Secure Edge-Based Energy Management Protocol in Smart Grid Environments with Correlation Analysis

Amjad Rehman 1, Khalid Haseeb 1,2, Gwanggil Jeon 1,3,*, and Saeed Ali Bahaj 4

1 Artificial Intelligence and Data Analytics (AIDA) Lab, CCIS Prince Sultan University, Riyadh 11586, Saudi Arabia
2 Department of Computer Science, Islamia College Peshawar, Peshawar 25120, Pakistan
3 Department of Embedded Systems Engineering, Incheon National University, Incheon 22012, Republic of Korea
4 MIS Department, College of Business Administration, Prince Sattam Bin Abdulaziz University, Alkhairj 11942, Saudi Arabia
* Correspondence: gjeon@inu.ac.kr

Abstract: For the monitoring and processing of network data, wireless systems are widely used in many industrial applications. With the assistance of wireless sensor networks (WSNs) and the Internet of Things (IoT), smart grids are being explored in many distributed communication systems. They collect data from the surrounding environment and transmit it with the support of a multi-hop system. However, there is still a significant research gap in energy management for IoT devices and smart sensors. Many solutions have been proposed by researchers to cope with efficient routing schemes in smart grid applications. But, reducing energy holes and offering intelligent decisions for forwarding data are remain major problems. Moreover, the management of network traffic on grid nodes while balancing the communication overhead on the routing paths is an also demanding challenge. In this research work, we propose a secure edge-based energy management protocol for a smart grid environment with the support of multi-route management. It strengthens the ability to predict the data forwarding process and improves the management of IoT devices by utilizing a technique of correlation analysis. Moreover, the proposed protocol increases the system’s reliability and achieves security goals by employing lightweight authentication with sink coordination. To demonstrate the superiority of our proposed protocol over the chosen existing work, extensive experiments were performed on various network parameters.

Keywords: smart grid; machine learning; communication privacy; conservation; cloud storage

1. Introduction

The IoT can connect people and things with anyone and anything at any time, anywhere, and over any network with the support of wireless technologies [1–3]. It is a vast, dynamic global network infrastructure comprising web-enabled, Internet-connected objects [4–6]. Smart grids are one of the most significant IoT applications that collect data from transmission lines, distribution substations, and consumers. The collected data are forwarded to cloud storage for processing and analysis. A smart grid needs endless, reliable, and real-time connectivity because it handles a significant amount of data and standards [7–9]. Smart meters generate a lot of data, and it might be difficult to store, process, and analyze the data because they vary in size and velocity. Thus, cloud computing is typically used to store and analyze the data produced by a smart grid since it offers real-time response with scalability for a variety of systems [10,11]. Smart technologies are interconnected with the support of sensors to sense the surrounding data and transmit them in a multi-hop manner toward the sink node [12–14].

Although numerous methods have been developed for the effective management of data routing in smart grid applications [15–17], selecting the optimal multipath while
including learning techniques for the autonomous system is a crucial responsibility [18–20]. The learning approaches with the integration of smart sensors have received much research interest. These methods enable autonomous systems to gather and understand the huge amount of data from remote devices [21–23]. Although IoT and wireless systems offer a variety of capabilities for smart grids, their combination causes many research hurdles for communication [24–26]. Such a communication system leads to compromising the sensitive data of a smart grid and decreases device-level trust. Therefore, the purpose of this work is to propose and develop a secure edge-based sensing protocol that efficiently uses energy resources and distributes collected data promptly. The proposed protocol uses numerous paths and trains the system to achieve sustainable communication by predicting the node’s behavior based on correlation analysis. Moreover, cryptographic approaches are capable of detecting malicious activities on grid data and defending the system from threats.

The following highlight the primary contributions of the proposed protocol.

i. A minimal cost value for smart devices is explored for the development and management of energy-efficient smart grids.

ii. A correlation technique is utilized for forwarding tables and extracting the optimal choices for the prediction of routing paths.

iii. To provide authorized access, the edge network and sink node collaborate securely to promptly communicate the sensed data.

iv. The proposed protocol is validated using extensive simulations and experimental results are discussed.

The remaining paper is organized as follows. Section 2 discusses the related work and highlights existing problems. Section 3 demonstrates the significance of the proposed protocol. Section 4 discusses the details of the proposed protocol with the network model. Section 5 explains the system configuration and experimental results. In Section 6, the research work is concluded.

2. Literature Review

Smart grid systems are expanding and developing due to the integration of IoT networks. Moreover, wireless technologies facilitate the grid environment obtaining environmental behaviors and conditions [27–29]. Such technologies manage the information collection and flow of data toward cloud systems with the support of edge computing. For smart grid WSNs, the authors [30] proposed an energy-efficient adaptive fuzzy-based multidisjoint routing protocol (MDRP). The protocol offers an energy-efficient way of choosing the next hop by exploring fuzzy logic. The sink node is used as the root of a spanning tree that is constructed when the next node is chosen to compute the optimal path cost for data transferring. Moreover, the proposed MDRP offers improved performance in terms of network lifetime, packet delivery ratio, and energy utilization. The authors in [31] proposed a unique dynamic-clustering-based, energy-efficient, and quality-of-service (QoS)-aware routing protocol (EQRP) that is motivated by the actual behavior of bird mating optimization (BMO). For WSN-based smart grid applications, the proposed distributed method considerably raises network dependability and decreases unnecessary packet retransmissions. Performance data demonstrated that the proposed protocol successfully decreased end-to-end latency and improved memory utilization, packet delivery ratio, residual energy, and throughput.

In [32], the authors provided an energy-efficient grid-based routing method for sensor networks to maintain the energy in sensor nodes and lengthen the lifetime of the network. To reduce the number of hops in the routing process, routing is also carried out by a grid coordinator that employs fuzzy rules to select the best route. The simulations performed for that work showed that the suggested routing algorithm outperformed other grid and cluster-based routing protocols in terms of residual energy and network lifetime. The authors in [33] proposed a real-time monitoring edge computing system and shift processing from a centralized cloud to edge servers that are close to the device. They developed a scheduling problem to further improve the framework to maximize the benefits.
and provided an intelligent heuristic approach based on the simulated annealing technique. The experiments showed that the proposed framework could enhance the monitoring frame rate by up to 10 times, and decrease the detection delay by up to 85% as compared to the cloud monitoring solution. In [34], preprocessing, clustering, feature selection, and classification were combined to improve security and learning practices. Initially, the network data were clustered using the Markov chain clustering (MCC) model after the feature values had been normalized. The rapid probabilistic correlated optimization (RPCO) process was then used to determine the matching score and particle likelihood in order to choose the optimal features. The predicted label was then classified using the block-correlated neural network (BCNN) method, where the relevancy score is determined by combining feature points and the kernel function. Different performance indicators were employed in the experiments to verify the outcomes of the proposed techniques.

To collect the sensed data by these cell nodes, the authors in [35] proposed a mechanism for geographically segmenting the network into several cells. Cells were split into two groups based on how they communicated with mobile sinks: single-hop communication cells (SCCs) and multi-hop communication cells (MCCs). Mobile sinks moved over two concentric diamond-shaped orbits, such that one sink was always covering one-half of the network. To collect data from sensor nodes, both sinks initially traveled in one direction and stopped at specific intervals in the corners of the orbits. SCCs delivered data directly to sinks when they are stationary, but MCCs used the proposed routing algorithm (EGRPM) to send data to mobile sinks. In [36], the authors provided an energy-aware cluster-based routing protocol (EACRP) for CRSN that simultaneously took into account both energy and dynamic spectrum problems. The reported CRSN schemes are energy-inefficient and have high re-clustering frequency caused by PU operations. The proposed method used self-organized distributed clustering to create an ideal number of clusters, resulting in reduced average node power. The proposed method created clusters with a greater number of common channels to lessen the impact of PU activity and used the idea of cooperative sensing to choose the data channels for intra-cluster communication. EACRP chooses gateway nodes with higher energy, closer proximity to the sink node, and a greater number of shared channels with nearby nodes to improve inter-cluster connectivity.

3. Significance of the Proposed Protocol

IoT devices are growing in the collection, processing, and forwarding of the data of smart grids. Such data must be delivered on time to cloud storage for additional data analysis and to quickly respond to distributed applications. Smart devices not only collect environmental data, but they must also make decisions intelligently before transferring environmental data to cloud systems. Recently, many schemes have been presented for coping with routing issues by reducing energy consumption for smart sensors. However, the majority of existing solutions are unable to effectively control traffic on multiple paths, and fail to maintain the least amount of data damage. Moreover, very few solutions can secure the smart grid, and the sensor network is vulnerable as a result of the presence of multifunctional devices. The proposed protocol examines machine-learning strategies for routing sensing data toward the sink node with the support of gateway devices. The edges perform the role of gateway services and facilitate communication for both the lower and upper tiers. Furthermore, with the support of cryptography principles, the proposed protocol protects the data over unreliable networks in terms of security objectives.

4. Proposed Secure Edge-Sink Collaborated Energy Management Protocol

This section presents a detailed discussion of the proposed protocol, developed for crucial wireless applications in a smart grid environment. To meet the requirements of a smart system with the incorporation of energy efficiency, reliable communication, and secure data management, the proposed protocol provides the least-costly solution with the collaboration of machine-learning techniques and securing sensing data against illegal
events. It also provides optimal multipath routes for the transmission of sensor data at a manageable cost.

4.1. System Assumption and Network Model

In the proposed protocol, each node including sink and edge devices has unique identities assigned. The network field comprises various sensors that are connected in the form of a grid to transmit the data to the sink node. Each sensor node has homogeneous resources with a fixed transmission radius $R$. The following are the system assumptions before designing and explaining the proposed protocol.

i. Smart sensors have minimal transmission range and mobility features.

ii. IoT sensors have a preinstalled global positioning system (GPS).

iii. The sink node is static and all the nodes are deployed randomly.

iv. Each node has enough memory to store and maintain its forwarding tables.

v. Edge devices are placed between the IoT and sink node.

The design of the proposed protocol was composed of two phases. In the first phase, smart sensors were arranged in a unidirectional graph $G$. There were separate links, also called edges $E$, between consecutive nodes $N$. At the start, a distinct value is assigned to each link using the distance parameter; accordingly, each node maintains its forwarding table. The routing is achieved in the form of a multi-hop to reduce the power consumption of the grid nodes. In the proposed protocol, the sink node is assumed to be stronger than the devices due to its adequate processing, storage, transmission, and energy resources. Each node maintains its local information and updates its neighbor to avoid problems in routing decisions. The block diagram for the proposed protocol is shown in Figure 1. It consists of three main phases. First, data are collected from the grid system using the sensors of IoT devices with the integration of wireless algorithms. With the support of edge devices, the data are verified and border nodes are authenticated. Second, using correlation analysis, the weighted value is determined by exploring certain factors. Such a factor balances the load and energy conversation among the grid nodes, and also prolongs the network lifetime. In the end, with the support of the sink node, a strong and more reliable security algorithm is developed that authenticates the devices using hybrid keys and performs integrity functions to attain the trust of the device.

4.2. Discussion

This section explains the proposed protocol. It comprises two components to cope with transmissions and securing data. After node initialization in the grid system, each node creates and stores the collected information inside its forwarding table. The format of the forwarding table consists of the node’s identity $ID$, distance $d$, mobility coordinates $(x, y)$, and value of neighborhoods $n$, as given in Table 1.

| 1 Byte | 1 Byte | 1 Byte | 1 Byte | 2 Bytes |
|--------|--------|--------|--------|---------|
| Identity $id$ | Distance $d_i$ | positioning coordinates $x, y$ | neighborhoods $n$ | fitness $f(x)$ |
Figure 1. Block diagram of the proposed protocol.

The proposed protocol collects the necessary data regarding device identities, and authenticities and stores them on the nearest edge devices. Edge devices also cooperate to transfer the data toward the sink node. Whenever any device $dev_i$ has data to transmit, it retrieves neighboring $N_i$ data from its forwarding table that fall in its transmission radius, as defined in Equation (1).

$$N(dist) \leq R(dev_i)$$  \hspace{1cm} (1)

First, the source node generates route request RREQ and chooses random routes $r_i$ for the available list $r_n$, as defined in Equation (2).

$$r_n = n_1, n_2, \ldots, n_j$$  \hspace{1cm} (2)

Later, it chooses the optimal route from $r'_i$ using K-NN regression, a machine-learning technique [37,38]. In the proposed protocol, we set a threshold to identify and refine the selection process. Accordingly, any node $n_j$ that satisfies the threshold limit is given privileges for competitive computing by using a weighted function. The intelligent approach is used to compute the weighted function. For learning practice, this process is repeated, so the system can become more reliable. Three groups $G_i$, named normal, average, and weak, are made and maintained by the proposed protocol. Furthermore, each node can belong to only one group at a time, as specified in Equation (3).

$$n_i \in G_i$$  \hspace{1cm} (3)
The proposed protocol determines the category of the group by exploring the fitness function \( f(n_i) \), as given in Equation (4).

\[
G_i = f(n_i)
\] (4)

To identify the nearest neighbors, the proposed protocol explores the K-NN regression machine-learning approach. First, it takes \( K \) closest neighbors \( z_k \) from the source node \( y_n \) based on Euclidean distance, as defined in Equation (5).

\[
(y_n)_{n=1}^K = z_1, z_2, z_3, \ldots, z_k
\] (5)

After determining the number of neighbors from the source node, the proposed protocol performs the fitness function for the selection of the most optimal node \( x_i \) for data transmission, as stated in Equation (6). Unlike most of the existing approaches, the proposed protocol explores energy \( e_i \), link estimator \( l_i \), and packet success rate \( p_i \) parameters. To evenly distribute the overhead and traffic distribution across the grid network, such parameters are estimated using weights \( \alpha, \beta, \) and \( \gamma \) with uniform values.

\[
x_i = \alpha e_i + \beta l_i + \gamma p_i
\] (6)

Each node computes the value of link estimation by determining the receiving time of acknowledgements for its transmitted messages. To further optimize the selection process, the proposed protocol utilizes \( f(X'_i) \) the \( n \) set of \( x_i \) computation with the incorporation of error rate \( \mu \), as defined in Equation (7).

\[
f(X'_i) = \sum_{i=0}^{n} X_i + \mu
\] (7)

The edge device stores the data it received and the node’s characteristics in its database. Later, it communicates the reselection process for the forwarder node with the source node whenever any attribute value falls below than threshold. Table 2 provides the table’s format. Figure 2 shows the flowchart of the proposed protocol with sensor technologies. Its main steps are identifying the nearest nodes using the KNN regression and reducing the transmission cost while forwarding the data from the grid system. The group identification divides the nodes into various categories by exploring their behavior and conditions. Lastly, the optimal node is responsible for forwarding the data toward the sink node.

### Table 2. Format of the edge table.

| Identity | Fitness Value | Group | Attributes |
|----------|---------------|-------|------------|
| ID       | \( f(x) \)    | \( G_i \) | \( e_i \)  |
|          |               |       | \( l_i \)  |
|          |               |       | \( p_i \)  |

4.3. Secure Sink Coordination for Route Maintenance

The edge device verifies the data with its store data after receiving them from the border node. If the incoming request is recognized as abnormal, then the identity of the node is blocked, and information is recorded in the database. Additionally, the edge device broadcasts an alarm message to all effective route nodes. Another major contribution of the proposed protocol is to offer a secure route with the highest degree of trust. For this, the proposed protocol utilizes metrics with the integration of secret keys, hashes, and authentication parameters. All these requirements are also satisfied within the sensing nodes and edges to the sink node. We considered the sink node to be more trustworthy and to have more sufficient computational capacity than edges and sensors do, and the proposed protocol gives the sink node the primary responsibility for achieving security. First, it generates a master key \( m_k \) and encrypts the session key \( s_k \) for each node with
associated public key $u_i$, as defined in Equation (8). Sink node $SN$ is responsible for creating the key pool and its management.

$$SN : n_i = Em_k(Eu_i(s_k))$$ (8)

Upon receiving the key, the source node decrypts the incoming message with the $m_k$ of the sink node; later, it decrypts its $s_k$ key using a private key. In this way, each node received its key authentically and securely. Such key information is also shared by the sink node with edge devices to verify the incoming data. Each device uses blocks of data and encrypts them with their keys using cryptographic methods. Additionally, hashing methods are integrated with the encrypted data to provide integrity for sensor data in the context of a smart grid. Figure 3 depicts the procedural flow of the proposed protocol for attaining a secure edge-oriented communication system with the support of a sink node. It has two main components. One is for key generation and node authentication, while the second component is edge verification with secure data transmission. Algorithm 1 shows the steps that govern the development of the proposed protocol.
Algorithm 1: Secure edge-based energy management protocol

Input:
N: nodes.
s_k: secret keys.
X_i: fitness function.
SN: sink node.
GW: gateway devices.
List_N: list of neighbors.

Output: Data forwarders, multiple routes, nearest neighbors, authentic nodes, privacy

Procedure multipaths
for (i=1; i<=N; i++)
do
construct routing tables
store the information
end for
for (i=1; i<=List_N; i++)
extact node information id, d_i, positioning coordinates
compute fitness function X_i = αe_i + βl_i + γp_i
identify group G_i using fitness function
compute error rate f(X_i) = \sum_{i=0}^{n} X_i + \mu
end for
end procedure

Procedure authentic_comm
for each node i ∈ [1 : list_N]
do
SN shares the keys for nodes and edges
Validate the incoming keys and store them in the table
if key = valid
call encryption()
else
record the information in the table
end if
end for

Procedure data_verification()
negotiate edge devices and SN
if authentication is verified
call data transmission()
end procedure

Figure 3. Flow diagram for security measures in the proposed protocol.

5. Simulations and Discussion

This section presents the experimental results and the system configuration. Using NS-3, the performance of the proposed protocol was evaluated in terms of varying nodes and
varying mobility speeds. The sensor nodes were deployed in a grid over a 1000 × 1000 m
area. With a 5 m transmission distance, the sensor nodes were positioned in the targeted
environment. During the simulations, the range of sensors was from 100 to 500. The sink
node was more capable in terms of computing and storage. To assess the security measures,
20 malicious nodes were deployed with 10 edge nodes. The size of the packet was 512 bits.
In comparison to other work, the proposed protocol was evaluated in terms of network
throughput, packet drop ratio, data latency, and energy consumption. During experimental
analysis, 20 simulations were run to validate the performance of the proposed protocol and
existing work. Initially, 12 simulation data were recorded in separate files to create a log for
training and testing the performance results. Each simulation was run for 5000 s. Table 3
shows the list of simulation parameters with their values.

| Table 3. List of simulation parameters. |
|----------------------------------------|
| **Parameters**                          | **Values**                |
| Simulation area                         | 1000 m × 1000 m           |
| Sensor nodes                            | 100–500                   |
| Mobility pattern                        | Random                    |
| Node mobility                           | 3 m/s to 15 m/s           |
| Malicious nodes                         | 20                        |
| Energy of nodes                         | 5J                        |
| Packet size                             | 512 bits                  |
| Number of sink nodes                    | 1                         |
| Control message                         | 25 bits                   |
| Transmission distance                   | 5 m                       |
| Traffic type                            | CBR                       |
| Individual simulation time              | 5000 s                    |
| Edge nodes                              | 10                        |

The experimental findings for network throughput against two scenarios are shown
in Figure 4a,b. Under a varying number of devices and varying node speed, the proposed
protocol gave a higher network throughput by averages of 15% and 18% as compared to
existing work. This was due to the multi-hop transmission of data from the sensors to the
device’s edges, and from the edges to the cloud systems. The proposed protocol also used
correlation analysis to select the most trustworthy neighbors from the routing tables, and it
recorded the updated data for preparing the system for a timely response. Furthermore,
the security of the proposed protocol with the coordination of the sink node lessens the
possibility of unwanted data traffic that interferes with the transmission system. Figure 5a,b
show the evaluation of the proposed protocol and related work in terms of packet loss
rates under a varying number of sensors and varying speed rates. Based on the findings,
the proposed protocol significantly lowered the ratio of packet drops by an average of
10% and 13% when compared to other work. This is because, when they reached their
threshold limits, intelligent and secure routes were obtained based on updated policies.
Furthermore, to train the system and store the estimated weight value in the forwarding
tables, the fitness function uses a variety of realistic characteristics. These values assist
in balancing the data traffic over the communication. Figure 6a,b show the experimental
results for the proposed protocol and existing work using various sensors and mobility
speed levels. According to the findings, the proposed methodology greatly reduced the
data delay by an average of 12% and 15% compared to other relevant studies. This is
because of the selection of data forwarders using correlation analysis and predicting the
most optimal value for the transmission of grid data while reducing unnecessary processing
delays. The proposed protocol also included edges between sensors and sink nodes, which
reduced the response time for the requested devices and efficiently managed the links for forwarding the data of smart sensors. Moreover, the communication sessions were kept secure and validated periodically to increase the longevity of the selected paths. Such methods in the proposed protocol reduce the possibility of communication failure and additional computing demands. Under varying sensors and mobility speed levels, the efficiency of the proposed protocol was evaluated for energy consumption, as shown in Figure 7a,b. According to the analysis of the results, the proposed protocol reduced energy consumption by an average of 11% and 14% when compared to other studies. This was a result of the introduction of reasonable multi-paths that balanced the distribution of energy resources across the devices using an intelligent approach. Furthermore, the proposed protocol used KNN regression analysis to update the route information in the neighboring tables without excessive complexity for the smart grid system. Unlike most of the existing work, the proposed protocol secures the communication routes by integrating authentic sessions among devices, edges, and remote systems. Such an approach reduces the control overheads on the nodes and ultimately increases the energy efficiency of the grid systems.

![Network Throughput Graph](image1)

**Figure 4.** Varying smart sensors and node speed levels in terms of network throughput. (a) Network throughput and varying sensors; (b) network throughput and varying node speed.

![Packet Drop Ratio Graph](image2)

**Figure 5.** Varying smart sensors and nodes speed in terms of packet drop ratio. (a) Packet drop ratio and varying sensors; (b) packet drop ratio and varying node speed.
Figure 6. Varying smart sensors and nodes speed in terms of data delay. (a) Data delay and varying sensors; (b) data delay and varying node speed.

Figure 7. Varying smart sensors and nodes speed in terms of energy consumption. (a) Energy consumption and varying sensors; (b) energy consumption and varying node speed.

6. Conclusions

WSN and IoT are integrated with various industrial applications for the smart monitoring of communication systems. This not only provides remote data collection but also increases the efficacy of wireless devices. In a smart grid, smart sensors and IoT devices perform crucial functions for coping with data gathering and forwarding practices. However, most proposed methods provide energy-efficient solutions at the cost of a huge number of data retransmissions and are not able to balance the overhead in the case of node mobility. In addition, many solutions fail to respond to the query of the requested device due to a lack of optimal routes. Ineffective decisions result in increased energy usage for smart grid applications and a shorter network lifetime. In this study, the following contributions were achieved.

- A secure edge-based sensing protocol was proposed that uses correlation analysis and node behavior based on performance parameters.
- The presence of edges provides prompt responses to the system in crucial circumstances.
- Even in the presence of network threats, sink-oriented collaborative security raises the level of trust across communication systems.
In future work, to increase the scalability and further reduce the overheads on smart sensors, we intend to combine the architecture of a software-defined network with the proposed protocol.

**Author Contributions:** Conceptualization, A.R. and K.H.; methodology, K.H. and A.R.; software, S.A.B. and A.R; validation, G.J. and A.R.; formal analysis, S.A.B. and K.H.; investigation, G.J. and A.R.; resources, G.J. and S.A.B.; data curation, A.R. and S.A.B.; writing—original draft preparation, A.R. and K.H.; writing—review and editing, S.A.B. and G.J; visualization, G.J. and S.A.B.; supervision, A.R. and G.J.; project administration, G.J.; funding acquisition, A.R. and G.J. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** All data are available in the manuscript.

**Acknowledgments:** This work was supported by the research SEED project “Mobile edge computing framework with secure machine learning enabled big data analytics”, Prince Sultan University, Riyadh Saudi Arabia, (SEED-CCIS-2022[108]) under the Artificial Intelligence and Data Analytics Research Lab, CCIS. The authors are thankful for the support.

**Conflicts of Interest:** Authors declare no conflict of interest.

**References**

1. Abdel-Basset, M.; Manogaran, G.; Mohamed, M.; Rushdy, E. Internet of things in smart education environment: Supportive framework in the decision-making process. *Concurr. Comput. Pract. Exp.* 2019, 31, e4515. [CrossRef]
2. Munirathinam, S. Industry 4.0: Industrial internet of things (IIoT). *Adv. Comput.* 2020, 117, 129–164. [CrossRef]
3. Islam, N.; Haseeb, K.; Rehman, A.; Alam, T.; Jeon, G. An adaptive and secure routes migration model for the sustainable cloud of things. *Clust. Comput.* 2022, 1–12. [CrossRef]
4. Al-Turjman, F.; Abujubbeh, M. IoT-enabled smart grid via SM: An overview. *Future Gener. Comput. Syst.* 2019, 96, 579–590. [CrossRef]
5. Chaudhry, H.; Khan, H. Systematic review of IoT security and privacy challenges: A survey. *Wirel. Pers. Commun.* 2020, 115, 1667–1693. [CrossRef]
6. Numani, A.; Gulfam, S.M.; Javed, M.A.; Muhammad, B.; Prasad, R.; Nawaz, S.J. Network Architecture and Wireless Ad Hoc Routing for Airborne Internet Services. *Wirel. Pers. Commun.* 2022, 122, 3529–3543. [CrossRef]
7. Tightiz, L.; Yang, H. A comprehensive review on IoT protocols’ features in smart grid communication. *Energies* 2020, 13, 2762. [CrossRef]
8. Kotsiopoulos, T.; Sarigianidis, P.; Ioannidis, D.; Tzovaras, D. Machine learning and deep learning in smart manufacturing: The smart grid paradigm. *Comput. Sci. Rev.* 2021, 40, 100341. [CrossRef]
9. Kumar, N.M.; Chand, A.A.; Malvoni, M.; Prasad, K.A.; Mamun, K.A.; Islam, F.R.; Chopra, S.S. Distributed energy resources and the application of AI, IoT, and blockchain in smart grids. *Energies* 2020, 13, 5739. [CrossRef]
10. Kumari, A.; Tanwar, S.; Tyagi, S.; Kumar, N.; Obaidat, M.S.; Rodrigues, J.J. Fog computing for smart grid systems in the 5G environment: Challenges and solutions. *IEEE Wirel. Commun.* 2019, 26, 47–53. [CrossRef]
11. Kobusińska, A.; Leung, C.; Hsu, C.H.; Raghavendra, S.; Chang, V. Emerging Trends, Issues and Challenges in Internet of Things, Big Data and Cloud Computing. *Future Gener. Comput. Syst.* 2018, 87, 416–419. [CrossRef]
12. Muthanna, M.S.A.; Muthanna, A.; Rafia, A.; Hammoudeh, M.; Alkanhel, R.; Lynch, S.; Abd El-Latif, A.A. Deep reinforcement learning based transmission policy enforcement and multi-hop routing in QoS aware LoRa IoT networks. *Comput. Commun.* 2022, 183, 33–50. [CrossRef]
13. Faheem, M.; Butt, R.A.; Raza, B.; Ashraf, M.W.; Ngadi, M.A.; Gunog, V.C. Energy efficient and reliable data gathering using internet of software-defined mobile sinks for WSNs-based smart grid applications. *Comput. Stand. Interfaces* 2019, 66, 103341. [CrossRef]
14. Shanmugapriya, R.; Santhosh Kumar, S.V.N. Comprehensive survey on data dissemination protocols for efficient reprogramming in Internet of Things. *Concurr. Comput. Pract. Exp.* 2022, 34, e7280. [CrossRef]
15. Abdella, J.; Shuaib, K. Peer to peer distributed energy trading in smart grids: A survey. *Energies* 2018, 11, 1560. [CrossRef]
16. Hossain, E.; Khan, I.; Un-Noor, F.; Sikander, S.S.; Sunny MS, H. Application of big data and machine learning in smart grid, and associated security concerns: A review. *IEEE Access* 2019, 7, 13960–13988. [CrossRef]
17. Bhattarai, B.P.; Paudyal, S.; Luo, Y.; Mohanpurkar, M.; Cheung, K.; Tonkoski, R.; Hovsapian, R.; Myers, K.S.; Zhang, R.; Zhao, P.; et al. Big data analytics in smart grids: State-of-the-art, challenges, opportunities, and future directions. *IET Smart Grid* 2019, 2, 141–154. [CrossRef]
18. Rani, S.; Koundal, D.; Ijaz, M.F.; Elhoseny, M.; Alghamdi, M.I. An optimized framework for WSN routing in the context of industry 4.0. *Sensors* 2021, 21, 6474. [CrossRef]

19. Tang, F.; Mao, B.; Kawamoto, Y.; Kato, N. Survey on machine learning for intelligent end-to-end communication toward 6G: From network access, routing to traffic control and streaming adaption. *IEEE Commun. Surv. Tutor.* 2021, 23, 1578–1598. [CrossRef]

20. Saba, T.; Rehman, A.; Haseeb, K.; Bahaj, S.A.; Jeon, G. Energy-Efficient Edge Optimization Embedded System Using Graph Theory with 2-Tiered Security. *Electronics* 2022, 11, 2942. [CrossRef]

21. Banafa, M.; Shayea, I.; Din, J.; Azmi, M.H.; Alashbi, A.; Dardkeh, Y.I.; Alhammadi, A. 6G Mobile Communication Technology: Requirements, Targets, Applications, Challenges, Advantages, and Opportunities. *Alex. Eng. J.* 2022, *in press*. [CrossRef]

22. Butt, O.M.; Zulqarnain, M.; Butt, T.M. Recent advancement in smart grid technology: Future prospects in the electrical power network. *Ain Shams Eng. J.* 2021, 12, 687–695. [CrossRef]

23. Jameel, F.; Hamid, Z.; Jabeen, F.; Zeadally, S.; Javed, M.A. A survey of device-to-device communications: Research issues and challenges. *IEEE Commun. Surv. Tutor.* 2018, 20, 2133–2168. [CrossRef]

24. Parra, G.D.L.T.; Rad, P.; Choo, K.-K.R. Implementation of deep packet inspection in smart grids and industrial Internet of Things: Challenges and opportunities. *J. Netw. Comput. Appl.* 2019, 135, 32–46. [CrossRef]

25. Kimani, K.; Oduol, V.; Langat, K. Cyber security challenges for IoT-based smart grid networks. *Int. J. Crit. Infrastruct. Prot.* 2019, 25, 36–49. [CrossRef]

26. Faheem, M.; Shah, S.B.H.; Butt, R.A.; Raza, B.; Anwar, M.; Ashraf, M.W.; Ngadi, M.A.; Gungor, V.C. Smart grid communication and information technologies in the perspective of Industry 4.0: Opportunities and challenges. *Comput. Sci. Rev.* 2018, 30, 1–30. [CrossRef]

27. Al-Obaidi, K.M.; Hossain, M.; Al-Duais, N.A.; Al-Duais, H.S.; Omrany, H.; Ghaffarianhoseini, A. A review of using IoT for energy efficient buildings and cities: A built environment perspective. *Energies* 2022, 15, 5991. [CrossRef]

28. Dileep, G. A survey on smart grid technologies and applications. *Renew. Energy* 2020, 146, 2589–2625. [CrossRef]

29. Lamnatou, C.; Chemisana, D.; Cristofari, C. Smart grids and smart technologies in relation to photovoltaics, storage systems, buildings and the environment. *Renew. Energy* 2021, 185, 1376–1391. [CrossRef]

30. Deepea, K. MDRP: An Energy-Efficient Multi-Disjoint Routing protocol in WSNs for Smart Grids. *Int. J. Smart Sens. Intell. Syst.* 2020, 13, 1–15. [CrossRef]

31. Faheem, M.; Gungor, V.C. Energy efficient and QoS-aware routing protocol for wireless sensor network-based smart grid applications in the context of industry 4.0. *Appl. Soft Comput.* 2018, 68, 910–922. [CrossRef]

32. Logambigai, R.; Ganapathy, S.; Kannan, A. Energy–efficient grid–based routing algorithm using intelligent fuzzy rules for wireless sensor networks. *Comput. Electr. Eng.* 2018, 68, 62–75. [CrossRef]

33. Huang, Y.; Lu, Y.; Wang, F.; Fan, X.; Liu, J.; Leung, V.C. An edge computing framework for real-time monitoring in smart grid. In Proceedings of the 2018 IEEE International Conference on Industrial Internet (ICII), Seattle, WA, USA, 21–23 October 2018.

34. Shitharth, S.; Prasad, K.M.; Sangeetha, K.; Kshirsagar, P.R.; Babu, T.S.; Alhelou, H.H. An Enriched RPCO-BCNN Mechanisms for Attack Detection and Classification in SCADA Systems. *IEEE Access* 2021, 9, 156297–156312. [CrossRef]

35. Naghibi, M.; Barati, H. EGRPM: Energy efficient geographic routing protocol based on mobile sink in wireless sensor networks. *Sustain. Comput. Inform. Syst.* 2020, 25, 103377. [CrossRef]

36. Yadav, R.N.; Misra, R.; Saini, D. Energy aware cluster based routing protocol over distributed cognitive radio sensor network. *Comput. Commun.* 2018, 129, 54–66. [CrossRef]

37. Zhang, S.; Li, X.; Zong, M.; Zhu, X.; Cheng, D. Learning k for knn classification. *ACM Trans. Intell. Syst. Technol.* 2017, 8, 1–19. [CrossRef]

38. Ahmad, R.; Waziralli, R.; Abu-Ain, T. Machine learning for wireless sensor networks security: An overview of challenges and issues. *Sensors* 2022, 22, 4730. [CrossRef]