International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2024/224440 Volume 11, Issue 2, March – April (2024)

REVIEW ARTICLE

Strategies for Achieving Energy Efficiency and Data Security Through Data Aggregation in IoT Healthcare Applications: A Comprehensive Study

Ganesh Srinivasa Shetty
Faculty of Engineering and Technology, JAIN (Deemed to be University), Bengaluru, India.
ganeshshetty27@gmail.com

Raghu N
Department of Electrical Engineering, Faculty of Engineering and Technology, JAIN (Deemed to be University), Bengaluru, India.
raghu1987n@gmail.com

Received: 09 October 2023 / Revised: 13 March 2024 / Accepted: 18 March 2024 / Published: 30 April 2024

Abstract – The healthcare sector has been completely transformed using the internet of technology (IoT) for patient monitoring, diagnosis, and treatment. The Data aggregation (DA) plays a crucial role in achieving both energy efficiency and data security goals in IoT based healthcare systems. The sensitive nature of health data, coupled with the interconnectedness of IoT devices raises significant data sensitivity and privacy concerns. The primary intention of this review is a thorough analysis of several protocols for data aggregation that have been developed to deal with problems such as energy consumption and data security in IoT networks. Since the invention of blockchain technology, many studies have investigated its potential application in the IoT to resolve security issues. Many systems aim to improve network lifetime by scheduling duty cycles; however, they struggle to manage redundant data and have deprived throughput. Cluster-based data aggregation algorithms remove redundancy and conserve energy. This overview highlights interesting future research topics in the areas of energy efficiency in IoTs, security and privacy of user data maintenance problems, and integration of machine learning and blockchain algorithms.

Index Terms – Internet of Health Things (IoHT), Secured Data Aggregation, Energy Efficiency, Blockchain Technology, Network Lifetime, Throughput.

1. INTRODUCTION

Recent advancements in wireless communications and the shift from 4G to 5G technology have enabled networks to link anything to anything. Wireless sensor networks (WSNs) have now propelled to a far broader application platform, manifesting as the IoT [1]. The IoT paradigm is rapidly being utilized to improve people's daily lives throughout the world. Figure 1 depicts the various domains encompassing IoT applications. The rapid expansion of IoT has resulted in disruptive advances in various fields, including healthcare. IoT technology has aided in the development of novel healthcare applications ranging from remote patient monitoring to wearable health devices (WHD), which provide real-time data collection and analysis to improve patient care and enable personalized medication [2]. These applications capture and communicate vital health-related data via interconnected devices such as sensors, actuators, and WHDs. However, this expanding space of networked devices creates substantial concerns, notably in the areas of energy efficiency and data security [3]. IoT healthcare applications must work within the limits of energy-constrained devices, which frequently have low battery capacity. To guarantee the smooth operation of these applications, it is critical to balance the necessity for constant monitoring and data transfer with the preservation of energy resources.

Nevertheless, the sensitive nature of health data necessitates stringent security measures. IoT healthcare device data are frequently very personal and sensitive, comprising patient health records, vital signs, and other confidential information. Maintaining patient confidence and complying with legal frameworks such as the "Health Insurance Portability and Accountability Act" (HIPAA) and the "General Data Protection Regulation" (GDPR) require ensuring the confidentiality, integrity, and availability of this data. Considering these issues, data aggregation appears to be strategic solution that can solve both energy efficiency and data security concerns [4]. DA is the task of consolidating and summarising acquired data at multiple levels to lower the volume of raw data delivered over the network. This strategy not only reduces the load on energy-constrained devices but also opens the potential to improve data security. The possible exposure of sensitive information is reduced by delivering

REVIEW ARTICLE

summarised data, lowering the danger of unauthorised access and breaches [5].

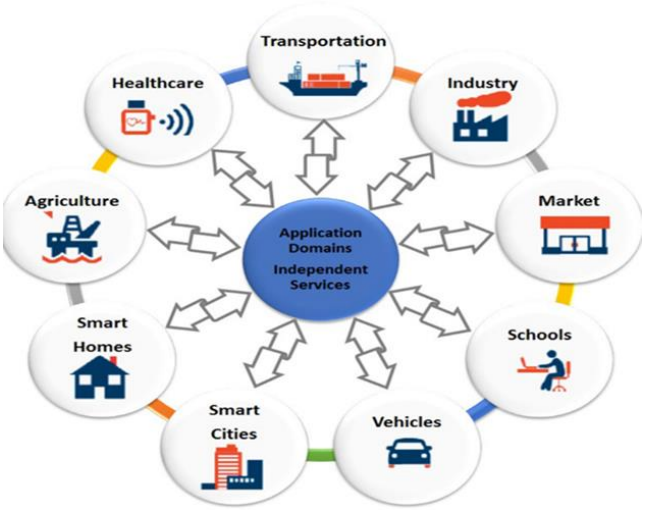

Figure 1 Verticals of IoT Applications

The inspiration for this review article originates from the necessity to thoroughly investigate solutions that use data aggregation to establish a harmonic balance between energy efficiency and data security in IoT healthcare applications. This article seeks to provide a clear understanding of how data aggregation (DA) may be exploited to optimise resource utilisation, increase data privacy, and ultimately advance the efficacy of IoT healthcare systems through an in-depth review of existing methodologies, case studies, and upcoming trends. Researchers, practitioners, and policymakers may gain significant insights into creating and implementing more robust and efficient IoT healthcare systems by examining the symbiotic link between energy usage and data security in the context of DA. This review article aims to add to the ongoing discussion on the convergence of IoT, healthcare, and data management by developing a better awareness of the difficulties and possibilities of these multidisciplinary areas.

1.1. Challenges in Energy Efficiency and Data Security

The expanding use of IoT technology in healthcare has yielded significant benefits, but it has also introduced difficult issues related to energy efficiency and data security. Addressing these issues is critical for ensuring the safe and reliable operation of IoT healthcare applications. This section explores the complexities of energy preservation and data security in the context of IoT based healthcare systems.

1.1.1. Energy Efficiency Challenges

- Limited Energy Resources: Many IoT healthcare devices, such as wearable sensors and remote monitoring systems, are powered by batteries with limited energy capabilities. Balancing the necessity for continuous data gathering and transmission with limited energy resources is an acute issue [6].
- Communication Overhead: Frequent data transfers from many IoT devices to centralized servers or cloud platforms result in significant communication overhead [7]. This can result in greater energy usage and network congestion, especially in highly placed healthcare contexts.
- Real-Time Processing: Some medical applications need real-time data processing and quick replies [8]. Real-time performance while optimizing energy usage is a difficult balance that frequently necessitates advanced algorithms and hardware optimization.

1.1.2. Data Security Challenges

- Privacy Concerns: Medical records, vital signs and personal identifiers are examples of sensitive patient data produced and handled through IoT healthcare (IoHT) apps. It is critical to protect patient privacy and prevent unauthorised access to these data to preserve patient confidence and comply with legislation [9].
- Data Breaches: Because IoT devices are networked, they provide possible entry sites for attackers [10]. A single hacked device can result in data breaches, revealing confidential health information and putting patients at risk.
- Lack of Standardization: IoT devices are frequently manufactured by different companies and may lack standardized security measures. Because of this variability, implementing consistent and comprehensive security measures for the entire ecosystem is difficult.
- Regulatory Compliance: The Health Insurance Portability and Accountability (HIPAA) and the General Data Protection Regulation (GDPR) are severe standards that apply to healthcare data [11]. These rules must be followed by IoT healthcare apps while ensuring security, adding another degree of complexity to the security environment.

Addressing these issues requires a multifaceted and multidisciplinary strategy that considers both energy efficiency and data security. To realise the full potential of IoT healthcare applications while retaining patient confidence and data integrity, the appropriate balance between optimizing energy usage and securing patient data is critical.

1.2. Role of Data Aggregation

In IoT healthcare applications, data aggregation (DA) appears to be a critical method for addressing the interwoven concerns of energy efficiency and data security. DA provides a multidimensional approach that optimizes resource utilization while improving privacy and security through the aggregation and summarization of acquired data before transmission. Data

REVIEW ARTICLE

from IoT healthcare devices are frequently redundant, with numerous devices providing similar information. By merging related data points into a compact form, DA reduces redundancies [12]. This minimizes the amount of data sent, lowering communication costs, and preserving energy resources.

Frequent transfer of raw data from many IoT devices may result in significant communication overhead and increased energy usage. DA minimizes the number of data packets sent, reducing network congestion, and preserving energy in both sending and receiving devices [13]. The protection of patient data is critical in healthcare applications. DA, before transmission, reduces the granularity of the sent information. Because aggregated data provides less insight into individual patients' illnesses, the danger of unauthorized access and data breaches is reduced.

DA at the device level necessitates local processing that may be adjusted to the device's energy capabilities. Energy-efficient algorithms can be used to optimize the usage of available energy resources by executing calculations closer to the data source. DA approaches can be employed with adaptive sampling strategies, in which sensors modify the frequency with which they provide data based on context or events [14]. This enables gadgets to consume less energy during moments of low activity while still providing critical information.

Aggregation of data aids in the scalability of IoHT applications. The aggregated data can be easily managed as the number of linked devices increases, thereby minimizing the burden on the network infrastructure and adding to overall system efficiency. Aggregated data can provide a more comprehensive picture of health trends and anomalies. Healthcare personnel may discover trends and abnormalities more efficiently by analyzing summarized data, allowing for prompt action and enhanced patient care. Data aggregation before transmission allows for the installation of resource-constrained security mechanisms. Encryption and authentication operations, for example, can be conducted on summarized data, lowering the computational burden on energy-constrained IoT devices.

2. LITERATURE REVIEW ON ENERGY EFFICIENCY IN IOT HEALTHCARE APPLICATIONS

Energy efficiency is critical in healthcare, particularly in the context of IoT devices and apps. The effective utilisation of energy resources within healthcare systems yields an abundance of benefits that go beyond power saving. Energy-efficient IoT devices in healthcare provide continuous patient monitoring and data collection. Uninterrupted data transmission provides healthcare workers with real-time patient information, allowing early diagnosis of irregularities and timely intervention. Continuous monitoring leads to more accurate diagnoses, personalized treatment strategies, and better patient outcomes. Energy-efficient design and operation make IoT healthcare equipment last longer. Devices can function for extended periods of time before needing battery replacements or maintenance if unwarranted energy usage is reduced. As a result, downtime is decreased, patient monitoring is less disrupted, and total device replacement costs are lower.

Several strategies and approaches have been developed in the quest for energy efficiency within IoT healthcare applications to optimize energy usage while retaining the appropriate degree of functionality and data quality. These methods encompass hardware optimizations, software algorithms, and clever data management strategies. This section provides an overview of several known energy optimization measures in the context of IoT based healthcare systems.

Fog and edge computing for emerging technologies is an open system that integrates cloud and IoT gadgets [15]. Cloud-based frameworks have recently been the focus of much research due to the limited computing resources of IoT devices and the growing demand for cloud services. Presently, fog computing lacks the infrastructure and user base to deliver on promises of efficiency, reliability, and security [16]. The authors presented an "Energy-efficient Data Transmission and Aggregation Protocol" (EDaTAP) for Periodic Sensor Networks (PSNs) based on fog computing. The protocol minimizes communication costs and saves energy by removing redundant data. It has been evaluated using real sensed data, demonstrating significant reductions in transmitted data, energy savings, decreased data loss, and improved detection of redundant datasets compared to other approaches. The paper also emphasizes the importance of fog computing in IoT and highlights the benefits of energy efficiency in sensor networks [17]. Data reduction and cleaning at the endpoints of IoT and the network edge offer numerous advantages, including reduced communication costs, diminished network traffic, lower energy consumption, a longer lifespan for IoT sensors, and more efficient use of scarce resources [18]. The study [19] delves into how cloud computing and big data may collaborate on the six characteristics of big data, how to collect, arrange, analyze, and show data, which common frameworks are, and how to investigate application technologies.

The authors proposed the Two-level Data Aggregation (TLDA) protocol for Periodic Sensor Networks (PSNs) in [20], integrating data gathering, data aggregation (DA), and transmission mechanisms to optimize energy usage and extend the network's lifetime. Comparative analysis against two other approaches demonstrated the TLDA protocol's superior effectiveness. This paper underscores the vital role of energy efficiency in sensor devices, emphasizing data aggregation as a critical process to reduce unnecessary data

REVIEW ARTICLE

and extend the network's life. To alleviate the load on IoT networks, researchers in [21] recommend the Distributed Energy-Efficient Data Reduction (DEDaR) method, using prediction and compression to minimize data size. Efficient data compression methods, such as 'adaptive piecewise constant approximation' (APCA), Symbolic Aggregate approximation (SAX) and a fixed code dictionary (FCD) based on Huffman encoding, are suggested for transmitting data, effectively eliminating unnecessary information. Table 1 presents a comparative analysis of related works on energy-efficient data aggregation in IoT for healthcare applications.

Table 1 Summary of Related Works

Reference	Contribution	Remarks	Performance Evaluation
[6]	Cluster-level data aggregation to conserve energy, reduced data volume.	Potential for further refinement and optimization to achieve longer battery life and lower energy consumption.	DA Accuracy: 97.3% (for 200 nodes)
[13]	A two-tiered data inference system designed to preserve battery life and secure personal information.	Based on the data, it appears that the inference system's accuracy was maximised when a variation rate of 1% to 2.5% was used.	DA Accuracy: 96.26%
[17]	Reduction of communication expenses by excluding redundant sensing data	Potential to reduce lost data, conserve energy, and clean up transmitted sensor data.	Energy Efficiency: 81.2%, Decreased Data Loss: 55.5%
[18]	Multi-tier data reduction technique using an optimum set selection framework.	Approach is based on a straightforward plan to combine data from the same area and time period.	DA Accuracy: 90%
[20]	Periodic Sensor Networks, Two Level Data Aggregation	Cuts down on the amount of unnecessary data that must be transmitted to the sink node	Reduces Data Gathered: 87% Energy Efficiency: 72%
[21]	Distributed energy-efficient data reduction	Energy conservation requires that data be compressed before being sent to the gateway, but data quality at the gateway must also be guaranteed.	Reduces Data Gathered: 92.48% Energy Efficiency: 95%

The table 1 provides an overview of several contributions aimed at enhancing the performance of IoT systems through data aggregation, reduction, and energy conservation. Notable achievements include cluster-level data aggregation with 97.3% accuracy [6], a two-tiered inference system with 96.26% accuracy [13], communication expense reduction with 81.2% energy efficiency [17], multi-tier data reduction with 90% accuracy [18], and periodic sensor network data aggregation with 87% reduced data and 72% energy efficiency [20].

The distributed energy-efficient data reduction approach achieved an impressive 92.48% reduction in data gathered and 95% energy efficiency [21]. These contributions offer valuable insights and techniques to enhance IoT device performance by conserving energy, reducing data volume, and improving data accuracy to meet the evolving demands of IoT applications.

3. LITERATURE REVIEW ON DATA SECURITY IN IOT HEALTHCARE APPLICATIONS

Safeguarding sensitive information is a major concern in the realm of IoT healthcare applications. Connected medical devices gather, store, and exchange data, including vital signs, medical histories, and other personally identifiable information about patients. Striking a balance between the advantages of data-driven healthcare and the need to safeguard patient privacy is crucial. Addressing data sensitivity and privacy issues in IoT healthcare applications requires multiple strategies. Essential measures include robust security precautions, effective anonymization methods, and adherence to open data usage regulations within the healthcare industry. Stakeholders can collaborate to establish a healthcare ecosystem that leverages the benefits of data while respecting individual privacy rights. This can be achieved by prioritizing patient permission, complying with

REVIEW ARTICLE

legislation, and implementing secure IoT device practices [22].

The integration of IoT technology into healthcare introduces complex regulatory and legal challenges to ensure the protection of patient data privacy and compliance with applicable regulations. Healthcare data management is subject to stringent regulations in various countries, such as the United States (HIPAA) and the European Union (GDPR). Non-compliance with HIPAA or GDPR may result in fines, penalties, legal proceedings, and reputational harm. Companies found in breach of these rules could face severe consequences that impact their daily operations and bottom line.

The intricate and interconnected nature of IoT devices, data transfers, and the necessity for specific patient permissions makes achieving compliance with HIPAA and GDPR challenging in IoT healthcare systems. Overcoming these obstacles requires the implementation of safeguards, including encryption, access limits, audit trails, and appropriate data sharing agreements [23].

As illustrated in Figure 2, IoHT follows the same three-layer structure as IoT, comprising a perception layer, a network layer, and an application layer. The perception layer serves as the healthcare sensing layer, housing IoT sensors such as medical equipment and sensors physically attached to patients. The network layer connects these sensors and healthcare equipment, enabling the transmission of patient health data to the cloud through WiFi or other communication modules. This data, analyzed in the cloud, provides medical professionals, patients, and healthcare facilities with valuable insights, monitoring results, reports, and notifications through various medical applications.

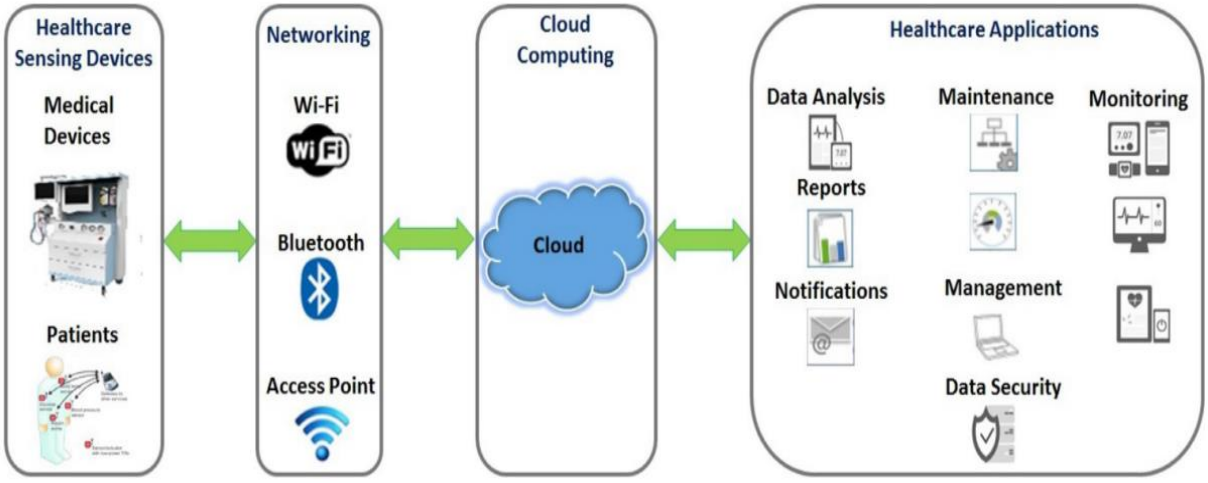

Figure 2. IoT Healthcare Network Context [24]

DA techniques [25] based on homomorphic encryption are extensively suggested to ensure the privacy of collected information. Patients may protect their privacy by encrypting their medical information prior uploading it to the cloud, where it will be aggregated in an unbreakable ciphertext from which only the aggregated results will be extracted. Advanced secure multiparty computation (SMC) based DA methods [26, 27] are used to broaden the scope of single-party secure DA to include data from several parties. SMC allows for several parties to pool their health information and share it securely by providing each with their own unique encryption key. The parties' ability to communicate with one another is often put to the test by the high degree of interactivity inherent in most SMC algorithms, which necessitates continued dialogue between them over the course of several iterations.

DA in smart grid under human-factor-attention differential assaults can be made private by dividing the metre value into sub-shares concealed in the matrix structure, as illustrated in [28]. To facilitate a broad variety of statistical aggregation operations, the authors of [29] developed a multifunctional DA technique with differential privacy using ML algorithms. The study [30] detects intrusions by combining a rule-based approach with the Random Forest model. The rules generated from the trained Random Forest can be used to identify several types of attacks, including Rank, DoS, and Selective Forwarding.

A unique method of detecting network intrusions [31], combining a multi-layer extreme learning machine (ELM) with a deep learning model. The model collects deep features from high-dimensional input by using several ELM-based auto-encoders in front hidden layers for unsupervised learning. Table 2 gives the analysis of some Secured DA mechanisms researched in the past years.

REVIEW ARTICLE

Table 2 Comparative Analysis of Secured Data Aggregation Methods

Reference	Contribution	Remarks	Performance Evaluation
[23]	Presents a low-overhead cryptographic approach for safeguarding patient privacy in cloud-based healthcare systems. Lacks device-based or identity-management-system-based authentication procedures.	Neither device-based nor identity-management-system-based authentication (IDMS) procedures are in place	Signing Time: 5.136ms Verification Time: 3.885ms
[25]	Using a homomorphic cryptosystem based on a lightweight lattice, presented a technique for aggregating power usage in an encrypted way	Several techniques of controlling IoT devices, including two-factor authentication, token-based solutions, access control, and key management, are not discussed	Computation delay: 33.3ms
[32]	Describes a low-overhead cryptographic approach for the IoTs perception layer	Lightweight cryptographic algorithm comparison to other device authentication methods; key management constraint.	Computation delay: 129.04ms
[33]	Methods of user authentication in the application layer are discussed, along with examples of attacks at other levels. The blockchain and its potential to enhance user authentication is another area of emphasis	Does not discuss the usage of blockchain or smart contracts in authenticating devices.	-
[34]	Describes IDMS and how blockchain technology might pave the way for identification solutions	Key management, security, and attack analysis are all lacking.	-
[35]	end-to-end security through sensor devices and base station	If a malicious node masquerading as a trustworthy node has a falsified node ID, the strategy will fail.	DA Accuracy: 69% Attack prevalence: 21.43%

A range of contributions addressing cryptographic approaches and security concerns in healthcare systems and IoT devices is presented. Reference [23] offers a low-overhead cryptographic method for safeguarding patient privacy, showcasing relatively efficient signing and verification times. However, it lacks essential device-based or identity management system-based authentication. Reference [25] introduces an encryption technique for power usage data, highlighting a significant computation delay but failing to comprehensively address IoT device security measures. Reference [32] presents a cryptographic approach for IoT perception layers with notable computation delays and key management constraints. Reference [33] discusses user authentication and the potential of blockchain but does not delve into its practical usage for device authentication. Reference [34] examines ID management systems and blockchain's potential but lacks robust security analysis. Reference [35] focuses on end-to-end security for sensor devices, achieving a 69% data accuracy rate but suffering from a relatively high attack prevalence of 21.43%. These contributions highlight various cryptographic techniques but underscore shortcomings in device authentication, security measures, and key management, emphasizing the need for further research in strengthening IoT and healthcare system security.

3.1. Privacy of Patient/User Information

Ensuring the protection of individuals' private information and preserving their anonymity when sharing data is a top priority [36]. Standardization is crucial to guarantee the confidentiality of e-health records throughout their collection, storage, transfer, and utilization [37]. The transmission of private information and open-access data in healthcare systems that rely on edge and cloud computing poses a significant challenge to privacy protection [38]. With the implementation of the Fog layer, the potential of IoHT rises.

REVIEW ARTICLE

Typically, data is gathered at the sensor layers, consolidated at the data collection layer, and then analyzed or processed at the Fog or cloud layer in IoT-enabled healthcare systems. Further research into privacy in three fundamental healthcare settings is imperative [39]. The current scenario necessitates the implementation of a privacy safeguarding system to protect data confidentiality and ensure that unauthorized parties have no access to critical healthcare information [40]. A study [41] demonstrates an electromagnetic attack on a decommissioned dog activity tracker during the Base64 encoding process, highlighting the susceptibility of pet wearables to side-channel attacks. In the reference [42], a secure Electronic Health Record (EHR) system with RSA digital signatures and strong authentication is proposed. In order to ensure the integrity of transferred data, the suggested system incorporates QR codes for safe prescription exchange. The study carries out both formal and informal security studies, showing a higher degree of security than earlier research, which makes it a complete and effective solution for safe healthcare information management.

3.2. Scalability and Resource Management

The term 'scalability' refers to the capacity of a system, network, or application to support and adapt to growing demands. As the quantity of interconnected medical devices and the complexity of the healthcare network increase, scalability problems may arise [43]. Fog and cloud-based healthcare systems face additional challenges in managing their resources [44]. Scalability is influenced by increases in both network bandwidth and consumer density. While formulating well-defined algorithms to function smoothly on small amounts of data is generally straightforward, achieving smooth operation on an enormous scale while maintaining reliability and efficiency is a challenging task [45]. The acquisition of an enormous quantity of information in a brief period of time and the security of sensitive data are all factors in data management. In the field of smart healthcare, data management presents its own unique set of difficulties. As an outcome, fog computing offers a remedy by mediating between smart sensing devices and cloud storage repositories, where data may be managed and processed locally [46]. Heterogeneity on the IoTs refers to an infrastructure that supports numerous protocols and endpoints. Fog computing also faces difficulties with diversity. In the current healthcare model, a variety of sensors manufactured by various firms are linked to the patient. And each gadget reports its own patient information to the healthcare hub.

4. LITERATURE REVIEW ON OPTIMIZATION PROBLEM

A scheme called Reliable Data Dissemination for the Internet of Things Using Harris Hawks Optimization (RDDI) is presented by authors [47]. This scheme focuses on ensuring secure and reliable data aggregation and forwarding in IoT. By employing a fuzzy hierarchical network model and the Harris Hawks Optimization (HHO) algorithm for optimized routing, the paper evaluates RDDI's performance and compares it to three other approaches. The results demonstrate that RDDI achieves superior reliability and performance. In a parallel context, the authors introduce F-LEACH in [48], a fuzzy-based data aggregation scheme designed for IoT-enabled healthcare systems. This scheme aims to maximize the network lifetime through efficient data aggregation. Emphasizing the importance of energy and resource management in large-scale, battery-powered IoT networks, the authors argue that fuzzy logic proves effective in healthcare applications due to its ability to handle complex and nonlinear scenarios. The proposed F-LEACH method outperforms similar works by 5-20%, as indicated by simulation results.

Problems with present data aggregation methods in IoT and similar approaches include a dearth of aggregation functions, excessive weight, and performance bottlenecks. Furthermore, excessive latency, scalability, storage, decreased dependability, and additional energy overhead would arise from the overload on fog node. Two strategies for safe transmission of data via the network and reduced energy usage during transmission have been presented by the authors to address these problems. Clusters are formed using the Clustered Particle Swarm Optimisation (CPSO) approach to cut down on transmission costs and energy consumption [49]. The parameters supplied by the patient's wearable sensor devices have been aggregated in this proposed study [50], utilising an effective “discrete grey wolf optimisation” (DGWO) based data aggregation approach employing “Elliptic curve Elgamal with Message Authentication code” (ECEMAC). Using DGWO, distant nodes will transmit information to the cluster leader in the nearest cluster. The amount of data transfers on the network will be lowered thanks to the aggregation strategy. To establish an information system that includes a large number of sensor nodes that properly interact with one another to provide a smart decision-making process, sensors play a crucial role in IoT systems. These sensor nodes, however, may be used under extreme conditions where frequent battery maintenance, such as swapping out or charging, is impractical. This work [51, 52] introduces a unique Particle Swarm Optimisation (PSO)-based methodology for clusters that combines adaptive mobility for mobile stations.

5. CASE STUDIES: APPLICATION OF BLOCKCHAIN AND MACHINE LEARNING ALGORITHMS IN IOTS FOR HEALTHCARE

5.1. Practical Byzantine Fault Tolerance (PBFT) Consensus Algorithm

Data from IoT devices may be efficiently collected, transferred, stored, and protected using blockchain

REVIEW ARTICLE

technology. But owing to the constraints on CPU resources, memory, and energy saving requirements, developing high-performance blockchain solutions for restricted IoT devices is exceedingly difficult. As a result, using traditional consensus procedures might be challenging. The authors examine the viability of blockchain technology for resource-limited IoT devices and investigate the possibility of developing an efficient consensus algorithm for them. Blockchain technology is under investigation for its potential to secure data from limited Internet of Things (IoT) devices, with the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm chosen for deployment on these devices. Key distributed ledger scenarios are simulated using this algorithm [53], and Figure 3 illustrates the overall system design. The authors have conducted a study on the features of real, restricted IoT devices in terms of computational power and data throughput. Additionally, they explore common IoT network situations that might disturb system performance. The simulation findings indicate that blockchain technology performs well on constrained devices, allowing us to gauge the boundaries of the previously settled-on consensus process.

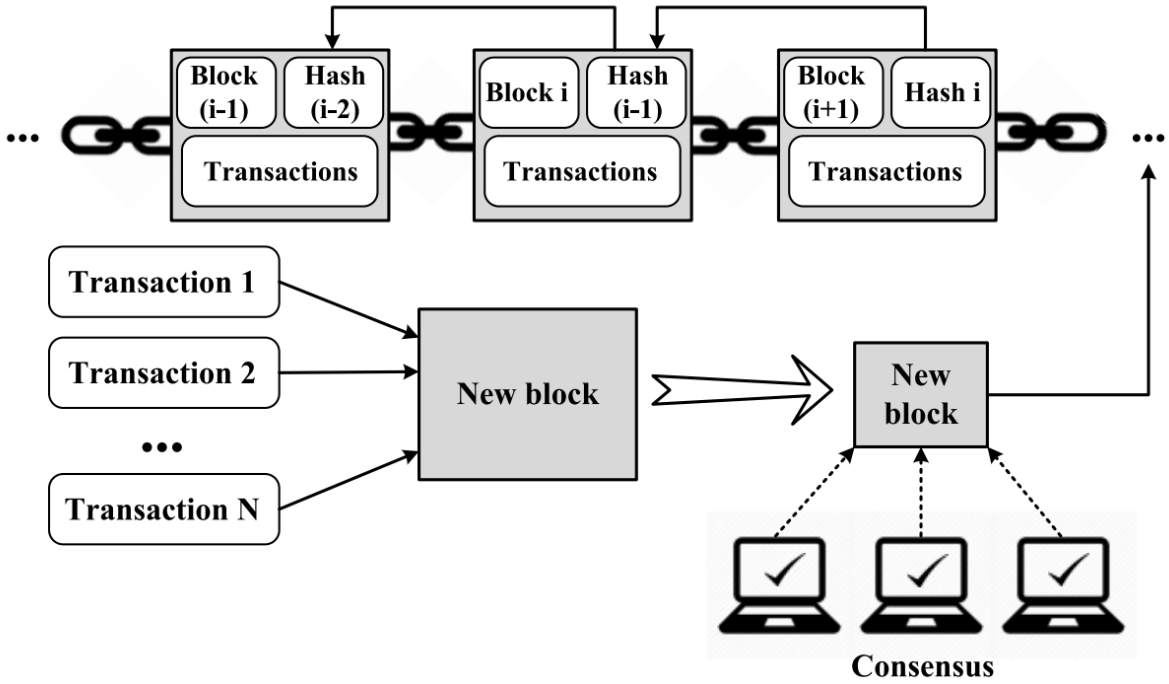

Figure 3 Architecture of Blockchain System [53]

There are two primary methods for determining consensus algorithm's or blockchain architecture's efficacy: mathematical statistics and computational trials. The first strategy involves studying working blockchain implementations, such as cryptocurrency networks, which can offer academics with useful information. Unfortunately, this method isn't available for exploration outside of a small subset of blockchain systems. Computational experiments are the second method, and they call for a tailored simulation environment to solve the problem at hand. A software simulator or pre-made programme is available for this purpose. The benefit of this method is that it takes into account all of the blockchain system's properties and details the behaviour of different consensus algorithms in system-specific scenarios [54].

Typical situations that disturb IoT system performance were the subject of the experimental research. These included an increase in the number of nodes, a node failure, and an increase in latency. Researchers conducted studies to assess the consensus algorithm's performance under varying latency distributions, looking at how block size, block creation rate, and latency all play a role. The experiment findings provide light on whether or not PBFT can be used in IoT scenarios. PBFT's scalability is limited by the bandwidth of the network, the number of verification nodes, and the processing power of those nodes. During the simulation, the load from each node was recorded, showing that a load of 85% was achieved with 25 running nodes, and a load of 90% was achieved with 30 nodes. The load was lowered to 45% using 30 devices to mimic restricted gadgets like electronic implants. Under these parameters, a maximum of 70 units can be used. PBFT stands out due to its low power usage. The simulation results demonstrate the PBFT algorithm's viability for use in resource-limited device systems.

REVIEW ARTICLE

5.2. Energy-Efficient Data Aggregation Mechanism (EEDAM) for IoT Secured by Blockchain

Since blockchain technology could function in a decentralized paradigm and provide security, decentralised architecture, and transparent systems, it is the subject of growing study. Low throughput, low latency, and delay-like concerns are common in existing blockchain topologies for IoT devices because of the high processing power and storage requirements. Organizations have moved to cloud servers as a solution to these problems, but blockchain technology might be a better option. To provide safe service provisioning and edge computing devices, blockchain-based cloud server architecture can rent out unused storage space to users. By removing the possibility of fraudulent activity from the network, blockchain technology makes edge servers a reliable source of security for IoT gadgets. Edge computing for IoT devices in the network's periphery improves efficiency, throughput, and safety in cloud architecture. To improve data aggregation processes in multi-hop wireless sensor networks, it is suggested to employ cluster strategies, such as the low-energy adaptive cluster hierarchy (LEACH) protocol, the dynamic sleep scheduling mode, and a two-tier distributed fuzzy logic-based protocol (TTDFP) [55].

Blockchain technology may be used to improve the security, efficiency, and accuracy of wireless sensor networks. To overcome the shortcomings of individual IoT architectures, a comprehensive hybrid approach that incorporates blockchain, cloud, edge, and fog is recommended. Using smart contracts for security and privacy services, a comprehensive blockchain infrastructure is planned to safeguard IoT networks. For IoT-based networks, edge computing is crucial for cloud data storage, cloud server load reduction, and real-time event detection. Edge data allocation, transmission costs, privacy, and security may all be determined with the use of blockchain and a federated learning technique [56].

The proposed EEDAM method estimates power utilization for long-distance transmissions of N-bit packets using the First Order Radio technique. Priority is given to establishing a regular bedtime, which is vital for both data redundancy and linguistic variety. Sleep and scheduling techniques conserve power by placing nodes in a hibernation state. The primary goal is to form groups of nodes that share a lot of data using the fuzzy matrix, and the cluster head (CH) then analyzes the information it receives from its members. Fuzzy similarity matrices are utilized for clustering in the proposed energy-efficient data aggregation technique for IoT protected by blockchain, with redundant nodes being chosen from across all clusters. Data redundancy, network congestion, and transmission costs may all be minimized with the help of the sleep scheduling mechanism. The overall system architecture of the suggested technique is depicted in Figure 4.

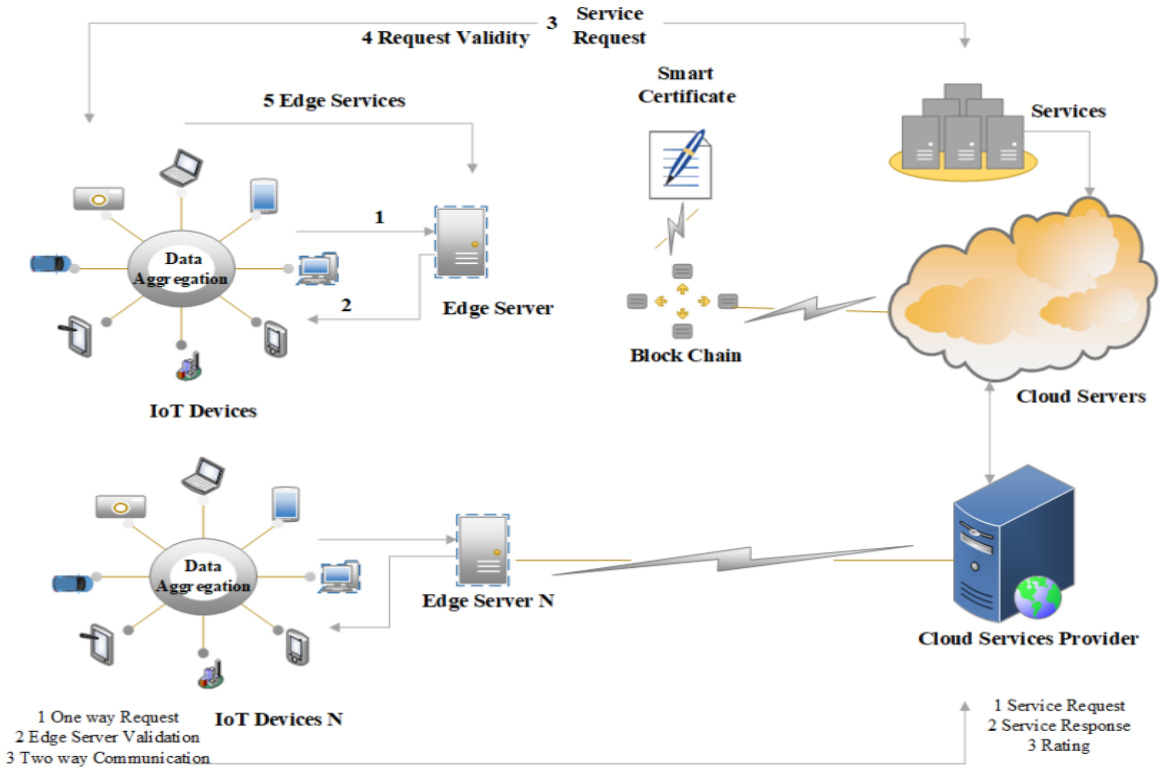

Figure 4 Proposed Architecture [56]

REVIEW ARTICLE

EEDAM is compared to other protocols in the model, such as EEHS and ESSM. IoT device feedback is also evaluated for correctness by the edge server. Gas consumption is a unit for transaction execution in blockchain technology, and more resources are utilized in a blockchain setting. In-depth experiments evaluated the suggested system's efficacy and efficiency. The consortium blockchain's middle-tier cloud server was modeled in this study. The energy mean and variation performance were analyzed, with a value of 0.5 indicating better performance. The communication distance of the CH was analyzed, showing a smaller transmission radius for CHs near the sink. The suggested method's performance may be evaluated without regard to the number of nodes involved. Two hundred nodes were used in a test of data accuracy. Data correlation is used to determine which duplicate nodes should be removed from the proposed scheme, and the remaining nodes are sufficient for achieving the identical anticipated degree of data integrity. Therefore, it is not necessary to maintain all nodes in active operation, resulting in less energy usage and increased precision of the collected data.

5.3. Reliable Cluster-Based Data Aggregation

Using a combination of hybrid deep learning algorithms, the authors of [57] have proposed a dependable cluster-based Data Aggregation (DA) approach, as illustrated in Figure 5, for IoT networks. The strategy aims to preserve both energy efficiency and dependability by reducing unnecessary data collection. Clusters are formed by clustering IoT sensors, and efficient data transport is ensured by the authors' introduction of a matrix and sine-cosine (MSC) algorithm. The degree of trust for each IoT sensor is calculated using several design metrics, and design constraints are optimized using a variant of the sunflower optimization (ISFO) method.

Data Aggregation (DA) is managed by the entity with the highest possible degree of trust ownership swelling. Researchers have started to support a wide range of healthcare sensor-related applications and scenarios due to the meteoric ascent of technology. The Internet of Things (IoT) consists of interconnected devices equipped with sensors to monitor environmental conditions and human health indicators. Security in IoT devices and applications is a crucial component in facilitating their wider adoption. Broadcast aggregation enhances power consumption and data provision quality during data gathering. End-to-end secure interactions between IoT entities are only possible when blockchain is used with IoT devices.

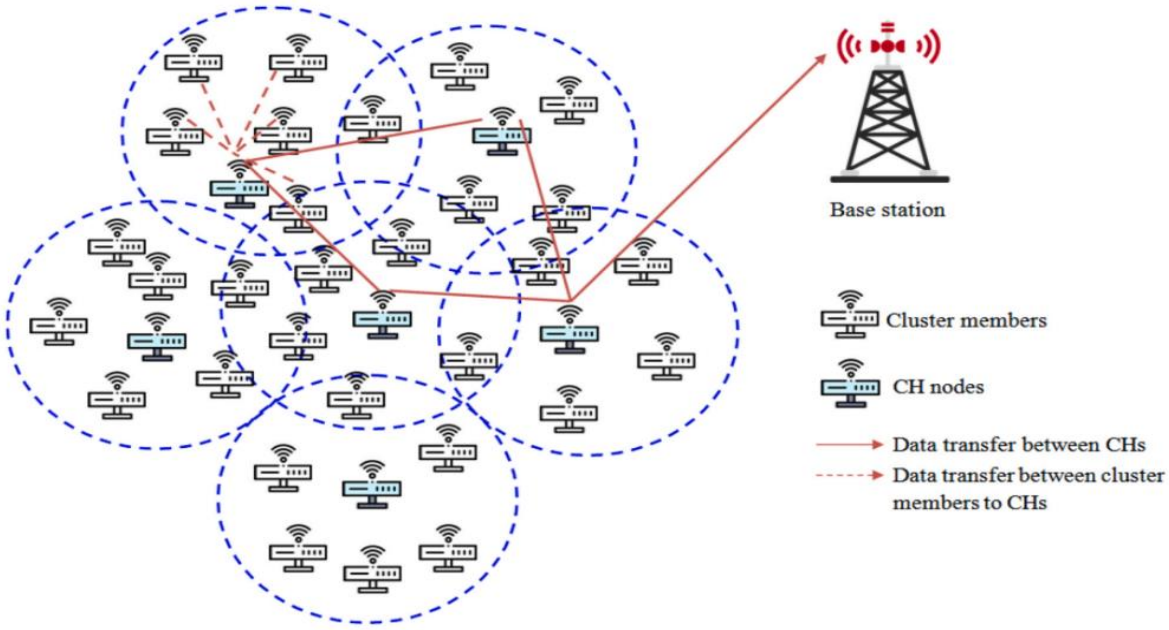

Figure 5 Architecture of Cluster-based Data Aggregation [57]

The Network Simulator (NS2) was employed to validate a potential Cluster-Based Reliable Data Aggregation (CRDA) approach. Current conditions, such as workforce plans, upgraded edge delicate stable political race convention (ETSSEP), stable energy-efficient clustering convention (SEECP), reliability Improved-Drain (SILEACH), and efficient multi-jump cluster-based collection (EMCA-CS), serve as benchmarks against which simulation results are evaluated. Energy, aggregation delay, network longevity, throughput, overhead, and data transfer rate are compared

REVIEW ARTICLE

between the planned CRDA design and existing schemes. As part of the simulation setup, a sink is placed in a 1000 m x 1000 m terrain, and a total of 100 nodes and 900 randomly placed vertices are used. Nodes engaged in sending utilize 24.92 mJ of energy for every 1 byte sent, whereas nodes engaged in receiving use only 19.72 mJ. Increasing the number of nodes in an Internet of Things (IoT) network does not degrade the performance of the CRDA system, which aggregates data from those nodes. The suggested strategy reduces energy consumption by 64.092%, 57.24%, 47.158%, and 30.854% compared to the state-of-the-art ETSSEP, SEECP, SILEACH, and EMCA-CS schemes, respectively. In comparison to the state-of-the-art ETSSEP, SEECP, SILEACH, and EMCA-CS schemes, it reduces aggregation latency by 31.221%, 28.212%, 24.927%, and 18.638%, respectively.

6. CONCLUSION

The convergence of IoT technology with healthcare applications holds immense potential, introducing transformative possibilities such as real-time monitoring, personalized medical treatment, and improved patient outcomes. However, this amalgamation also presents complex challenges that necessitate innovative solutions. This study focuses on reviewing data aggregation methods in IoT healthcare applications to enhance efficiency and security. The longevity and dependability of IoT healthcare equipment crucially hinge on their energy efficiency. The continuous monitoring, data transmission, and processing demanded by these devices require meticulous management and optimization of their limited energy resources. Achieving a balance between meeting operational demands and conserving energy can be accomplished through strategies such as low-power hardware design, duty cycling, and adaptive sampling. The collection and transmission of sensitive patient data by IoT devices raises serious concerns about data security and privacy, which are of critical importance in healthcare. Maintaining patient confidence and protecting private health information requires the use of strong encryption, secure communication protocols, and compliance with legal frameworks like HIPAA and the General Data Protection Regulation. Energy efficiency, data security, and data aggregation are all interdependent in the context of IoT healthcare applications. Future developments in energy efficiency and data security may benefit from new trends like blockchain integration and edge computing. IoT healthcare applications may maintain their innovative spirit while staying true to their patient-centric roots by taking advantage of these developments.

REFERENCES

[1] H. F. Nweke, Y. W. Teh, G. Mujtaba, and M. A. Al-garadi, "Data fusion and multiple classifier systems for human activity detection and health monitoring: Review and open research directions," Information Fusion, vol. 46, pp. 147–170, Mar. 2019, doi: 10.1016/j.inffus.2018.06.002.

[2] A. I. Taloba et al., "A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare," Alexandria Engineering Journal, vol. 65, pp. 263–274, Feb. 2023, doi: 10.1016/j.aej.2022.09.031.

[3] S. Selvaraj and S. Sundaravaradhan, "Challenges and opportunities in IoT healthcare systems: a systematic review," SN Appl. Sci., vol. 2, no. 1, p. 139, Jan. 2020, doi: 10.1007/s42452-019-1925-y.

[4] X. Zhou, W. Liang, K. I.-K. Wang, H. Wang, L. T. Yang, and Q. Jin, "Deep-Learning-Enhanced Human Activity Recognition for Internet of Healthcare Things," IEEE Internet Things J., vol. 7, no. 7, pp. 6429–6438, Jul. 2020, doi: 10.1109/JIOT.2020.2985082.

[5] [H. Elayan, M. Aloqaily, and M. Guizani, "Digital Twin for Intelligent Context-Aware IoT Healthcare Systems," IEEE Internet Things J., vol. 8, no. 23, pp. 16749–16757, Dec. 2021, doi: 10.1109/JIOT.2021.3051158.

[6] A. Ahmed, S. Abdullah, M. Bukhsh, I. Ahmad, and Z. Mushtaq, "An Energy-Efficient Data Aggregation Mechanism for IoT Secured by Blockchain," IEEE Access, vol. 10, pp. 11404–11419, 2022, doi: 10.1109/ACCESS.2022.3146295.

[7] P. A. Apostolopoulos, E. E. Tsiropoulou, and S. Papavassiliou, "Cognitive Data Offloading in Mobile Edge Computing for Internet of Things," IEEE Access, vol. 8, pp. 55736–55749, 2020, doi: 10.1109/ACCESS.2020.2981837.

[8] A. Rehman, T. Saba, K. Haseeb, T. Alam, and J. Lloret, "Sustainability Model for the Internet of Health Things (IoHT) Using Reinforcement Learning with Mobile Edge Secured Services," Sustainability, vol. 14, no. 19, p. 12185, Sep. 2022, doi: 10.3390/su141912185.

[9] S. S. Rani, J. A. Alzubi, S. K. Lakshmanaprabu, D. Gupta, and R. Manikandan, "RETRACTED ARTICLE: Optimal users based secure data transmission on the internet of healthcare things (IoHT) with lightweight block ciphers," Multimed Tools Appl, vol. 79, no. 47–48, pp. 35405–35424, Dec. 2020, doi: 10.1007/s11042-019-07760-5.

[10] M. A. Rahman, M. S. Hossain, A. J. Showail, N. A. Alrajeh, and M. F. Alhamid, "A secure, private, and explainable IoHT framework to support sustainable health monitoring in a smart city," Sustainable Cities and Society, vol. 72, p. 103083, Sep. 2021, doi: 10.1016/j.scs.2021.103083.

[11] M. Mamdouh, A. I. Awad, A. A. M. Khalaf, and H. F. A. Hamed, "Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions," Computers & Security, vol. 111, p. 102491, Dec. 2021, doi: 10.1016/j.cose.2021.102491.

[12] M. A. Rahman, M. S. Hossain, M. S. Islam, N. A. Alrajeh, and G. Muhammad, "Secure and Provenance Enhanced Internet of Health Things Framework: A Blockchain Managed Federated Learning Approach," IEEE Access, vol. 8, pp. 205071–205087, 2020, doi: 10.1109/ACCESS.2020.3037474.

[13] J. J. Kang, M. Dibaei, G. Luo, W. Yang, P. Haskell-Dowland, and X. Zheng, "An Energy-Efficient and Secure Data Inference Framework for Internet of Health Things: A Pilot Study," Sensors, vol. 21, no. 1, p. 312, Jan. 2021, doi: 10.3390/s21010312.

[14] E. M. Abou-Nassar, A. M. Iliyasu, P. M. El-Kafrawy, O.-Y. Song, A. K. Bashir, and A. A. A. El-Latif, "DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems," IEEE Access, vol. 8, pp. 111223–111238, 2020, doi: 10.1109/ACCESS.2020.2999468.

[15] K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, "A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities," IEEE Commun. Surv. Tutorials, vol. 22, no. 4, pp. 2489–2520, 2020, doi: 10.1109/COMST.2020.3011208.

[16] P. Singh, A. Nayyar, A. Kaur, and U. Ghosh, "Blockchain and Fog Based Architecture for Internet of Everything in Smart Cities," Future Internet, vol. 12, no. 4, p. 61, Mar. 2020, doi: 10.3390/fi12040061.

[17] A. K. Idrees and A. K. M. Al-Qurabat, "Energy-Efficient Data Transmission and Aggregation Protocol in Periodic Sensor Networks

REVIEW ARTICLE

Based Fog Computing," J Netw Syst Manage, vol. 29, no. 1, p. 4, Jan. 2021, doi: 10.1007/s10922-020-09567-4.
[18] L. Feng, P. Kortoçi, and Y. Liu, "A multi-tier data reduction mechanism for IoT sensors," in Proceedings of the Seventh International Conference on the Internet of Things, Linz Austria: ACM, Oct. 2017, pp. 1–8. doi: 10.1145/3131542.3131557.
[19] Junkuo Cao, Mingcai Lin, and Xiaojin Ma, "A Survey of Big Data for IoT in Cloud Computing," IAENG International Journal of Computer Science, vol. 47, no.3, pp585-592, 2020
[20] A. K. M. Al-Qurabat and A. K. Idrees, "Two level data aggregation protocol for prolonging lifetime of periodic sensor networks," Wireless Netw, vol. 25, no. 6, pp. 3623–3641, Aug. 2019, doi: 10.1007/s11276-019-01957-0.
[21] A. M. Hussein, A. K. Idrees, and R. Couturier, "Distributed energy-efficient data reduction approach based on prediction and compression to reduce data transmission in IoT networks," Int J Communication, vol. 35, no. 15, Oct. 2022, doi: 10.1002/dac.5282.
[22] M. El-hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A Survey of Internet of Things (IoT) Authentication Schemes," Sensors, vol. 19, no. 5, p. 1141, Mar. 2019, doi: 10.3390/s19051141.
[23] J. Liu, H. Tang, R. Sun, X. Du, and M. Guizani, "Lightweight and Privacy-Preserving Medical Services Access for Healthcare Cloud," IEEE Access, vol. 7, pp. 106951–106961, 2019, doi: 10.1109/ACCESS.2019.2931917.
[24] M. R. Naqvi, M. Aslam, M. W. Iqbal, S. Khuram Shahzad, M. Malik, and M. U. Tahir, "Study of Block Chain and its Impact on Internet of Health Things (IoHT):Challenges and Opportunities," in 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey: IEEE, Jun. 2020, pp. 1–6. doi: 10.1109/HORA49412.2020.9152846.
[25] A. Abdallah and X. S. Shen, "A Lightweight Lattice-Based Homomorphic Privacy-Preserving Data Aggregation Scheme for Smart Grid," IEEE Trans. Smart Grid, vol. 9, no. 1, pp. 396–405, Jan. 2018, doi: 10.1109/TSG.2016.2553647.
[26] F. Leukam Lako, P. Lajoie-Mazenc, and M. Laurent, "Privacy-Preserving Publication of Time-Series Data in Smart Grid," Security and Communication Networks, vol. 2021, pp. 1–21, Mar. 2021, doi: 10.1155/2021/6643566.
[27] D. Mercier, A. Lucieri, M. Munir, A. Dengel, and S. Ahmed, "PPML-TSA: A modular privacy-preserving time series classification framework," Software Impacts, vol. 12, p. 100286, May 2022, doi: 10.1016/j.simpa.2022.100286.
[28] L. Wu, W. Zhang, and W. Zhao, "Privacy Preserving Data Aggregation for Smart Grid with User Anonymity and Designated Recipients," Symmetry, vol. 14, no. 5, p. 847, Apr. 2022, doi: 10.3390/sym14050847.
[29] M. Yang, T. Zhu, B. Liu, Y. Xiang, and W. Zhou, "Machine Learning Differential Privacy with Multifunctional Aggregation in a Fog Computing Architecture," IEEE Access, vol. 6, pp. 17119–17129, 2018, doi: 10.1109/ACCESS.2018.2817523.
[30] Manjula C Belavagi, and Balachandra Muniyal, "Intrusion Detection Using Rule Based Approach in RPL Networks," IAENG International Journal of Computer Science, vol. 50, no.3, pp988-999, 2023.
[31] Li Wuke, Yin Guangluan, and Chen Xiaoxiao, "Application of Deep Extreme Learning Machine in Network Intrusion Detection Systems," IAENG International Journal of Computer Science, vol. 47, no.2, pp136-143, 2020
[32] A. Kumar, R. Saha, M. Alazab, and G. Kumar, "A Lightweight Signcryption Method for Perception Layer in Internet-of-Things," Journal of Information Security and Applications, vol. 55, p. 102662, Dec. 2020, doi: 10.1016/j.jisa.2020.102662.
[33] J. Al-Jaroodi, N. Mohamed, and E. Abukhousa, "Health 4.0: On the Way to Realizing the Healthcare of the Future," IEEE Access, vol. 8, pp. 211189–211210, 2020, doi: 10.1109/ACCESS.2020.3038858.
[34] X. Zhu and Y. Badr, "Identity Management Systems for the Internet of Things: A Survey Towards Blockchain Solutions," Sensors, vol. 18, no. 12, p. 4215, Dec. 2018, doi: 10.3390/s18124215.
[35] M. Kumar, M. Sethi, S. Rani, D. K. Sah, S. A. AlQahtani, and M. S. Al-Rakhami, "Secure Data Aggregation Based on End-to-End Homomorphic Encryption in IoT-Based Wireless Sensor Networks," Sensors, vol. 23, no. 13, p. 6181, Jul. 2023, doi: 10.3390/s23136181.
[36] W. Ding, X. Jing, Z. Yan, and L. T. Yang, "A survey on data fusion in internet of things: Towards secure and privacy-preserving fusion," Information Fusion, vol. 51, pp. 129–144, Nov. 2019, doi: 10.1016/j.inffus.2018.12.001.
[37] T.-Y. Wu, T. Wang, Y.-Q. Lee, W. Zheng, S. Kumari, and S. Kumar, "Improved Authenticated Key Agreement Scheme for Fog-Driven IoT Healthcare System," Security and Communication Networks, vol. 2021, pp. 1–16, Jan. 2021, doi: 10.1155/2021/6658041.
[38] X. Jia, D. He, N. Kumar, and K.-K. R. Choo, "Authenticated key agreement scheme for fog-driven IoT healthcare system," Wireless Netw, vol. 25, no. 8, pp. 4737–4750, Nov. 2019, doi: 10.1007/s11276-018-1759-3.
[39] V. Tudor, V. Gulisano, M. Almgren, and M. Papatriantafilou, "BES: Differentially private event aggregation for large-scale IoT-based systems," Future Generation Computer Systems, vol. 108, pp. 1241–1257, Jul. 2020, doi: 10.1016/j.future.2018.07.026.
[40] H. Huang, T. Gong, N. Ye, R. Wang, and Y. Dou, "Private and Secured Medical Data Transmission and Analysis for Wireless Sensing Healthcare System," IEEE Trans. Ind. Inf., vol. 13, no. 3, pp. 1227–1237, Jun. 2017, doi: 10.1109/TII.2017.2687618.
[41] Alla Levina, Vladimir Varyukhin, Dmitry Kaplun, Anna Zamansky, and Dirk van der Linden, "A Case Study Exploring Side-Channel Attacks On Pet Wearables," IAENG International Journal of Computer Science, vol. 48, no.4, pp878-883, 2021.
[42] Aqeel A. Yaseen, Kalyani Patel, Ali A. Yassin, Abdulla J. Aldarwish, and Haitham A. Hussein, "Secure Electronic Healthcare Record Using Robust Authentication Scheme," IAENG International Journal of Computer Science, vol. 50, no.2, pp468-476, 2023
[43] B. Wang, F. Wu, Y. Long, L. Rimanic, C. Zhang, and B. Li, "DataLens: Scalable Privacy Preserving Training via Gradient Compression and Aggregation," in Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, Nov. 2021, pp. 2146–2168. doi: 10.1145/3460120.3484579.
[44] X. Liu et al., "Secure Data Aggregation Aided by Privacy Preserving in Internet of Things," Wireless Communications and Mobile Computing, vol. 2022, pp. 1–14, Mar. 2022, doi: 10.1155/2022/4858722.
[45] J. Wang, L. Wu, S. Zeadally, M. K. Khan, and D. He, "Privacy-preserving Data Aggregation against Malicious Data Mining Attack for IoT-enabled Smart Grid," ACM Trans. Sen. Netw., vol. 17, no. 3, pp. 1–25, Aug. 2021, doi: 10.1145/3440249.
[46] K. T. Kadhim, A. M. Alsahlany, S. M. Wadi, and H. T. Kadhum, "An Overview of Patient's Health Status Monitoring System Based on Internet of Things (IoT)," Wireless Pers Commun, vol. 114, no. 3, pp. 2235–2262, Oct. 2020, doi: 10.1007/s11277-020-07474-0.
[47] A. Seyfollahi and A. Ghaffari, "Reliable data dissemination for the Internet of Things using Harris hawks optimization," Peer-to-Peer Netw. Appl., vol. 13, no. 6, pp. 1886–1902, Nov. 2020, doi: 10.1007/s12083-020-00933-2.
[48] S. N. Sajedi, M. Maadani, and M. Nesari Moghadam, "F-LEACH: a fuzzy-based data aggregation scheme for healthcare IoT systems," J Supercomput, vol. 78, no. 1, pp. 1030–1047, Jan. 2022, doi: 10.1007/s11227-021-03890-6.
[49] M. Manicka Raja and S. Manoj Kumar, "Aggregated PSO for Secure Data Transmission in WSN Using Fog Server," Intelligent Automation & Soft Computing, vol. 34, no. 2, pp. 1017–1032, 2022, doi: 10.32604/iasc.2022.025665.
[50] S. Siamala Devi, K. Venkatachalam, Y. Nam, and M. Abouhawwash, "Discrete GWO Optimized Data Aggregation for Reducing Transmission Rate in IoT," Computer Systems Science and Engineering, vol. 44, no. 3, pp. 1869–1880, 2023, doi: 10.32604/csse.2023.025505.
[51] K. A. Darabkh, A. B. Amareen, M. Al-Akhras, and W. K. Kassab, "An innovative cluster-based power-aware protocol for Internet of Things

REVIEW ARTICLE

sensors utilizing mobile sink and particle swarm optimization," Neural Comput & Applic, vol. 35, no. 26, pp. 19365–19408, Sep. 2023, doi: 10.1007/s00521-023-08752-1.
[52] D. D. Datiri and M. Li, "Effects of Particle Swarm Optimisation on a Hybrid Load Balancing Approach for Resource Optimisation in Internet of Things," Sensors, vol. 23, no. 4, p. 2329, Feb. 2023, doi: 10.3390/s23042329.
[53] Y. Meshcheryakov, A. Melman, O. Evsutin, V. Morozov, and Y. Koucheryavy, "On Performance of PBFT Blockchain Consensus Algorithm for IoT-Applications with Constrained Devices," IEEE Access, vol. 9, pp. 80559–80570, 2021, doi: 10.1109/ACCESS.2021.3085405.
[54] S. B. ElMamy, H. Mrabet, H. Gharbi, A. Jemai, and D. Trentesaux, "A Survey on the Usage of Blockchain Technology for Cyber-Threats in the Context of Industry 4.0," Sustainability, vol. 12, no. 21, p. 9179, Nov. 2020, doi: 10.3390/su12219179.
[55] A. Ahmed, S. Abdullah, M. Bukhsh, I. Ahmad, and Z. Mushtaq, "An Energy-Efficient Data Aggregation Mechanism for IoT Secured by Blockchain," IEEE Access, vol. 10, pp. 11404–11419, 2022, doi: 10.1109/ACCESS.2022.3146295.
[56] J. Lockl, V. Schlatt, A. Schweizer, N. Urbach, and N. Harth, "Toward Trust in Internet of Things Ecosystems: Design Principles for Blockchain-Based IoT Applications," IEEE Trans. Eng. Manage., vol. 67, no. 4, pp. 1256–1270, Nov. 2020, doi: 10.1109/TEM.2020.2978014.
[57] G. Ravi, M. Swamy Das, and K. Karmakonda, "Reliable cluster-based data aggregation scheme for IoT network using hybrid deep learning techniques," Measurement: Sensors, vol. 27, pp. 1-12, Jun. 2023, doi: 10.1016/j.measen.2023.100744.

Authors

Mr. Ganesh Srinivasa Shetty has received his Bachelor of Engineering from Malnad College Of Engineering, Hassan and completed his M.Tech degree from Sri Jayachamarajendra College Of Engineering Mysore. He is a part time research scholar at JAIN (Deemed to be University) in Bengaluru, India. Currently, he is working as Senior Assistant Professor in Shri Madhwa Vadiraja Institute of Technology and Management (SMVITM) Vishwothama Nagar, Bantakal-5764115, Udupi, Kanataka, India. His interests lie in the areas of Cryptograhy and Artificial Intelligence and Machine Learning. He has authored 5+ research articles/conference.

Dr. Raghu N has received his PhD in Image Processing from JAIN (Deemed-To-Be-University) Bangalore, India during the period of 2020 and he has completed his master in Digital Electronics and Communication Engineering from Nitte Mahalinga Adyanthaya Memorial Institute of Technology, Karnataka in 2011. Currently, he is working as Associate Professor in JAIN (Deemed-To-Be-University) Bangalore, India. His research has included IRNSS position mapping & accuracy, HV & LV Hazards. He is serving as an editorial member of several reputed journals & expert Reviewers for journals& Conferences. He has authored 24+ research articles/books/ book chapters. He is a member of International Association of Engineers, International Association of Computer Science and Information Technology and Asia-Pacific Chemical, Biological& Environmental Engineering Society (APCBEES).

How to cite this article:

Ganesh Srinivasa Shetty, Raghu N, "Strategies for Achieving Energy Efficiency and Data Security Through Data Aggregation in IoT Healthcare Applications: A Comprehensive Study", International Journal of Computer Networks and Applications (IJCNA), 11(2), PP: 127-139, 2024, DOI: 10.22247/ijcna/2024/224440.