



Paper Type: Original Article

Secure IoT based Cloud Computing for Smart Grid Application

Simran Rath* 

School of Computer Engineering, KIIT (Deemed to Be) University, Bhubaneswar -751024, Odisha, India;
simranrath3003@gmail.com.

Citation:

Received: 29 March 2024

Revised: 12 June 2024

Accepted: 2 August 2024

Rath, S. (2024). Secure IoT based cloud computing for smart grid application. *Smart internet of things*, 1(2), 128-138.


Abstract

The integration of secure Internet of Things (IoT) cloud services within Smart Grid (SG) applications is critical for safeguarding energy management systems against emerging cyber threats. As the reliance on connected devices increases, the security vulnerabilities also escalate, potentially compromising data integrity and system reliability. This paper proposes a robust security framework designed specifically for IoT cloud services in SGs, incorporating advanced encryption, role-based access control, and real-time anomaly detection. We evaluated the framework's effectiveness through simulations that modeled various attack scenarios, yielding a decrease in data breach incidents and an improvement in response times to unauthorized access attempts. These results underscore the framework's potential to bolster the security posture of SG systems significantly. By addressing the unique challenges posed by IoT integrations, our research paves the way for more resilient energy management solutions, contributing to the advancement of security protocols that can be universally applied across IoT applications.

Keywords: Secure IoT services, Smart grid applications, Cybersecurity framework, Data integrity.

1 | Introduction

The Internet of Things (IoT) is a significantly growing technology. IoT connects diverse smart devices that perform distributed sensing tasks to communicate with other devices or central servers and repositories and exchange data over the networks, enabling automation and efficient real-time monitoring [1]. It has received importance in research areas. *Fig. 1* shows different applications of IoT in the real world.

 Corresponding Author: simranrath3003@gmail.com



Licensee System Analytics. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>).

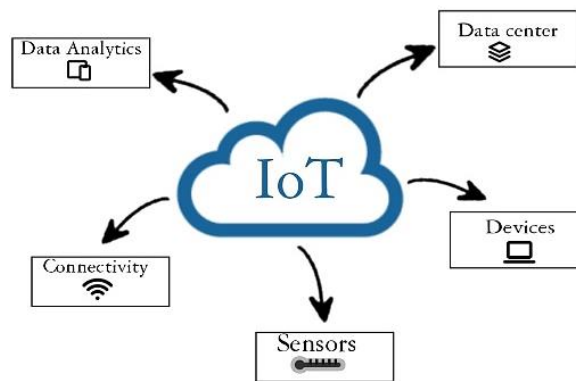


Fig. 1. Shows various applications of IoT.

A Smart Grid (SG) is an electrical grid with communications and information technology. It has overcome various challenges faced by traditional electric grid technology [2]. With ICT (information and communications technology) consumer's electricity consumption behaviour is automatically collected. This is in terms of increased reliability, sustainability of energy, and efficiency due to smart electricity transmission and efficient smart electricity networks that utilize cutting-edge technology. SGs are an intricate setup consisting of communication networks, sensors, and data analytics to enhance distribution, generation, and electricity consumption [3]. SGs can convert consumers into energy manufacturers through hydropower, solar energy, wind turbines, and additional sources of energy.

Smart meters IoT have gained reliability among people for smarter energy management at their homes, and companies for energy efficiency [4]. SG technology functions using a bidirectional communication model, allowing smooth interaction among different components. Real-time data collection is achieved through the coordination of IoT devices and sensors throughout grid infrastructure. Analysis of this information is then done to streamline energy flow, detection of failures, and response to evolving requirements in a dynamic way. Many electricity providers have already upgraded or incorporated SG technology into their current grid [2]. It works by tracking energy usage and enhancing efficient operations to control power systems by electric utilities. When energy consumption peaks, signals are transmitted to customers to lower their energy usage, helping to balance the energy load. The control center monitors the complete power supply system and protective devices to ensure the security of the load-balancing system during communication. Cloud Computing (CC), which provides resources as services, is used to communicate between power supply companies, power plants and substations [5]. The reliability, robustness, and security of this communication are increased through built-in redundancy.

In a standard Smart Grid-IoT network setup, multiple smart devices are connected to a smart meter. The meter tracks the energy usage of each device. It transmits this information to a central aggregator that is mostly an honest entity and ensures the user's privacy the smart meter readings are sent in encrypted form. The aggregator gathers the encrypted readings before delivering them which ensures privacy as well as saves time [6].

Recently, there have been developments in cloud-based SG systems, in which smart meters and fog devices from different domains send consumption data to the cloud through a central cloud hub. SG requires real-time data processing, and, in such scenarios, Fog computing is advantageous because it considerably enhances resilience, reliability, and efficiency. SGs analyze large amounts of real-time data by placing computing resources near sensors and meters. This facilitates quick decision-making and caters to changing needs with quicker response. For instance, analysis of power usage patterns, detection of anomalies, and grid operations optimization is done by fog nodes at substations. This strengthens grid security and reduces the load on network bandwidth [7]. Data consolidation is another technique that integrates summarization and combination of multiple data packets into a single larger packet for transmission that, in terms decreases the

number of packets sent over the network, enhancing the network's overall efficiency and saving bandwidth. When data is consolidated, it reduces redundant information and minimizes the overhead linked to packet transmission, improving data transfer and boosting network performance [8].

Additionally, potential interference or tampering of data packets is reduced, improving data security through data consolidation. SG has recently implemented fog computing for efficient data consolidation. In the SG-IoT environment, there are several well-known groups. First, information from smart meters is uploaded to fog devices in an acyclic or cyclic manner before transmitting to cloud servers, and this data is collected through static nodes and sinks that monitor power consumption in smart homes. Second, there are mobile sensor nodes linked to static sinks, which is similar to delivery drones equipped with sensors flying around a city. Due mobility of sensor nodes and sinks that are deployed globally for monitoring poses a significant challenge in determining optimal pathways where data consumption consolidation arises at fixed-location fog devices [6]. This information has the potential to be utilized for invoicing, making predictions based on data, and estimating power requirements. However, there are also privacy concerns. Sending this data to the cloud may cause considerable delays in response time, especially when dealing with a high volume of smart meters [9]. This could potentially overload the cloud's ability to process requests efficiently. Transmitting large amounts of data from each smart meter can result in transmission network delays and overhead. To address these challenges, a model based on encryption has been developed for SGs. This model utilizes fog computing to partly offload the storage and processing capabilities of the cloud to terminal devices. Data from smart meters can be sent in acyclic format in compressed form to reduce transmission obstacles [10]. Smart meters condense data for transmission, whereas fog devices use cloud-fog techniques to centralize data. For effective data consolidation, built-in data centralization is crucial which uses fog devices for efficient communication, processing, and storage in comparison to traditional methods depending on a "consolidator" for data centralization and storage.

2 | Literature Review

Various research studies have examined how SG applications can leverage CC to improve their reliability and efficiency. For instance, Kumar et al. [11] investigated how CC can optimize a SG's Demand Response (DR). This was achieved by using a scalable and flexible model of cloud virtual machines to evaluate resource availability for on-demand usage and to relinquish resources when idle. Moreover, cloud virtual machines were used to introduce redundancy for critical SG applications to duplicate computations and replicate data by the addition of extra virtual machines. In the study conducted by Rusitschka et al. [12], they introduced an alternative CC model designed for the real-time extraction of data and simultaneous processing for SG applications. In a different study carried out by Bhowmick et al. [13] for a SG condition monitoring application, it was found that CC offers effective and protected storage management. Moreover, CC presents numerous other benefits to a SG concerning cost-effectiveness and expandability. Kim et al. [14] proposed a DR framework based on customer communication, which aims to deliver rapid responses to customers by facilitating direct interaction between consumers and utilities.

Several studies have been conducted on grid-aware CC routing algorithms to address service request routing problems. Mohsenian-Rad and Leon-Garcia [15], Fayyaz and Nazir [16], and Mishra et al. [17] have focused on combining SG applications with CC to address security and reliability issues. Additionally, there are products in the market that implement SG applications using CC, such as Hohm, Microsoft's energy management tool, which is hosted on a cloud platform and designed for use in special residential buildings [18]. Hohm provides proprietary power-saving suggestions [18]. It allowed for the scalable monitoring of consumers' energy usage. Several other applications are also available for testing and observing the performance of CC in SG applications [19]–[21], with some already in use and others still under research. When integrating Cloud-IoT with SGs, a variety of techniques are used to improve security and encryption. Fog computing improves SG systems by providing a decentralized approach for securely consolidating data. It facilitates efficient communication and privacy protection through encryption, addressing issues posed by large IoT systems.

On the other hand, edge computing deals with the management of extensive data in SGs by enabling real-time data processing and decision-making closer to data sources. This enhances predictive capabilities and economic analysis through advanced algorithms such as LSTM and GAN. The use of Blockchain technology [22] could completely transform DR in SGs by improving efficiency, security, and consumer involvement while addressing issues related to scalability, interoperability, and regulatory complexities. Homomorphic Encryption [23], which utilizes the Paillier cryptosystem, can enhance the security of SGs by enabling computations on encrypted data, thus ensuring data privacy and non-repudiation and reducing cyber threats in interconnected power systems. Finally, Multi-Factor Authentication (MFA) [24] can improve data security and user privacy in SGs by requiring multiple verification methods, such as biometrics, to ensure that only authorized users can access sensitive information. By using the Puzzle Optimization Algorithm and Elliptic Curve Cryptography, this method helps reduce the chances of data leakage and unauthorized access, ultimately enhancing the security of power grid communication. These strategies collectively contribute to fortifying the security measures of SG applications.

Table 1. List of techniques for improving IoT-SG.

S/N	Technique	Description	Security Solution
1	Fog computing	Cloud capabilities extended closure to the edge for local data processing.	Reduces bandwidth, latency and security is enhanced through encryption.
2	Blockchain technology	Decentralised system ensures secure and tamper-proof transactions.	Enhances security by device authentication and data integration.
3	Data encryption	Data converted to coded format to prevent unauthorized access.	End-to-end encryption is provided.
4	Multi-Factor Authentication (MFA)	Multiple layers of verification for ensuring secure access	Combines passwords with biometrics or one-time code.
5	Intrusion detection system	Network traffic monitoring for suspicious activities	Identification and mitigation of potential security threats.

This paper is organized as follows. Section 2 provides a literature review of already developed techniques for secure SGs. In Section 3, the SG architectures are presented. In Section 4, CC was integrated with the SG to overcome these security concerns presented. In Section 5, Encryption-based secure-preserved mechanism for SGs. Finally, this paper is concluded in Section 6.

3 | Proposed Work

3.1 | Smart Grid Infrastructure

The SG started advancing with the onset of the distribution system of electrical networks by the time-varying requirements needed like control, monitoring, prices, and services of transmission and distribution of electrical power [25]. SG helps enhance the performance of the electric grid and reliability. Therefore, according to the Strategic Deployment Document for Europe Electricity Networks of the Future, a SG integrates the actions of all stakeholders' generators and consumers and supplies electricity with efficiency, sustainability, economically and securely [26]. The European Technology Platform is researching on preparation of a SG Policy that can overcome many challenges in the current electricity supply in terms of DR support, reliability, flexibility, efficiency, load adjustment, peak power cut, permanency and market supply.

3.1.1 | Reliability

SG systems success relies on customer needs, measured by reliability that ensures error-free continuous power supply. SGs can detect faults and enable self-healing. It also overcomes conventional grid shortcomings by remote monitoring of hybrid generation, storing and estimating service reliability and grid management, and

advanced communication. For these technologies, Dynamic Stochastic Optimal Power Flow (DSOPF) is used to optimize power flow [27].

3.1.2 | Security

There are security challenges in SG evolution due to increased automation and remote monitoring where cybersecurity is a critical issue due to vulnerabilities to cyber-attacks. Suleiman et al. proposed identifying weaknesses using SG Systems Threat Analysis and Security Threat Model. Eusufzai et al. addressed cyber-physical security issues for Wide-Area Monitoring against coordinated attacks. Ongoing research includes privacy-preserving smart metering, Ortho code privacy mechanisms, and Security Threat Models to overcome security barriers [28].

4 | Cloud Computing Was Integrated with the Smart Grid to Overcome These Security Concerns

CC provides resources as a service over a network. It includes IaaS, PaaS and DaaS. It reduces cost and complexity and allows computations and resource sharing over the internet [29]. CC's Enterprise Data Center shifts resources to meet application needs, including security, network devices, and storage systems. Services are distributed across numerous computers, enabling easy access for systems like SGs. CC enhances SG scalability, efficiency, and security and provides real-time responses, self-healing, and reliable communication through multi-homing.

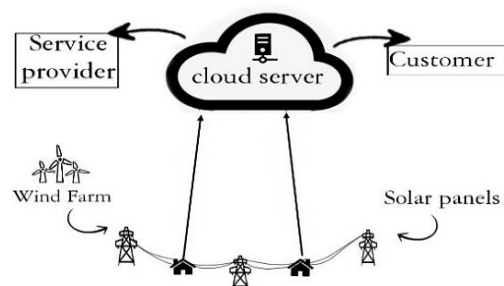


Fig. 2. Integration of cloud with smart grid.

4.1 | How CC Helps Improve Smart Grids

CC helps improve SGs by its agility which helps in reconstructing SG technology infrastructure and also by providing a communication medium between machines and cloud software via Application Programming Interfaces (APIs) [24]. The public cloud delivery system helps in lowering costs. Device and location independence maintenance and virtualization enabling flexible resource sharing as well as multitenancy are some benefits along with disaster recovery capabilities that ensure reliability. System performance is enhanced by web services and preventing connection losses. CC is secure with automatic management of cloud services, which provides easier and better protection against attacks. However, there are still existing challenges faced in CC integration with SGs [30].

4.2 | Challenges

- I. Data location: business enterprises do not know the cloud server location that carries out the storage and processing of SG applications, which becomes a critical issue in meeting the requirements of SG's data management. Therefore, specifying the data position by Cloud Service Providers is vital for the security of SG applications [31].

- II. Data aggregation: the security and scalability of multiuser applications in CSIs are an open issue for enterprises because CC enables the model to access the application through location location-independent resource pool. Therefore, enhancing security through methods such as data encryption algorithms must be applied to CSPs for reliability and confidentiality in SG applications [32].
- III. Inadequate security policies: potential disagreements between utilities in the SG sector due to some cloud service providers having less strict security policies than others [33]. To address this issue, utilities can establish service-level agreements with each other to ensure that SG applications meet the necessary security standards. In cases where commercial documents containing stored data in the cloud are involved, utilities may incur significant charges from cloud service providers after the service level agreement expires.
- IV. Dependence of CSP's Application Programming Interfaces (APIs): the implementation of numerous CC applications is carried out by Cloud Service Providers and is designed to work with specific utility APIs [34]. This makes it challenging and time-consuming to transfer SG services in CC from one CSP to another.
- V. Compatibility: CC is not meeting the necessary audit requirements, which is a significant obstacle for CC to fulfill SG auditing compliance standards. CC faces several challenges related to data location, ineffective security policies, and other factors, making it hard for CC to align with auditing requirements, including privacy regulations [35].
- VI. Redundant data management and disaster recovery: the primary concern for SG utilities in emergencies is data recovery, as CC distributes data across multiple servers in various geographic locations. Therefore, CC cannot guarantee sufficient reliability for SG applications when data is not readily accessible. Currently, SG Utilities can locate and access its data in the event of a disaster recovery [36]. However, in the CC system, CSPs can delegate benefits, services, and recovery processes to other parties, leading to complexity when the main CSP does not store data.

To address this, IoT was integrated with CC in SG applications. The use of IoT technology allows for effective and dependable communication with SGs. It improves customer satisfaction and effectiveness by enabling adaptable interactions with the grid, facilitating diagnostics, and conducting meter readings across entire neighborhoods.

In summary, IoT enhances the intelligence of the SG by enhancing functionality and reducing costs. The SG system faces challenges with numerous smart meters generating large amounts of data, leading to congestion in IoT environments, especially during cyclic data transmission. To address this issue, we require selective or sustainable sensing techniques. By compressing data before transmission, we can enhance the efficiency of source processes and help smart meters conserve energy [6]. Unlike conventional methods that consolidate data without compressing, our approach resolves these issues and ensures security through encryption while avoiding the drawbacks associated with asymmetric keys, such as increased communication costs, extensive data length, memory requirements, and processing time.

We utilize robust security encryption methods to safeguard IoT devices, as they may not have sufficient strength. Fog computing acts as an intermediary between cloud data centers and IoT devices, offering computational networking, location awareness, and storage capabilities to bring cloud-based services closer to IoT devices. It resolves response time and throughput issues in a large number of IoT devices by facilitating communication between fog and cloud. Additionally, sensing devices such as smart meters exchange data based on delays or requests from fog devices rather than in a consistent cyclic fashion. We implement strong security encryption techniques to protect IoT devices, and fog computing serves as an intermediate layer between cloud data centers and IoT devices. Smart meters and fog devices exchange data based on delays or requests rather than in a consistent cyclic fashion [24]. The information collected by the fog devices can be sent to the cloud server. This model illustrates the concept of fog devices connecting smart meters to cloud servers through a control center and then to a trusted authority. It can accommodate a large number of fog devices, allowing smart meters to transmit data directly to them. Network design and model include the following components:

- I. Trusted authority: in the planned network layout, a reliable third party is in charge of initializing the system, managing the inventory of keys, and allocating keys to all domains, including IoT devices, fog devices, and the control center [37]. It's crucial to understand that this trusted entity will no longer be accessible after the system is initialized and will not be involved in future operations.
- II. Smart meters: smart meters monitor the usage of all appliances and use encryption to verify the sender, ensure data integrity, and maintain confidentiality. They send this usage information to nearby fog devices.
- III. Fog devices: fog devices play a vital role in fog computing by serving as an intermediary between IoT domains and the control center. They collect data from all IoT-connected devices (g_1, g_2, \dots, g_m) and transmit it to the control center. Additionally, they aid the control center in selectively filtering out certain incoming data to protect against external intruders.
- IV. Cloud: the cloud checks the authenticity and security of the combined data it receives from the fog devices.
- V. Control center: the data from all IoT domains (g_1, g_2, \dots, g_m) is sent to the control center through the fog device for analysis based on the application's needs. Due to their diverse origins, directly processing all the data is not practical. Therefore, in this research, the control center will compute the Mean (I_a) and Variance (I_a) for each subset I_a in m .

The main goal of the proposed model is to develop an encryption-based, secure-preserved mechanism for the IoT domains. The four purposes can be achieved:

- I. Private data preservation: the implemented system should be operational to protect the privacy of data. This means that the control center can assess the average and variability of each subset I_b , but cannot access the data from individual IoT devices [38].
- II. Reliability: by inputting false information on the fog device, the created aggregation method can protect against fraudulent data injections from external attackers.
- III. Risk tolerant: the developed system needs to be able to handle risks. If smart meters are unable to share data, fog devices should identify and send the missing data at a later time. If devices cease functioning or fail to report to fog devices during data transmission, the fog device will remove any suspected compromised data and send the rest to the control center for each area.
- IV. Computational cost and effectiveness: cost for different domains, fog devices, and control centers must be minimized as needed for the developed system to be efficient. To reduce communication expenses, a single encrypted message is made by combining multiple data.

5 | Encryption Based Mechanisms for Securing Smart Grids

In this section, we outline the established mechanism, which is divided into four subsections [6].

- I. Initialization.
- II. Authorization.
- III. Generation of reports (smart meters).
- IV. Consolidated data.

The primary objective is to secure data from external hackers and ensure that it is preserved securely in a unified manner.

5.1 | Initialisation

An advanced system that uses a hash chain mechanism to verify data sources regularly has been developed to protect data from external hackers. Each IoT domain, consisting of various devices, has a unique hash value combined with a time stamp for authentication. Devices within each domain are directly connected to fog devices and smart meters, ensuring the domain sends data during a specific time slot and a valid hash is

received by the fog device so that it can pinpoint any malicious data, safeguarding the system from external threats.

5.2. | Authorization

The steps required for registration of all smart meters, cloud centers, and fog devices are as follows: first, in the process of authorization of smart meters (SM_ab where a is a number from 1 to r₁), an identification ID_ab is selected after which the trusted authority randomly selects a number, evaluates it, and securely transmits the data to the smart meters. Second, the trusted authority randomly selects a number from identification ID_b selected by fog devices, evaluates it, and securely delivers the data to fog devices. Finally, secret data is transmitted to a trusted authority by the cloud center after selecting the identification ID_{cc} [6].

5.3 | Generation of Reports

The smart device encrypts the data as the domain devices' data is regularly reported to fog devices for data safeguarding from hackers. Therefore, data is evaluated and produced by every smart meter connected with all the domains. In this, let us assume nm is the number of bits that denotes each data type. Smart meters encrypt the nm types of data into data and construct I_{ab} [6].

After the encryption,

SM_ab evaluates I_{ab}.

$$I_{ab} = I_{ab} + r_{ab} \text{mod} m. \quad (1)$$

The smart meters select the random number and evaluate the private ciphertext as:

$$C_{I_{ab}} = h_{I_{ab}} * r_{nm} \text{abmod} m. \quad (2)$$

The private key is used by smart meters for the evaluation of signatures. Lastly, smart meters transmit the domain data to the respective fog devices; it is crucial to be concerned that each smart meter should generate and encode the message I_{ab}.

6 | Conclusion

In this research, the integration of IoT-based CC in a SG environment and an architecture for secure data consolidation deploying a data compression mechanism is proposed. The primary objectives of our proposed mechanism are:

Secure transmission of data is ensured by the system from IoT devices to fog devices, the aggregated data is sent to the cloud through a central cloud server. The fog device utilizes an algorithm to prepare consolidated data after the collection of data from multiple smart meters. Compression techniques are also employed by fog devices to reduce data size and energy usage during communication. The data extraction algorithm by the cloud server first extracts data from each fog device, followed by further splitting to gather data from each fog device. However, a significant challenge still prevalent is to proactively manage potential cyber threats facing the IoT-enabled SG system. Future research could focus on addressing emerging cyber threats while ensuring optimal performance and enhancing data security, advanced encryption techniques such as homomorphic encryption and quantum cryptography, real-time anomaly detection using machine learning, integration of blockchain technology, the design of systems capable of adapting to dynamic security needs could be considered by the development of robust communication protocols.

Acknowledgments

The author extends sincere gratitude to KIIT (Deemed to Be) University for providing the necessary resources and a supportive research environment. Special thanks to colleagues and mentors for their valuable insights and constructive feedback, which significantly contributed to the improvement of this work.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Data Availability

The data supporting the findings of this study are available upon reasonable request from the corresponding author.

Conflicts of Interest

The author declares no conflict of interest related to this research.

References

- [1] Yalli, J. S., Hasan, M. H., & Badawi, A. (2024). Internet of things (IOT): origin, embedded technologies, smart applications and its growth in the last decade. *IEEE access*, 12, 91357–91382. <https://doi.org/10.1109/ACCESS.2024.3418995>
- [2] Khalid, M. (2024). Smart grids and renewable energy systems: perspectives and grid integration challenges. *Energy strategy reviews*, 51, 101299. <https://doi.org/10.1016/j.esr.2024.101299>
- [3] Kiasari, M., Ghaffari, M., & Aly, H. H. (2024). A comprehensive review of the current status of smart grid technologies for renewable energies integration and future trends: The role of machine learning and energy storage systems. *Energies*, 17(16), 4128. <https://doi.org/10.3390/en17164128>
- [4] Raza, A., Jingzhao, L., Ghadi, Y., Adnan, M., & Ali, M. (2024). Smart home energy management systems: research challenges and survey. *Alexandria engineering journal*, 92, 117–170. <https://doi.org/10.1016/j.aej.2024.02.033>
- [5] Aldeen, Y. A. A. S., Jaber, M. M., Ali, M. H., Abd, S. K., Alkhayyat, A., & Malik, R. Q. (2024). Electric charging station management using IoT and cloud computing framework for sustainable green transportation. *Multimedia tools and applications*, 83(10), 28705–28728. <https://doi.org/10.1007/s11042-023-16630-0>
- [6] Shruti, Rani, S., Shabaz, M., Dutta, A. K., & Ahmed, E. A. (2024). Enhancing privacy and security in IoT-based smart grid system using encryption-based fog computing. *Alexandria engineering journal*, 102, 66–74. <https://doi.org/10.1016/j.aej.2024.05.085>
- [7] Mohapatra, H., & Rath, A. K. (2019). Fault tolerance in WSN through PE-LEACH protocol. *IET wireless sensor systems*, 9(6), 358–365. <https://doi.org/10.1049/iet-wss.2018.5229>
- [8] Manikandan, J., & Srilakshmi, U. (2024). Data transmission with aggregation and mitigation model through probabilistic model in data centre. *Informatica (Slovenia)*, 48(6), 157–172. <https://doi.org/10.31449/inf.v48i6.5425>
- [9] Priyadarshi, S., Subudhi, S., Kumar, S., Bhardwaj, D., & Mohapatra, H. (2025). Analysis on enhancing urban mobility with IoT-integrated parking solutions. In *Interdisciplinary approaches to transportation and urban planning* (pp. 143–172). IGI Global. <https://doi.org/10.4018/979-8-3693-6695-0.ch006>
- [10] Tooki, O. O., & Popoola, O. M. (2024). A comprehensive review on recent advances in transactive energy system: concepts, models, metrics, technologies, challenges, policies and future. *Renewable energy focus*, 50, 100596. <https://doi.org/10.1016/j.ref.2024.100596>
- [11] Kumar, A., Bag, A., Anand, A., Saha, S., Mohapatra, H., & Kolhar, M. (2025). Examining healthcare services utilizing cloud technology in intelligent urban environments. *Revolutionizing healthcare systems through cloud computing and IOT* (pp. 77–98). IGI Global. <https://www.igi-global.com/>
- [12] Rusitschka, S., Eger, K., & Gerdes, C. (2010). Smart grid data cloud: A model for utilizing cloud computing in the smart grid domain. *2010 first IEEE international conference on smart grid communications* (pp. 483–488). IEEE. <https://doi.org/10.1109/smartgrid.2010.5622089>

- [13] Bhowmick, R., Mishra, S. R., Tiwary, S., & Mohapatra, H. (2024). Machine learning for brain-stroke prediction: comparative analysis and evaluation. *Multimedia tools and applications*, 1–33. <https://doi.org/10.1007/s11042-024-20057-6>
- [14] Kim, H., Kim, Y. J., Yang, K., & Thottan, M. (2011). Cloud-based demand response for smart grid: architecture and distributed algorithms. *2011 IEEE international conference on smart grid communications, smartgridcomm 2011* (pp. 398–403). IEEE. <https://doi.org/10.1109/SmartGridComm.2011.6102355>
- [15] Mohsenian-Rad, A.-H., & Leon-Garcia, A. (2010). Coordination of cloud computing and smart power grids. *2010 first ieee international conference on smart grid communications* (pp. 368–372). IEEE. <https://doi.org/10.1109/smartgrid.2010.5622069>
- [16] Fayyaz, S., & Nazir, M. M. (2012). Handling security issues for smart grid applications using cloud computing framework. *Journal of emerging trends in computing and information sciences*, 3(2), 285–287. <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=86f178580db14611701f34672bf9bbb269d4ad6e>
- [17] Mishra, S. R., Mishra, S. R., Mohapatra, H., & Gourisaria, M. K. (2024). A robust approach for deepfake detection using SWIN transformer. <https://doi.org/10.21203/rs.3.rs-4672886/v1>
- [18] Mohapatra, H., Kolhar, M., & Dalai, A. K. (2024). Efficient energy management by using sjf scheduling in wireless sensor network. *International conference on advances in distributed computing and machine learning* (pp. 211–221). Springer. https://doi.org/10.1007/978-981-97-1841-2_15
- [19] Bernardo, V., Curado, M., Staub, T., & Braun, T. (2011). Towards energy consumption measurement in a cloud computing wireless testbed. *2011 first international symposium on network cloud computing and applications* (pp. 91–98). IEEE. <https://doi.org/10.1109/NCCA.2011.22>
- [20] Bjelica, M. Z., Mrazovac, B., Vojnovic, V., & Papp, I. (2012). Gateway device for energy-saving cloud-enabled smart homes. *2012 proceedings of the 35th international convention MIPRO* (pp. 865–868). IEEE. <https://ieeexplore.ieee.org/abstract/document/6240764>
- [21] Hong, I., Byun, J., & Park, S. (2012). Cloud computing-based building energy management system with zigbee sensor network. *2012 sixth international conference on innovative mobile and internet services in ubiquitous computing* (pp. 547–551). IEEE. <https://doi.org/10.1109/IMIS.2012.20>
- [22] Johnson, E., Seyi-Lande, O. B., Adeleke, G. S., Amajuoyi, C. P., & Simpson, B. D. (2024). Developing scalable data solutions for small and medium enterprises: challenges and best practices. *International journal of management & entrepreneurship research*, 6(6), 1910–1935. <https://doi.org/10.51594/ijmer.v6i6.1206>
- [23] Bhadani, U. (2024). Pillars of power system and security of smart grid. *International journal of innovative research in science engineering and technology*, 13(7), 13888–13902. <https://www.researchgate.net>
- [24] Boopathy, P., Liyanage, M., Deepa, N., Velavali, M., Reddy, S., Maddikunta, P. K. R., ... & Pham, Q. V. (2024). Deep learning for intelligent demand response and smart grids: A comprehensive survey. *Computer science review*, 51, 100617. <https://doi.org/10.1016/j.cosrev.2024.100617>
- [25] Vieira, C. C. A., Bittencourt, L. F., Genez, T. A. L., Peixoto, M. L. M., & Madeira, E. R. M. (2024). RAaaS: Resource allocation as a service in multiple cloud providers. *Journal of network and computer applications*, 221, 103790. <https://doi.org/10.1016/j.jnca.2023.103790>
- [26] Agnew, D., Boamah, S., Bretas, A., & McNair, J. (2024). Network security challenges and countermeasures for software-defined smart grids: A survey. *Smart cities*, 7(4), 2131–2181. <https://doi.org/10.3390/smartcities7040085>
- [27] Knapp, E. D. (2024). *Industrial network security: securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems*. Elsevier. <https://doi.org/10.1016/C2022-0-02315-1>
- [28] Eusufzai, F., Bobby, A. N., Shabnam, F., & Sabuj, S. R. (2024). Personal internet of things networks: An overview of 3GPP architecture, applications, key technologies, and future trends. *International journal of intelligent networks*, 5, 77–91. <https://doi.org/10.1016/j.ijin.2024.02.001>
- [29] Borra, P. (2024). Comparison and analysis of leading cloud service providers (AWS, Azure and GCP). *International journal of advanced research in engineering and technology (IJARET)*, 15(3), 266–278. <https://www.researchgate.net>

- [30] Mohammed, A. J., Abdulrahman, L. M., Abdulkareem, N. M., & Salim, B. W. (2024). Web technology and cloud computing security based machine learning algorithms for detect DDOS attacks. *Journal of information technology and informatics*, 3(1). <https://scholar.google.com>
- [31] Gorantla, V. A. K., Gude, V., Sriramulugari, S. K., Yuvaraj, N., & Yadav, P. (2024). Utilizing hybrid cloud strategies to enhance data storage and security in e-commerce applications. *2024 2nd international conference on disruptive technologies, ICDT 2024* (pp. 494–499). IEEE. <https://doi.org/10.1109/ICDT61202.2024.10489749>
- [32] Mahajan, H., & Reddy, K. T. V. (2024). Secure gene profile data processing using lightweight cryptography and blockchain. *Cluster computing*, 27(3), 2785–2803. DOI:10.1007/s10586-023-04123-6
- [33] El Mestari, S. Z., Lenzini, G., & Demirci, H. (2024). Preserving data privacy in machine learning systems. *Computers and security*, 137, 103605. <https://doi.org/10.1016/j.cose.2023.103605>
- [34] Abba Ari, A. A., Ngangmo, O. K., Titouna, C., Thiare, O., Kolyang, Mohamadou, A., & Gueroui, A. M. (2024). Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges. *Applied computing and informatics*, 20(1–2), 119–141. <https://doi.org/10.1016/j.aci.2019.11.005>
- [35] Sundarasan, S., Ibrahim, I., Alsmady, A. A., & Krishna, T. (2024). Corruption's crossroads: exploring firm performance and auditors' role in emerging markets. *Economies*, 12(9), 239. <https://doi.org/10.3390/economies12090239>
- [36] Liu, Z., Wu, Q., Shen, X., Tan, J., & Zhang, X. (2024). Post-disaster robust restoration scheme for distribution network considering rerouting process of cyber system with 5G. *IEEE transactions on smart grid*, 15(5), 4478–4491. <https://doi.org/10.1109/TSG.2024.3385377>
- [37] Hasan, M. K., Weichen, Z., Safie, N., Ahmed, F. R. A., & Ghazal, T. M. (2024). A survey on key agreement and authentication protocol for internet of things application. *IEEE access*, 12, 61642–61666. <https://doi.org/10.1109/ACCESS.2024.3393567>
- [38] Aouedi, O., Vu, T. H., Sacco, A., Nguyen, D. C., Piamrat, K., Marchetto, G., & Pham, Q. V. (2024). A survey on intelligent internet of things: applications, security, privacy, and future directions. *IEEE communications surveys and tutorials*. <https://doi.org/10.1109/COMST.2024.3430368>