JOURNAL OF RENEWABLE ENERGY AND SMART GRID TECHNOLOGY

Vol. 20, No. 2, July-December 2025

A Survey of Techniques for Secured and Swift Data Transfer in Smart Grid System

R. R. Ramya*, J. Banumathi

Department of Information Technology, University College of Engineering, Nagercoil, Tamilnadu 629004, India

***Corresponding author's email:** ramyarr628@gmail.com

Article info:

Received: 9 May 2025
Revised: 18 July 2025
Accepted: 24 August 2025
DOI:
10.69650/rast.2025.262073

Keywords:

IoT-Internet of Things
Routing Protocols
Cryptography
Genetic Algorithm
Smart Grid
Base Station

ABSTRACT

The integration of Internet of Things (IoT) technology into smart grids is essential for enabling uninterrupted, bidirectional communication across all components of the power system. This connectivity enhances system reliability, efficiency and operational effectiveness. Among the various domains within the smart grid, sensor networks present the greatest potential for IoT deployment due to their role in real-time data collection and monitoring. The architecture of IoT-based smart grids encompasses key layers facilitating distributed generation and intelligent control. These structures span from power generation to end-user consumption, allowing each segment of the grid to benefit from IoT applications. In this study, Routing protocols, Optimization approaches and Cryptographic techniques are studied and analysed to ensure secure and efficient data transmission within intelligent grids. The comparative analysis of these techniques is conducted to evaluate the performance, highlighting their effectiveness in enhancing smart grid communication and management.

Abbreviations

NSM	-	Network scheduling message
IoT	-	Internet of Things
GA	-	Genetic Algorithm
BS	-	Base station
RL	-	Reinforcement Learning
MARL	-	Multi-Agent Reinforcement Learning
DMM	-	Distributed Mobility Management
NILM	-	Non-Intrusive Load Monitoring
SPCA	-	Sequential Parametric Convex Approximation
EDP	-	Economic Dispatch Problem
SEMS	-	Smart Energy Management System
SCT	-	Smart Contract Token
TEM	-	Transactive Energy Management
PAR	-	Peak-to-Average Ratio
ACO	-	Ant Colony Optimization
BPSO	-	Binary Particle Swarm Optimization
DES	-	Data Encryption Standard
AES	-	Advanced Encryption Standard
3DES	-	Triple Data Encryption Standard
ECC	-	Elliptic Curve Cryptography
HEC	-	Hyperelliptic Curve
SM	-	Smart Meter
ELM	-	Extreme Learning Machine
MOSFP	-	Multi-Objective Sperm Fertilization Procedure
ADR	-	Automated Demand Response
SDN	-	Software Defined Network
GMN	-	Grid Monitoring Network
CH	-	Cluster Head
ESMR	-	Energy-aware and secure multi-hop routing protocol
HA	-	Home Agent
LMA	-	Local Mobility Anchor
CBSRE	-	Certificate-based signcryption with proxy re-encryption
SSM	-	Smart Socket Module
SA	-	Simulated Annealing
PMU	-	Phasor Measuring Units
WSN	-	Wireless Sensor Networks
OMS	-	Online Monitoring System
PMU	-	Phasor Measuring Units
SEM	-	Smart Energy Management
HToU	-	Hourly-time-of-use
ULT	-	User local task
ADMM	-	Alternate direction method of multipliers
AMI	-	Advanced Metering Infrastructure
TDMA	-	Time Division Multiple Access
P2P	-	Peer 2 Peer

1. Introduction

An interlinked architecture known as a power grid or an electric grid transports current from generators to consumers. While it is true that the demand for and usage of grid power have grown significant over the past few decades, the classical electric grid was built over a century ago with little change to its basic infrastructure. This calls for more effective management and control of both electric utility production and use on a larger scale. Devices and transmissions will be used extensively in prospective power grids to monitor energy in genuine and in reaction to consumption. Via power supply monitoring and data analytics, smart sensing technologies may create new opportunities for in-the-moment selection. Rising energy demand necessitates increased renewable energy production. The public electric system is undergoing a fundamental overhaul as we speak. For instance, the presence of distributed power plants makes energy flow bidirectional. Based on regional demand, electricity is distributed throughout the power grid's numerous microgrid nodes. Therefore, even the direction of energy flow needs to alter dynamically. Traditionally, electricity must be moved from distributed generation with abundant energy to those with scarce capacity. However, a variety of elements, including the sporadic generation of energy from renewable sources [1-2], affect this ultimate parameter. The smart power grid is depicted in Fig. 1 and is made up of a power grid, an interconnectivity and consumers with energy meter.

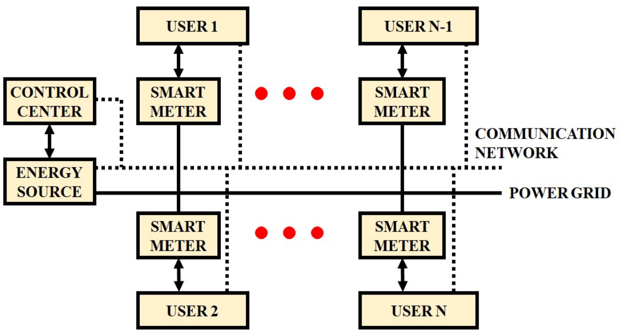

Fig. 1 A smart power grid is made up of an electricity system, a networking, and users who have various sensor.

The "smart grid," the most recent wave of these power sources, has been updated with internet and telecommunications technology to support more effective resource consumption. In the context of smart grids, transceivers**,** control planes and big data play pivotal roles in enabling intelligent and efficient energy management. Transceivers are essential components that facilitate two-way communication between devices, sensors and control centers across the grid. These modules allow data to be transmitted and received wirelessly, enabling real-time monitoring, fault detection and dynamic response to changing load demands. The control plane serves as the brain of the smart grid, managing and coordinating data flow, system configurations and communication pathways. It ensures that control decisions such as load balancing, demand response or fault isolation are made efficiently based on the incoming data. Meanwhile, big data analytics processes the massive volume of real-time data generated from distributed energy sources, smart meters and sensors. It helps uncover consumption patterns, predict system failures, and optimize grid operations by providing actionable insights. The "Internet of Things," a branch of technology that is currently undergoing rapid development, offers a wide range of trimming capabilities in numerous application areas. By converting outdated energy grids into modernised Smart Energy Grid systems, IoT could eliminate such unavoidable problems. The electricity grid's current surveillance system only considers important electrical metrics; it does not assess the internal parts of the local distribution cable network health. One of the primary reasons for recurring DT failures, arising from a lack of a well-established transparent system, is the absence of regular maintenance and follow-up inspections. Therefore, in order to install software-defined infrastructure and enable genuine management of each converter station of the local grid, a trustworthy monitoring and demand forecast are necessary. SDN is a brand-new paradigm for programmable networks that has just been proposed to make traffic management and access control systems simpler. SDN separates the transmitting hardware from the framework for making decisions, such as routing and intelligent machines, by dividing the control plane from the information plane [3-4]. Fig. 2 illustrates the structure of IoT.

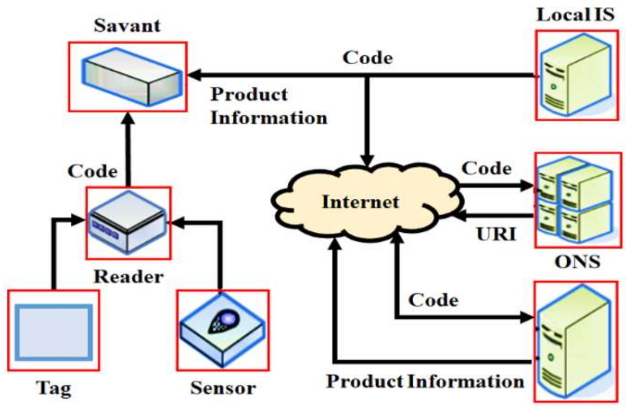

Fig. 2 Structure of IoT.

A basic Internet of Things design comprises three layers: Sensors, electronics and other innovations that aid with perception (the sensors, gadgets and other devices) (The connection between gadgets) (the connectivity between devices) Application (the component the participants interact with) (the layer the user interacts with). Many clever methods have been put up to address the demand side energy management problem. These include developing resource management systems that combine a variety of techniques, such as distributed generation based on renewable resources. With the incorporation of IoT in EMS, smart EMS has been created. In IoT-based smart grids, intelligent electrical devices not only collect data from a variety of sensors but also transmit it efficiently to the control center. However, employing many radios and channels causes the network to experience greater interference [5-6].

Prospective Smart Grids might be outfitted with ubiquitous Interties devices in line with the burgeoning Internet-of-Things paradigm to allow improved management of distribution networks and RES. According to the IoT vision, anything could be linked to the web or another transnational network at any time and from any location. As a conclusion, the Internet of Things' selected medium for transmitting sensory data and activator commands permits two-way communication between Smart Grids' equipment and parts. The term "Internet-of-Energy" also describes the fusion of decentralised RES, IoT and the Smart Grid approach. For the transportation and management of Big Data, these networks must be constructed. Two parts comprise the GMN:

a) Each DT uses the WSN component, which varies depending on the zone. Numerous sensors, including overcharge, whistling noise, humidity and fuel pressure sensors, are installed on each machine. These instruments represent the comprehensive health assessment of each DT. Long-range LoRa WAN connectivity links each of these detectors to a Transceiver.

b) Wireless-static data centre is the second component of the architecture. In order to provide redundancy and fault tolerance with route recovery, the data centre has numerous pathways. The cable network Control plane serves as the static data centre's bridge entry node [7-8].

The infrastructure for DRM in Singapore has markedly increased in recent years as a result of IoT advancements and the introduction of 5G technology. By enabling two-way communication across the generation, distribution, transmission and consumption elements of the grid, DRM comprises of programmes that increase the SG's efficacy. A larger, more dependable and more secure network is produced by combining 5G and DRM. An infrastructure of this kind would also cover a huge number of links while using less energy. In real-time DRM algorithms, where accuracy and speed are essential factors, this is especially critical. Due to the high cost of gadgets and compliance problems, distributed sensing becomes a desirable alternative. A home area network is needed to enable the fusion of all electronic equipment. This transmitter transmits command signals from the utility to the home gateway-registered products as well as commands generated by sensors connected to that equipment. This entire information makes it possible to think of an ILM technology as an internet-of-things platform for load monitoring and its associated potential uses. In terms of resident autonomy, detecting ADLs is a good decision among technologies. Another of the most popular ones is that it has made it possible for older persons to receive nursing care at home. It also has made it possible to develop a consumer profile that may help with more effective energy demand [9-10].

These challenges have gained significant attention as key areas of research, driven by the emergence of transformative technologies such as edge computing, big data, IoT, artificial intelligence and advancements in power generation. In order to construct smart grids, businesses and academic institutions have spent a lot of time and money. Investigations are carried to incorporate these innovative methods into already-existing electricity networks. The main parts of conventional power systems are power generation, power conversion, voltage regulation and switchgear. Many different types of power fasteners and actuators, such as those that support IoT-based intelligent energy systems, are present in power buildings. These include intelligent video sensing devices, current permeability sensors, motion sensors, soaking sensors, moisture sensor and others. In this mechanism, the electric current is generated in accordance with the connected of power equipment or household appliances. The intelligence of the dc microgrid is increased by the installation of a large number of IoT endpoints to gather timely data about the state of the electricity system for the command centre. [11-12].

The power system uses Technology household devices and technologies. They produce effective energy techniques to execute low-loss, efficient and environmentally friendly electricity control in contrast to the traditional generation capacity. One of the main goals of the sensor network is to make greater use of the modern digital communication infrastructure to help with electric grid administration. A more dependable and effective electric grid is being created by developing and deploying an increasing number of Internet of Things devices with measuring and/or control capabilities. As a result, the role of communication systems has changed. A test bed that replicates a connected power grid and communication network would be useful for assessing the effectiveness of the control algorithms for these systems. It is possible to exchange data due to the Internet of Things, which is an important data transit infrastructure. The system entails software, electronics and detectors. IoT provides data collecting and protection. The Internet of Things connects people and organisations on a global scale. IoT systems can help with things like communities, quick emergency services and vehicle responsiveness to cars, acute stress management and intelligent cities. Today's internet operates as a wide worldwide organization that may link a variety of devices [13-15].

2. Different Routing Protocols in IoT

In order to communicate the data that allows networking to select routes between nodes in a computer server, they interact with each other via a process known as programming. Number of packets is transferred from router to modem through the webpage infrastructure until they get to the target hardware. The task of routing system functions falls on controllers. Routers choose a particular path. Each gateway only knows the networks that are directly connected to it. This information is originally exchanged among nearby neighbours through a routing mechanism prior to getting spread online. Using this method, routers are taught approximately system components. Telecommunications systems differ specifically in how they avoid electrical cycles, select favoured connections, use hop accounting reports, take a long time to reach routing protocol connectivity and are highly adjustable. These traits are in furthermore to relay multipathing and cloud access requirements specific requirements. Future technological advancements, such as multilevel interaction, might also be used to deploy secure networking gateways to designated ports. This also has the benefit of preventing routing technology loop issues. Numerous network implementations are specified in RFCs, which are significant documents.

2.1 Internet of Things in Mobility Techniques

A modification to the LOADng procedure for movement in IoT situations. By utilising the control signals that are exchanged back and forth during the route discovery mechanism, the anticipated technique, LOADng-IoT-Mob, presents a novel system. It enables swellings to better organise the data in its Forwarding Set and better accommodate architecture changes brought on by device migration.

The ability to shorten journeys to known locations, which could be getting closer due to mobility, is another benefit. A new transmitting statistic based on the established signal strength display is now present in LOADng-IoT-Mob to assist the nodes in building connections with more proximate and reliable nodes (RSSI). As was already indicated, LOADng-IoT-Mob has other improvements that improve presentation in IoT networks, as shown in subsection II-B. As a result, the suggested solution permits the employment of two distinct route discovery techniques. The original suggestion therefore allows for the use of two different route discovery methodologies [16].

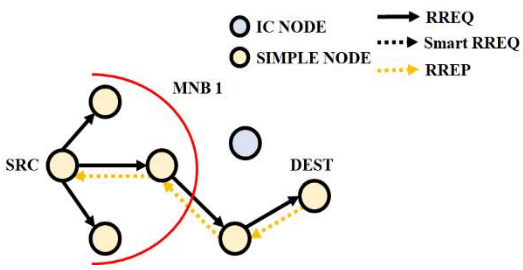

Fig. 3 Increasing ring inundation is used in the LOADng-IoT-Mob basic route finding procedure to build a path for a simple node.

2.2 Mobile IoT Hub Management Technique

Location data is delivered by the IoT hub to the coordination tree device. All participating tree sensors will subsequently have access to the redesigned IoT hub, as depicted in Fig. 4. Every time the IoT hub moves towards a new location, it transmits a beacon packet.

The flash packet helps in identifying a peer within the IoT center. The IoT node selects one of its peers to forward the geolocation data, based on criteria such as the shortest path and highest remaining energy. The selected device then follows the same process to retransmit the data. This procedure continues until the data reaches the nearest spine tree device. Once it has the precise position, a device in the backbone tree rotates throughout the tree [17].

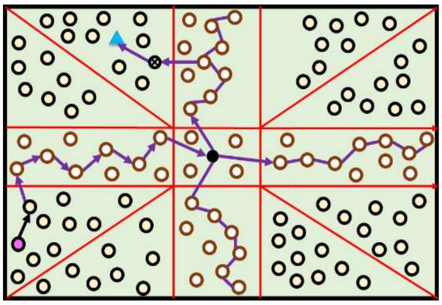

Fig. 4 IoT hub meet specifications.

2.3 Network Scheduling Technique

Network configuration is one of the primary challenges in developing WSN protocol designs. Without an efficient setup, devices consume more resources while attempting to access the communication channel or waiting for a chance to transmit their data. The network scheduling method proposed in this research takes the shape of an NSM, which is configured by the Grid deposit and is shown in Fig. 5. This message and the delivery address of the MS are used to arrange the CHs' sleep and wake schedules. Additionally, the network device uses TDMA to arrange the time for data transport.

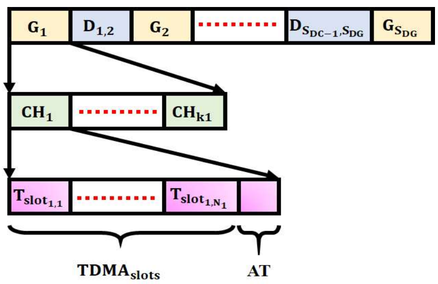

Fig. 5 Network scheduling message.

In order to conserve energy, each CM also lowers their radio in accordance with the TDMA scheduling, sending their remaining energy, ID and data to the designated CH for the period of their particular slot. The suggested scheduling method's structure is shown in Fig. 5, where each network device is given a specific time slot for data transmission. If the MS has not yet received it, all CMs and CHs could be likewise turn off their radios to save energy; however, under NSM, the equipment could be turn them back on once it has. The formula below could be used to calculate the overall cable network latency, which is the same as the time it takes the MS to execute one lap, conferring to Fig. 5. [18].

2.4 Routing Protocols in IoT Technique

While enhancing the currently used and well-known fundamental protocols, routing protocol suggested for IoT/LLN was implemented. Primary as well as most recent approaches, however, are RPL-based. Peer-to-peer is a significant categories: - used mostly in Internet of Things devices. The RoLL WG put forth a fresh idea for enhancing P2P transmission efficiency. As a result, the P2P-RPL point-to-point routing protocol is suggested by the IETF standard. Condense the amount of control communications by using the geographic routing technique GeoRank, which combines RPL with greedy other adaptive face routing. Since most peer-to-peer (P2P) routing algorithms establish routes by actively manipulating packets resulting in significant energy and financial costs, Zhao et al. proposed an energy-efficient, region-based routing system designed to enhance network reliability. This approach aims to reduce energy consumption in P2P communications while maintaining performance. To effectively implement such energy-aware routing in real-world scenarios, it is essential to consider the diverse routing requirements of various IoT applications. RPL based on ad hoc on-demand proximity routing seeks to enhance P2P incoming traffic of RPL by taking into account symmetric and asymmetric links in the path discovery process [19].

2.5 Non Cross Layer Routing Protocol Technique

Utilizing data from the network layer through a non-cross-layer routing mechanism uses more energy. Cross-layer solutions must be used by WSNs in order to tackle the problem. It is clear that cross layer conventions are more complex than their incrusted equivalents. Main objective of this idea is to decrease energy usage as much as possible in order to escalation the lifecycle of the WSNs. When making decisions, the cross-layer model is designed to take into account data from all layers. For instance, before creating a path, the routing protocol may consult every other layer. As a result, WSN complexity could not be avoided and uses some energy in comparison to its layered version. When opposed to energy loss from greater complexity, complexity that results from cross stacking gains more energy. If the proposed method's energy consumption is shown by ECX due to its increased complexity and its energy savings are indicated by ESP, then ESP >>> ECX [20].

2.6 One-Hop Delay Modeling Technique

There are both fixed and mobile node forms, as well as real-world IoT application scenarios that frequently include wired and wireless hybrid links. An entire control network with capabilities for worldwide management and monitoring is typically present in manufacturing technologies. We use a local production unit's network as an example in our study and other components could be extrapolated. Finally, the entire network could be benefit from the ultimate decision. The best growth control centre, secondary production control institutions, control establishments, multiple production apparatus types, inspection robots and vegetation managing nodes could be all connect with one another through the network. The platform could give directions; all nodes could be quickly communicated. This is conducted on the presumption of reduced latency to meet the needs of transmitted data, phone and subscription service. As seen in Fig. 6, there are both hardwired and wirelessly links present throughout the entire scenario.

The wired link in Fig. 6 is represented by the thick line and the remote controller by the narrow path. Data communication between nodes is subject to strict latency limitations and each node has a corresponding level.

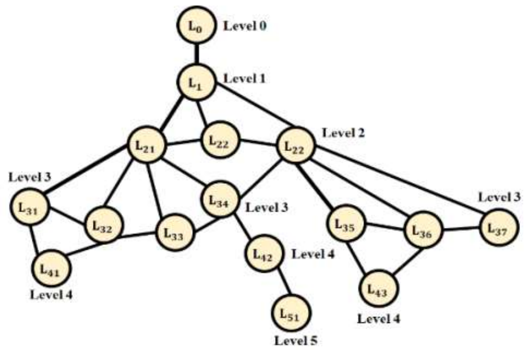

Fig. 6 Frame format.

Table 1 Illustrates the Comparative Analysis of routing protocol techniques in IoT.

Sl. No	Author/Year of Publications	Methodology	Advantages	Limitations
1.	Khalid Haseeb *et al* (2019)	The many safe network protocols designed for wireless device systems entail some common encryption and identification techniques, which increases computing capacity and increases routing costs [22].	An energy-aware and protected multi-hop directing (ESMR) procedure that combines multi-hop data safeguarding against fraudulent activity with a rise in energy consumption.	• A solution does not take into account secure multi-point conversations against rogue nodes. • Nearly all of the current technologies offer multi-hop packet forwarding as opposed to single hop connectivity.
2.	Rakesh Kumar Lenka *et al* (2018)	Sensor networks expand in size and take in a lot of information. The adoption of data distribution strategies is necessary due to vast volume of data that has spread over entire network. The approaches for disseminating data could be collect and make existing data that is pertinent to the user [23].	In the IoT, a device is referred to as "a gadget or a thing" that has evolutionary algorithms built into it and could be connect to a network.	The WSN-Assisted IoT system may become unattached or secluded because IoT diplomacies closest to the IoT-Hub use resources more quickly than other Sensor nodes do due to the increased transmission they must undertake.
3.	Inam Ullah Khan *et al* (2020)	An innovative AntHocNet-based routing for FANET. Compared to other traditional optimal path selection strategies, ant colony optimization technique or metaheuristics in general have demonstrated higher predictability and effectiveness [24].	Due to FANET's high mobility and diverse properties, a routing algorithm needs to be flexible enough to react to the program's shifting needs.	The dynamic spatial and temporal movement of FANET clusters increases the situation's difficulty and variety.
4.	Alessandro Biason *et al* (2017)	Educational approaches should be used to uncover the connections amongst user contexts within the environment of the technical specifications [25].	The initial reports encourage survivability of proposed operation approach and show how the use of dynamic encoding and channel access techniques allows an IoT network to adaptively tune life span for transmission loss in conformance with the legislation's requirements.	In multi-hop connections, where network connectivity is hampered by energy and resource limitations of IoT nodes, upwards data packet may not have enough electricity in some cases—as well as by the energising proposed method.
5.	Jenn-Wei Lin *et al* (2018)	Innovative mistake strategy uses virtual CH and flow bipartite graph approaches. Energy that is now available from all failure-free CHs is organised to create the virtual CH. We could be determine the median amount of received signal that each weakness CH could be communicate using the virtual CH [26].	• Many WSN routing strategies have been put out to handle the transportation of received signal from sensor nodes to sink node. • These routing protocols could be divided into two groups: constellation and flat based routing systems.	We looked into the accident constellation routing problem in IoT WSNs. The robust base station could be also play the CH job. When a CH malfunctions, a second, failure free CH should be deployed as an alternative CH to continue to provide service to the impact prediction by the malfunction.
6.	Daemin Shin *et al* (2019)	A new CH is not created by the participate approach. Alternatively, it forces the problematic CH's personnel to work for one maybe more already functioning weakness CHs. [27].	A strong replacement for PMIPv6, DMM has gained prominence but hasn't yet undergone standardisation, leaving just the few channel algorithms with an efficiency-only focus.	There is a limit to how much the network could be expanded by increasing the load on the anchor because the amount of data traffic and signalling instructions geometrically grows with the quantity of MNs.

Currently, only large-scale fixed connections may make use of network adapter management technologies like rip and Open Shortest Path First. Moreover, this approach is not well-suited for industrial environments that involve mobility and complex operating conditions. In scenarios with a standard network infrastructure and strict delay constraints, an active routing system may be more appropriate to ensure timely and reliable communication. In other words, as providing as the path to the destination node exists, a node could be transfer info back when it requires to do so, resulting in a reduced latency [21].

2.7 Comparative Analysis

A Comparative analysis is carried out amid different routing protocol techniques in IoT.

In order to lower the cost of processing and communication for IoT devices using smart networks. An employed 80-bit key, small-parameter hyper elliptic curve block cypher to assess efficacy and security of proposed CBSRE technique. Also, suggested system satisfies security requirements for forward secrecy, unlink ability, or all three (IND-CBSRE-CCA2-I and IND-CBSRE-CCA2-II). To overcome the current SP-requirements RE's in terms of efficacy and quality, we are forced to suggest a revolutionary approach known as certificate based Signcryption with proxy re-encryption CBSRE. Since the CBSRE method is based on the HEC concept, which requires smaller key sizes than RSA, ECC and BP, it could be regarded as lightweight. [28].

3. Cryptographic Techniques in Smart Grid IoT

Cryptography is the use of codes to safeguard data and transactions in a way that only the intended recipients could be understood and handle it. In this way, unauthorised individuals are prohibited from getting information. Cryptography and crypto means, "written" and "hidden" respectively. In order to alter signals in a method that makes them difficult to receive, cryptographic uses a set of rule-based calculations known as procedures. Data protection methods use cryptographic methods. Data is encoded using the method of encryption, which transforms it from its original plaintext representation into a distinct version known as cypher text. In order to alter signals in a method that makes them difficult to receive, cryptographic uses a set of rule-based calculations known as procedures. Data protection methods use cryptographic methods. The creation of digital certificates, the implementation of identifiers and authenticity, the safeguarding of sensitive data, security of internet surfing and security of private transactions like bill and acclaim card payments all make use of these procedures. Data is encoded using the mechanism of encryption, which transforms it from its original plaintext representation into a distinct version known as cipher text.

3.1 Proxy Re-Encryption Technique for Signcryption

3.2 Multiagent Reinforcement Learning Technique

Instead, the agents must use learning to find a solution on their own. The study of reinforcing learning strategies is an important component of multi agent learning methods. These strategies integrate current developments in game theory, single-agent RL and more thorough direct policy search techniques. An extensive investigation of MARL is what this essay aims to provide. As a result, we select a sample set of techniques that allowed us to establish the field's architecture, provide information on the state of art and identify some essential research directions [29].

3.3 Cyber-security Key Components Techniques

The sensor network might be the target of innumerable hacks that could result in severe energy outages and irreparable harm to the systems that provide power. They might also jeopardise the objectives and standards of digital technologies. It is challenging to include every prospective assault due to the breadth and diversity of the network system. In light of the security objectives for the smart grid, we consequently split attackers into different forms. The aforementioned discussions on security for smart grids show that while creating answers to threats, a variety of constraints, situations and issues must be considered. For instance, encryption alone is unable to effectively thwart every potential threat. Cryptography makes a substantial contribution to the development of the concealment and reliability of the power system, even though it is not the sole solution. Encryption techniques must be used in a smart grid to ensure data confidentiality and security. Encryption greatly reduces replay and spying activities. Many of the most recent encryption and authorization technologies are utilised by the sensor network. Symmetric cryptography—such as symmetric cyphers like DES, AES and 3DES or public-key cryptography is widely used to guard against cyberwar fare in the power system. Furthermore, it is predicted that the maximum of electrical components in a smart grid will have basic cryptographic skills [30].

3.4 Security and Privacy-Preserving Techniques

Every home has a smart meter installed as part of smart grid, which provides utilities with real time data regarding electricity consumption for a variety of uses. Malicious parties could be trace a user's electricity usage habit and learn confidential information about them by evaluating their energy usage profile. A block chain-based plan for effective data aggregation and privacy protection was put forth by the authors. To safeguard their privacy within the community, the users utilise pseudonyms. Although it could be not be used alone to ensure privacy and security, block chain technology could be utilised in concert with advanced encryption techniques to do so. Linkable Solitaire diamond Authentication, Zero Understanding Proof and Elliptic Curve Digital Signature Algorithm [31].

Table 2 Cryptographic Technique.

Cryptographic Techniques	Advantages	Limitations
Bilinear Pairs Functional Hash Exponentiations Using A Modular Approach	• Common substantiation • Conference main formation	• Susceptible to transient undisclosed outflow attack • No sturdy identifications' secrecy of clever meter
One-way hash functions ECC	• Reciprocated confirmation • Assembly crucial establishing	• Defenceless to ESL attack • No secrecy • No faultless onward safety
Bilinear coupling One-way confusion purposes	Crucial covenant	No communal substantiation does not funding Block chain explanation.

Table 3 Illustrates the Comparative analysis for different cryptographic techniques in IoT.

Sl. No	Author/Year of Publications	Methodology	Advantages	Limitations
1.	Aarti Agarkar *et al* (2018).	Cryptography encryption techniques come in two varieties: partially homomorphic encryption and fully homomorphic encryption [33].	The benefit of cryptography methods is that the accumulator node could be not comprehend the actual data gathered from SMs.	The submitted work does not contain the precise decryption algorithms. Additionally, no other schemes are compared to the system.
2.	Md Zakirul Alam Bhuiyan *et al* (2019).	A safe and private bidder technique for expectation ADR systems. For data security, we employ the decryption method rather than relying on any reliable third parties. Through simulations carried out in different simulation scenarios [34].	• The groundwork for autonomous, efficient and well-organized system management is laid forth by the data that PMUs collect. • The goal is to build a protected, efficient and privacy oriented ADR-DB bidding process for IoT based smart grid.	• The effectiveness assessment of the encryption techniques of an IoT based smart grid. • Requirement bidding is frequently used to solve the share and assignment issues in the energy market for Micro - grids and Security Sensors.
3.	Kim-Kwang Raymond Choo *et al* (2018).	The use of encrypting and other mathematical methods is frequently seen as the best way to guarantee security in IoT applications and systems. [35].	A break glass access mechanism enables someone, such a doctor at an emergency room abroad, to get around access policy and access patient's data.	• Because IoT systems are networked and integrated, data management security is a concern. • Low installation costs: Putting IoT into practise does come at a price.
4.	Jacob Sakhnini *et al* (2020)	Heterogeneous techniques are additionally employed to identify quantitative variations in threat vectors [36].	As an illustration of such prevention measures, step information that gauge the significant of specific substations could be defined.	• The smart grid's growing susceptibility to cyber assaults is one of its key problems. • As a result, numerous threats and countermeasures are put out in writings.
5.	Ahsan Saleem *et al* (2019)	It is suggested to use new fog enabled privacy preserving data aggregation approach (FESDA). Message integrity and source authentication are achieved through symmetric key MAC method [37].	The use of flow measurement data for data analyses to support operational strategies such as power demand estimation, clear end device monitoring and improved management and optimization of current both supply and distribution.	Fog computing has been used in conjunction with power buildings in recent decades in order to get around some of the constraints of typical data collecting systems for smart grids, which have high processing and communications costs.

3.5 Nonintrusive Load Monitoring Technique

The wireless technology will inevitably be a fashion in contemporary cities. The occupants of these residences are beginning to place more importance on load control and efficiency preservation. In order to examine the fuel consumption of particular electrical loads in residential buildings at a specific sampling stage, the internet of things now uses the non-invasive load monitoring technique. The consistency of residential electricity loads is a serious problem in this technology. To solve this issue, Ghosh et al. created the load image retrieval approach, an upgraded version of the NILM methodology that uses fuzzy rule-based cognitive segmentation and harmonic distortion characteristic assessment to track various energy demands. The simulation's findings show that, in compared to current alternatives, the presented method improves the accuracy of residential power loads. Energy unquestionably has a big impact on every single home and on society as a whole. The authors claim that constructions are the major energy consumers. Mir et al. conducted a complete examination of power buildings for clever dwellings and structures to assist green energy trend for smart homes and buildings. They have offered a wide range of solutions, techniques, approaches and problems in particular to conserve energy for homes and other buildings. The identity electric grid, or SES, paradigm was also made public [32].

3.6 Comparative Analysis

A Comparative analysis is carried out amid the different Encryption and Decryption techniques employed for analyzing the Cryptographic techniques in smart grid IoT.

4. Optimization Techniques Used in Smart Grid IoT

4.1 Side Energy Management Technique

The suggested SEMS control system is made up of sophisticated connecting devices that allow different client equipment to interconnect with SEM Gateway using XBee modules operating in AT mode. In the suggested method, SEM entry point receives energy consumption statistics from each embedded step in enhancing as well as the utility's authorised peak power limit. Additionally, SEM employs a powerful algorithm for power bargaining to organize each machine in the best possible manner. The proposed SEMS's SEM Gateway and Smart Socket Module incorporate the following technologies to conduct macro-economic power control for effective energy utilisation.

1 SEM Gateway (Central controller)

- Implementation of a significant procedure during Smart Metering
- Personality function to deal with unresponsive appliances

2 Smart Socket Module (Appliance end)

- Distribution of controllers at the appliance end
- Methodology for Efficiency Measures

The fundamental procedure used in the SEMS microcontroller board is the key component of specified SEMS approach (Gateway). The decisive algorithm is additionally used to direct all operational procedures. A major tool for avoiding significant supply constraints and saving energy is requirement electricity administration. Instead of controlling utilization by choosing to consume less power during peak usage hours, Energy Company focused on reducing the cost of electrical as a whole [38].

4.2 Simulated Annealing Technique

One optimization technique, called SA, is based on the idea of thermodynamics, particularly how metal cools and then anneals. Among numerous local optima, SA is utilised to identify the optimal global optima. An objective function from a related optimization issue is used in this algorithm. The hill-climbing method is comparable to this optimization approach. The computational technique employs a random move, but the mountain methodology chooses the move that is best for the goal function. If the randomised move improves the response, it will be accepted. If not, the algorithm operates with a probability of less than 1. This possibility is provided by the method below.

$$Prob(uphill\_move) \approx 1 - exp(-\Delta E/kT)) \qquad (1)$$

In the mechanics annealing problem, ΔE is the change in the objective function, the parameter "T" is based on temperature, which aids in determining the likelihood. Typically, "T" begins with a large value and decreases with each step. Temperature and energy are related by the parameter "k". It is equivalent to Boltzmann's constant in thermodynamics. The Traveling Salesman Problem, routing in VLSI and other very large and discrete search spaces could be all be solved with SA. The Internet of Things system will include a number of wireless sensor nodes. The IoT base station could get overwhelmed and transmit redundant data if all of these devices make an effort to interact with it [39].

4.3 Economic Dispatch Problem Technique

Three control layers that generally function on hierarchical time scales in power networks are fundamental, intermediate and quaternary control. For the integrity of electrical grids, fundamental control, the fundamental control layer, ensures that all devices are synchronised to coherent power flow. Independent droop controllers are typically used to accomplish this purpose. It is possible to design the control gains to guarantee equal power distribution among the generators. The goal of secondary control is to get rid of power imbalance-related static resonance errors. Distributed averaging integral controllers could be used to achieve it. Tertiary control, as the top control layer, is now less concerned with grid frequency and more concerned with a range of practical goals. In tertiary education, the goal of an EDP is typically achieved. A sample framework for economic dispatch in smart grids is shown in Fig. 7.

The amount of secrecy is increased by the agents exchanging the converted dual concern variable. This approach could be also force all generates to agree in a finite amount of time, which corresponds to the minimum value of the complete cost function. This approach performs the finite-time convergence, which is significant superior to the approximate interconnection in EDP [40].

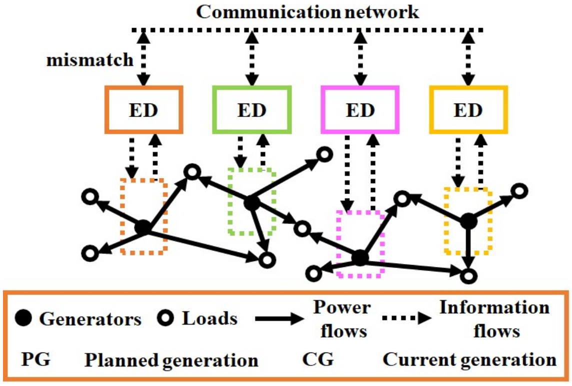

Fig. 7 Framework of economic dispatch in smart grids.

4.4 Phasor Measuring Units Technique

It has been noted that the use of PMUs and WSNs for tracking electric energy elements is a growing field. A sensing device that monitors PMU operation and reports it to the OMS is necessary to make the grid's operation sharper and more efficient. As a result, this method of projects supported provides the path for avoiding critical grid circumstances like high power consumption loss. Despite being present, the GPS receiver could be only be used to track PMUs' positions. Additionally, the control centre will get any observations that the PMU provides after they have been transmitted to the satellite. There is no method to detect errors like incorrect measurement data with noise that may occur while uploading the resulting statistics. Additionally, it is only possible to control uncertainties after identifying the specific PMU issue at hand. No rapid corrective action could be performed because this calls for a lot of personnel. Therefore, there may be a substantial chance of losing electricity and further blackouts may occur quickly. The main reason for conducting this research is to keep an eye on the voltage level, the PMU's condition in the grid and to find a quick solution to the blackouts that result from PMU failure. Any defects will be quickly detected by installed sensor group, which will then notify the control centre. Security systems that can identify fault data in PMUs while consuming less energy could be coupled with PMUs for better control methods. The primary PMU approaches are only practical after a precise sensor has been put on the power system.

Only once a precise sensor has been mounted on the grid are the control mechanisms of PMU feasible. However, the main flaw in is that only the PMU installation choices that might potentially replace the conventional converter are considered [41].

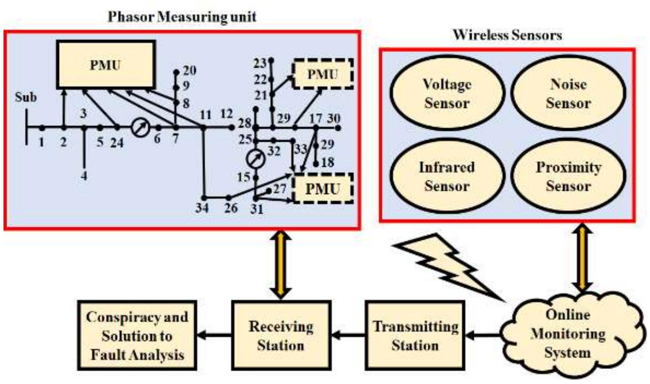

Fig. 8 Integrating detectors with PMU to identify faults.

4.5 Heuristic Optimization Techniques

Node MCU and Android have been used in the development of the SEM system, which is a part of the smart home application. With the help of this system, it is possible to keep track of residential energy usage in real time and collect data on each smartphone's operation times and energy usage. In addition, the SEM system ensures that the energy needs are met to greatest extent possible during times when energy costs are at their lowest. Along with the ability to create a daily and weekly schedule, the Android interface gives customers the chance to track and modify their current use habits in order to maximise fuel economy. Fuzzy reasoning and heuristic optimization methods consider user comfort and the PAR (UC). The findings of the simulation indicate a significant decrease in energy use, cost and PAR. The research compares the effectiveness of home energy management controllers that use heuristic algorithms like the genetic algorithm BPSO and optimizing the ant colony to plan energy use (ACO). The traditional grid has a variety of drawbacks including obsolete infrastructure, increasing energy demands and security issues. Anyway, smart grid has created a network of information and communication technologies that enable bidirectional contact between people and the internet [42].

4.6 Distributed Optimization Technique

The bit coin design and the transactive energy management algorithm are modified for IoT devices in this study and their usefulness on a real-world IoT network is verified. It is a decentralised method that safeguards privacy and gives users the strongest quality parallelism control over their energy consumption. In order to guarantee user privacy, we develop a distributed system for managing transactive energy that relies on each user making their own transactive energy decisions via a smart contract. To provide a distributed optimization technique that the TEM blockchain network container employ to achieve the optimal outcome while safeguarding the consumers' data. The user-local work and the smart contract job are separated from the TEM using a various loading technique of increasing. Users remotely use the ULT to design an ideal power usage plan and make their own transactive power choices. The SCT functions as a smart card on the IoT platform, accumulating users' typical trading choices to determine the trade that is best for the world. One type of horizontal transaction that smart houses could be carry together with other peers is peer-to-peer electricity exchange. However, the shortcomings of the typical demand response energy control system include single-point failure, security infringement and low productivity [43].

Table 4 Illustrates the Comparative analysis for different Optimization techniques in IoT.

Sl. No	Author/Year of Publications	Methodology	Advantages	Limitations
1.	*Zunaira Amjad et al* (2020)	In this work, we provide an improved design that could be serve numerous users according to their needs. Depending on their needs, customers will be able to select the type of complete guide they utilise [45].	The main benefits of are a decrease in PAR and improving user comfort. Additionally, it offers the best option for resolving anticipated issues with managing energy resources.	The typical electrical energy system's significant drawback of peak bonding to unscheduled load usage is that customers must pay high electricity bills and utility also encounters an increase in demand for electricity, which results in power cuts, power failures and floods.
2.	William Sanchez-Huertas *et al* (2018)	In order to address the problems raised, this study suggests optimization techniques as the Colony of Ants, Genetic Algorithm and Tabu Simulated Annealing [46].	When compared to a single formulation, the use of two or more optimization methods has better advantages. As a result, the realization of the hybrid architecture is on the rise.	Their primary drawback Is the discontinuities of their creation, which is why a massive power generation system is suggested to turn these techniques into tactics that are practically competent.
3.	Kun Wang *et al* (2018)	The difficult that the changeable effort masses and secreted coat in the ELM could benot provide the highest possible accuracy of the ELM model for information access is resolved by a genetic algorithm-ELM approach [47].	Communication networks have certain special advantages in deployment, expansion and cost effectiveness when compared to conventional cable mobile communications.	• This original article main concern is wireless big data computing in the context of smart grids. • We start by looking into the similarities and differences amongst big data and smart grid data.
4.	Albert Molderink *et al* (2019)	A three-step control methodology that focuses on household energy supplies is presented to manage the collaboration between these techniques [48].	The benefits of a local neighbourhood are its ease of realization, lack of communication with others and lack of known to enhance regarding which products are turned on or off (social acceptance).	The discrepancy was brought on by the deviations excess supply. In order to avoid prediction mistakes, the scheduler attempted to increase power production in order to meet the predicted consumption.
5.	Hisham A. Shehadeh *et al* (2019)	Based on the aforementioned considerations, a MOSFP approach is used to select the proper process transmitting size. The model for this technology is the plasma-based gestation process [49].	The benefit of MOSFP for both of these approaches is that it accurately locates the Pareto front and pays close attention to the actual Maximum advance.	To allow the high-performance processes of the clever network and to promote trustworthy and continuous access to base technology, controlling directions are issued from/to identifying or measuring measurement in various locations.
6.	Ke Zhang *et al* (2020)	The problem that the changeable input bulks and secreted layer in ELM dismiss give the best accuracy of ELM model for information access is resolved by a genetic algorithm-ELM approach [50].	Although the excessively machine has a significant bet benefit, the variability of input weights and hidden layer skew prevent it from addressing the stochastic optimization dilemma.	• On a technical and practical level, the sensor network has developed tremendously and the ensuing security issues have garnered more attention. • The life of individuals will be significant impacted by strikes on the electricity meters.

4.7 Sequential Parametric Convex Approximation Technique

The issue of precise metre data gathering could be resolved by looking at the secondary spectrum market in cell towers. Transmission of metre data across leased secondary lines would lower the price of making electrical reservations. In order to reduce overall cost of power and communication, a job called Cost Minimization is established for Meter Data Collection (CMM), which seeks to determine the optimal option for pick and broadcast sequencing. By introducing a new linear constraint whose corresponding line is parallel to curve produced by no curved constraint at the location, it is solved in the previous instalment. The relaxed CMM problem identified as CMM be quickly solved using the SPCA approach. The Transmission AMI, which provides efficient status monitoring, control and pricing through the installation of numerous smart metres in homes, office buildings and enterprises is one of the most crucial components of a power system. The enormous volumes of data that these smart metres will generate would be exceedingly difficult for communication networks to effectively capture. Because to its adaptability, breadth and low cost, network topologies have been considered as more ideal for usage in IoT systems due to the privacy and cost issues with current wired channels of information [44].

4.8 Comparative Analysis

A Comparative analysis is carried out amid the different optimization techniques in smart grid IoT.

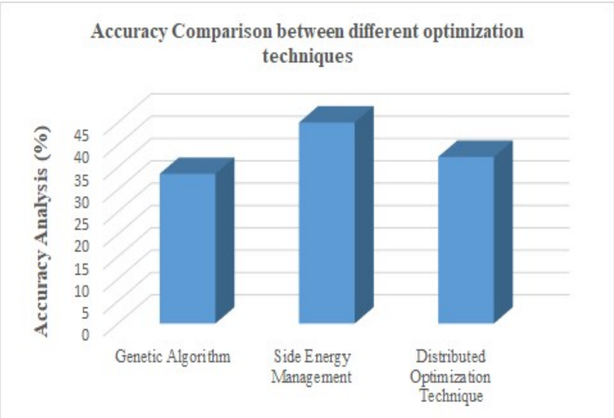

Fig. 9 Various Error test ratings using various techniques.

Fig. 9 shows the different types of error test ratings depending on various types of techniques.

In comparison of these given techniques the average accuracy received by Side energy management technique as 45% is determined to be better and the comparative results will displayed in the Fig. 9. Hence, Side energy management technique has the best prediction of error test monitoring.

5. Conclusion

This study provides a comprehensive analysis of various routing protocols used in the IoT domain, highlighting their operational mechanisms, strengths and limitations. By conducting a detailed comparative evaluation, the survey brings forward the unique characteristics of each protocol to dynamic environments. The discussion also extends to a comparison of cryptographic and optimization techniques applied within these routing frameworks, particularly focusing on their accuracy and effectiveness in enhancing overall network performance. Through this comparative approach, the survey not only emphasizes the trade-offs associated with each protocol but also identifies the suitability of specific routing strategies for different IoT applications. On the whole, this work serves as a valuable reference for researchers and system designers, enabling a deeper understanding of existing routing solutions and assisting in the selection or development of more robust and efficient routing protocols tailored to the evolving needs of IoT networks.

References

[1] Al Mhdawi, A. K., Al-Raweshidy, H. S., A smart optimization of fault diagnosis in electrical grid using distributed software-defined IoT system. *IEEE Systems Journal*. 14 (2020) 2780–2790, doi: https://doi.org/10.1109/JSYST.2019.2921867.

[2] Li, L., Zhao, X., Geng, S. and Zhang, Y., An efficient partially overlapping channels assignment for smart grid IoT with differentiated QoS. *IEEE Access.*7 (2019) 165207–165216, doi: https://doi.org/10.1109/ACCESS.2019.2952125.

[3] Ahmadzadeh, S., Parr, G. and Zhao, W., A review on communication aspects of demand response management for future 5G IoT-based smart grids. *IEEE Access.* 9 (2021) 77555–77571, doi: https://doi.org/10.1109/ACCESS.2021.3082430.

[4] Franco, P., Martinez, J. M., Kim, Y.C. and Ahmed, M. A., IoT based approach for load monitoring and activity recognition in smart homes. *IEEE Access.* 9 (2021) 45325–45339, doi: https://doi.org/10.1109/ACCESS.2021.3067029.

[5] Chen, S., Wen, H., Wu, J., Lei, W., Hou, W., Liu, W., Xu, A. and Jiang, Y., Internet of things based smart grids supported by intelligent edge computing. *IEEE access.* 7 (2019) 74089–74102, doi: https://doi.org/10.1109/ACCESS.2019.2920488.

[6] Guan, Z., Li, J., Wu, L., Zhang, Y., Wu, J. and Du, X., Achieving efficient and secure data acquisition for cloud-supported internet of things in smart grid. *IEEE Internet of Things Journal.* 4 (2017) 1934–1944, doi: https://doi.org/10.1109/JIOT.2017.2690522.

[7] Wang, Z., Liu, Y., Ma, Z., Liu, X. and Ma, J., LiPSG: Lightweight privacy-preserving Q-learning-based energy management for the IoT-enabled smart grid. *IEEE Internet of Things Journal.* 7 (2020) 3935–3947, doi: https://doi.org/10.1109/JIOT.2020.2968631.

[8] Li, X., Huang, Q. anad Wu, D., Distributed large-scale co-simulation for IoT-aided smart grid control. *IEEE Access.* 5 (2017) 19951–19960, doi: https://doi.org/10.1109/ACCESS.2017.2753463.

[9] Ghosh, S., Neuro-Fuzzy-Based IoT assisted power monitoring system for smart grid. *IEEE Access.* 9 (2021) 168587–168599, doi: https://doi.org/10.1109/ACCESS.2021.3137812.

[10] Hussain, S., Ullah, I., Khattak, H., Adnan, M., Kumari, S., Ullah, S. S., Khan, M. A. and Khattak, S. J., A lightweight and formally secure certificate based signcryption with proxy re-encryption (CBSRE) for Internet of Things enabled smart grid. *IEEE Access.* 8 (2020) 93230–93248, doi: https://doi.org/10.1109/ACCESS.2020.2994988.

[11] Saleem, M. U., Usman, M. R. and Shakir, M., Design, implementation, and deployment of an IoT based smart energy management system. *IEEE Access.* 9 (2021) 59649–59664, doi: https://doi.org/10.1109/ACCESS.2021.3070960.

[12] Barbierato, L., Estebsari, A., Pons, E., Pau, M., Salassa, F., Ghirardi, M. and Patti, E., A distributed IoT infrastructure to test and deploy real-time demand response in smart grids. *IEEE Internet of Things Journal.* 6 (2019) 1136–1146, doi: https://doi.org/10.1109/JIOT.2018.2867511.

[13] Abir, S. M. A. A., Anwar, A., Choi, J. and Kayes, A. S. M., IoT-enabled smart energy grid: Applications and challenges. *IEEE access.* 9 (2021) 50961–50981, doi: https://doi.org/10.1109/ACCESS.2021.3067331.

[14] Morello, R., De Capua, C., Fulco, G. and Mukhopadhyay, S. C., A smart power meter to monitor energy flow in smart grids: The role of advanced sensing and IoT in the electric grid of the future. *IEEE Sensors Journal.* 17 (2017) 7828–7837, doi: https://doi.org/10.1109/JSEN.2017.2760014.

[15] Saleem, M.U., Usman, M. R., Usman, M. A. and Politis, C., Design, deployment and performance evaluation of an IoT based smart energy management system for demand side management in smart grid. *IEEE Access.* 10 (2022) 15261–15278, doi: https://doi.org/10.1109/ACCESS.2022.3147484.

[16] Sobral, J. V. V., Rodrigues, J. J. P. C., Rabêlo, R. A. L., Saleem, K. and Kozlov, S. A., Improving the performance of LOADng routing protocol in mobile IoT scenarios. *IEEE Access.* 7 (2019) 107032–107046, doi: https://doi.org/10.1109/ACCESS.2019.2932718.

[17] Lenka, R. K., Rath, A. K. and Sharma, S., Building reliable routing infrastructure for green IoT network. *IEEE Access.* 7 (2019) 129892–129909, doi: https://doi.org/10.1109/ACCESS.2019.2939883.

[18] Al-Janabi, T. A. and Al-Raweshidy, H. S., A centralized routing protocol with a scheduled mobile sink-based AI for large scale I-IoT. *IEEE Sensors Journal.* 18 (2018) 10248–10261, doi: https://doi.org/10.1109/JSEN.2018.2873681.

[19] Tsai, R. -G., Tsai, P. -H., Shih, G. -R. and Tu, J., RPL Based Emergency Routing Protocol for Smart Buildings. *IEEE Access.* 10 (2022) 18445–18455, doi: https://doi.org/10.1109/ACCESS.2022.3150928.

[20] Patel, N. R., Kumar, S. and Singh, S. K., Energy and collision aware WSN routing protocol for sustainable and intelligent IoT applications. *IEEE Sensors Journal.* 21 (2021) 25282–25292, doi: https://doi.org/10.1109/JSEN.2021.3076192.

[21] Zhu, M., Chang, L., Wang, N. and You, I., A smart collaborative routing protocol for delay sensitive applications in industrial IoT. *IEEE Access*. 8 (2020) 20413–20427, doi: https://doi.org/10.1109/ACCESS.2019.2963723.

[22] Haseeb, K., Islam, N., Almogren, A., Din, I. Ud., Almajed, H. N. and Guizani, N., Secret sharing-based energy-aware and multi-hop routing protocol for IoT based WSNs. *IEEE Access.* 7 (2019) 79980–79988, doi: https://doi.org/10.1109/ACCESS.2019.2922971.

[23] Lenka, R. K., Rath, A. K., Tan, Z., Sharma, S., Puthal, D., Simha, N. V., Prasad, M., Raja, R. and Tripathi, S. S., Building scalable cyber-physical-social networking infrastructure using IoT and low power sensors. *IEEE Access.* 6 (2018) 30162–30173, doi: https://doi.org/10.1109/ACCESS.2018.2842760.

[24] Khan, I. U., Qureshi, I. M., Aziz, M. A., Cheema, T. A. and Shah, S. B. H., Smart IoT control-based nature inspired energy efficient routing protocol for flying ad hoc network (FANET). *IEEE Access.* 8 (2020) 56371–56378, doi: https://doi.org/10.1109/ACCESS.2020.2981531.

[25] Biason, A., Pielli, C., Rossi, M., Zanella, A., Zordan, D., Kelly, M., Zorzi, M., EC-CENTRIC: An energy-and context-centric perspective on IoT systems and protocol design. *IEEE Access.* 5 (2017) 6894–6908, doi: https://doi.org/10.1109/ACCESS.2017.2692522.

[26] Lin, J. -W., Chelliah, P. R., Hsu, M. -C. and Hou, J. -X., Efficient fault-tolerant routing in IoT wireless sensor networks based on bipartite-flow graph modeling. *IEEE access.* 7 (2019) 14022–14034, doi: https://doi.org/10.1109/ACCESS.2019.2894002.

[27] Shin, D., Yun, K., Kim, J., Astillo, P. V., Kim, J. -N. and You, I., A security protocol for route optimization in DMM-based smart home IoT networks. *IEEE Access.* 7 (2019) 142531–142550, doi: https://doi.org/10.1109/ACCESS.2019.2943929.

[28] Hussain, S., Ullah, I., Khattak, H., Adnan, M., Kumari, S., Ullah, S. S., Khan, M. A. and Khattak, S. J., A lightweight and formally secure certificate based signcryption with proxy re-encryption (CBSRE) for Internet of Things enabled smart grid. *IEEE Access.* 8 (2020) 93230–93248, doi: https://doi.org/10.1109/ACCESS.2020.2994988.

[29] Bera, B., Saha, S., Das, A. K. and Vasilakos, A. V., Designing blockchain-based access control protocol in IoT-enabled smart-grid system. *IEEE Internet of Things Journal.* 8 (2021) 5744–5761, doi: https://doi.org/10.1109/JIOT.2020.3030308.

[30] Gunduz, M. Z. and Das, R., Cyber-security on smart grid: Threats and potential solutions. *Computer networks.* 169 (2020) 107094, doi: https://doi.org/10.1016/j.comnet.2019.107094.

[31] Saleem, A., Khan, A., Malik, S. U., Pervaiz, H., Malik, H., Alam, M. and Jindal, A., FESDA: Fog-enabled secure data aggregation in smart grid IoT network. *IEEE Internet of Things Journal.* 7 (2020) 6132–6142, doi: https://doi.org/10.1109/JIOT.2019.2957314.

[32] Minh, Q. N., Nguyen, V. -H., Quy, V. K., Ngoc, L. A., Chehri, A. and Jeon, G., Edge Computing for IoT-Enabled Smart Grid: The Future of Energy. *Energies.* 15 (2022) 6140, doi: https://doi.org/10.3390/en15176140.

[33] Agarkar, A. and Agrawal, H., A review and vision on authentication and privacy preservation schemes in smart grid network. *Security and Privacy.* 2 (2019) e62, doi: https://doi.org/10.1002/spy2.62.

[34] Bhuiyan, M. Z. A., Zaman, M., Wang, G., Wang, T., Rahman, M. A. and Tao, H. Protected bidding against compromised information injection in IoT-based smart grid. in *Pathan, AS., Fadlullah, Z., Guerroumi, M. (eds) Smart Grid and Internet of Things (SGIoT 2018)*, (2019) 78–84, doi: https://doi.org/10.1007/978-3-030-05928-6_8.

[35] Choo, K. -K. R., Gritzalis, S. and Park, J. H., Cryptographic solutions for industrial Internet-of-Things: Research challenges and opportunities. *IEEE Transactions on Industrial Informatics.* 14 (2018) 3567–3569, doi: https://doi.org/10.1109/TII.2018.2841049.

[36] Sakhnini, J., Karimipour, H., Dehghantanha, A., Parizi, R. M. and Srivastava, G., Security aspects of Internet of Things aided smart grids: A bibliometric survey. *Internet of things.* 14 (2021) 100111, doi: https://doi.org/10.1016/j.iot.2019.100111.

[37] Alladi, T., Chamola, V., Rodrigues, J. J. P. C. and Kozlov, S.A., Blockchain in smart grids: A review on different use cases. *Sensors.* 19 (2019) 4862, doi: https://doi.org/10.3390/s19224862.

[38] Pawar, P. and Vittal K. P., Design and development of advanced smart energy management system integrated with IoT framework in smart grid environment. *Journal of Energy Storage.* 25 (2019) 100846, doi: https://doi.org/10.1016/j.est.2019.100846.

[39] Iwendi, C., Maddikunta, P. K. R., Gadekallu, T. R., Lakshmanna, K., Bashir, A. K. and Piran, M. J., A metaheuristic optimization approach for energy efficiency in the IoT networks. *Software: Practice and Experience.* 51 (2021) 2558–2571, doi: https://doi.org/10.1002/spe.2797.

[40] Mao, S., Dong, Z., Schultz, P., Tang, Y., Meng, K., Dong, Z. Y. and Qian, F., A finite-time distributed optimization algorithm for economic dispatch in smart grids. *IEEE Transactions on Systems, Man, and Cybernetics: Systems.* 51 (2021) 2068–2079, doi: https://doi.org/10.1109/TSMC.2019.2931846.

[41] Manoharan, H., Teekaraman, Y., Kirpichnikova, I., Kuppusamy, R., Nikolovski, S. and Baghaee, H. R., Smart grid monitoring by wireless sensors using binary logistic regression. *Energies.* 13 (2020) 3974, doi: https://doi.org/10.3390/en13153974.

[42] Tastan, M., Internet of things based smart energy management for smart home. *KSII Transactions on Internet and Information Systems.* 13 (2019) 2781–2798, doi: https://doi.org/10.3837/tiis.2019.06.001.

[43] Yang, Q. and Wang, H., Privacy-preserving transactive energy management for IoT-aided smart homes via blockchain. *IEEE Internet of Things Journal*. 8 (2021) 11463–11475, doi: https://doi.org/10.1109/JIOT.2021.3051323.

[44] Li, P., Guo, S. and Cheng, Z., Joint optimization of electricity and communication cost for meter data collection in smart grid. *IEEE Transactions on Emerging Topics in Computing.* 1 (2013) 297–306, doi: https://doi.org/10.1109/TETC.2013.2273890.

[45] Amjad, Z., Shah, M. A., Maple, C., Khattak, H. A., Ameer, Z., Asghar, M. N. and Mussadiq, S., Towards energy efficient smart grids using bio-inspired scheduling techniques. *IEEE Access.* 8 (2020) 158947–158960, doi: https://doi.org/10.1109/ACCESS.2020.3020027.

[46] Sanchez-Huertas, W., Gómez, V., Hernández, C. Optimization algorithms for solving microgrid and smart grid integration problems. International Journal of Applied Engineering Research. 13(21) (2018)14886–14892.

[47] Wang, K., Wang, Y., Hu, X., Sun, Y., Deng, D. J., Vinel, A. and Zhang, Y., Wireless big data computing in smart grid. *IEEE Wireless Communications.* 24 (2017) 58–64, doi: https://doi.org/10.1109/MWC.2017.1600256WC.

[48] Molderink, A., Bakker, V., Bosman, M. G. C., Hurink, J. L. and Smit, G. J. M., Management and control of domestic smart grid technology. *IEEE transactions on Smart Grid.* 1 (2010) 109–119, doi: https://doi.org/10.1109/TSG.2010.2055904.

[49] Shehadeh, H. A., Idna Idris, M. Y., Ahmedy, I., Ramli, R. and Mohamed Noor, N., The multi-objective optimization algorithm based on sperm fertilization procedure (MOSFP) method for solving wireless sensor networks optimization problems in smart grid applications. *Energies.* 11 (2018) 97, doi: https://doi.org/10.3390/en11010097.

[50] Zhang, K., Hu, Z., Zhan, Y., Wang, X. and Guo, K., A smart grid AMI intrusion detection strategy based on extreme learning machine. *Energies.* 13 (2020) 4907, doi: https://doi.org/10.3390/en13184907.