IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 6 September 2023, accepted 15 September 2023, date of publication 22 September 2023,
date of current version 27 September 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3317883

RESEARCH ARTICLE

Data Encryption-Enabled Cloud Cost Optimization and Energy Efficiency-Based Border Security Model

MOHAMMED F. ALOMARI[1], MOAMIN A. MAHMOUD[2], (Member, IEEE), YUNUS BIN YUSOFF[2], (Member, IEEE), NIAYESH GHARAEI[3], REEMA AHMED ABDALLA[2], AND SARASWATHY SHAMINI GUNASEKARAN[2]

[1]College of Graduate Studies, Universiti Tenaga Nasional, Kajang 43000, Malaysia
[2]Institute of Informatics and Computing in Energy, Department of Computing, College of Computing and Informatics, Universiti Tenaga Nasional, Kajang 43000, Malaysia
[3]Department of Computer Engineering, Engineering Faculty, Ostim Teknik Üniversitesi, 06374 Ankara, Turkey

Corresponding author: Moamin A. Mahmoud (moamin@uniten.edu.my)

This work was supported in part by Tenaga Nasional Berhad (TNB), and in part by Universiti Tenaga Nasional (UNITEN) through the Bold Refresh Publication Fund under Project J510050002-IC-6 BOLDREFRESH2025-Centre of Excellence.

ABSTRACT Effective monitoring of illegal border crossings is a complex problem. Therefore, Border Security Systems (BSS) are deployed at border crossings to detect unauthorised intrusions. Sensor nodes continuously monitor the environment in a BSS and send the generated data to a Control Station (CS). This is then synchronised with the online data storage in the cloud. However, the data that is not needed is also written to the cloud storage, which leads to an increase in the cost of the cloud service. In addition, sensor nodes have limitations in battery performance that lead to irreparable damage in BSSs. Therefore, to overcome the above limitations, a new solution is required to optimize cloud costs and provide energy services for BSSs. To this end, we present a data encryption-enabled cloud cost optimization and energy efficiency-based innovative border security model. In the proposed model, evaluators check the importance of the collected data and send only the data required to CS to reduce the cloud storage cost. Furthermore, the proposed model enhances the energy efficiency of the sensor nodes by utilizing a Power Transmitter Device (PTD) that can charge the consumer devices while moving along a predefined mobility pattern. The proposed model optimizes cloud costs by up to 93%, energy efficiency by up to 50%, and network throughput by up to 11%. Based on the simulation results, the proposed model is plausible and practical compared to similar models.

INDEX TERMS Border security systems, wireless power transmission, wireless sensor networks, cloud storage cost optimization, energy efficiency.

I. INTRODUCTION

In national security and protection, border surveillance is a paramount responsibility. It plays a pivotal role in upholding peace and safeguarding the well-being of a country's citizens; the borders must be monitored around the clock. In recent decades, terrorist infiltrations and illegal movements by living and non-living entities have become common. The least that can be done to curb such operations in border areas is constant surveillance. At present, border security forces carry out this surveillance manually to permanently monitor the borders. Since the boundaries span hundreds of kilometres and are subject to extreme terrain and climatic conditions, this requires a significant workforce commitment and resources. Therefore, it is necessary to develop an automated BSS that can perform the monitoring task without human assistance [1]. It can disregard the need for human intervention in hostile conditions at any given time. In a BSS,sensors are placed at strategic locations along the border to detect people or vehicles entering the country illegally.

The associate editor coordinating the review of this manuscript and approving it for publication was Guangjie Han.

Video monitors and night vision scopes are also used to detect illegal entries. In the past decades, several study groups [2], [3] have attempted to develop Internet of Things (IoT)-based BSSs to improve border security and reduce manpower [4], [5], [6]. A BSS consists of multiple heterogeneous sensor nodes (infrared sensors, CCTVs, fire detectors, radar sensors, etc.) that continuously generate data from their environment and forward it to a Control Station (CS) [7]. The collected data is immediately synchronized with the cloud's online storage as a popular alternative to the local storage system [8]. Each time data is written to the cloud, there is a cost for the write operation, which leads to an increase in the cloud service cost [9], [10]. Nevertheless, to our knowledge, prior systems still need to address this particular issue adequately. As a result, this paper takes the initiative to employ a novel model by utilizing evaluators to distinguish necessary data from cost-wasting ones. Each evaluator is responsible for receiving data from sensor nodes with the same output type and verifying the importance of the collected data. If there is an illegal movement, the data is kept for further processing; otherwise, it is neglected.

Besides, sensors and IoT devices in BSS generate large amounts of sensitive data and transmit it over unsecured Internet. Consequently, ensuring privacy, integrity, and authentication become critical research areas for real-time applications [11]. Moreover, malicious nodes in BSSs can falsely handle the network data and expose the confidentiality of the data. Sensitive data disclosure is even more critical when sensor nodes are used in military applications. Over the past decade, several research groups have conducted experiments to improve data security in IoT-based border surveillance systems. However, in most cases, all data encryption and encoding tasks are performed by the sensor nodes with low-power resources, resulting in end-user devices being burdened with computational overhead.

In addition, energy efficiency is always one of the main concerns of BSSs due to the energy resources available to the sensor nodes [12], [13], [14], [15]. Wireless Power Transmission (WPT) technology has gained considerable and more serious attention in recent years [16], [17]. In WPT-based technology and Power Transmitter Devices, Power Transfer Devices (PTDs) which Consumer devices used to facilitate the movement and recharging of their power supplies [18], [19], [20]. There are several types of research to optimize the movement path of PTD, which result in high computational costs and overhead [21], [22]. Conversely, moving the PTD under a predictable trajectory reduces computational costs and system overheads [23]. Furthermore, in most existing WPT-based systems, PTDs must receive charging requests from sensor nodes and reside at charging locations to charge ground devices within their range [24], [25]. However, charging the consumer devices before reaching a critical threshold improves network performance. Similarly, charging the sensor nodes while the PTD moves along predetermined charging points increases PTD efficiency and extends the network lifetime. Therefore, the proposed model uses a PTD that moves at a constant speed along a predefined motion pattern and continuously charges the nodes in its charging area. When a node reaches a predefined limit, it requests the PTD for recharging, and the PTD moves to its location at the fastest possible speed. The PTD charges the critical node until its remaining energy exceeds the threshold. Then the PTD returns to its previous location along the predefined path. It should also be mentioned that in our proposed model, the threshold of each node depends on its waiting time to reach PTD at its position. A sensor node crosses its threshold if its energy is expected to be depleted before PTD arrives at its location. In addition, to the best of our knowledge, previous border monitoring systems have not considered energy and storage constraints simultaneously. Therefore, this paper presents a data encryption-enabled cloud cost storage optimization and energy efficiency-based border security model to overcome the shortcomings mentioned. The main contributions and novelties of our proposed model are summarised as follows:

- Unlike previous models, this work considers energy constraints, data security, and cloud costs simultaneously.
- Another contribution of the proposed model is the use of evaluators to verify the importance of the collected data, resulting in a reduction of write operations to the cloud storage.
- In this work, we present a secure data collection model that reduces the computational overhead of sensor nodes by shifting data encryption from the energy-limited sensor nodes to the deployed evaluators.
- Unlike existing work, PTD moves according to a predefined mobility pattern, reducing computational costs and overhead.
- PTD in our proposed model can charge the consumer devices while moving along a predefined mobility pattern, resulting in higher efficiency of PTD.
- In our proposed BSS, the batteries of the consumer devices are charged before they reach a threshold, and when the energy level of a device exceeds the threshold, PTD charges it out of order.
- Unlike previous models, we employ a dynamic threshold that varies based on the energy status of each node. It is determined based on the waiting time required for PTD to arrive at its location. This ensures that the sensor nodes do not deplete their energy before arriving at PTD, resulting in longer uptime for the consumer devices.

The subsequent sections of this paper are as follows. Section II reviews the related works. Section III presents the model architecture. The proposed model is presented in section IV. Section V is the simulation results. Section VI provides the discussions on the results. Section VII summarizes the findings.

II. RELATED WORK

This section presents existing studies on cloud cost optimization models, wireless power transmission-based schemes, and secure data-gathering schemes. In [26] to minimize the cost of

data storage management in the cloud, authors proposed optimal and near optimal data object placement algorithms, that minimize residential (i.e., storage, data access operations), delay, and potential migration costs in a dual cloud-based storage architecture (i.e., the combination of a temporal and a backup data center). They evaluate their algorithms using real word traces from twitter. Results confirm the importance and effectiveness of the proposed algorithms and highlight the benefits of leveraging pricing differences and data migration across cloud storage providers. Authors in [27], formulated a system model that consists of a local and a global optimization problem which considers historical data access information and predefined quality of service requirements to select a cost-effective storage solution. they also presented a heuristic optimization approach for global optimization. Detailed evaluations show the benefits of their work compared to a baseline solution that follows a state-of-the-art approach. they showed that their solutions save up to 30% of the cumulative cost compared to the baseline solution.

Authors in [28] proposed two practical online object placement algorithms that assume no knowledge of future data access. The first online cost optimization algorithm uses no replication and initially places the object in the hot tier. Then, based on read/write access pattern following a long tail distribution, it may decide to move the object to the cool tier to optimize the storage service cost. The second algorithm with replication initially places the object in the cool tier, and then replicates it in the hot tier upon receiving read/write requests to it. Additionally, they analytically demonstrate that the online algorithms incur less than twice the cost in comparison to the optimal offline algorithm that assumes the knowledge of exact future workload on the objects. The experimental results using a Twitter Workload and the CloudSim simulator confirm that the proposed algorithms yield significant cost savings (5%–55%) compared to the no-migration policy which permanently stores data in the hot tier. Cosine [29], is a self-designing key-value storage engine that gathers high-quality training data to train its concurrency-aware CPU model. The model requires the workload's degree of parallelism to be known. Cosine learns this by sweeping across different factors (e.g., cloud instance type, number of operations, number of CPU cores) as it executes the workload. In [30],, an optimal data access framework is presented to cache the statistical data of the patients in the application server. The main memory database and cache use internal tracking in the main memory to track records that are not accessed by transferring the data to the disk. This mechanism retains the keys and all indexed fields of evicted records in the main memory which prevents potential memory space savings for the application that have many keys and secondary indexes. Therefore, to overcome the mentioned problems, the cloud database is categorised into three partitions (hot, warm, cold). In addition, a cache memory image in the application server is provided for the hot partition of the cloud database. The use of cache memory image reduces the number of reading operations from the cloud and saves the space of the main memory.

A new recharging model is presented in [13] to enhance the operational duration and efficiency of Wireless Sensor Networks (WSNs), and a novel system is proposed. This scheme utilizes multiple power banks as intermediaries between the sensor nodes and the power transmission device. The power banks act as receivers of power from an energy generator and distribute it to the sensor nodes. Through extensive simulations, the results indicate that the introduced system significantly improves both the operational time of the sensor nodes and enhances security at national borders. While these mechanisms can be essential for improving the performance of boundary protection systems, such work immediately synchronizes all generated data with the cloud's online data storage. It charges a fee for the write operation, thus increasing the cost of the cloud service. Nevertheless, more attention should be paid to solving this problem.

WPT is one of the hottest topics being actively researched and widely commercialized. In particular, the use of WPT in rechargeable sensor networks has developed rapidly. In recent years, several well-designed empirical studies have attempted to deploy energy harvester-equipped PTDs capable of wirelessly transmitting power to rechargeable devices. In [31], a PTD is responsible for moving and recharging the sensor nodes at the charging stations. The researchers employ a heuristic algorithm to identify potential charging locations and determine the best charging time to prevent node failures. Additionally, they utilize a Q-learning technique to ascertain the optimal charging point among the identified candidates. In another study [32], a novel algorithm is proposed to optimize the movement parameters of PTD (Preserving Topological Dynamics) to enhance energy efficiency and prolong the network's lifetime. In their work, the network area is divided into charging regions to charge multiple nodes simultaneously and reduce the waiting time of sensor nodes. In addition, the residual energy of the nodes and the travel time of the PTD are considered when optimizing the travel path of the PTD. The charging time's residual energy is also optimized to extend the network's lifetime. In [33], An innovative two-mode PTD scheduling method is presented, which effectively addresses both wireless energy transfer and data collection in a unified manner. The proposed scheme comprises two main sections: (i) a novel clustering algorithm that takes into account node delay, load balancing, and network topology considerations, the nodes belonging to other charging regions are considered in design issues, (ii) two heuristic PTD scheduling algorithms to meet the different delay requirements of models.

In [34], a fair power distribution scheme has been designed aiming at a durable network operation time. Consequently, the authors aim to enhance the energy efficiency of the wireless sensor nodes by optimizing the energy level transmitted from PTD. This is achieved by identifying the ideal charging time for the PTD at each charging location. In [35], a Charge

Time Optimization of Wireless Mobile Charger (CTOWMC) algorithm is presented that replenishes the nodes' batteries while considering the lifetime of the other sensor nodes, thus reducing the waiting time of the consumer devices and increasing the network lifetime. In [36], the authors try to identify the ideal dwell time for mobile devices within each cluster, ensuring a balanced lifespan for nodes across different network layers. The primary contribution of CMS2TO is the collaboration among nodes from various layers to calculate the dwell time for mobile devices within the residence cluster, thereby enhancing overall network performance. Based on the above discussion, in the previous WPT-based models, PTD can only perform charging while at the charging stations. However, charging the consumer devices while the PTD is moving leads to an increase in the performance and efficiency of PTD. Moreover, in most prior related works, the consumer devices must exceed a threshold to be charged by PTD, reducing the sensor nodes' lifespan.

Wireless sensor networks are particularly vulnerable to attacks because of their inherent characteristics: dynamic topology, large-scale, self-organising, and limited resources. Attacks on WSNs can lead to network anomalies reflected in the information collected about the network. These collected facts are valuable and can be used to detect attacks on the network [37]. In [38], a blockchain-based technology was used to enhance the data security of WSNs. The authors try to reduce data trafficking by using a reset mechanism of the blockchains that constantly updates the data transmission. Their study implemented a system control mechanism and a streamlined process for hash function calculation. Additionally, they enhanced the security of the blockchain by replacing the asymmetric encryption method with symmetric encryption, thereby simplifying the overall security of the system.

In [39], a proposed authentication mechanism aims to identify anti-nodes that manipulate legitimate nodes into staying in active mode continuously. Anti-nodes can not provide a correct acknowledgement (ACK) message in response to encrypted challenge messages from cluster heads. The mechanism is designed for stationary networks, enabling accurate detection of malicious nodes. The authors employ a hash chain for mutual authentication and session key agreement. A hash function and symmetric encryption algorithm ensure confidentiality and integrity. In [40], The authors presented the RED (Randomized, Efficient, and Distributed) protocol to detect replication node attacks in a stationary Wireless Sensor Network (WSN). In this protocol, every node in the network possesses knowledge of its location, which is determined using the technique described in [41]; To enhance security, each node in the network keeps an ID-based pairwise key [42]. To establish its identity and location, a node broadcasts a claim that contains its ID and location, signed with its secret key. Neighbouring nodes participate in the claim broadcasting process with a probability of p. These claims are sent to randomly selected nodes to detect potential collisions. This protocol has been implemented in a stationary network. It can detect malicious nodes and reduce the communication overhead. Reference [49] introduces an intelligent and secure edge-enabled computing (ISEC) model for data transport in Green IoT to improve the monitoring and operation of sustainable cities in terms of energy management and security. Moreover, the linear activation function based on multiple criteria generates reliable actions for data transport with energy saving and improved data delivery performance. It also provides an intelligent and trustworthy routing strategy to measure congestion conditions, which reduces the percentage of data and route failures. Reference [50] aims to provide a secure and energy-efficient framework that supports the Internet of Medical Things (IoMT) for e-Health (SEF-IoMT), whose main objective is to reduce the communication overhead and energy consumption between biosensors while transmitting health data in a convenient way, and on the other hand, to protect patients' medical data from inauthentic and malicious nodes to improve the privacy and integrity of the network. Although previous work has improved secure data transmission, most impose a high network and communication overhead on battery-powered sensor nodes.

III. MODEL ARCHITECTURE

This study presents a model to protect a country's borders from foreign threats using WSNs. The main issue in the proposed model is monitoring areas inaccessible to humans and discovering a secure and energy-efficient border protection model which reduces the cost of cloud services. Remote or isolated locations often need more resources regarding energy and communication capabilities [43]. The proposed model tackles this challenge by implementing diverse Wireless Sensor Networks (WSNs) in regions that demand comprehensive and meticulous surveillance. These heterogeneous WSNs incorporate various sensor types for identification, communication, storage, and processing purposes. This heterogeneity is crucial since a standardized model is not viable when designing a border surveillance system for a country. Different borders exhibit distinct topographies, weather patterns, and threat profiles, necessitating adaptable and tailored solutions. The model should be established based on these characteristics. Radar sensors, infrared sensors, fire detectors, and Closed-Circuit Televisions (CCTV) are the main technologies typically used to detect terrorist activity in border security. In a relatively safe environment, CCTV cameras are the primary means of ensuring security. However, this study focuses on the dangerous border areas and includes CCTVs, infrared sensors, radar sensors, and fire detectors randomly distributed across the border area, as shown in Figure 1. Likewise, using different security sensors provides complete coverage of the scenarios to be detected. In a BSS, the infrared sensors, radars, and fire detectors can only detect an object but cannot discern the object, whether it is benevolent or malevolent. Therefore, CCTVs are used to detect the intent of the object. The optimal solution for border surveillance systems is achieved by leveraging a combination of four

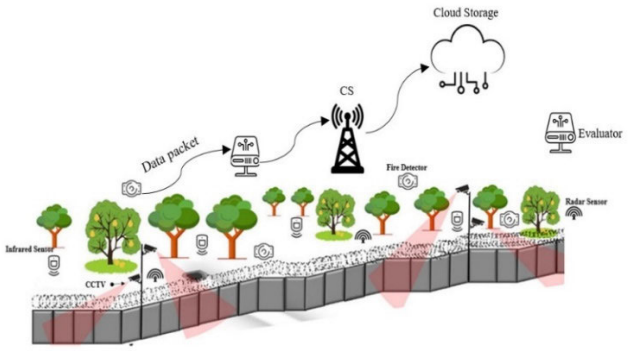

FIGURE 1. Model scenario.

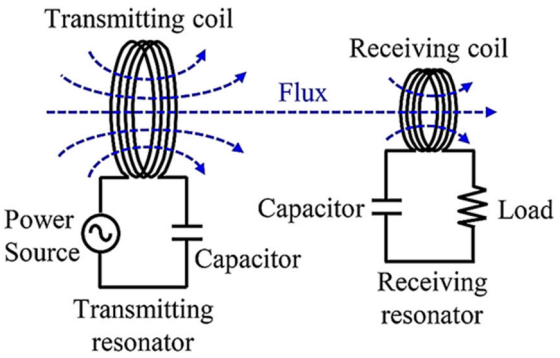

FIGURE 2. Power transmission model.

distinct sensor types [44]. In this work, the radar, infrared, and fire alarm sensors output a logic 1 on the digital output when an object is detected and a logic 0 when there is no object. However, a CCTV outputs analog video images and sends them to an evaluator for further processing. Since the type of output from CCTVs differs from other sensors, two evaluators are used in this model to verify the meaning of the captured data.

The ground devices are equipped with limited batteries, and each consumer device consumes energy to generate data and send it to the respective evaluators. The evaluators evaluate the importance of data and then send it to CS, which is outside the network area. It is assumed that the CS and evaluators have unlimited energy supplies. In the proposed model, a PTD is used to charge the batteries of the consumer devices. It is equipped with solar cells to collect solar energy, and the ground devices are equipped with wireless radio frequency receiving technology that allows them to receive power from the PTD wirelessly as shown in Figure 2. The charging model proposed in [45] is used in this study. Based on [46], The received power (Pr) and transmitted power (Pt) are interconnected, and their relationship is expressed in Eq. (1) as follows:

$$P_r = \frac{G_s G_r \eta P_t}{L_P} \left(\frac{\lambda}{4\pi\ (d+\beta)} \right)^2 \tag{1}$$

The transmitter and receiver are denoted as Gs and Gr, respectively. Likewise, the rectifier efficiency, polarization

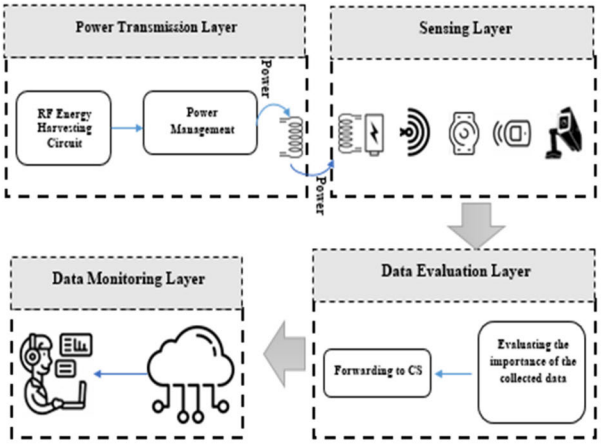

FIGURE 3. System architecture.

loss, and wavelength are represented by η, LP, and λ, respectively. The distance between the receiver and transmitter is indicated by d.

The model architecture comprises four layers, illustrated in Figure 3. The initial sensing layer, comprises security sensor nodes responsible for monitoring the surrounding environment and transmitting the gathered data to their respective evaluators. The data evaluation layer consists of two evaluators responsible for receiving data from a sensor and verifying the importance of the collected data. In the data monitoring layer, the collected data is monitored in real-time by a guardian online 24/7 and uses a Graphical user interface (GUI). In the power transmission layer, a PTD is equipped with solar cells to harvest solar energy, and the sensor nodes are provided with wireless radio receiving technology to receive power from the PTD wirelessly. Figure 4 shows the block diagram of the model.

IV. DATA ENCRYPTION-ENABLED CLOUD COST OPTIMIZATION AND ENERGY EFFICIENCY-BASED BORDER SECURITY MODEL

The proposed model consists of three mechanisms called the Pre-Evaluation-based Cloud Storage Cost Optimization (PECSCO) mechanism, Evaluator-side Secure Data Gathering (ESDG) mechanism, and the Real-time Recharging of Consumer Devices (R2CD) mechanism. The first mechanism aims to improve cloud storage optimization using evaluators, the second aims to achieve secure data transmission between nodes to the cloud, and the third seeks to increase consumer devices' energy efficiency through a PTD.

A. PRE-EVALUATION-BASED STORAGE OPTIMIZATION (PECSCO) MECHANISM

For the last few years, cloud computing got attention from the research community. The cloud computing platform is designed to provide compute-intensive and storage-intensive services to users on a pay-as-you-use basis. Cloud computing resources are distributed across different locations in the form

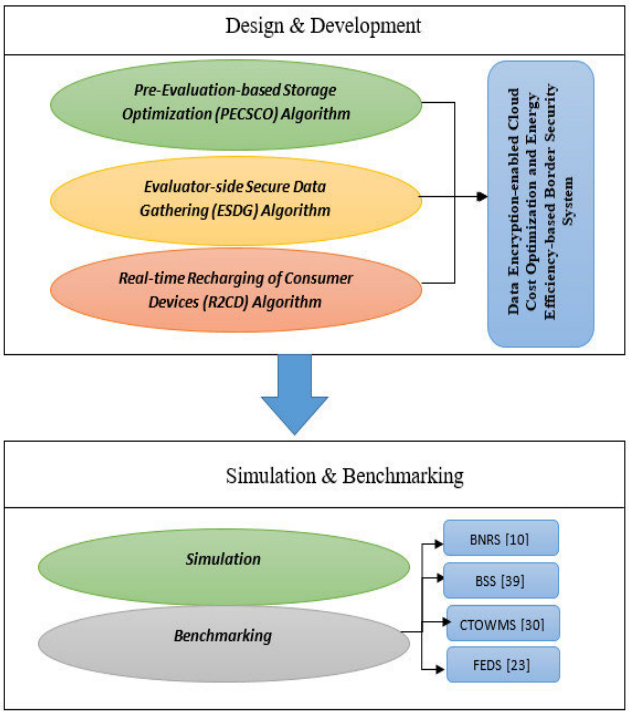

FIGURE 4. Block diagram of the model.

of large data centers that are interconnected in a distributed manner. Then, the data collected by the sensors is forwarded to the computing engine or the cloud for analysis and displayed to the user. Each time data is written to the cloud storage, a mandatory cost is charged for the WSN. This cost is different from a cloud server provider to another one. During the last few years, several cloud cost optimization-based schemes have been presented to reduce the write and read operation costs in cloud storage. Most of them could enhance cloud cost optimization with high computational overhead. Based on the literature review, most previous works attempt to partition the cloud storage using data object placement algorithms, increasing the computational overhead. In most applications, such as border security systems, the deployed sensor nodes continuously monitor the environment. The generated data is sent to a CS and then synchronized with cloud storage without verifying the meaning of the synchronized data. However, the cloud servers charge their users for the amount of data transferred to and from the cloud storage, and the systems incur a higher cost for the cloud storage. Therefore, it is necessary to evaluate and verify the importance of the data before synchronizing it with cloud storage. One of the contributions of this research is to develop the PECSCO mechanism, which aims to eliminate the drawbacks mentioned above of existing schemes.

In the PECSCO mechanism, two evaluators are employed to receive the data generated by the sensor nodes, distinguish the necessary data from the cost-wasting data, and send it to a CS. The evaluators are intermediaries between the consumer sensor nodes and CS. In this mechanism, a GA is utilized to determine the optimal positions of evaluators. After deploying the evaluators, they receive data from nodes and check their importance. The first evaluator receives the recorded analog video from the video surveillance equipment and reviews the recorded video. In case of illegal movements, the data is sent to the CS. The second evaluator receives the digital output from the radar, infrared and fire detection sensors and verifies the data. If an unsafe situation exists, the collected data is sent to CS. Then, the generated data is sent from CS to the cloud storage. The proposed mechanism consists of three phases: Recognizing Sensor Output Data, Optimal Position of Evaluators and Checking the Importance of Data. In the first phase, the CS is responsible for detecting the sensors' output type. Then, in the second phase, Genetic Algorithm (GA) is exploited to optimize evaluators' positions, and in the third phase, the importance of data is checked.

1) RECOGNIZING OF SENSORS OUTPUT

In the proposed model, as there are two types of data (analogue video output and digital output) in the network, CS needs to recognizes the type of sensors and their outputs. Therefore, first, CS broadcasts its location to the sensor nodes and requests them to send their locations and generated data to its location. Then, it divides the nodes into two groups. The first group comprises the CCTVs with analogue video outputs, and the second group includes other nodes with digital outputs. Then, CS assigns an Evaluator_ID to each sensor node which can be 1 or 2, which denotes that each sensor node belongs to which evaluator. To inform sensor nodes about their Evaluator_ID, CS sends information packets to sensor nodes.

2) OPTIMAL POSITIONS OF EVALUATORS

In the WSNs, sensor nodes consume energy for transmitting their data packets to their destination devices [51]. In addition, the energy consumption of sensor nodes for transmitting sensory data depends on their communication distance. Accordingly, the distances between nodes and evaluators as their destination should be optimized to reduce their energy consumption. Therefore, in this phase, the optimal locations of evaluators are determined. To this end, CS is responsible for calculating their locations.

Since the evaluator's positioning is an NP-hard problem, the GA technique is utilized to obtain the optimal exclusive positions of evaluators. The cost function is defined based on the minimization of the distance between nodes and evaluators. Therefore, the cost function of the proposed GA can be formulated by Equation, where n is the total number of nodes in the network.

$$Cost = \min\left(\sum_{i=1}^{n} distance(Evaluator, Node(i)\right) \quad (2)$$

3) CHECKING THE IMPORTANCE OF DATA

After deploying evaluators at the optimal locations, each evaluator floods advertisement messages to its sensor nodes

to make all nodes within the network aware of the evaluators. The advertisement message comprises the evaluator's identity (ID), its geographical position. Upon receiving the message, sensor nodes forward it to their neighbours until all the nodes inside the network are informed about evaluator information. Nodes ignore the advertisement message if their ID differs from their Evaluator_ID received from CS.

In the proposed model, the first evaluator receives the recorded analogue video from the video surveillance system and reviews the recorded video. In case of illegal movements, the evaluator cuts out the desired part of the video and sends it along with the details (date, time, and location of the video surveillance) to CS. The second evaluator receives the digital output from the radar, infrared, and fire detection sensors and verifies the data. If an unsafe situation exists (the digital output is logic 1), the event's details (date, time, location) are sent to the CS in addition to the collected data. Then, the generated data is sent from CS to the cloud storage, which is available to the guard who is online 24/7.

B. EVALUATOR-SIDE SECURE DATA GATHERING (ESDG) MECHANISM

Wireless sensor networks (WSNs) are used in a variety of applications. Attackers can jam the devices and eavesdrop on conversations. Attackers can also modify the transmitted data or connect unauthorized devices to the network when such devices are deployed in the physical environment. Security or cybersecurity is about keeping transmitted information safe and secure from unwanted access. Weak security measures mean unauthorized access to data. In a military application that uses the IoT, unauthorized access to sensitive data will cost more than money. There are several approaches to prevent unauthorized access, such as strong authentication, data encryption, monitoring tools, etc. Data encryption is one of the most effective techniques to ensure end-to-end security. The application of encryption algorithms by sensor nodes is impossible due to the technical limitations of nodes in an IoT network, such as limited memory and low processing power. Therefore, it is required to develop a mechanism that reduces the burden of encryption duty from the low-power nodes to other resource-rich devices. One of the contributions of this research is to develop the ESDG mechanism, which aims to eliminate the drawbacks of existing schemes.

In the ESDG mechanism, the utilized evaluators are responsible for encrypting the essential data before forwarding it to the CS. To this end, the input of the first evaluator is the videos received from CCTVs, and the input of the second evaluator is 1 or 0 received from other sensor nodes. The evaluators evaluate the data before forwarding it to the CS. If there is any illegal movement, they encrypt the data. After adding the authentication code of the node that generates the corresponding data and the details of the event (date, time, location), the evaluator forwards the encrypted data packet to the CS. After successfully verifying the secret value by CS, the encrypted data is forwarded towards cloud servers to access data. This section presents the detailed working of the ESDG model to secure the data transferred from nodes to the cloud storage. The proposed mechanism consists of two main phases, Agreement and Data Encryption. In the first phase, an agreement between CS, evaluators and cloud storage is performed, and in the second phase, data is encrypted using the proposed methods. A detailed discussion of each stage is presented in the following subsections.

1) AGREEMENT

In the proposed algorithm, after receiving and evaluating the data, evaluators encrypt the data packets and send them to the CS. The proposed protocol uses the International Data Encryption Algorithm (IDEA) [25], based on symmetric-key block cyphers. This algorithm is based on mathematically related keys; the data information encrypted using a key can be decrypted by using only a specific related key. A pair of keys comprises a public key and an undisclosed or private key. For example, a public key is like a bank account, while a private key is like the account's password or the account owner's signature. In the proposed mechanism, at each time unit, the CS creates a key stream as given $\sum_{i=1}^{n} K$ from the set of random bits and then encrypts K using the private key as given K' = PRCS (K), later the evaluators decrypt the incoming K' from the public key of CS as given PUCS (K'). CS also forwards the exact information of K to cloud servers using PRCS and PUCS keys.

2) DATA ENCRYPTION

In the proposed mechanism, upon receiving the data packets from nodes and K' from CS, the evaluators evaluate the data, encrypt the required data, and send it to the CS. As evaluators have different collected data types, the evaluators use other models to encrypt the collected data. To this end, the first evaluator generates a secret key as given $K' = \sum_{i=1}^{n} SK$ from the set of random bits and determines the decimal value of K' as k= Decimal(K'). To encrypt the data packets, the evaluator divides the data into k equal-sized blocks and adds each bit of SK at the end of each block as given in Eq.2. After adding the authentication code of the node that generates the corresponding data and the details of the event (date, time, location), evaluator forwards the encrypted data packet to the CS.

$$ED = \left(\sum_{i=1}^{k} \left(\sum_{j=(i-1)(\frac{Length(Data)}{k})}^{(i)(\frac{Length(Data)}{k})} Data\,(j) + SK(i) \right) \right) + MAC + Details \tag{3}$$

After successfully verifying the secret value, CS transfers the encrypted data to the cloud server, and the cloud server decrypts the data as follows.

$$D = \left(\sum_{i=1}^{Decimal\,(K')-1} \left(\sum_{j=(i)\left(\frac{Length(E)}{Decimal(x)}\right)+1}^{(i)(\frac{Length(E)}{Decimal(x)})} ED\,(j) \right) \right) \tag{4}$$

The input of the second evaluator is 0 or 1. After evaluating the received data, the evaluator generates a secret key as

given $\sum_{i=1}^{m} SK$ and calculates the decimal value of K' as k=Decimal(K'). Then, the evaluator encrypts the required data packets by dividing the SK into two unequal-sized sections and adding the data between two sections as follows:

$$ED = \left(\sum_{i=1}^{k} (SK(i)) + Data + \sum_{i=k+1}^{m} SK(i)\right) + MAC + Details \quad (5)$$

Then, the authentication code of the node that generates the corresponding data is added to the end of the data packet, and ED is forwarded to the CS. After successfully verifying the secret value, CS transmits the encrypted data to cloud servers that access data as given following:

$$D = (ED(k+1)) \quad (6)$$

C. REAL-TIME RECHARGING OF CONSUMER DEVICES (R2CD) MECHANISM

Power constraint of consumer devices is one of the significant challenges in BSSs, as these sensors are deployed in inaccessible areas where it is impossible to replace or recharge the sensor node batteries manually. The WPT technique is a promising solution to improve the energy efficiency of consumer devices in harsh and inaccessible areas. This technique uses a PTD that moves within devices on the ground to recharge their energy supplies wirelessly. There are several researches which have been conducted to optimize the movement path of PTD that leads to high computational cost and overheads. However, moving the PTD under an unpredictable trajectory results in reducing computational cost and system overheads. Furthermore, in most existing WPT-based systems, PTDs must receive charging requests from sensor nodes and reside at charging locations to charge ground devices within their range. However, charging the consumer devices before reaching a critical threshold leads to an improve system performance. Likewise, recharging the sensor nodes during movement of PTD along predetermined charging locations leads to an increase in PTD efficiency and enhances the network lifetime. Therefore, to address the aforementioned limitations, in this section, a Real-time Recharging of Consumer Devices (R2CD) mechanism is presented.In our R2CD algorithm, the PTD starts to move from the centre of the network on a predefined spiral mobility pattern with constant angular velocity and charges the nodes. The reason for choosing the spiral motion of the PTD is that the PTD can cover and meet all the devices during its movement. Likewise, in the proposed mechanism, the PTD moves on a predefined mobility pattern and recharges the sensor nodes during its movement. We calculate a threshold for each sensor node. If any node exceeds its threshold, the PTD moves toward the node and starts to recharge its battery until the node exits the critical situation. Then, PTD comes back to its previous location as fast as possible. It should be noted that if PTD receives multiple charging requests from different nodes simultaneously, the node with the lower lifetime gets the higher priority. The lifetime of a consumer device is calculated as follows:

$$LT\ (i) = \frac{E_{Rem}(i)}{E_{Con}(i)} \quad (7)$$

where ERem and ECon denote the remaining energy of the node and energy consumption of the node at each time unit, respectively.

1) ON-SCHEDULE RECHARGING

In this phase, the PTD moves on a predefined spiral mobility pattern with constant angular velocity and charges the nodes. To this end, in the beginning, the PTD broadcasts a request message among sensor nodes and requests their position information. After receiving the information from sensor nodes, it starts to move from the centre of the network, and in each unit of time, it calculates the distance between nodes to its current location using Equation 8.

$$d = \sqrt{(x_{node} - x_{PTD})^2 + (y_{node} - y_{PTD})^2} \quad (8)$$

If the distance between a node and its location is less than its charging range, it recharges the node's battery until it exists from its charging range.

2) THRESHOLD CALCULATION

The sensor nodes consume energy in the proposed mechanism to generate and transmit data packets. Therefore, they may exhaust their energy reserves before the PTD arrives at their location. To address this problem, a threshold must be set for each sensor node that allows them to be recharged off-schedule. When a node's remaining energy is below its threshold, the sensor node informs the PTD of its remaining energy and requests a recharge from the PTD as soon as possible. Unlike previous schemes, a unique threshold is determined for each sensor node as follows:

$$Thr(i) = \frac{\omega}{Speed} \times E_{Con}(i) \quad (9)$$

In the above equation, Speed denotes the velocity of PTD, Econ is the energy consumption of the ith node in a time unit, and ω is the distance between PTD which is calculated as follows:

$$\omega = \left(\int_{0}^{(2\eta)\pi} (r^2 + \frac{dr}{d\theta})d\theta\right) \quad (10)$$

where r is the radius of the network area, and η is determined by dividing r by the power transmission range of PTD. After receiving the charging request, the PTD leaves its current location and moves toward the critical node as fast as possible. If PTD receives multiple charging requests from different nodes simultaneously, the node with the lower lifetime receives the higher priority. The lifetime of a consumer device is calculated as follows:

$$LT\ (i) = \frac{E_{Rem}(i)}{E_{Con}(i)} \quad (11)$$

where ERem denotes the remaining energy of the node.

3) OFF-SCHEDULE RECHARGING

After arriving at the PTD at the location of the critical sensor node, it starts charging the battery of the critical node as much as it left the pressing situation. The required energy level is calculated as follows:

$$\sigma\ (i) = Thr\ (i) - E_{Rem}\ (i) + \beta(\beta \geq E_{Con}) \tag{12}$$

Eq. (13) represents the charging time of PTD (Power Transfer Device) at the critical node location, where ERem denotes the remaining energy of the node. A constant value β is incorporated to ensure that the remaining energy of the node remains above the threshold after the critical node has left. Then, the charging time is calculated as follows:

$$CT\ (i) = \frac{\sigma(i)}{T'} \tag{13}$$

where T' is the amount of energy transferred to the node's batteries over time. Then, it sets its timer and recharges the node until it expires. At the end of the charging time, the PTD returns to the previous location and continues moving along the predefined path.

V. SIMULATION RESULT

A. SIMULATION ENVIRONMENT

In this paper, OMNET++ is used to simulate the proposed model. OMNET++ is a network simulation framework built on an object-oriented, modular architecture and utilizes discrete event modelling. Due to its flexible design and modularity, OMNET++ has gained tremendous popularity in the research community and network communication. In the proposed model, we studied the U.S.-Mexico border because this border has experienced a massive security upgrade since 2001, and the borderline has hardened and slowly divided people into both sides. In fiscal year 2021, the U.S. Border Patrol documented over 1.6 million instances of encountering migrants along the U.S.-Mexico border. This figure surpassed the previous fiscal year's numbers by more than fourfold and represents the highest annual total ever recorded [4]. In the proposed model, an area of 3,145 km is populated with randomly distributed 500 to 800 sensor nodes of various types. The default simulation parameters, which are chosen in this study, are summarized in Table 1. Moreover, the simulation parameters for Physical (PHY), Medium Access control (MAC), transport and network layer are defined in Table 2.

TABLE 1. Simulation parameters.

parameter	Define of parameters	Value
n	Path loss exponent	2
α	Energy dissipated in the op-amp	0.0013e-12
E_{elec}	The electrical energy consumption	50e-9
E_{agg}	Energy consumption for data aggragation	5e-9
M	Total number of nodes	100~450
R	The network radius	50~2000 m^2
$\mathcal{E}0$	Initial energy of each node	0.5 J
speed	The velocity of PTD	0.5m per sec
l	Data packet length	2000 bit

TABLE 2. PHY, MAC, network and transport layers parameters.

Parameters	Values
MAC	IEEE 802.15.4
Transport Layer Protocol	UDP
Antenna	Omni-Directional
Propagation Model	Two Ray Ground
Channel Bandwidth	11Mbps

B. PERFORMANCE EVALUATION

The accuracy of the simulation results of proposed PECSCO, ESDG and R2CD remarkably shows the credibility of these mechanisms when compared with other relevant algorithms. In this paper, the performance of proposed three mechanisms is evaluated under numerous set of simulation experiments. PECSCO is compared to relevant cloud cost optimization based schemes that were utilized in ODAF [30] and COSINE [29]. PECSCO is compared to such mechanisms as they attempt to reduce the cloud cost using different methods. ESDG is compared to relevant secure data transmission based algorithms that were utilized in SEF-IoMT [50] and ISEC [49]. Finally, R2CD is compared to CTOWMC [35] and FEDS [34]. R2CD is compared to such WPT based mechanisms as they attempt to optimize the trajectory of PTD. To validate the experimental results, our proposed mechanisms and relevant algorithms are evaluated under same network environment.

Figure 4.2 shows the number of writes to the cloud storage in three other models in varying number of write operations. As can be seen, the number of writes to the cloud storage decreased in PECSCO in compared with two other models. The reason behind this, employing evaluators as the brokers between nodes and CS. In both ODAF-TS and OCOA models, it is attempted to reduce the write operations by partitioning the cloud storage to avoid writing the redundant data packets. However, utilizing evaluators and checking the importance of data before forwarding to cloud storage leads to reduce the number of write operations at the cloud storage remarkably.

Figure 5 shows the cloud cost during a month in three different models. We consider 0.5 dollar for each write operation at the cloud storage. Obviously, over time leads to increase the cloud cost in three models. However, as can be observed, PECSCO reduces the cloud cost due to utilizing the evaluators and checking the importance of data before forwarding to the cloud storage.

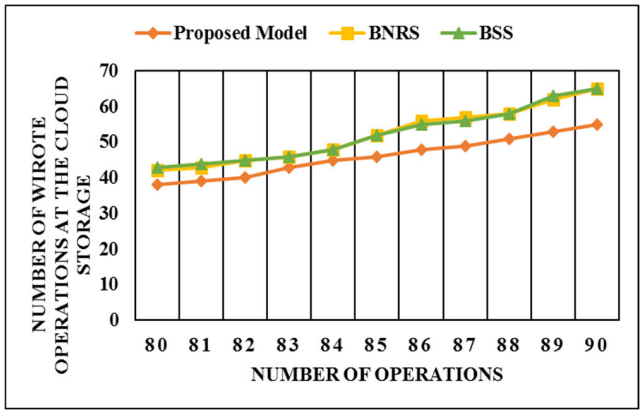

FIGURE 5. Number of write operation.

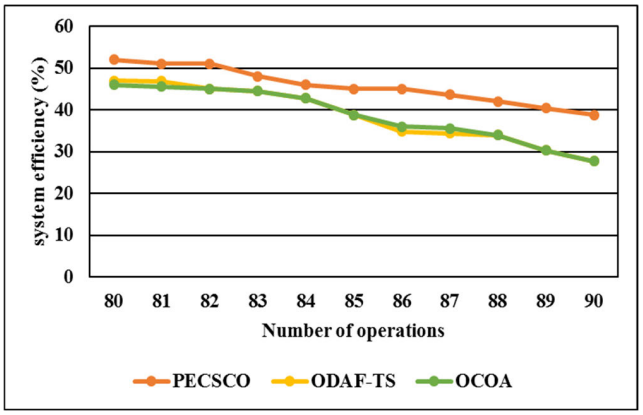

FIGURE 7. System effeciency.

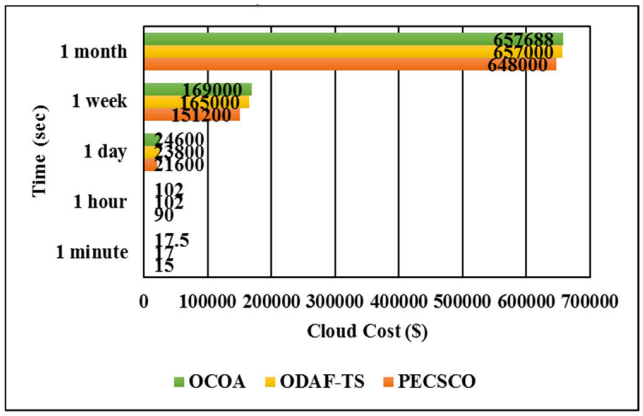

FIGURE 6. Cloud cost.

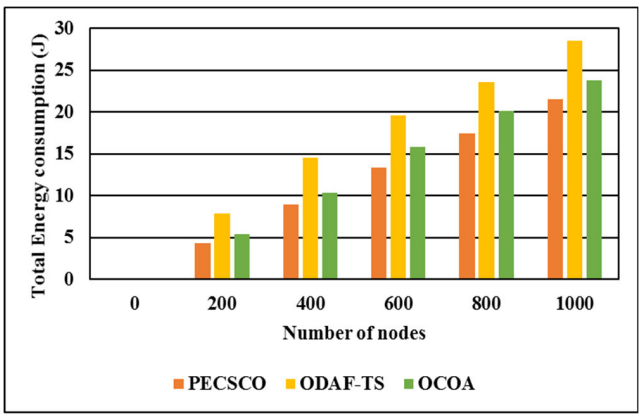

FIGURE 8. Total energy cosumtion.

Figure 6 depicts the system efficiency in three different models by varying number of operations. System efficiency is defined as the number of write operations reduced by employing different schemes. Higher the system efficiency signifies better network performance. obviously, by increasing the number of operations the system efficiency is reduced. This is because, by increasing the number of operations, the number of write operations and important data increases. As seen, employing evaluators leads to enhance the system efficiency in our proposed PECSCO in compared with OCOA and ODAF-TS.

Utilizing evaluators as intermediaries between sensor nodes and CS reduces the nodes' data transmission range and energy consumption. This is because there is a direct relationship between a node's energy consumption and distance from the target device. Figure 8 shows the energy consumption of sensor nodes in three different schemes by varying number of deployed nodes. evidently, increasing the number of sensor nodes leads to increase the energy consumption of the network. likewise, from the result shown in Figure 8, it can be seen that the total energy consumption of the nodes could be reduced by up to 17% after using evaluators.

In figure 9, the experimental results are illustrated to show the performance evaluation of energy consumption.

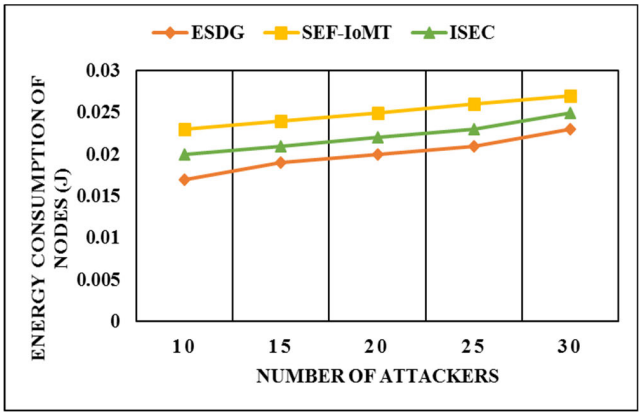

FIGURE 9. Total energy consumtion of nodes.

It is observed that the energy consumption increases due to transmitting of excessive control messages. However, the numerical analysis reveals that the ESDG model improves the energy consumption by 14% and 8% as compared to the existing solutions under a varying number of attackers. This improvement is due to the fact that, unlike related works, in the ESDG model, the data encryption and transmitting control messages duties are transferred from energy limited

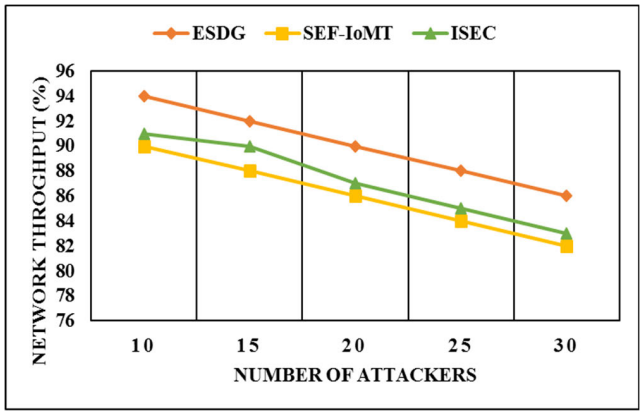

FIGURE 10. Network throughput.

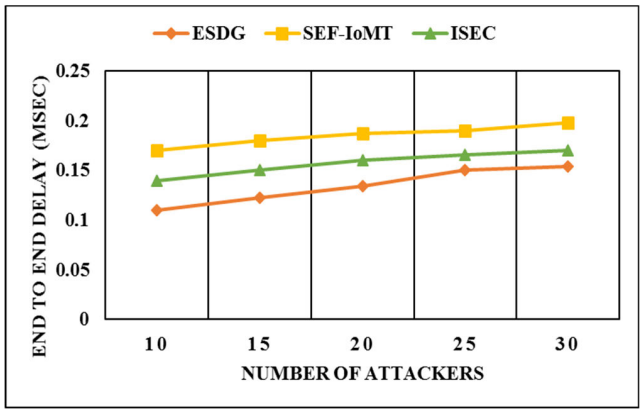

FIGURE 11. End to end delay.

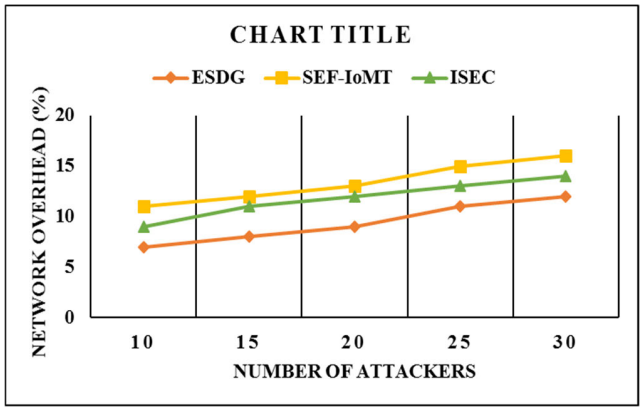

FIGURE 12. Network overhead.

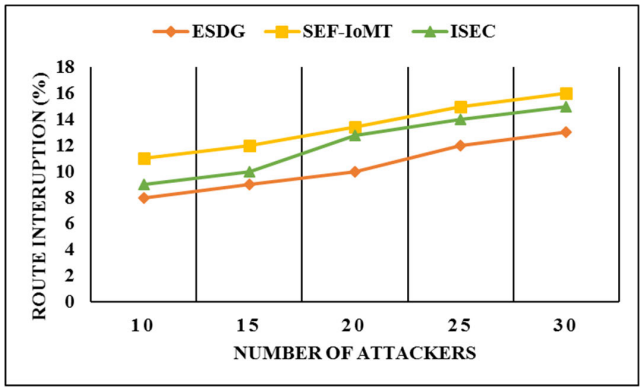

FIGURE 13. Route interuption.

sensor nodes to power rich evaluators, which leads to reduce the energy consumption of sensor nodes and enhance their energy saving. Further, employing evaluators leads to reduce the data transmission range of nodes and enhance their energy efficiency.

Figure 10 compare the network throughput of the ESDG mechanism with the existing schemes. The numerical results indicate that the ESDG mechanism has an increase in the network throughput by an average of 5 % and 4 % in comparison with other work for the varying number of attackers. The improvement of the ESDG against the existing schemes is due to energy-efficient, and secure design with the least network overheads. Also, it increases the fraction of delivery performance due to avoiding fake malicious packets by network attackers and reduces the options of congestion which leads to enhance the data delivery ratio and increase the network throughput.

Figure 11 depict the experimental results of the ESDG model against the existing solutions for the varying number of attackers and edge servers. It is revealed from the numerical analysis that the ESDG model decreases the delay ratio by an average of 22 % and 9 %, respectively. The reason of delay reduction in sending the sensors' data from a source point to the destination is that the ESDG model adopts reliable and secure based data transmission from nodes to cloud server. Moreover, unlike previous schemes, the proposed mechanism employed direct data transmission manner between nodes and their destination, which leads to reduce the latency and end to end delay.

Figure 12 demonstrate the experimental results for varying network attackers and edge servers. The numerical analysis reveal that the ESDG mechanism decreases the network overheads by an average of 14 % and 16 %, respectively. The improvement of the ESDG mechanism is due to an evaluator side secure data transmission manner, which reduces the data encryption duty from nodes to evaluators. In addition, as there is a direct relationship between the energy consumption of nodes and network overhead, utilizing evaluators leads to reduce the data transmission range of nodes and their energy expenditure leads to enhance the energy saving of nodes and reduce the network overhead.

Figure 13 illustrate the performance comparison of the ESDG model with the existing solutions for route interruption under varying attackers. The numerical analysis shows that the ESDG mechanism minimizes route breaches by 19 % and 13 % in comparison with the existing studies. This reason is such that the ESDG offers more reliable and secure communication channels among data forwarders. The sensors' data is forwarded in the form of blocks, and each block is

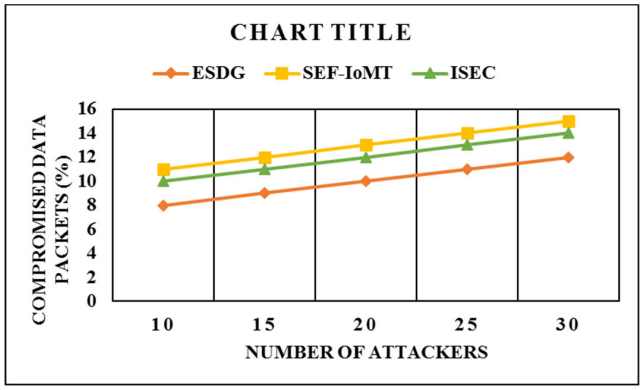

FIGURE 14. Compromised datapackets.

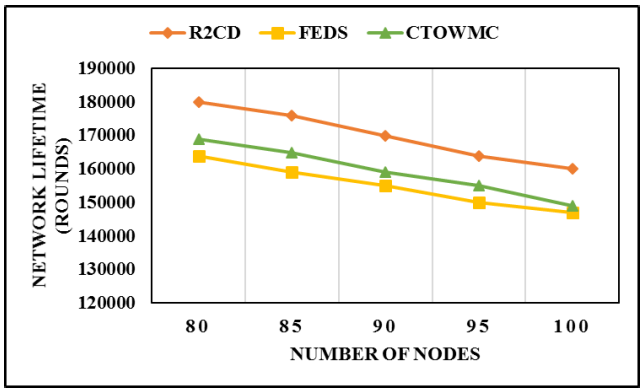

FIGURE 15. Network lifetime.

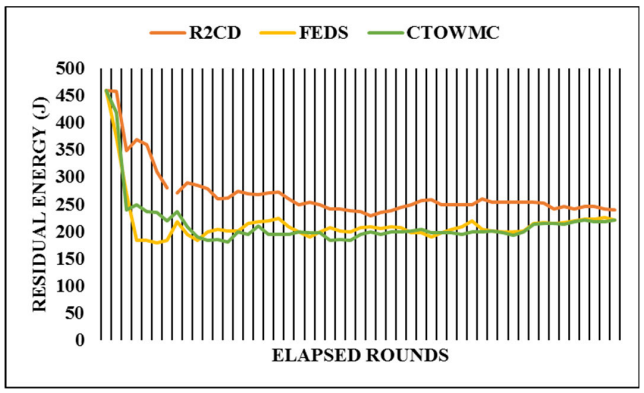

FIGURE 16. Residual energy.

encrypted using the block-chain technology. All the blocks are encrypted in the form of chains and their dependencies increase the level of data protection. In the proposed protocol, CS recomputed the hash value based on the decimal value of secret key, which leads to making the authentication and integrity of the data block more confident. Therefore, unlike other solutions, the ESDG increases the security level on the constructed routes and avoids the chances for attackers to leak the confidentiality, manipulation, and packet drop ratio.

Figure 14 demonstrate the performance evaluation of the ESDG with existing work under the varying malicious nodes in terms of compromised data packet ratio. It is noticed from the analysis of the performed experiments that the ESDG improved the data security in terms of compromised packets by 20% and 14% as compared to other solutions. This is due to the ESDG offers a more consistent and secure routing process by incorporating the block cipher based cryptographic functions. During data forwarding, the evaluators are firstly authenticated and after their identities, the data packets are transmitted towards the sink node in the form of blocks. The data blocks are transmitted towards CS using single hop based on encryption and decryption functions, which significantly increases the data confidentiality and integrity. The ESDG avoids the chances for malicious nodes to capture the smart data packets and alter their contents. Also, the intermediate evaluators are authenticated using private and public keys cryptography and leads to robust and secure data transmissions.

Figure 15 shows the plotted network lifetime in terms of rounds against different number of nodes. The simulation results show that R2CD mechanism outperforms than other approaches as it has longer network lifetime by 13.7% and 23% at different number of nodes. Unlike the existing schemes, in R2CD, the utilized PTD recharges the nodes even when its moving along nodes, which results in increased energy of nodes and improved network lifetime. Moreover, in R2CD, PTD does not wait to receive charging request from the nodes and it starts to charge the nodes from the beginning, which leads to reduce the idle time of PTD and enhance the recharging time of nodes.

In this experiment, the remaining energy of the network is measured as time increases. The purpose of this measurement is to depict how R2CD reduces the total energy consumption of the network. Figure 16 shows the comparison of R2CD with two other algorithms in terms of residual energy of the network. As can be observed in Figure 16, R2CD increases the residual energy of the network by 10% and 46% as compared to previous schemes. Unlike existing mechanisms, in R2CD, the PTD starts to recharge the nodes before entering them to a critical situation which leads to enhance their remaining energy. Moreover, the utilized PTD recharges the nodes even when its moving along nodes, which results in increased energy of nodes.

The computation time of the three techniques is shown in Figure 17. the computational time is the length of time required to perform a computational process. As can be seen, the computation time of our proposed model is lower than the other two techniques because the PTDs move according to a predefined mobility pattern. In the CTOWMC and FEDS techniques, the PTD motion path must be optimized frequently, incurring additional computational costs.

Figure 18 shows the network throughput of R2CD against two other mechanisms. Based on the numerical results, the R2CD model has a significant increase in the network throughput by an average of 18 % and 11 % in comparison

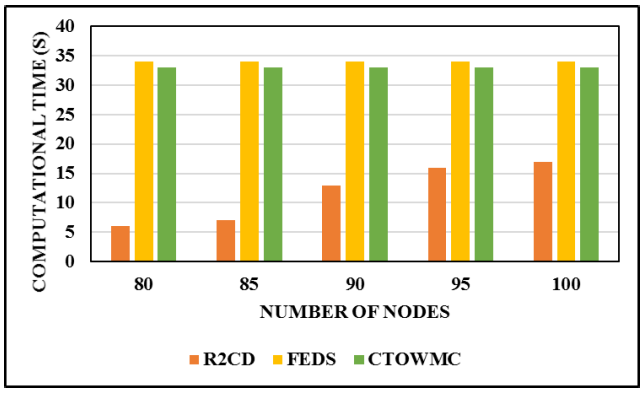

FIGURE 17. Computational time.

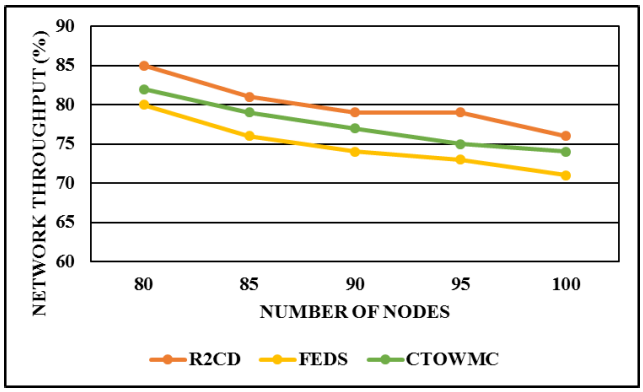

FIGURE 18. Network throughput.

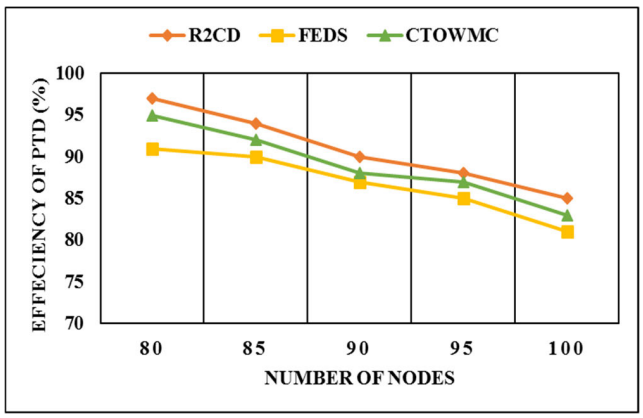

FIGURE 19. Effeciency of PTD.

with other work for the varying number of nodes. As there is a direct relationship between the energy efficiency and network throughput, enhancing the remaining energy of nodes leads to increasing the network throughput. Figure 19 depicts the efficiency of PTD in three different mechanisms. The efficiency of PTD is the fraction of the supplied energy that is transferred in a useful way. As can be observed, in our proposed mechanism, the PTD has higher efficiency in compared with relevant schemes. This is because, the PTD used in the R2CD

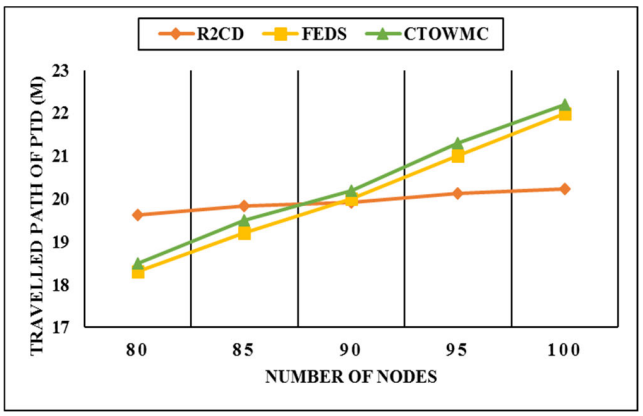

FIGURE 20. Travelled path of PTD.

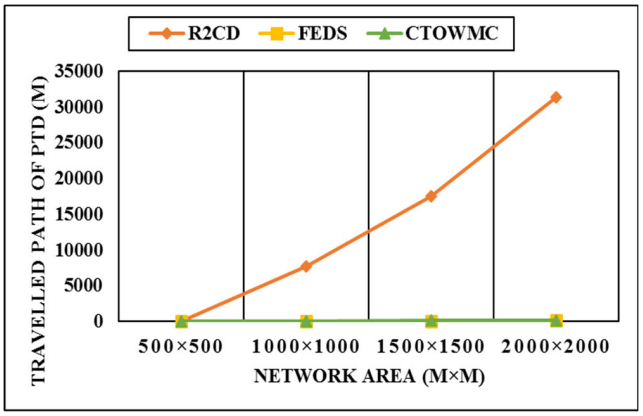

FIGURE 21. Travelled path of PTD.

model recharges the nodes even while moving along ground devices.

The travelled path of PTD is depicted in Figures 20 and 21 under two different scenarios. As can be observed from figure 20, in R2CD, increasing the number of nodes does not impact the travelled path of PTD. this is because, in our proposed mechanism, the PTD moves under a predefined spiral mobility pattern. However, in two other works, the PTD moves along nodes. Then, in such schemes, increasing the number of nodes leads to increasing the travelled path of PTD. Moreover, Figure 21 shows the travelled path of PTD under varying network area. As can be observed, in R2CD, increasing the network area leads to increase the travel path of PTD due to moving the PTD under a path that can meet all sensor nodes. likewise, in our proposed mechanism, the PTD starts to move along nodes before receiving the charging request from nodes. However, in previous works, the PTD waits to be informed by sensor nodes and then starts to move along critical nodes. generally, the travel path of PTD shows the idle time of PTD, then more travel path, low idle time of PTD which leads to increase the efficiency of PTD.

VI. DISCUSSION

The validation results verified the ability of the presented model to reduce the cloud cost, enhance secure data transmission, and improve the energy-efficiency. The proposed model

could reduce the cloud cost by up to 93% compared with BNRS and BSS due to employing evaluators and checking the importance of data before synchronizing with the cloud storage. Likewise, the simulation results demonstrated that the proposed model could enhance the network lifetime by up to 50% and network throughput by up to 11%. Our study involves the implementation of advanced technology while ensuring cost-effectiveness for the various components of the model. The primary objective is promptly transmitting any detected infiltration at the border and initiating necessary actions. By utilizing this model effectively, our border security forces can more precisely enhance their ability to identify and control unwanted and suspicious activities. Compared to existing competing algorithms, our model demonstrates significant improvements. Notably, the energy consumption by sensors is reduced, and the cost of cloud infrastructure is optimized, all while ensuring the network's monitoring objectives are met. This enhances the overall effectiveness and efficiency of border surveillance, minimizing the need for extensive physical presence along the fence and reducing risks to personnel. Moreover, it allows for allocating existing surveillance equipment to other essential tasks [27], [29].

However, some limitations are worth to be noted. the study needs to address potential challenges related to deploying and maintaining Power Transmitter Devices (PTDs). Practical considerations such as the cost, scalability, and reliability of the PTDs, as well as the required infrastructure for their operation, should be considered for real-world implementation.Additionally, the study must consider other vital metrics such as security robustness, scalability, and real-time responsiveness. Future studies should incorporate a more comprehensive evaluation framework to assess the proposed model's effectiveness in various operational scenarios. In addition, using some deep learning techniques [47], [48] to improve the energy effieicny and network lifetime of the proposed model is planed in the future. Despite these limitations, the study provides valuable insights into the potential benefits of optimizing cloud costs and improving energy efficiency in border security systems. However, further research and practical experimentation are necessary to validate and enhance the feasibility and effectiveness of the proposed model in real-world border security deployments.

VII. CONCLUSION

This paper aims to present a joint cloud cost optimization and energy efficiency-based border security model. In the proposed model, evaluators are first used as intermediaries between nodes and CS to verify the importance of collecting data before forwarding it to CS. Using evaluators leads to a reduction in the number of write operations to the cloud storage, thus reducing the cloud cost. After evaluating the received data packets, if there is any illegal movement, the data is forwarded to CS and then immediately synchronized with the cloud storage; otherwise, it is neglected. Similarly, we used a PTD to move along sensor nodes according to a predefined mobility pattern and charge the nodes during the movement. In the proposed model, the batteries of the consumer devices are charged before they reach a threshold, resulting in higher efficiency of the PTD and a more extended network lifetime. When the energy level of a device exceeds the threshold, PTD charges it unscheduled. Each node's energy level threshold is determined based on its wait time for PTD to arrive at its location. This ensures that the sensor nodes do not deplete their energy before arriving at PTD, resulting in a longer operating time for the consumer devices. The experimental analysis conducted in this study involves a comprehensive comparison between the proposed model and existing techniques, considering multiple metrics. The simulation results unequivocally demonstrate that the proposed model exhibits significantly higher efficiency when compared to state-of-the-art models.

REFERENCES

[1] N. Bhadwal, V. Madaan, P. Agrawal, A. Shukla, and A. Kakran, "Smart border surveillance system using wireless sensor network and computer vision," in *Proc. Int. Conf. Autom., Comput. Technol. Manage. (ICACTM)*, Apr. 2019, pp. 183–190.

[2] L. A. Albert, A. Nikolaev, and S. H. Jacobson, "Homeland security research opportunities," *IISE Trans.*, vol. 55, no. 1, pp. 22–31, Jan. 2023.

[3] N. Fatima, S. A. Siddiqui, and A. Ahmad, "IoT based border security system using machine learning," in *Proc. Int. Conf. Commun., Control Inf. Sci. (ICCISc)*, vol. 1, Jun. 2021, pp. 1–6.

[4] M. Sharma and C. R. S. Kumar, "Machine learning-based smart surveillance and intrusion detection system for national geographic borders," in *Artificial Intelligence and Technologies*. Cham, Switzerland: Springer, 2021, pp. 165–176.

[5] M. Nazir, H. M. U. Haque, and K. Saleem, "A semantic knowledge based context-aware formalism for smart border surveillance system," *Mobile Netw. Appl.*, vol. 27, no. 5, pp. 2036–2048, Oct. 2022.

[6] S. Coulthart and R. Riccucci, "Putting big data to work in government: The case of the United States border patrol," *Public Admin. Rev.*, vol. 82, no. 2, pp. 280–289, Mar. 2022.

[7] M. Gheisari, A. A. Abbasi, Z. Sayari, Q. Rizvi, A. Asheralieva, S. Banu, F. M. Awaysheh, S. B. H. Shah, and K. A. Raza, "A survey on clustering algorithms in wireless sensor networks: Challenges, research, and trends," in *Proc. Int. Comput. Symp. (ICS)*, Dec. 2020, pp. 294–299.

[8] M. Alshehri, A. Bhardwaj, M. Kumar, S. Mishra, and J. Gyani, "Cloud and IoT based smart architecture for desalination water treatment," *Environ. Res.*, vol. 195, Apr. 2021, Art. no. 110812.

[9] S. Fugkeaw and P. Sanchol, "A review on data access control schemes in mobile cloud computing: State-of-the-art solutions and research directions," *Social Netw. Comput. Sci.*, vol. 3, no. 1, pp. 1–11, Jan. 2022.

[10] N. Gholipour, E. Arianyan, and R. Buyya, "A novel energy-aware resource management technique using joint VM and container consolidation approach for green computing in cloud data centers," *Simul. Model. Pract. Theory*, vol. 104, Nov. 2020, Art. no. 102127.

[11] I. L. H. Alsammak, M. F. Alomari, I. S. Nasir, and W. H. Itwee, "A model for blockchain-based privacy-preserving for big data users on the Internet of Thing," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 26, no. 2, pp. 974–988, 2022.

[12] H. Mostafaei, M. U. Chowdhury, and M. S. Obaidat, "Border surveillance with WSN systems in a distributed manner," *IEEE Syst. J.*, vol. 12, no. 4, pp. 3703–3712, Dec. 2018.

[13] N. Gharaei, Y. D. Al-Otaibi, S. Rahim, H. J. Alyamani, N. A. K. K. Khani, and S. J. Malebary, "Broker-based nodes recharging scheme for surveillance wireless rechargeable sensor networks," *IEEE Sensors J.*, vol. 21, no. 7, pp. 9242–9249, Apr. 2021.

[14] M. F. Alomari, I. L. H. Alsammak, and S. M. Rasool, "Lifetime enhancement of mobile nodes based wireless sensor networks using routing algorithms," *Webology*, vol. 18, no. SI05, pp. 672–685, Oct. 2021.

[15] M. F. Alomari, M. A. Mahmoud, and R. Ramli, "A systematic review on the energy efficiency of dynamic clustering in a heterogeneous environment of wireless sensor networks (WSNs)," *Electronics*, vol. 11, no. 18, p. 2837, Sep. 2022.

[16] H.-V. Tran and G. Kaddoum, "RF wireless power transfer: Regreening future networks," *IEEE Potentials*, vol. 37, no. 2, pp. 35–41, Mar. 2018.
[17] A. M. Jawad, R. Nordin, S. K. Gharghan, H. M. Jawad, and M. Ismail, "Opportunities and challenges for near-field wireless power transfer: A review," *Energies*, vol. 10, no. 7, p. 1022, Jul. 2017.
[18] N. Nowrozian and F. Tashtarian, "A mobile charger based on wireless power transfer technologies: A survey of concepts, techniques, challenges, and applications on rechargeable wireless sensor networks," *J. AI Data Mining*, vol. 9, no. 3, pp. 383–402, 2021.
[19] S. K. Mothku and R. R. Rout, "Fuzzy logic based adaptive duty cycling for sustainability in energy harvesting sensor actor networks," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 1, pp. 1489–1497, Jan. 2022.
[20] A. Amin, X.-H. Liu, M. A. Saleem, S. Henna, T.-U. Islam, I. Khan, P. Uthansakul, M. Z. Qurashi, S. S. Mirjavadi, and M. Forsat, "Collaborative wireless power transfer in wireless rechargeable sensor networks," *Wireless Commun. Mobile Comput.*, vol. 2020, pp. 1–13, Jun. 2020.
[21] Y. Yu and Q. Cheng, "Charging strategy and scheduling algorithm for directional wireless power transfer in WRSNs," *Alexandria Eng. J.*, vol. 61, no. 10, pp. 8315–8324, Oct. 2022.
[22] G. K. Ijemaru, K. L.-M. Ang, and J. K. P. Seng, "Mobile collectors for opportunistic Internet of Things in smart city environment with wireless power transfer," *Electronics*, vol. 10, no. 6, p. 697, Mar. 2021.
[23] N. Gharaei, K. A. Bakar, S. Z. M. Hashim, and A. H. Pourasl, "Inter- and intra-cluster movement of mobile sink algorithms for cluster-based networks to enhance the network lifetime," *Ad Hoc Netw.*, vol. 85, pp. 60–70, Mar. 2019.
[24] S. P. R. Banoth, P. K. Donta, and T. Amgoth, "Dynamic mobile charger scheduling with partial charging strategy for WSNs using deep-Q-networks," *Neural Comput. Appl.*, vol. 33, no. 22, pp. 15267–15279, Nov. 2021.
[25] X. Liu, M. S. Obaidat, C. Lin, T. Wang, and A. Liu, "Movement-based solutions to energy limitation in wireless sensor networks: State of the art and future trends," *IEEE Netw.*, vol. 35, no. 2, pp. 188–193, Mar. 2021.
[26] Y. Mansouri and R. Buyya, "To move or not to move: Cost optimization in a dual cloud-based storage architecture," *J. Netw. Comput. Appl.*, vol. 75, pp. 223–235, Nov. 2016.
[27] P. Waibel, J. Matt, C. Hochreiner, O. Skarlat, R. Hans, and S. Schulte, "Cost-optimized redundant data storage in the cloud," *Service Oriented Comput. Appl.*, vol. 11, no. 4, pp. 411–426, Dec. 2017.
[28] A. Erradi and Y. Mansouri, "Online cost optimization algorithms for tiered cloud storage services," *J. Syst. Softw.*, vol. 160, Feb. 2020, Art. no. 110457.
[29] S. Chatterjee, M. Jagadeesan, W. Qin, and S. Idreos, "Cosine: A cloud-cost optimized self-designing key-value storage engine," *Proc. VLDB Endowment*, vol. 15, no. 1, pp. 112–126, Sep. 2021.
[30] A. Muhammed, "An optimal data access framework for telerehabilitation system," *J. Adv. Comput. Technol. Appl. (JACTA)*, vol. 3, no. 1, pp. 25–36, 2021.
[31] T. D. Nguyen, T. Nguyen, T. H. Nguyen, K. Nguyen, and P. Le Nguyen, "Joint optimization of charging location and time for network lifetime extension in WRSNs," *IEEE Trans. Green Commun. Netw.*, vol. 6, no. 2, pp. 1186–1197, Jun. 2022.
[32] S. Malebary, "Wireless mobile charger excursion optimization algorithm in wireless rechargeable sensor networks," *IEEE Sensors J.*, vol. 20, no. 22, pp. 13842–13848, Nov. 2020.
[33] A. Boukerche, Q. Wu, and P. Sun, "A novel two-mode QoS-aware mobile charger scheduling method for achieving sustainable wireless sensor networks," *IEEE Trans. Sustain. Comput.*, vol. 7, no. 1, pp. 14–26, Jan. 2022.
[34] A. O. Almagrabi, "Fair energy division scheme to permanentize the network operation for wireless rechargeable sensor networks," *IEEE Access*, vol. 8, pp. 178063–178072, 2020.
[35] N. Gharaei, Y. D. Al-Otaibi, S. A. Butt, S. J. Malebary, S. Rahim, and G. Sahar, "Energy-efficient tour optimization of wireless mobile chargers for rechargeable sensor networks," *IEEE Syst. J.*, vol. 15, no. 1, pp. 27–36, Mar. 2021.
[36] N. Gharaei, K. A. Bakar, S. Z. Mohd Hashim, A. Hosseingholi Pourasl, and S. Ashfaq Butt, "Collaborative mobile sink sojourn time optimization scheme for cluster-based wireless sensor networks," *IEEE Sensors J.*, vol. 18, no. 16, pp. 6669–6676, Aug. 2018.
[37] H. Xie, Z. Yan, Z. Yao, and M. Atiquzzaman, "Data collection for security measurement in wireless sensor networks: A survey," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2205–2224, Apr. 2019.
[38] S.-J. Hsiao and W.-T. Sung, "Employing blockchain technology to strengthen security of wireless sensor networks," *IEEE Access*, vol. 9, pp. 72326–72341, 2021.
[39] C.-T. Hsueh, C.-Y. Wen, and Y.-C. Ouyang, "A secure scheme against power exhausting attacks in hierarchical wireless sensor networks," *IEEE Sensors J.*, vol. 15, no. 6, pp. 3590–3602, Jun. 2015.
[40] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, "A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks," in *Proc. 8th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, Sep. 2007, pp. 80–89.
[41] J. Newsome and D. Song, "GEM: Graph EMbedding for routing and data-centric storage in sensor networks without geographic information," in *Proc. 1st Int. Conf. Embedded Netw. Sensor Syst.*, Nov. 2003, pp. 76–88.
[42] C. Cocks, "An identity based encryption scheme based on quadratic residues," in *Proc. 8th IMA Int. Conf. Cryptogr. Coding*, in Lecture Notes in Computer Science, vol. 2260, B. Honary, Ed. Heidelberg, Germany: Springer, Dec. 2001, pp. 360–363.
[43] N. Sharmin, A. Karmaker, W. L. Lambert, M. S. Alam, and M. S. A. Shawkat, "Minimizing the energy hole problem in wireless sensor networks: A wedge merging approach," *Sensors*, vol. 20, no. 1, p. 277, Jan. 2020.
[44] N. Vadivelan, S. Taware, R. R. Chakravarthi, C. A. Palagan, and S. Gupta, "RETRACTED: A border surveillance system to sense terrorist outbreaks," *Comput. Electr. Eng.*, vol. 94, Sep. 2021, Art. no. 107355.
[45] W. Na, J. Park, C. Lee, K. Park, J. Kim, and S. Cho, "Energy-efficient mobile charging for wireless power transfer in Internet of Things networks," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 79–92, Feb. 2018.
[46] F. Liu, H. Lu, T. Wang, and Y. Liu, "An energy-balanced joint routing and charging framework in wireless rechargeable sensor networks for mobile multimedia," *IEEE Access*, vol. 7, pp. 177637–177650, 2019.
[47] C. Li, G. Wang, B. Wang, X. Liang, Z. Li, and X. Chang, "DS-Net++: Dynamic weight slicing for efficient inference in CNNs and vision transformers," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 45, no. 4, pp. 4430–4446, Apr. 2023.
[48] C. Yan, X. Chang, Z. Li, W. Guan, Z. Ge, L. Zhu, and Q. Zheng, "ZeroNAS: Differentiable generative adversarial networks search for zero-shot learning," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 44, no. 12, pp. 9733–9740, Dec. 2022.
[49] K. Haseeb, I. U. Din, A. Almogren, I. Ahmed, and M. Guizani, "Intelligent and secure edge-enabled computing model for sustainable cities using green Internet of Things," *Sustain. Cities Soc.*, vol. 68, May 2021, Art. no. 102779.
[50] T. Saba, K. Haseeb, I. Ahmed, and A. Rehman, "Secure and energy-efficient framework using Internet of Medical Things for e-healthcare," *J. Infection Public Health*, vol. 13, no. 10, pp. 1567–1575, Oct. 2020.
[51] D. K. Shukla, J. Singh, S. Muthusamy, S. Satpathy, and V. Goyal, "Workflow task scheduling for homogeneous environments on multiprocessing based on IoT variant of beta artificial bee colony," *Trans. Emerg. Telecommun. Technol.*, Dec. 2022, Art. no. e4685.

MOHAMMED F. ALOMARI received the bachelor's degree in computer science from the College of Science, University of Wasit, Iraq, in 2012, and the master's degree in information communication technology from Utara University Malaysia (UUM), Malaysia, in 2015. He is currently pursuing the Ph.D. degree in information and communication with Universiti Tenaga Nasional (UNITEN). His current research interests include wireless sensor networks and the IoT, working on a project for border security systems using WSN.

MOAMIN A. MAHMOUD (Member, IEEE) received the bachelor's degree in mathematics from the College of Mathematics and Computer Science, University of Mosul, Iraq, in 2007, and the master's degree in information technology and the Ph.D. degree in information and communication technology from the College of Graduate Studies, Universiti Tenaga Nasional (UNITEN), Malaysia, in 2010 and 2013, respectively. He has been a Senior Lecturer with the Department of Software Engineering, UNITEN, since 2014. He is currently the Deputy Dean of research and innovation with the College of Computing and Informatics, UNITEN. He has a thorough knowledge of research and supervision. He has produced more than 100 articles in WoS/Scopus-indexed journals. Under his supervision has successfully graduated more than 50 undergraduates, nine master's, and five Ph.D. students. He has been invited to assess master's and Ph.D. thesis and evaluate grant proposals. Apart from this, he has secured as the leader of nine research grants funded from different national and international sources and three consultancy projects with industry. Besides, he also has filed four copyrights and one patent titled "A Computer-Implemented Method and System for Modeling and Predicting Failure of a Power Grid Configuration." His core expertise is in data analytics. His current research interests include the application of artificial intelligence techniques to other domains, such as health, energy, social, transportation, and drones. He was awarded a Machine Learning Certification from Cornell University, USA, and a Professional Technologist Certification from the Malaysia Board of Technologists (MBOT), Malaysia. He served on the editorial board/technical committee/reviewer for many journals and conferences.

YUNUS BIN YUSOFF (Member, IEEE) is currently the Director of the International Office and an Associate Professor with the College of Computing and Informatics, Universiti Tenaga Nasional (UNITEN). His current research interests include computer applications, cyber security, and digital forensics. He was a member of the Association of Computing Machinery (ACM), in 2002, and the Malaysian National Computer Confederation (MNCC), in 2008.

NIAYESH GHARAEI received the Ph.D. degree in computer science from Universiti Teknologi Malaysia. She is currently an Assistant Professor with Ostim Teknik University, Ankara, Turkey. Her current research interests include vehicular communications, wireless ad-hoc networks, and mobile computing.

REEMA AHMED ABDALLA received the B.Sc. degree in computer science and engineering from Aden University, Yemen, in 2004, the M.Sc. degree in information technology from Universiti Utara Malaysia (UUM), Malaysia, in 2016, and the Ph.D. degree in computer science from Universiti Putra Malaysia (UPM), Malaysia, in 2022. She was a Lecturer with the Aden Community College, Yemen, from 2005 to 2013. She has been a Senior Lecturer of cybersecurity with the Computing Department, Universiti Tenaga Nasional (UNITEN), Malaysia, since 2023. In this role, she teaches various subjects in the cybersecurity program for degree students and supervises undergraduate and postgraduate students in their projects and thesis. Her current research interests include data privacy, steganography, cryptography, watermarking, and the IoT security using machine learning.

SARASWATHY SHAMINI GUNASEKARAN is currently a Senior Lecturer with UNITEN, where she is focusing on enriching the academic realm of her students through a fun and engaging classroom environment. She is also with Smart University Blueprint with IBM. Her current research interest includes artificial intelligence. She looks forward to collaboration possibilities in the areas of agent technology, essentially in the field of social commerce and smart sustainable cities. She has bagged her gold and silver awards in international competitions, apart from actively engaging herself with potential industries to further commercialize her research ideas.