. This software platform uses public cloud computing and these services need strict privacy rules.

DVP is recommended for smart grid cloud data storage security [12] as it prevents accidental and intentional data leaks. Yang et al. [13] identified many power-cloud computing security issues. Service quality improvement and technology security may be addressed together. Maheshwari et al. [14] recommend cloud applications for real-time state estimations. Wen et al. [15] present cloud range searches for data access. The recommended approach protects users' data in the cloud. Thus, the cloud-based solution helps support several enterprises on one platform while maintaining user privacy and data integrity.

2.2 Security of Smart Grid Network using Edge Computing

With the advent of smart grids, the system's complexity is increased to a new level, allowing for a larger spread of inexpensive information technology (IT), two-way communication, energy flows, and interaction with other information systems [6]. We can employ Internet of Things (IoT) devices to establish a two-way communication channel. IoT devices produce enormous volumes of data, but have finite resources. IoT device application workloads should thus be transferred to distant cloud data centers. When all jobs are relocated to the cloud, the network is heavily used. Edge computing may be used to tackle this issue.

Edge Computing for IoT-Enabled Smart Grid Network

The Internet of Things (IoT) is rapidly expanding, with numerous smart devices being connected online. This results in bandwidth shortages, privacy concerns, security issues, and slow response times with traditional cloud computing. To address these problems, a new computing paradigm called "edge" has emerged

[18]. Millions of interconnected smart devices in composite networks can provide crucial infrastructure and communication monitoring and control.

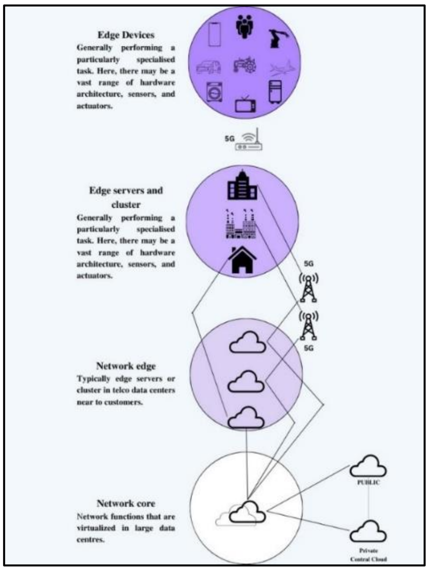
Edge Devices
Generally performing a particularly specialised task. Here, there may be a vast range of hardware architecture, sensors, and actuators.
5G
Edge servers and cluster
Generally performing a particularly specialised task. Here, there may be a vast range of hardware architecture, sensors, and actuators.
5G
5G
Network edge
Typically edge servers or cluster in telco data centers near to customers.
Network core
Network functions that are virtualized in large data centres.
PUBLIC
Private Central Cloud

Fig. 2. Edge Computing – Processing data at the edge

The processing and computation of client data closer to the data source rather than a centralized server is referred to as edge computing. The processed data can be then sent to cloud for further computation as shown in Figure 2. Essentially, edge brings computing resources, data storage, and business applications closer to the end-users, enabling them to access information more efficiently.

Edge computing offers various benefits to the smart grid, such as the following:

1) Reduced delay: When delivering power, the final few miles to end customers, power distribution and transmission networks are crucial. Edge computing can ensure low latency, enabling real-time grid frequency monitoring and proactive decision-making to reduce power factor fines.

2) Data security: Smart grids are dealing with private and sensitive user data as smart houses and meters are becoming more common. Edge computing reduces data risk by processing it locally, deciding which data needs to go to the cloud and which can stay local. This is crucial as public cloud services are often located outside the region, limiting local control over data for residents and government.

3) Lower bandwidth equals greater data collection: Renewable energy is popular because users can save or profit by selling excess electricity back to the grid. To

do this, users need to estimate their energy generation or consumption. Edge computing can help create precise forecasts and models, taking into account factors like weather and location, and bypass the expense and resource drain of sending data to the cloud. This allows for more local data acquisition, filtering, and processing, which can enrich the models. As a result, the demand for renewable energy will increase, and people may prefer to purchase it rather than produce it themselves [16].

Smart grid and 5G enabled IoT

Future smart grid infrastructure incorporating IoT devices offers numerous benefits, such as enhanced SCADA (Supervisory control and data acquisition) capabilities, advanced measurement infrastructure, and improved monitoring and management of operational assets. The digitization of power grids with 5G cellular networks provides low latency, ultra-high speed, and enhanced reliability, which can alleviate smart grid difficulties faced by energy firms. These difficulties include connecting a large number of sensors and providing universal coverage with high security and dependability. 5G technology also enables an increase in the number of distributed generation sites that distribution networks can accommodate while fulfilling the required security criteria and providing solutions to discovered risks [9]. The edge computing-based computational framework is required for the real-time processing of a sizable volume of data produced by IoT devices in smart grids. The 5G specifications provide edge computing tools for data processing, application hosting, and storage close to end devices [9].

Table 3 presents a summary of various research papers related to edge computing and 5G applications in smart grids. The advantages include improved efficiency, dependability, and fulfillment of security standards, while disadvantages include increased security risks and potential wireless security issues. Some papers do not address security concerns and associated costs. Overall, they highlight the need for robust security systems and real-time capabilities in smart grid implementation.

TABLE 3. Content, advantage and disadvantage in Research papers used in this survey.

Ref.	Content	Advantage	Disadvantage
[1]	Examines infrastructure, protection, and smart systems management.	The paper introduces G2V/V2G and microgrid.	A robust security system required to use such advanced technology.
[8]	Explores characteristics -based application scenarios of Edge.	Thorough analysis of Edge Computing applications in Smart Grid.	Geographic dispersal of edge resources increases risk of physical attack.
[18]	Key needs for putting Edge-IoT-based smart grid into practice.	Resolves the real-time requirements, heterogeneous linkage of data & intelligence.	There is no specific security given.

Ref.	Content	Advantage	Disadvantage
[9]	The security benefits of 5G are examined and analyzed in smart grids.	5G contributes to the fulfilment of security standards and the mitigation of recognized dangers.	5G implementation may introduce new wireless security issues, not resolving all existing ones.
[19]	Examines security technologies, such as PKI and trusted computing.	Distributed intelligence and broadband capabilities enhance efficiency and dependability.	By 2030, 3DES systems are expected to lose their security, according to NIST.
[20]	Edge computing framework for real-time surveillance.	The delay is minimized by 53% - 79% when compared to cloud surveillance.	No mention of associated costs with establishing this entire system.
[21]	User requests are maximized while respecting bandwidth constraints.	More requests could be fulfilled by this algorithm than by earlier works.	Issue of module deployment in edge computing with constrained resources.

2.3 Security of Smart Grid Network–Blockchain based approach

Employing Blockchain in Smart Grid

Blockchain, with its improved security features and functions, provides a secure solution in the intricate smart grid architecture. Prosumers and consumers are able to transact in a peer-to-peer environment without a centralized authority thanks to the inclusion of blockchain in smart grids.

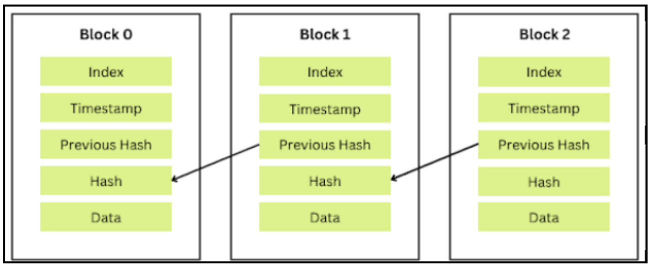

Fig. 3. Overview of Blockchain Technology

Blockchain is a blend of record-keeping concepts, digital certificates, asymmetric-key cryptography, and cryptographic hash functions. The data is handled automatically by the peer-to-peer architecture after being recorded in a public ledger, where any alteration to the ledger is duplicated in all versions throughout the network [7]. With the use of nodes, blockchain technology transmits data transactions within the grid network called a block. Each block carries the hash address information of the block preceding it, and these blocks are linked to one another as shown in Figure 3. The network would not accept any changed blocks broadcast by any participant.

How blockchain technology can start a microgrid revolution

Blockchain technology can simplify the process of monitoring and certifying renewable energy sources, which is necessary for energy grids. Currently, energy generators measure the energy they produce manually and enter the data into a spreadsheet, which is sent to a certifying organization, a process that can take several weeks. The government issues green energy certificates, which energy firms can resell on the open market after validating the data. However, connecting energy producers and consumers to trade certificates is difficult. Using blockchain can simplify the process, as electricity meters at power plants can directly and immediately record data to the blockchain. This can provide a dependable revenue flow for new energy enterprises, while homeowners with solar panels can benefit by selling their excess energy to their neighbors. Brooklyn already has a blockchain-based microgrid where neighbors can trade power, and blockchain can serve as the foundation for decentralized energy production. Blockchain technology has the potential to revolutionize the microgrid industry by streamlining certification, measurement, and sale of renewable energy [17].

Electric Vehicle Charging system using blockchain

The system comprises of three components: the utility company or grid, Electric Vehicles (EVs) and charging stations. Initially, the utility registers each EV and charging station as a user on the smart contract and adds wallet balances. When an EV requests a specific price and amount of electricity to charge, the smart contract returns an auction id and notifies nearby charging stations. The charging stations send their sealed bids, which are hashed versions of their prices, and get a bid id. After the auction closes, the smart contract selects the winner with the lowest price, and the utility takes the mean of the lowest seller's price and the EV's price. It updates the balances of the buyer and seller, and if the auction fails, the EV is notified to send another charging request [17].

Various Blockchain-based approaches for Smart Grid Security

Deep Coin Framework: The author suggests Deep Coin, a smart grid energy system that utilizes deep learning and blockchain through a recurrent neural network algorithm. The proposed model involves three stages: preprocessing, training, and testing of datasets. To sell excess energy to nearby users, Deep Coin users can use short signatures and hash functions, but this may compromise their privacy [22].

Decentralized NIST Conceptual Model: This paper outlines a theoretical framework by the National Institute of Standards and Technology for blockchain's three key characteristics: decentralization, incentive, and trust. It utilizes specific sub-domains from the NIST Smart Grid Conceptual Model, including Customers, Markets, Generation, Service providers, Operations, Transmission, and Distributions. The paper identifies primary focus areas within each domain and specifies a NIST model version for each focus area that is decentralized and blockchain-based [23].

Open Smart Grid Protocol (OSGP): This protocol produces security using encryption methods. But this comes with its fair share of limitations: Incorrect message transmitted while using stream cypher encryption, one key is used to encrypt and one key is utilized for verification. Some other frameworks like Open Smart Grid Protocol (OSGP), WEP, ISO/IEC 14908 and RC4 protocol are also proposed, but these too compromise on security [24].

DS^2 Approach: This paper gives a data-driven, smart, and safe solution for peer-to-peer trading in the local energy market. Smart contracts are used on a private Ethereum blockchain to optimize the trade procedures. DS2 protocol is implemented and evaluated for each household in the market. Smart contracts are used for transactions between prosumers and customers. The algorithms used are Power usage prediction, Demand prediction, Bipartite Graph Trading [25].

3. Privacy and Security Issues in Smart Grid Network

Implementation of smart grid technologies raises privacy and safety concerns as they are internet-connected and susceptible to cyber-attacks. These systems collect energy usage data, potentially revealing people's daily routines and behavior patterns, leading to questions about data access and usage [3]. This gives rise to questions such as who will have access to the data and how it will be utilized going forward.

In these systems, there is the potential for a wide variety of cyber and physical security problems to manifest. Among these problems are the following:

1. Data breaches: Smart grid systems gather and store enormous quantities of data, which leaves the data open to the possibility of being breached. If these data are stolen or compromised in any way, it might have huge consequences, such as a delay in service or a power outage.
2. System vulnerability: Because of the inherently complex structure of smart grid systems, there are a large number of possible failure sites. In the event that only one part of the system is hacked, the consequences may be severe enough to render the whole thing inoperable.
3. Reliance on technology: Smart grid systems place a significant amount of reliance on technology, making them potentially vulnerable to cyber assaults. It is possible that a significant disruption to the system will have an effect on the electricity grid.

4. Privacy concerns: Smart grid systems can potentially compromise personal privacy and lead to identity theft, as the information they collect may be exploited for malicious purposes.
5. Security breaches: Smart grids may result in cyber-attacks and other types of harm, including theft and property damage, as they can provide access to critical information and infrastructure.

4. Analysis of Related Work

Following our examination and analysis of the aforementioned research publications, the following is a table that provides a detailed comparison of the works in question.

TABLE 4. The evaluation of cloud-based, edge-based, blockchain-based and traditional surveillance techniques.

Parameters	**Traditional surveillance**	**Cloud-based approach**	**Edge-based approach**	**Blockchain-based approach**
Manual or automated	Manual	Automated	Automated	Automated
Surveillance frequency	Long-term periodic inspection	Real-time	Real-time	Real-time
Threat detection	Manual inspection	Approaches based on deep learning	Approaches based on deep learning	Threats not possible
Server hardware	No server required	Large storage	Medium storage	No server required
Server location	No server required	Placed in server farms by size.	Put wireless access points close together	Decentralized system
Network latency	No network	Typically, between 50 to 500 ms	Few tens of milliseconds or less	A lot more than other two approaches
Network traffic	No traffic	Large traffic	Little network traffic.	Little to no traffic
Data privacy	No worries about data leakage	Captured data may leak on the Internet.	Safer data.	Safest option for data protection
Reliability	Poor dependability	Low dependability	High dependability	Highest degree of reliableness
Price	Extremely high.	Very high.	Average price.	High one-time costs

5. CONCLUSION & FUTURE SCOPE

We studied different research papers on Security of smart grid network using three approaches: cloud computing-based, edge computing-based and blockchain-based. We mentioned their research findings in this paper. Despite cloud computing's limitations, it's expected to enhance smart grid pricing, computation, data management, power management, and security monitoring as it is superior to conventional technologies. Even though the use of edge computing in smart grids is at an early stage, it is a promising one for tackling challenges, especially for energy management and improving sustainability. Whereas the Blockchain approach with its distinct features like decentralized structure, traceability and resilience is one of the most reliable techniques to overcome grid security related issues. Based on the related work, the privacy and security issues in smart grid network are identified and the comparative study of all three approaches is done.

Going forward, a three-layer smart grid architecture can be designed consisting of cloud, edge and blockchain for transmission of smart meter data and peer to peer energy trading while applying appropriate security protocols on it.

6. References

1. X. Fang, S. Misra, G. Xue and D. Yang, "Smart Grid — The New and Improved Power Grid: A Survey," in IEEE Communications Surveys & Tutorials, vol. 14, no. 4, pp. 944-980, Fourth Quarter 2012, doi: 10.1109/SURV.2011.101911.00087.
2. Alternative Fuels Data Center: Electricity Production and Distribution. afdc.energy.gov/fuels/electricity_production.html.
3. Boroojeni, K. G., Amini, M. H., & Iyengar, S. S. (2016). Overview of the Security and Privacy Issues in Smart Grids. Smart Grids: Security and Privacy Issues, 1–16. doi:10.1007/978-3-319-45050-6_1
4. Techopedia. “Smart Grid.” Techopedia.com, 26 Jan. 2017, www.techopedia.com/definition/692/smart-grid.
5. Amir-Hamed Mohsenian-Rad and Alberto Leon-Garcia “Coordination of Cloud Computing and Smart Power Grids”
6. Palensky, Peter and Kupzog, Friederich, Smart Grids (October 2013). Annual Review of Environment and Resources, Vol. 38, pp. 201-226, 2013, Available at SSRN: https://ssrn.com/abstract=2343668 or http://dx.doi.org/10.1146/annurev-environ-031312-102947
7. What is blockchain and how does it work? Synopsys. (n.d.). Retrieved November 24, 2022, from https://www.synopsys.com/glossary/what-is-blockchain.html
8. Cheng Feng, Yi Wang, Qixin Chen, Yi Ding, Goran Strbac, Chongqing Kang, "Smart grid encounters edge computing: opportunities and applications",Advances in Applied Energy,Volume1,2021,100006,ISSN26667924,https://doi.org/10.1016/j.adapen.2020.100006.
9. Borgaonkar, R, Anne Tøndel, I, Zenebe Degefa, M, Gilje Jaatun, M. Improving smart grid security through 5G enabled IoT and edge computing. Concurrency Computat Pract Exper. 2021; 33:e6466. https://doi.org/10.1002/cpe.6466

10. W. Yanliang, D. Song, L. Wei-Min, Z. Tao, and Y. Yong, “Research of electric power information security protection on cloud security,” in Proc. of IEEE POWERCON, 2010, pp. 1–6.
11. Y. Simmhan, A. Kumbhare, B. Cao, and V. Prasanna, “An Analysis of Security and Privacy Issues in Smart Grid Software Architectures on Clouds,” in Proc. of IEEE Intl. Conf. on CLOUD, 2011, pp. 582–589.
12. B. Ugale, P. Soni, T. Pema, and A. Patil, “Role of cloud computing for smart grid of India and its cyber security,” in Proc. of IEEE NUiCONE, 2011, pp. 1–5.
13. Y. Yang, L. Wu, and W. Hu, “Security architecture and key technologies for power cloud computing,” in Proc. of IEEE Intl. Conf. on TMEE, 2011, pp. 1717–1720.
14. K. Maheshwari, M. Lim, L. Wang, K. Birman, and R. van Renesse, “Toward a reliable, secure and fault tolerant smart grid state estimation in the cloud,” in Proc. of IEEE PES on ISGT, 2013, pp. 1–6.
15. M. Wen, R. Lu, K. Zhang, J. Lei, X. Liang, and X. Shen, “PaRQ: A Privacy-Preserving Range Query Scheme Over Encrypted Metering Data for Smart Grid,” IEEE Trans. on Emerging Topics in Computing, vol. 1, no. 1, pp. 178 – 191, June 2013.
16. STL Partners. “How Can Smart Grids Benefit From Edge Computing?” STL Partners, 18 Feb. 2022, stlpartners.com/articles/edge-computing/smart-grids-edge-computing.
17. Erturk, E., Lopez, D., & Yu, W. Y. (2020). Benefits and Risks of Using Blockchain in Smart Energy: A Literature Review. Contemporary Management Research, 15(3), 205-225. https://doi.org/10.7903/cmr.19650
18. M. Yasir Mehmood, Ammar Oad, Muhammad Abrar, Hafiz Mudassir Munir, Syed Faraz Hasan, H. Abd ul Muqeet, Noorbakhsh Amiri Golilarz, "Edge Computing for IoT-Enabled Smart Grid", Security and Communication Networks, vol. 2021, Article ID 5524025, 16 pages, 2021. https://doi.org/10.1155/2021/5524025
19. A. R. Metke and R. L. Ekl, "Security Technology for Smart Grid Networks," in IEEE Transactions on Smart Grid, vol. 1, no. 1, pp. 99-107, June 2010, doi: 10.1109/TSG.2010.2046347.
20. Y. Huang, Y. Lu, F. Wang, X. Fan, J. Liu and V. C. M. Leung, "An Edge Computing Framework for Real-Time monitoring in Smart Grid," 2018 IEEE International Conference on Industrial Internet (ICII), 2018, pp. 99-108, doi: 10.1109/ICII.2018.00019.
21. J. -P. Sheu, Y. -C. Pu, R. B. Jagadeesha and Y. -C. Chang, "An efficient module deployment algorithm in edge computing," 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), 2018, pp.208-213, doi: 10.1109/WCNCW.2018.8369032
22. M. A. Ferrag and L. Maglaras, "DeepCoin: A Novel Deep Learning and Blockchain-Based Energy Exchange Framework for Smart Grids," in IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1285-1297, Nov. 2020, doi: 10.1109/TEM.2019.2922936.
23. A. Aderibole et al., "Blockchain Technology for Smart Grids: Decentralized NIST Conceptual Model," in IEEE Access, vol. 8, pp. 43177-43190, 2020, doi: 10.1109/ACCESS.2020.2977149.
24. Aldabbagh, Ghadah & Bamasag, Omaimah & Almasari, Lola & Alsaidalani, Rabab & Redwan, Afnan & Alsaggaf, Amaal. (2021). Blockchain for Securing Smart Grids. International Journal of Distributed Sensor Networks. 21. 255. 10.22937/IJCSNS.2021.21.4.31.
25. Z. Zeng, M. Dong, W. Miao, M. Zhang and H. Tang, "A Data-Driven Approach for Blockchain-Based Smart Grid System," in IEEE Access, vol. 9, pp. 70061-70070, 2021, doi: 10.1109/ACCESS.2021.3076746.