IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 10 October 2023, accepted 17 October 2023, date of publication 20 October 2023, date of current version 27 October 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3326155

RESEARCH ARTICLE

Blockchain-Integrated Security for Real-Time Patient Monitoring in the Internet of Medical Things Using Federated Learning

MOHAMMAD FAISAL KHAN[1] **AND MOHAMMAD ABAOUD**[2]
[1]Department of Basic Sciences, College of Science and Theoretical Studies, Saudi Electronic University, Riyadh 11673, Saudi Arabia
[2]Department of Mathematics and Statistics, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh 11564, Saudi Arabia

Corresponding author: Mohammad Faisal Khan (f.khan@seu.edu.sa)

This work was funded by the Deputyship for Research and Innovation, Ministry of Education, Saudi Arabia, under Project IFP-IMSIU-2023137; and managed by the Deanship of scientific Research at Imam Mohammad Ibn Saud Islamic University (IMSIU).

ABSTRACT The Internet of Medical Things (IoMT) heralds a transformative era in healthcare, with the potential to revolutionize patient care, healthcare services, and medical research. As with all technological progressions, IoMT introduces a suite of complex challenges, predominantly centered on security. In particular, ensuring the integrity, confidentiality, and availability of health data in real-time communication stands paramount, given the sensitivity of the information and the ramifications of potential breaches or misuse. In light of these challenges, existing security frameworks, while commendable, exhibit limitations. Specifically, they often grapple with comprehensive anomaly detection, effective resistance to replay attacks, and robust protection against threats like man-in-the-middle attacks, eavesdropping, data tampering, and identity spoofing. The proposed framework integrates state-of-the-art encryption techniques, cutting-edge pattern recognition modules, and adaptive learning mechanisms. These components collaboratively ensure data integrity during transmission, provide robust resistance against conventional and novel attack vectors, and adapt to evolving threats through continuous learning. Moreover, the framework incorporates sophisticated checksum techniques and advanced behavioral analysis, further enhancing its protective capabilities. Our system demonstrated significant improvements in anomaly detection and attack resistance metrics, consistently outperforming benchmark solutions like MRMS and BACKM-EHA.

INDEX TERMS Anomaly detection, blockchain, federated learning, homomorphic encryption, Internet of Medical Things, privacy preservation, real-time patient monitoring, security.

I. INTRODUCTION

The Internet of Medical Things (IoMT) represents a transformative convergence of healthcare and information technology [1], [2], epitomizing the modern age of digital medicine. As medical devices become increasingly interconnected, generating and relaying voluminous amounts of patient data [3], the IoMT has positioned itself as a linchpin for enhanced patient care, remote health monitoring [4], and personalized medical interventions [5]. While these advancements hold immense promise for redefining the contours of healthcare delivery [6], they simultaneously usher in a set of multifaceted challenges. Paramount among these are the issues of data privacy [7], [8], security [9], [10], and the ever-present tension between the computational constraints of devices and the necessity for prompt, accurate patient monitoring [11]. As healthcare systems globally grapple with these challenges, it becomes imperative to seek innovative solutions that not only harness the potential of the IoMT but also address its inherent vulnerabilities [12].

The exponential growth of the IoMT has laid bare a myriad of challenges [13], both technical and ethical, arising from the confluence of healthcare and cutting-edge technology [14]. Foremost among these challenges is the safeguarding of patient data privacy. With IoMT devices routinely collecting [15], transmitting [16], and processing vast troves of sensitive patient data [17], the risk of inadvertent data leaks or malicious breaches becomes an ever-present concern. Traditional

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

centralized systems, being potential single points of failure, exacerbate this risk. The transmission of raw patient data, which is standard in many systems, further amplifies the vulnerability of the patient's privacy [17]. Equally pressing is the challenge of ensuring data security [18]. In an interconnected IoMT environment, the data is not only susceptible to breaches but also to manipulations, posing threats not just to privacy but also to the accuracy and reliability of medical insights derived from the data. Authenticity and integrity of data, therefore, become paramount, demanding foolproof mechanisms to validate and verify every piece of information that flows through the network. Moreover, IoMT devices, often designed to be lightweight and energy-efficient [7], face inherent computational constraints. Balancing these constraints against the need for real-time, accurate monitoring presents a significant technical hurdle. This study zeroes in on these pivotal challenges, proposing a novel approach that leverages the strengths of federated learning and blockchain technologies to holistically address the intertwined issues of privacy, security, data integrity, and efficient real-time monitoring in the IoMT space.

The IoMT signifies a paradigm shift in healthcare, emphasizing remote real-time monitoring, tailored treatment protocols, and insights powered by voluminous patient data. These advancements promise a healthcare system optimized for cost, patient outcomes, and proactive health monitoring [19]. With the rapid interconnection of medical devices and ceaseless data flow, new challenges emerge, especially concerning the privacy and security of sensitive patient information. Historically, data from IoMT devices has been anchored to centralized storage and processing units. However, such centralization can become a vulnerability, exposing the system to potential breaches or single points of failure. Transmitting raw patient data across networks further magnifies the privacy challenges. As the IoMT infrastructure expands, the exigency for solutions that encapsulate data privacy, robust security, and real-time monitoring efficiency comes to the forefront. The traditional architecture, characterized by central repositories, presents critical challenges. Firstly, how can the IoMT landscape ensure that devices process and analyze patient data without resorting to the transfer of sensitive raw information to these central hubs? Secondly, in a world with increasing cyber threats [20], which mechanisms can guarantee the security of the transmitted model updates and data over the network? The third question pertains to ensuring the authenticity and integrity of data transmissions within a decentralized IoMT environment [21]. Finally, given the inherent computational limitations of IoMT devices, how can the system maintain its real-time monitoring efficacy without compromising device performance. In light of these concerns, there is a compelling need to explore methodologies that synergize federated learning with blockchain technologies. Such integration might offer a blueprint for addressing the multifaceted challenges inherent in the burgeoning IoMT domain.

The proposed approach articulates a decentralized framework that seamlessly integrates privacy, security, and real-time efficiency in the IoMT. Central to this design is the adoption of federated learning, a decentralized machine learning paradigm. In this construct, IoMT devices, equipped with essential computational prowess, gather and preprocess patient data at the edge. This ensures that sensitive patient data remains localized, obviating the need for raw data transmission. Instead, devices periodically send model weights or updates to a central server, having first encrypted them through advanced homomorphic encryption techniques. Such encryption permits the central server to aggregate these updates without ever glimpsing the raw data, reinforcing data confidentiality. To augment security and enhance traceability, blockchain technology is integrated. Every IoMT device, together with the central server, acts as a node in this secure network. By harnessing the immutable properties of blockchain ledgers, all model updates and device authentications are meticulously logged, establishing both transmission integrity and device verifiability. Another salient feature is the embedded anomaly detection tool within each IoMT device. This tool vigilantly monitors for irregular patterns or potential security breaches. On identifying any such deviation, real-time alerts can be activated, thereby facilitating prompt risk intervention. Furthermore, when the global model discerns pivotal health trends, these insights are securely relayed to the pertinent IoMT device via encrypted notifications. The device then decrypts and displays this information, ensuring patient privacy remains uncompromised. The notable contributions of our approach, especially when contextualized against the backdrop of pertinent studies in the IoMT domain, are:

1) Introduction of a *decentralized learning paradigm* tailored for IoMT devices. This emphasis on local data processing minimizes the transmission of raw, sensitive patient data, thereby bolstering data privacy.
2) Adoption of *homomorphic encryption* techniques, which facilitate secure aggregation of model updates at the server-side. This method ensures robust data protection without compromising the integrity of the computational process.
3) Deployment of *blockchain technology for traceability and authentication*. This not only ensures the transparency and accountability of model iterations but also strengthens the authentication of connected devices.
4) Implementation of an *embedded anomaly detection mechanism* to provide an enhanced layer of security. This feature is optimized for real-time identification and mitigation of potential threats.
5) Formulation of a privacy-centric alert system, proficient in dispatching crucial health alerts without divulging specific patient information to the server.

The structure of the rest of the article is as Section II, offering a critical survey of existing IoMT security measures and challenges. This foundation sets the stage for the introduction of our novel Section III, which highlights its decentralized and robust nature. A key component of our framework, Section IV, is then detailed, underscoring our commitment to patient data privacy. The Section V section provides insights into our testing environment and methodologies. Following this, Section VI unveils empirical results, demonstrating the efficacy of the proposed system. In Section VII segment, a reflective analysis of our findings with existing benchmarks, also touches upon potential limitations. The manuscript culminates in Section VIII, summarizing the pivotal contributions and implications of our study for the evolving IoMT domain.

II. LITERATURE REVIEW

The literature review offers a systematic exploration of prior research pertinent to the Internet of Medical Things (IoMT), with an emphasis on its evolutionary trajectory, inherent privacy and security challenges, and emerging solutions. The ensuing discourse critically evaluates seminal works, revealing the dynamic interplay between technology and healthcare, and underscores the imperative for data-centric solutions. By furnishing this contextual backdrop, this review not only positions the current research within the broader scholarly conversation but also accentuates the areas where innovation remains both promising and paramount.

The evolution of healthcare technologies is consistently steering towards more personalized and patient-centric approaches. One significant advancement in this domain is the concept of continuous patient monitoring using patient-centric agents. Uddin et al. [22] proposed a block architecture for such continuous monitoring, emphasizing the creation of an environment that is focused on individual patient needs. This framework relies on the seamless integration of health data acquisition, processing, and predictive analysis to optimize patient care. Such architectures provide the foundation for efficient and effective real-time health monitoring systems, facilitating rapid response to any emerging health complications.

Further reinforcing the potential of modern technologies in healthcare, the integration of the IoT and deep learning approaches has shown promising results in patient monitoring and disease prediction. A study by Sarmah [23] presents an efficient IoT-based system for patient monitoring that couples with a deep learning modified neural network for predicting heart diseases. The innovation resides not only in the real-time acquisition of health data but also in the utilization of sophisticated deep learning techniques to process and analyze the data for proactive healthcare measures. Such combined approaches underscore the potential of IoT and advanced machine learning in revolutionizing patient care and preemptive disease management.

A. EVOLUTION OF THE INTERNET OF MEDICAL THINGS (IoMT)

The IoMT has evolved as an intricate synthesis of medical devices and applications that are intricately linked to healthcare information technology systems via online computer networks [24]. Grounded in the broader ecosystem of the IoT, which itself has witnessed substantial transformational changes over the past twenty years, the IoMT has carved a niche for itself [25]. Transitioning from the generic framework of the IoT, IoMT underscores specialized medical interventions, pivoting around real-time patient monitoring and tailored healthcare services [26]. The proliferation and advancements in IoMT are not only the result of technological innovations but also the culmination of rigorous research endeavors undertaken over the years. A structured summary of key milestones, the scholars instrumental in those advancements, and their notable contributions to the IoMT evolution is presented in Table 1.

TABLE 1. Key milestones in the evolution of IoMT.

Ref.	Milestone/Aspect	Key Contribution/Findings
[24]	Overview of IoMT	Architectural components and advancements
[25]	IoT Evolution over 20 Years	Transformational changes in IoT ecosystems
[27]	DL-driven SDN for Malware Detection	Hybrid deep learning approach in IoMT
[28]	GANs for IoMT Data	Advanced ML application in medical interconnectivity
[29]	Mobile Edge Computing in IoMT	Reduction in system latency and improved efficacy
[30]	Blockchain-enabled EMRs	Secured electronic medical records using blockchain
[31]	Cybersecurity in IoMT	Exploration of potential threats and countermeasures
[32]	Transition from Blockchain to IOTA	Evolution from basic paradigms to advanced technologies

In understanding this evolution, Razdan and Sharma provide an astute exploration of IoMT, elaborating on its architectural components, salient technological advancements, and transformative case studies [24]. This intricate mesh is not just about inter-device communication; it represents an ecosystem teeming with intelligence. As an illustration, Khan and Akhunzada's work stands out, where they developed a hybrid mechanism rooted in deep learning, harmoniously functioning within the Software-Defined Networking (SDN) ecosystem, adeptly targeting malware within IoMT environments [27].

Historically, IoMT's trajectory is adorned with milestones that accentuate its collaborative synergy with other frontier technologies. An exemplary integration is showcased by Vaccari et al., who introduced the concept of Generative Adversarial Networks (GANs) for handling IoMT data, epitomizing the marriage between advanced machine learning and medical device interconnectivity [28]. In tandem, the assimilation of mobile edge computing with IoMT paves the way for swift data computations, effectively reducing system latency and significantly enhancing the efficacy of medical applications [29]. The inclusion of blockchain in

TABLE 2. Comparative analysis of IoMT privacy approaches.

Ref.	Primary Focus	Methodology	IoMT Application	Outcome
[34]	Multimedia Security	Layers of Safeguards	General	Enhanced Data Integrity
[35]	Device Risk Assessment	Heterogeneous Analysis	Diverse Devices	Identified Risks
[36]	Device Authentication	Feature-based Assessment	Device Verification	Secure Device Integration
[37]	Network Protection	Federated Reinforcement-based	Network Security	Reduced Cyber Threats
[38]	Big Data Analysis	Federated Learning & Edge Computing	Data Analysis	Privacy-preserved Analytics
[39]	Holistic Security & Privacy	Comprehensive Analysis	General	Identified Challenges & Trends
[40]	Security & Privacy Framework	IoMT Framework Analysis	Infrastructure Security	Robust IoMT System
[41]	Decentralized Models	Federated Learning	Healthcare Systems	Enhanced Data Privacy
[42]	Personalized Healthcare	AI & Embedded Technology	Human Identity Chips	Trajectory for Personalized Healthcare
[43]	AIoMT Integration	Federated Learning	Social Implementations	Transformative Potential

the IoMT tapestry further solidifies its stance on secure and decentralized data transactions, as explored by Qu et al. They particularly focus on the transformative potential of using blockchain for safeguarding electronic medical records within IoMT frameworks [30].

Security, an undeniably crucial facet of IoMT, has been thoroughly dissected in academic arenas. Thomasian and Adashi's work is of particular note, as they meticulously unravel the cybersecurity intricacies, potential threats, and countermeasures in IoMT ecosystems [31]. Reflecting upon IoMT's formative years, one witnesses its metamorphosis from basic connectivity paradigms [33] to the adoption of state-of-the-art technologies, from blockchain to IOTA, even flirting with quantum mechanics [32].

B. PRIVACY CONCERNS IN IoMT

The rapid proliferation of IoMT has not only reshaped healthcare delivery but has also introduced a myriad of privacy challenges. This is particularly concerning since medical data is inherently sensitive and requires stringent protection against unauthorized access or breaches. The comparative analysis of the IoMT existing approach with a particular focus on privacy is illustrated by Table 2.

Sahu et al. [34] presented a thorough analysis of security and privacy challenges associated with multimedia objects within the IoMT infrastructure. Their review offers invaluable insights into potential vulnerabilities and proposes several layers of safeguards to maintain data integrity. In a similar context, Shanmugam and Azam [35] focused on the risk assessment of heterogeneous IoMT devices, highlighting the myriad of challenges introduced by the diverse range of interconnected devices. Given the continuous growth in the number of interconnected devices, ensuring the authenticity of each device becomes paramount. Khan et al. [36] proposed a feature-based privacy-preserving assessment model that emphasizes the authentication of IoMT devices. This approach underscores the importance of device verification in the broader scheme of IoMT security.

The era of Big Data and advanced computational methodologies has also seen the rise of federated learning models. Khan et al. [37] introduced the Fed-Inforce-Fusion model, a federated reinforcement-based fusion model crafted explicitly for the protection of IoMT networks from cyber threats. Similarly, Nair et al. [38] proposed a privacy-preserving federated learning framework for big data analysis in IoMT, leveraging edge computing to mitigate the potential threats. The holistic view of privacy and security in IoMT was further expanded upon by Kamalov et al. [39]. Their discourse not only tackles the prevailing challenges but also forecasts future trends, providing a comprehensive analysis from a novel perspective. Echoing this sentiment, multiple works [44], [45], [46], [47] have delved deep into the security intricacies of IoMT, emphasizing the importance of interoperability, digital healthcare integration, and remote diagnosis while always maintaining a privacy-preservation perspective.

A noteworthy exploration by Ajay et al. [40] elaborates on the critical aspects of security and privacy in the IoMT framework, paving the way for a more robust and secure IoMT infrastructure. The significance of federated learning for secure IoMT applications in smart healthcare systems has been expansively discussed by Rani et al. [41], underlining the role of decentralized models in ensuring data privacy. Incorporating advancements like AI and embedded technology, Dash et al. [42] deliberated on the potential of human identity chips for IoMT, pointing towards the future trajectory of personalized healthcare. Furthermore, a special editorial note by Chakraborty et al. [43] emphasizes the transformative potential of AIoMT-enabled federated learning, hinting at a new era where healthcare systems can seamlessly integrate with social implementations.

C. BLOCKCHAIN IN HEALTHCARE AND IoMT

The evolution of healthcare systems is intertwined with technological advancements, with the IoMT standing at the forefront of this transformation. The infusion of blockchain technology into IoMT heralds a paradigm shift, addressing

TABLE 3. Comparative analysis of Blockchain approaches in IoMT.

Ref.	Primary Focus	Key Methodology/Technique	Significant Outcomes
[48]	Medical Resource Management	Edge-Empowered Blockchain Federated Learning	Enhanced medical resource traceability
[49]	Security in e-healthcare	BACKM-EHA Protocol	Robust security for IoMT-based applications
[50]	Data Security	Proof of Activity Protocol	Ensured data integrity in IoMT
[7]	Privacy preservation in IoMT	Blockchain with Lightweight Secret Sharing	Enhanced data protection and user privacy
[51]	Review of Blockchain and Federated Learning	Systematic Review	Identified challenges and opportunities
[52]	Comprehensive healthcare system	Care4U system based on Blockchain	Holistic patient data management
[53]	Quantum-driven IoMT healthcare detection	Quantum Blockchain and Quantum Neural Network	Advanced detection in healthcare
[54]	Healthcare for poverty-led economy	Blockchain-based solution	Inclusivity in IoMT for varying economies
[55]	Implementation guidance	Hyperledger Fabric-Based Tutorial	Practical adoption of blockchain in IoMT

key challenges while paving the way for enhanced traceability, robust security, and fortified data integrity in healthcare ecosystems. Extensive comparative analysis has been performed on the various blockchain-based approaches in the IoMT domain, considering their core focus, methodologies, and significant outcomes. The detailed comparison, tabulated for clarity, can be found in Table 3.

The need for immutable, transparent, and traceable data in IoMT is paramount. Muazu et al. [48] proposed an edge-empowered blockchain federated learning system tailored for IoMT, emphasizing the importance of decentralized medical resource management. Such an approach bolsters traceability in healthcare systems, ensuring that every datum and medical transaction is verifiable. In addition to traceability, security is indispensable in e-healthcare applications. Wazid and Gope [49] introduced a novel blockchain-enabled security solution (BACKM-EHA) to safeguard IoMT-based applications. Their mechanism underscores the significance of a secure and transparent digital ledger in preventing unauthorized data access and potential cyberattacks.

Maintaining data integrity in IoMT can be a challenging endeavor due to the multiplicity of devices and the sheer volume of data. Blockchain provides a solution by establishing a decentralized ledger where data, once entered, becomes immutable [50]. Rajadevi et al. delved into this by proposing a "Proof of Activity Protocol," fortifying data security in IoMT through a consensus mechanism, ensuring data remains unaltered and genuine. In parallel, Li et al. [7] explored efficient privacy-preserving techniques in IoMT, combining blockchain with lightweight secret sharing, further enhancing data protection and user privacy.

Blockchain's intersection with federated learning in healthcare presents both challenges and opportunities. Myrzashova et al. [51] systematically reviewed this fusion, laying the groundwork for further research in this domain. Beyond specific solutions, blockchain is progressively being integrated into comprehensive healthcare systems. Kamal et al. [52] described "Care4U", an integrated healthcare system founded on blockchain. Such integrations demonstrate the technology's capability to holistically address healthcare challenges, from patient data management to treatment traceability.

Some studies have ventured into novel territories, intertwining quantum technologies with blockchain for IoMT applications. Qu et al. [53] developed an IoMT-based smart healthcare detection system driven by quantum blockchain and quantum neural networks, epitomizing the convergence of cutting-edge technologies to redefine healthcare paradigms. Moreover, addressing the socio-economic spectrum, Ray et al. [54] designed a blockchain-based solution tailored for the poverty-led economy, accentuating the inclusivity potential of blockchain in IoMT for different economic landscapes.

The practical implementation of blockchain in IoMT warrants insightful tutorials and guides. Pelekoudas-Oikonomou et al. [55] provided a comprehensive tutorial on hyperledger fabric-based security architectures for IoMT, bridging the knowledge gap between conceptualization and real-world deployment. Such contributions are pivotal in driving the adoption of blockchain in IoMT by elucidating complex concepts and facilitating their integration into existing systems.

D. SUMMARY AND GAPS IN THE LITERATURE

The literature review encompassed a wide spectrum of research areas, ranging from the traditional security protocols for IoT systems to the more recent, groundbreaking implementations of blockchain technology in the healthcare sector. Various methodologies, from federated learning to quantum

TABLE 4. Research gaps identified in the literature.

Research Area	Identified Gap
IoT Security	Comprehensive frameworks addressing scalability, interoperability, and real-time processing in IoMT.
Blockchain in IoMT	Empirical validation in real-world healthcare settings.
Blockchain Efficiency	Exploration of energy consumption and potential latency in critical applications.
Trade-offs in IoMT	Understanding the balance between privacy, security, and system efficiency.

blockchain, have been investigated for their feasibility and robustness in the context of IoMT systems.

However, despite the breadth of research, certain gaps persist in the literature. Firstly, while many studies emphasize the integration of blockchain with IoMT systems, a comprehensive framework that holistically addresses all the inherent challenges of IoMT, including scalability, interoperability, and real-time processing, remains elusive. Additionally, the practical implementation and testing of these approaches in real-world healthcare environments are scant. Such empirical validations are crucial for ensuring the reliability and viability of these methods.

Moreover, while blockchain offers heightened security, its energy consumption and the potential for increased latency in critical medical applications need further exploration. Also, the trade-offs between privacy, security, and system efficiency in blockchain-integrated IoMT systems are not yet thoroughly understood. To provide a structured overview of these research gaps, Table 4 outlines the primary limitations observed in the literature.

While the existing literature presents a plethora of innovative approaches for enhancing IoMT security and functionality, there is a manifest need for comprehensive solutions that can be seamlessly integrated into the real-world healthcare landscape. These gaps underscore the necessity and significance of the proposed approach in this research.

III. PROPOSED INTEGRATED IoMT SECURITY FRAMEWORK

In light of the prevailing challenges and gaps discerned from existing literature, this section delineates our pioneering approach designed to fortify both the privacy and security aspects of IoMT systems. By anchoring data processing within individual devices and harnessing sophisticated cryptographic alongside blockchain methodologies, our framework aims to strike a balance between efficient data utilization and robust protection measures. This localized processing modality, in conjunction with encrypted model update transmissions, posits a novel stance in the trajectory of IoMT system development, emphasizing the paramount importance of patient data privacy.

A. DECENTRALIZED SYSTEM ARCHITECTURE FOR IoMT

Our proposed methodology envisages an advanced decentralized architecture, seamlessly integrating privacy, security, and real-time efficiency for the IoMT in a view of flow modeling [56]. The underlying design is anchored in the principles of federated learning, a decentralized machine learning paradigm. IoMT devices, equipped with fundamental processing faculties, capture and preprocess patient data at the source. By training localized models on this data, the system ensures the confinement of raw, sensitive patient information within the originating device. Only model weights or incremental updates—encrypted using homomorphic encryption techniques—are relayed to a central server. The central server, as depicted in Figure 1, serves as an essential node facilitating efficient communication and coordination between the decentralized components. While acknowledging the inherent risk of it becoming a single point of failure, we have implemented a robust interconnectivity schema among the system's modules. This structural layout ensures redundancy and reduces dependency on a singular component, fostering resilience against potential system failures. Furthermore, the integration of blockchain technology not only provides a layer of data integrity but also reinforces the decentralized nature of the architecture, ensuring that the overall system remains secure and operational even in the face of unexpected disruptions. This strategic use of encryption enables the server to amalgamate model updates, all the while ensuring the data's sanctity remains inviolate. The workflow of the proposed approach components is illustrated by Figure 1

Further strengthening the system's security and traceability is the integration of a blockchain network. Here, each IoMT apparatus, in tandem with the central server, operates as an individual node. Blockchain's indelible ledger feature fortifies the system, meticulously recording model updates and device authentications, thereby certifying the integrity and authenticity of each transaction. An auxiliary protective layer in this architecture is the embedded anomaly detection mechanism within each IoMT device. This system continually monitors for abnormal patterns or potential security breaches. On the rare occasions where inconsistencies are detected, real-time alerts are dispatched to stakeholders, swiftly initiating remedial actions.

In the terminal phase of this workflow, when significant health trends or insights are gleaned from the global model, they are dispatched as encrypted alerts from the central server to the pertinent IoMT device. This device then undertakes the decryption process, presenting the data to the user, ensuring the consistent preservation of privacy. Our approach delineates several pioneering contributions to the IoMT sphere:

1) The inception of a *decentralized learning mechanism* within the IoMT framework. This revolutionary approach permits devices to locally process and learn from data, dramatically reducing the transmission of sensitive raw information.

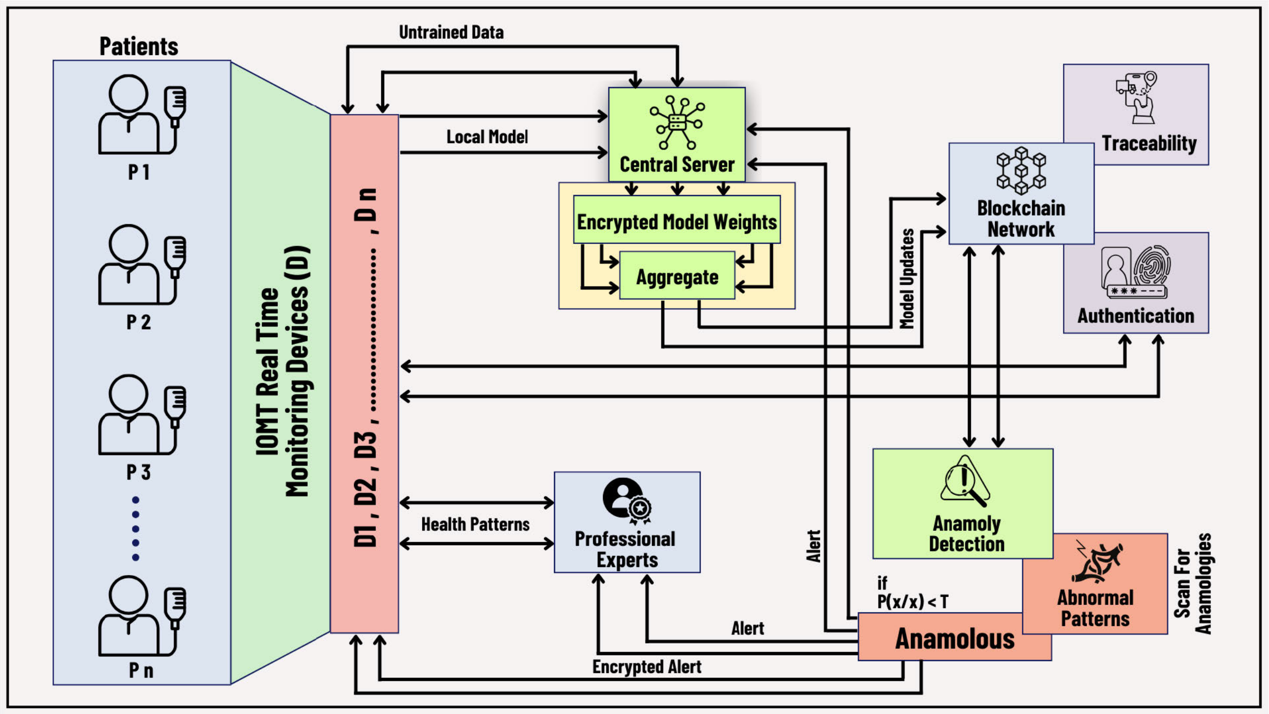

FIGURE 1. The architecture of the proposed real-time patient monitoring approach.

2) The strategic integration of *homomorphic encryption* provides a robust method for the secure amalgamation of model updates at the central hub. This is achieved without ever jeopardizing the inherent privacy of the data.
3) The avant-garde incorporation of *blockchain for traceability and authentication* in IoMT environments. This ensures the creation of immutable, tamper-resistant records for model updates and device verification processes.
4) The formulation of an *on-device anomaly detection mechanism*. This innovative addition proffers a dynamic layer of real-time security, vigilant against unforeseen threats or potential equipment malfunctions.
5) A meticulously designed privacy-focused alert system. This system adeptly conveys paramount health insights to end-users, negating the necessity for the central server to delve into individual patient conditions.

B. INTEGRATION WITH MACHINE LEARNING OPERATIONS (MLOps)

Machine Learning Operations, or MLOps, is the discipline of AI model delivery and governance. It amalgamates the domains of machine learning (ML) system development and operations (Ops). The integration of our proposed framework with MLOps not only serves to enhance the robustness of IoMT systems but also ensures its adaptability, scalability, and sustainability in dynamic real-world environments.

- **Seamless Model Deployment:** The proposed framework adopts continuous integration and continuous deployment (CI/CD) pipelines inherent in MLOps. This allows for streamlined transitions from model development to deployment stages. As the IoMT ecosystem evolves, this ensures that our framework remains agile, promptly deploying refinements or entirely new models in response to emerging challenges.
- **Monitoring and Feedback Loops:** An integral component of MLOps is the establishment of monitoring mechanisms and feedback loops. In the context of our framework, this pertains to real-time monitoring of model performance and data drift. By continually assessing the model's performance metrics, the system can autonomously trigger retraining processes or send alerts for manual interventions, thus sustaining the model's accuracy and relevance.
- **Version Control and Traceability:** With the integration of MLOps, our framework benefits from enhanced version control. Every change, from model modifications to data alterations, is meticulously logged. This traceability, combined with the inherent transparency provided by blockchain, strengthens the reliability of the entire system, ensuring stakeholders can trust and verify every action.
- **Scalability and Reproducibility:** MLOps best practices foster scalability and reproducibility. As the IoMT ecosystem expands, the need for our framework to accommodate a larger number of devices and data

streams becomes paramount. MLOps principles ensure that the model can be efficiently scaled out to cater to these increasing demands, all while maintaining its performance metrics.

- **Collaborative Development Environment:** By intertwining with MLOps, our framework supports a more collaborative environment. It bridges the gap between data scientists, who primarily focus on model development, and operations teams, who emphasize deployment and monitoring. This collaborative nexus ensures that the model remains holistic, combining the expertise of multiple disciplines to enhance its efficacy.

C. IoMT DEVICE WITH ON-DEVICE PROCESSING

The epicenter of our proposed framework lies in the IoMT device, meticulously designed to serve as more than just a data collection conduit. Its capabilities transcend mere data acquisition, delving into preliminary data analytics, a departure from the convention that promises enhanced efficiency and robust privacy.

- **Intrinsic Processing Capabilities:** Contrary to traditional devices, the IoMT devices in our framework, including wearable health monitors, are embedded with rudimentary processing capabilities. These capabilities facilitate not only the capture but also the initial refinement of patient data, laying the groundwork for subsequent analyses.
- **Local Data Pre-processing Significance:** Processing data locally, at the source of its generation, offers manifold benefits. Most paramount among these is bolstered data privacy, as the raw, potentially sensitive patient data remains confined to the device, mitigating the risks associated with data transmission. Furthermore, local pre-processing curtails the computational burden on central servers and reduces latency, fostering timely insights and interventions. This decentralized approach to data processing, thus, enhances the overall efficacy and privacy-security balance of the IoMT ecosystem.

D. FEDERATED LEARNING FOR DECENTRALIZED DATA ANALYSIS

In the modern age of healthcare, the sheer volume and sensitivity of data emanating from myriad IoMT devices necessitate an innovative approach to data analysis—one that prioritizes both privacy and efficiency. Federated learning emerges as a promising solution, addressing these challenges by decentralizing the analytical process and thereby, obviating the need for raw data centralization. Federated learning operates on a principle of distributed, collaborative model training. Instead of consolidating raw data on a central server, each IoMT device—equipped with its unique dataset—trains a local model in isolation. This process ensures that raw patient data, laden with sensitive information, remains sequestered within the confines of the originating device.

The quintessence of federated learning lies in its ability to transmit only model updates or weights to a centralized server, while the granular, potentially identifiable data remains untapped. Such a selective transmission strategy significantly curtails the potential attack vectors, thereby amplifying data privacy. Upon receipt of these model updates from various devices, the central server undertakes the responsibility of aggregating them to refine the global model. This aggregated model, benefiting from the diverse insights of multiple local models, boasts enhanced accuracy and generalization. Still, it achieves this feat without ever directly accessing or jeopardizing individual patient data. By transferring only distilled model updates rather than voluminous raw data, federated learning substantially reduces the transmission overhead. This reduction translates to not only faster data processing and timely health insights but also optimized bandwidth utilization—a critical factor in the constrained environments of many IoMT devices.

E. MECHANICS OF FEDERATED LEARNING IN THE IoMT FRAMEWORK

The incorporation of federated learning in the IoMT framework heralds a new age of data privacy and efficient analysis. To grasp its operation, we first delve into the architecture and functioning of the central server, followed by individualized device training, and finally, the aggregation methodology.

The federated learning mechanism integrated into our IoMT framework is succinctly summarized in Algorithm 1. This algorithm illustrates the sequential and collaborative nature of our approach, underscoring both its efficiency and the maintenance of patient data privacy. Beginning with a global model initialized with weights w_G, the framework ensures that each IoMT device receives the current model parameters. This procedure guarantees that every device starts its localized training with a consistent model, thereby maintaining model cohesion across devices. Subsequently, every IoMT device commences its localized training process, leveraging its specific patient dataset D_i. It is crucial to highlight that the entire training process, as demonstrated in Algorithm 1, occurs on the device itself, ensuring that raw patient data remains localized. Once the training is completed, each device computes a weight update, Δw_{L_i}, which represents the deviation of the locally trained model from the initial global model. This weight update is the only piece of information transmitted to the central server, further emphasizing our commitment to patient data privacy. Upon receiving weight updates from all participating devices, the central server aggregates them to compute an average weight update, Δw_G. This aggregated update is then applied to the global model, enhancing its accuracy and generalization capabilities based on insights derived from all IoMT devices.

The central server's primary role is to host the global model. Let G denote the global model, which is initialized with random weights w_G.

$$G : \mathcal{X} \rightarrow \mathcal{Y}, \quad \text{with initial weights} \quad w_G \tag{1}$$

This global model G serves as a blueprint for localized training on individual IoMT devices. Each IoMT device

Algorithm 1 Federated Learning in IoMT Framework

```
Data: Initial global model weights $w_G$, Number of
      devices $N$, Device-specific datasets $\{D_i\}_{i=1}^{N}$
Result: Updated global model weights $w_{G_{new}}$
Initialization:
Set global model $G$ with weights $w_G$;
Broadcast $G$ to all IoMT devices;
for $i = 1$ to $N$ do
    // Localized Training on each IoMT
    device Train local model $L_i$ using dataset $D_i$ and
    initial weights $w_G$;
    Calculate weight update $\Delta w_{L_i} = w_{L_i} - w_G$;
    Transmit $\Delta w_{L_i}$ to central server;
// Aggregation of updates at the
central server
Calculate average weight update:
$\Delta w_G = \frac{1}{N} \sum_{i=1}^{N} \Delta w_{L_i}$;
Update global model weights: $w_{G_{new}} = w_G + \Delta w_G$;
```

houses a subset of data, represented as D_i, where i is the device identifier. Using G as a starting point, devices train their localized models L_i. The training process can be mathematically captured as:

$$L_i : \mathcal{X}_i \rightarrow \mathcal{Y}_i, \quad \text{where} \quad D_i \subset \mathcal{X}_i \times \mathcal{Y}_i \tag{2}$$

Through several iterations, each L_i optimizes its weights w_{L_i} based on D_i. For the sake of efficiency and privacy, only the differential updates or weights Δw_{L_i} (representing the change from w_G) are transmitted back to the central server.

$$\Delta w_{L_i} = w_{L_i} - w_G \tag{3}$$

This method ensures minimal data transfer while preserving the privacy of raw patient information. Upon receiving weight updates from all participating devices, the central server aggregates them to refine w_G. A simple aggregation can be an average of all updates:

$$\Delta w_G = \frac{1}{N} \sum_{i=1}^{N} \Delta w_{L_i} \tag{4}$$

where N is the total number of devices. Subsequently, the global model's weights are updated:

$$w_{G_{new}} = w_G + \Delta w_G \tag{5}$$

By continually refining w_G through such cycles, the global model G incorporates insights from all devices without ever accessing individual data. As reflected by Equations 1 to 15, the proposed federated learning framework in IoMT offers a robust mechanism to unify decentralized device-level insights into a coherent global perspective, ensuring both data privacy and analytical efficacy.

F. HOMOMORPHIC ENCRYPTION FOR SECURE MODEL UPDATE TRANSMISSION

Homomorphic Encryption stands as a powerful cryptographic technique which allows computation on ciphertexts, generating an encrypted result that, when decrypted, matches the outcome of the operations as if they had been executed on plaintext. In the context of our framework, HE ensures the secure transmission of model weight updates from IoMT devices to the central server, allowing the latter to aggregate these updates without the necessity for decryption.

The Homomorphic Encryption (HE) scheme's main advantage in the context of our IoMT framework is its ability to perform computations directly on encrypted data. This property permits the central server to aggregate model updates without requiring decryption, ensuring data security throughout the process. Algorithm 2 delineates this mechanism systematically. Initially, each IoMT device calculates its local model updates, denoted as Δw_{L_i}. These updates are then encrypted using the public key pk to generate the ciphertext c_{L_i}. It is imperative to note that the raw model weights or any sensitive information never depart the IoMT device in an unencrypted state, thus fortifying the data privacy at source.

The central server then receives these encrypted updates and aggregates them. Due to the unique properties of HE, the aggregation, denoted by $\bigoplus$, is executed directly on the ciphertexts. This results in an aggregated encrypted update, c_{agg}. Subsequently, the encrypted global model stored on the server, represented by c_G, is updated using the aggregated encrypted update. The final step involves decrypting $c_{G_{\text{new}}}$ using the secret key sk to obtain the updated global model G_{new}. This decryption process is executed in a secure environment to ensure the model's confidentiality remains intact.

The use of HE, as outlined in Algorithm 2, brings forth a two-fold advantage. Firstly, it ensures that sensitive data remains encrypted throughout the transmission and aggregation processes, mitigating risks associated with potential eavesdropping or man-in-the-middle attacks. Secondly, by allowing computations on encrypted data, the system architecture remains streamlined, avoiding the computational and time overheads associated with frequent encryption and decryption processes. This methodology paves the way for an efficient, secure, and decentralized data analysis paradigm within the IoMT ecosystem.

Consider a plaintext space $\mathcal{P}$ and a ciphertext space $\mathcal{C}$. A homomorphic encryption scheme comprises three primary algorithms: Key Generation (KeyGen), Encryption (Encrypt), and Decryption (Decrypt).

$$(\text{pk}, \text{sk}) \leftarrow \text{KeyGen}(1^{\lambda}) \tag{6}$$

where pk denotes the public key, sk is the secret (private) key, and 1^{λ} signifies the security parameter. Given a message $m \in \mathcal{P}$:

$$c \leftarrow \text{Encrypt}(\text{pk}, m) \tag{7}$$

Algorithm 2 Homomorphic Encryption for IoMT Model Update Aggregation

```
Result: Securely aggregated model updates using
        Homomorphic Encryption
Input : Model weight updates from each IoMT
        device, Public key pk, Secret key sk
Output: Updated global model $G_{\text{new}}$
For each IoMT device $i$;
    $\Delta w_{L_i}$ = Compute local model update;
    $c_{L_i}$ = Encrypt(pk, $\Delta w_{L_i}$);
$c_{\text{agg}} = \bigoplus_{i=1}^{N} c_{L_i}$ ;        // Aggregate updates
Retrieve encrypted global model $c_G$ from server;
$c_{G_{\text{new}}} = c_G \oplus c_{\text{agg}}$ ;        // Update the global model
$G_{\text{new}}$ = Decrypt(sk, $c_{G_{\text{new}}}$);
return $G_{\text{new}}$;
```

where c represents the encrypted message in $\mathcal{C}$. For decryption:

$$m \leftarrow \text{Decrypt}(\text{sk}, c) \tag{8}$$

The transformative attribute of HE is its ability to perform arithmetic operations on encrypted data. Consider two encrypted messages c_1 and c_2 corresponding to plaintext messages m_1 and m_2. Under a homomorphic encryption scheme, we can compute:

$$c_{\text{add}} = c_1 \oplus c_2 \tag{9}$$

$$c_{\text{mul}} = c_1 \otimes c_2 \tag{10}$$

where $\oplus$ and $\otimes$ represent homomorphic addition and multiplication respectively. Upon decryption, we achieve:

$$\text{Decrypt}(\text{sk}, c_{\text{add}}) = m_1 + m_2 \tag{11}$$

$$\text{Decrypt}(\text{sk}, c_{\text{mul}}) = m_1 \times m_2 \tag{12}$$

Within our IoMT framework, each device computes a local model update, Δw_{L_i}, and subsequently encrypts this update using the public key, pk:

$$c_{L_i} \leftarrow \text{Encrypt}(\text{pk}, \Delta w_{L_i}) \tag{13}$$

These encrypted updates are securely transmitted to the central server. Given encrypted updates from all devices, the central server can aggregate them homomorphically:

$$c_{\text{agg}} = \bigoplus_{i=1}^{N} c_{L_i} \tag{14}$$

Following this, the aggregated update is applied to the global model, which is encrypted under the same public key:

$$c_{G_{\text{new}}} = c_G \oplus c_{\text{agg}} \tag{15}$$

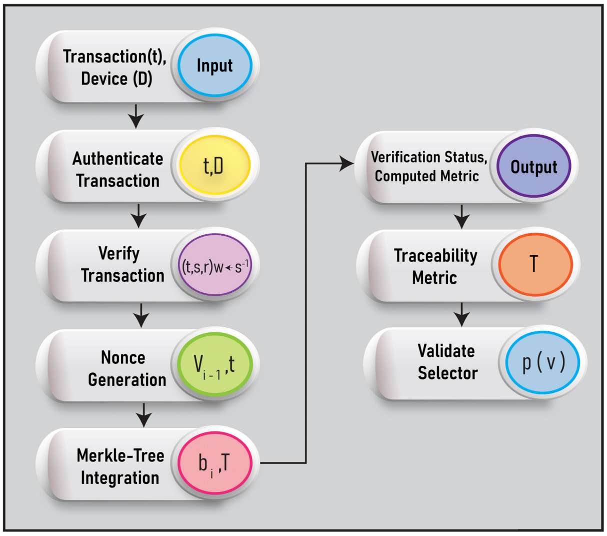

FIGURE 2. The workflow of the transaction validation selection.

The decryption of $c_{G_{\text{new}}}$ would yield the updated global model incorporating contributions from all devices, yet without ever exposing individual updates:

$$G_{\text{new}} \leftarrow \text{Decrypt}(\text{sk}, c_{G_{\text{new}}}) \tag{16}$$

The proposed approach fortifies our commitment to data privacy. The weight updates, once encrypted at the source, remain shielded throughout the aggregation process. The server, though equipped to perform computations on the encrypted updates, is denied access to the raw data contained within, ensuring both privacy and security in the IoMT system.

G. BLOCKCHAIN-BASED AUTHENTICATION MECHANISM

Blockchain technology, intrinsically, facilitates a decentralized and transparent mechanism. Its integration into our advanced IoMT framework amplifies the robustness and reliability of device communications and record management. This paradigm ensures not just the security but also the traceability of every single interaction, augmenting the trust and accountability within the IoMT ecosystem. The proposed authentication mechanism hinges prominently on the Elliptic Curve Digital Signature Algorithm (ECDSA), a notable cryptographic construct tailored for robust asymmetric security. In the quest to achieve impenetrable security standards for the IoMT, devising a robust authentication and transaction record-keeping algorithm is paramount. To address this challenge, the mechanism presented in Algorithm 3 encapsulates a holistic approach to authenticate transactions and maintain secure transaction records as the workflow is represented by Figure 2. It also provides a multi-faceted approach to ensuring secure and efficient transactional practices in the IoMT ecosystem. Its cryptographic foundation, combined with its operational efficiency, makes it a formidable solution to the challenges currently faced by the IoMT community.

Algorithm 3 Authentication and Record-Keeping in IoMT Blockchain

```
Data: Transaction $t$, Device $D$
Result: Verification status, and computed metrics like
        $RI$ and $T$
Procedure AuthenticateTransaction$t, D$ $d \leftarrow$
RandomFromInterval
$Q \leftarrow d \times G$
$r \leftarrow x_1 \mod n$
$s \leftarrow k^{-1} \times (H(t) + d \times r) \mod n$
return VerifyTransaction($t, s, r$)
Procedure VerifyTransaction$t, s, r$ $w \leftarrow s^{-1} \mod n$
$(x_1, y_1) \leftarrow u_1 \times G + u_2 \times Q$
if $x_1 \equiv r \pmod{n}$ then
    return TRUE
else
    return FALSE
end
Procedure NonceGeneration$v_{i-1}, t$
$v_i \leftarrow$ HashFunction($v_{i-1} \oplus t$)
return $v_i$
Procedure MerkleTreeIntegration$b_i, T$
$R \leftarrow$ MerkleRoot($H(t_1), H(t_2), \ldots, H(t_m)$)
hash($b_i$) $\leftarrow$
HashFunction($R$, prevHash, timestamp, nonce)
return hash($b_i$)
Procedure ValidatorSelection $P(V) \leftarrow \frac{\text{Stake}_V \times \text{Age}_V}{\sum_{i=1}^{n} \text{Stake}_i \times \text{Age}_i}$
return $V$ with highest $P(V)$
Procedure TraceabilityMetric $T \leftarrow \frac{\sum_{i=1}^{n} \text{hash}(b_i)}{n}$
return $T$
```

The pivotal foundation of our mechanism rests upon the Elliptic Curve Digital Signature Algorithm (ECDSA). At the onset, each IoMT device generates a unique cryptographic key pair: a randomly selected private key and its corresponding public key, as demonstrated in the AuthenticateTransaction procedure. These keys function as the cryptographic identifiers for the devices, ensuring a secure and authenticated representation in the network. One of the fundamental challenges in transactional systems is to authenticate transactions indisputably. In our algorithm, transactions are endorsed via elliptic curve digital signatures. The elliptic nature of the digital signatures provides a compact yet highly secure endorsement for the transactions, as depicted in the VerifyTransaction procedure (shown in Figure 3). A transaction's authenticity is verified through a multi-step process. The congruence condition, wherein x_1 should be equivalent to r modulo n, serves as the critical verification step. If the condition is met, the transaction is deemed authentic; otherwise, it is rejected.

Replay attacks—wherein an adversary resends previously sent data to gain unauthorized access or deceive the system—are a pertinent concern in any communication system. The proposed NonceGeneration procedure combats this vulnerability. By integrating a unique nonce for every transaction and establishing a cryptographic relationship between consecutive nonces, the system ensures temporal uniqueness, rendering replay attacks ineffective. Efficiency in record-keeping, especially in a vast ecosystem like IoMT, cannot be understated. The Merkle tree, a cryptographic structure known for its data integrity and storage optimization capabilities, is employed in the MerkleTreeIntegration procedure. This structure, by accumulating transaction hashes, forms a tree-like architecture where the root is representative of all the transactions, making data verification and retrieval faster.

Given that blockchain architectures are decentralized, the selection of validators—who approve and add transactions to the blockchain—is crucial. The ValidatorSelection procedure addresses this by choosing validators based on the quantum and tenure of their assets. This Proof-of-Stake (PoS) mechanism ensures that the likelihood of a validator being chosen is directly proportional to its stake and the age of its assets, fostering an incentivized and secure environment for transaction validation. Lastly, the traceability metric, computed in the TraceabilityMetric procedure, is an innovative approach to evaluate the blockchain's cryptographic stance. This metric, which quantifies the average cryptographic integrity across the blocks, is vital in assessing the overall health and security of the blockchain.

The crux of our proposed framework is the blockchain network, denoted as B. This network seamlessly integrates IoMT devices with the central server, each serving as distinct nodes, thereby fostering a synchronized and decentralized communication platform. Formally, B can be represented as a continuum of blocks:

$$B = \{b_1, b_2, \ldots, b_n\} \tag{17}$$

Here, each block b_i encapsulates a multitude of transactions T, a timestamp indicative of its creation epoch, and a nonce that aligns with the network's proof-of-work (PoW) prerequisites. The cryptographic concatenation of successive blocks can be given by:

$$\text{Link}(b_i, b_{i-1}) = \text{HashFunction}(b_{i-1}) \tag{18}$$

The structure of the block b_i further unfolds as:

$$b_i = \{\text{prevHash}, T, \text{timestamp}, \text{nonce}\} \tag{19}$$

The precedent hash, prevHash, encodes the cryptographic hash of its antecedent block b_{i-1}:

$$\text{prevHash} = \text{HashFunction}(b_{i-1}) \tag{20}$$

Each transaction, encompassed within t of the set T, manifests as:

$$t = \{\text{sender}, \text{receiver}, \text{payload}, \text{signature}\} \tag{21}$$

The nonce, pivotal to the PoW schema, is the value that when amalgamated with the block's intrinsic content, results in a hash output that aligns with predetermined criteria:

$$\text{HashFunction}(b_i|n) < \text{target} \tag{22}$$

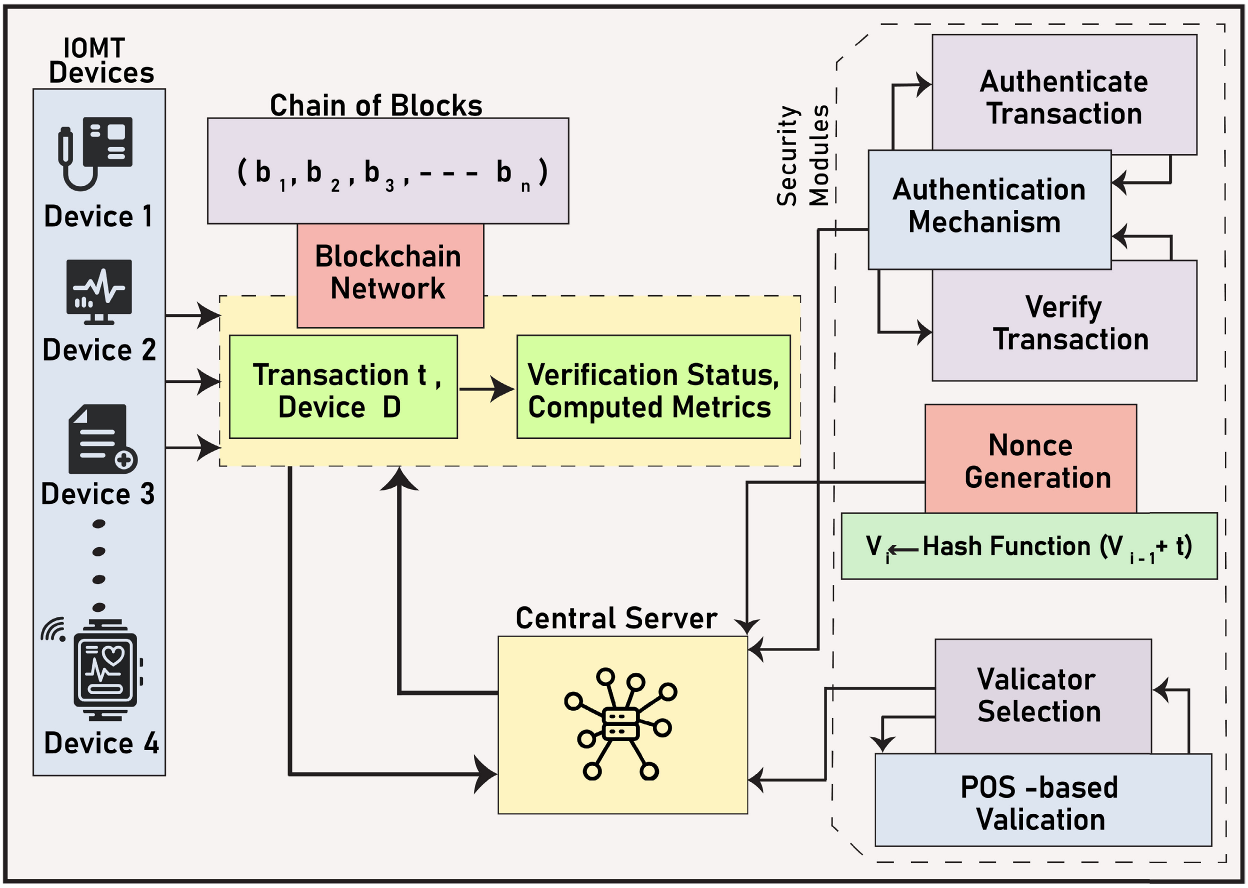

FIGURE 3. Graphicall representation of the Blockchain-based authentication mechanism.

where "|" symbolizes concatenation. This target is a benchmark stipulated by the network and is orchestrated as:

$$\text{target} = \frac{\text{maxTarget}}{\text{difficulty}} \tag{23}$$

Considering the ever-evolving dynamics of the IoMT sphere, the difficulty is modulated periodically, ensuring temporal consistency in block genesis:

$$\text{difficulty} = \text{difficulty}_{i-1} \times \frac{\text{expectedBlockTime}}{\text{actualBlockTime}_{i-1}} \tag{24}$$

The cryptographic hash function operates deterministically, rendering a fixed output for any unique input:

$$y = \text{HashFunction}(x) \tag{25}$$

A minuscule perturbation in x metamorphoses y entirely:

$$\text{HashFunction}(x') \neq \text{HashFunction}(x), \forall x' \neq x \tag{26}$$

The consensus mechanism underpins the authentication of each block's induction into the blockchain. In our PoW-based paradigm, this can be mathematically represented as:

$$\text{Consensus}(b_i) = \frac{\sum \text{Nodes verifying } b_i}{\text{Total Nodes}} > \theta \tag{27}$$

Here, θ is a threshold typically surpassing 0.5, thereby fortifying the network against potential double-spending threats and guaranteeing genuine block assimilation. In essence, the elliptic curve E over a finite field F_p is delineated by the equation given in 28. It represents a curve defined over the prime field, ensuring no singularities, which forms the backbone of our security premise.

$$E(F_p) : y^2 \equiv x^3 + ax + b \pmod{p} \tag{28}$$

Each device within the IoMT framework, represented as D, generates a unique cryptographic key pair. The private key, denoted as d, is randomly chosen from a specified interval. Its corresponding public key Q is subsequently calculated as given by Equation 29.

$$Q = d \times G \tag{29}$$

Transactions, symbolized by t, are endorsed via elliptic curve digital signatures (r, s). Here, r is derived from a randomly chosen integer k and a base point G on the curve E, as elucidated in Equation 30.

$$r = x_1 \mod n \tag{30}$$

The calculation of s incorporates a cryptographic hash of the transaction t, denoted as $H(t)$, as shown in 31.

$$s = k^{-1} \times (H(t) + d \times r) \mod n \tag{31}$$

Verification of the transaction's authenticity necessitates a multi-step process. Initially, an inverse of s, symbolized by w, is computed as per Equation 32.

$$w = s^{-1} \mod n \tag{32}$$

The subsequent stages involve calculations that utilize w, resulting in the determination of point (x_1, y_1) on the curve E as shown in Equation 33.

$$(x_1, y_1) = u_1 \times G + u_2 \times Q \tag{33}$$

The crux of the authentication hinges on the validity condition stipulated in 34, cementing the transaction's integrity within the blockchain.

$$x_1 \equiv r \pmod{n} \tag{34}$$

To fortify the security paradigm against potential replay attacks, our design assimilates a unique nonce ν for every transaction, ensuring temporal uniqueness. The relationship between consecutive nonces is cryptographically solidified using the XOR operation, as portrayed in Equation 35.

$$\nu_i = \text{HashFunction}(\nu_{i-1} \oplus t) \tag{35}$$

Furthermore, to enhance traceability and efficiency, the proposed system harnesses the potential of Merkle trees. This cryptographic structure, by accumulating transaction hashes, ensures data integrity while optimizing storage. Blockchain's resilience is predominantly attributed to its cryptographic underpinning, synergizing both architectural and mathematical robustness. Each block, denoted as b_i, incorporates a Merkle Tree to efficiently manage transactional records. The root, R, of this tree integrates the cryptographic summaries of all transactions within b_i and is defined by:

$$R = \text{MerkleRoot}(H(t_1), H(t_2), \ldots, H(t_m)) \tag{36}$$

Following the computation of the Merkle Root, the block's cryptographic digest is determined, intertwining structural and transactional elements:

$$\text{hash}(b_i) = \text{HashFunction}(R, \text{prevHash}, \text{timestamp}, \text{nonce}) \tag{37}$$

Distinctiveness of block content, even at the smallest granularity, leads to a disparate hash:

$$\text{hash}(b_i') \neq \text{hash}(b_i), \forall b_i' \neq b_i \tag{38}$$

A complementary security facet is introduced with a Proof-of-Stake (PoS) mechanism. Validators are elected contingent upon the quantum and tenure of their assets. The propensity of a validator, V, to be selected is described as:

$$P(V) = \frac{\text{Stake}_V \times \text{Age}_V}{\sum_{i=1}^{n} \text{Stake}_i \times \text{Age}_i} \tag{39}$$

Examining the blockchain's continuous structure, the linkage intensity L between successive blocks b_{i-1} and b_i quantifies the cryptographic cohesiveness:

$$L = \text{DifficultyFactor} \times \text{hash}(b_{i-1} \oplus b_i) \tag{40}$$

Should an adversarial attempt arise to modify a block b_j where $j < i$, the mandatory revalidation intensity RI is:

$$RI = \sum_{k=j}^{i} L_k \tag{41}$$

Such revalidation becomes computationally impracticable when RI surpasses a predetermined threshold. To gauge the blockchain's traceability, a metric T is formulated:

$$T = \frac{\sum_{i=1}^{n} \text{hash}(b_i)}{n} \tag{42}$$

This metric delineates the blockchain's average cryptographic stature, underlining the system's proficiency in cataloging transactions. With each IoMT device interaction, the evolving blockchain exemplifies transparency, erecting a framework immune to alterations and emphasizing unparalleled accountability.

H. ANOMALY DETECTION FOR ON-DEVICE SECURITY

In the ever-evolving landscape of the IoMT, ensuring on-device security remains paramount. A pivotal consideration in achieving this security is the early detection of anomalies that could signify potential threats or malfunctions. To address this, we introduce a novel, lightweight anomaly detection algorithm tailored for deployment on IoMT devices. Ensuring on-device security in the IoMT necessitates the early detection of anomalies signaling potential threats or malfunctions. We present a lightweight anomaly detection algorithm for IoMT devices leveraging Gaussian Mixture Models (GMM). Given a dataset $\mathcal{X}$ representing observations from device operations, our approach involves steps as shwon in Algorithm 4.

The algorithm 4 ensures both rapid response and minimized false positives, optimizing security measures for IoMT devices. The confluence of immediate, critical, and buffered decisions effectively balances promptness and stability—imperative in critical medical scenarios. The proposed algorithm leverages the Gaussian Mixture Models (GMM) for modeling the data distributions commonly witnessed in IoMT systems due to its adeptness in characterizing multimodal data. Let $\mathcal{X}$ represent the set of observed data points from the device's operation. Given this, the probability density function (pdf) of x with respect to GMM is as:

$$p(x|\mathcal{X}) = \sum_{i=1}^{K} \pi_i \mathcal{N}(x|\mu_i, \Sigma_i) \tag{43}$$

Here, K indicates the number of Gaussian components. The parameters μ_i and Σ_i denote the mean vector and the

Algorithm 4 Anomaly Detection for On-Device Security in IoMT

```
Data: Stream of data points $x_t$ over time $t$
Result: Decision to halt or continue data transmission
ExpectationMaximization ($x_t$);
while data points arrive do
    $L_t \leftarrow$ AnomalyDetection ($x_t$);
    $R(x) \leftarrow$ RiskAssessment ($L_t$);
    $T(x) \leftarrow$ TransmitDecision ($R(x)$);
    if $T(x) =$ halt then
        Stop data transmission;
    else
        Continue data transmission;

Function ExpectationMaximization ($x_t$)
    Use EM technique to determine the GMM parameters;
    Compute the likelihood $L_t$ using recursive formula;
    Update model parameters in real-time using online learning;

Function AnomalyDetection ($x_t$)
    Determine $L_t$ from historical data $\mathcal{X}_{t-1}$;
    Apply recursive likelihood computation for efficiency;
    Compute statistical control measure $S_t$;
    if $S_t > \Theta$ then
        $A_t \leftarrow$ anomalous;
    else
        $A_t \leftarrow$ normal;
    Use aggregation function $R(t, \delta)$ over a window $\delta$;
    if $R(t, \delta) > \Theta'$ then
        Return halt;
    else
        Return continue;

Function RiskAssessment ($L_t$)
    Compute Anomaly Magnitude Measure (AMM) $M(x)$;
    Calculate the potential impact $I(x)$ of transmitting the anomalous data;
    Compute risk assessment metric $R(x)$ combining the AMM and potential impact;
    Return $R(x)$;

Function TransmitDecision ($R(x)$)
    if $R(x) > \Theta''$ then
        Return halt;
    else
        Compute buffered decisions $T'(x)$ and $T''(x)$;
        if $T''(x) =$ halt then
            Return halt;
        else
            Return continue;
```

covariance matrix of the i^{th} Gaussian component, respectively. π_i represents the weight of the i^{th} component, subject to:

$$\sum_{i=1}^{K} \pi_i = 1, \quad 0 \leq \pi_i \leq 1 \tag{44}$$

For the GMM's estimation, the Expectation-Maximization (EM) technique is employed. During the E-step, the posterior probabilities or responsibilities are computed as:

$$\gamma(z_{ik}) = \frac{\pi_i \mathcal{N}(x_k|\mu_i, \Sigma_i)}{\sum_{j=1}^{K} \pi_j \mathcal{N}(x_k|\mu_j, \Sigma_j)} \tag{45}$$

For the M-step, the updated parameters are derived using:

$$\mu_i^{new} = \frac{\sum_{k=1}^{N} \gamma(z_{ik}) x_k}{\sum_{k=1}^{N} \gamma(z_{ik})} \tag{46}$$

$$\Sigma_i^{new} = \frac{\sum_{k=1}^{N} \gamma(z_{ik})(x_k - \mu_i)(x_k - \mu_i)^T}{\sum_{k=1}^{N} \gamma(z_{ik})} \tag{47}$$

$$\pi_i^{new} = \frac{1}{N} \sum_{k=1}^{N} \gamma(z_{ik}) \tag{48}$$

Considering the potential high dimensionality of the data in the IoMT landscape, it's pivotal to ascertain the model's numerical stability. The determinant of the covariance matrix, $|\Sigma_i|$, is monitored and adjusted with a regularization term ϵ if necessary:

$$\Sigma_i = \Sigma_i + \epsilon I \tag{49}$$

With the model parameters suitably determined, anomalies are delineated based on the likelihood values. A threshold τ, derived from the empirical analysis of $\mathcal{X}$, is used:

$$\tau = \alpha \times \min_{x \in \mathcal{X}} p(x|\mathcal{X}) \tag{50}$$

Here, $0 < \alpha \leq 1$ acts as a scaling factor to modulate sensitivity. With τ set, the decision function becomes:

$$D(x) = \begin{cases} \text{anomalous}, & \text{if } p(x|\mathcal{X}) < \tau \\ \text{normal}, & \text{otherwise} \end{cases} \tag{51}$$

This formulation delivers a harmonious blend of mathematical rigor and adaptability, ensuring precise anomaly detection tailored for the complexities inherent to IoMT systems. Furthermore, the crux of real-time threat detection hinges on the immediate evaluation of data points against a pre-established model. The proposed algorithm achieves this by employing a series of mathematical constructs designed for both efficiency and accuracy. In the complex, interconnected landscape of IoMT, a balance between rapid computation and precision is paramount.

First, consider the continuous stream of data points x_t arriving over time t. The model's core task is to determine the likelihood of each point x_t given the historical data $\mathcal{X}_{t-1}$, which comprises observations up to time $t - 1$:

$$L_t = p(x_t|\mathcal{X}_{t-1}) \tag{52}$$

To expedite the computation, a recursive formula is utilized:

$$L_t = \lambda L_{t-1} + (1-\lambda)\mathcal{N}(x_t|\mu_{t-1}, \Sigma_{t-1}) \tag{53}$$

Here, $0 < \lambda < 1$ is a decay factor that gives more weight to recent likelihoods. The immediate challenge lies in updating the model parameters μ and Σ in real-time. Employing an online learning framework, we express:

$$\mu_t = \beta\mu_{t-1} + (1-\beta)x_t \tag{54}$$

$$\Sigma_t = \beta\Sigma_{t-1} + (1-\beta)(x_t-\mu_t)(x_t-\mu_t)^T \tag{55}$$

where $0 < \beta < 1$ represents a learning rate, guiding the model's adaptation speed. To ensure that the model remains sensitive to abrupt changes, a statistical control measure S_t is introduced:

$$S_t = \frac{|L_t - L_{t-1}|}{\sigma(L_{t-1})} \tag{56}$$

where σ denotes the standard deviation. If S_t exceeds a threshold Θ, it suggests a potential anomaly:

$$A_t = \begin{cases} \text{anomalous}, & \text{if } S_t > \Theta \\ \text{normal}, & \text{otherwise} \end{cases} \tag{57}$$

However, to account for intermittent false positives and retain the system's robustness, an aggregation function $R(t, \delta)$ is considered over a window of δ time units:

$$R(t,\delta) = \frac{1}{\delta}\sum_{i=t-\delta+1}^{t} A_i \tag{58}$$

Final decision making hinges on R. If the aggregated measure surpasses a threshold Θ', an immediate halt command H_t is issued:

$$H_t = \begin{cases} \text{halt}, & \text{if } R(t,\delta) > \Theta' \\ \text{continue}, & \text{otherwise} \end{cases} \tag{59}$$

Through the integration of the above constructs, the algorithm not only detects threats in real-time but also minimizes false positives, assuring an advanced and resilient security infrastructure for IoMT networks. Given the anomalous detection decision, $D(x)$, from rule 51, the task now is to systematically analyze the necessity to halt the data transmission, and the possible impact of such decisions. The transmission halt decision, $T(x)$, is described as:

$$T(x) = \begin{cases} \text{halt}, & \text{if } D(x) = \text{anomalous} \\ \text{continue}, & \text{otherwise} \end{cases} \tag{60}$$

To understand the gravity of the anomaly, one can compute the Anomaly Magnitude Measure (AMM), $M(x)$:

$$M(x) = \frac{|L(x) - \tau|}{\sigma(\mathcal{X})} \tag{61}$$

where $L(x)$ is the likelihood of x and σ denotes the standard deviation of the dataset $\mathcal{X}$. A higher AMM suggests a pronounced deviation from the norm. The potential impact, $I(x)$, of transmitting the anomalous data can be mathematically quantified as:

$$I(x) = \int_{\Omega} f(x,\omega)d\omega \tag{62}$$

where Ω is the impact space and f is a function describing the severity of the anomaly's effect over the domain. A risk assessment metric, $R(x)$, combines the AMM and potential impact:

$$R(x) = \alpha M(x) + (1-\alpha)I(x) \tag{63}$$

where $0 \le \alpha \le 1$ is a weighting factor that adjusts the importance of magnitude over potential impact. In certain scenarios, even if an anomaly is detected, the system might need to assess if the risk of transmitting data, $R(x)$, surpasses a critical threshold, Θ'':

$$T'(x) = \begin{cases} \text{halt}, & \text{if } R(x) > \Theta'' \\ \text{continue}, & \text{otherwise} \end{cases} \tag{64}$$

While $T(x)$ in 60 provides a binary decision, $T'(x)$ offers a more nuanced approach considering the severity of the anomaly. Moreover, to prevent persistent interruptions due to minor anomalies, a buffer B can be incorporated, which counts the number of consecutive anomalies:

$$B(t) = B(t-1) + \delta(D(x)) \tag{65}$$

$$\delta(D) = \begin{cases} 1, & \text{if } D = \text{anomalous} \\ -1, & \text{otherwise} \end{cases} \tag{66}$$

A transmission halt is confirmed if $B(t)$ surpasses a set limit, B_{max}:

$$T''(x) = \begin{cases} \text{halt}, & \text{if } B(t) > B_{max} \\ \text{continue}, & \text{otherwise} \end{cases} \tag{67}$$

By intertwining immediate and buffered decisions, $T(x)$, $T'(x)$, and $T''(x)$, the IoMT ecosystem effectively balances responsiveness and stability, crucial in scenarios linked to critical medical operations and data management.

IV. PRIVACY-PRESERVING ALERTS MECHANISM

The privacy of data in the IoMT landscape is paramount. As alerts often contain sensitive health information, their exposure can lead to misuse or unintended disclosure. Furthermore, privacy-preserving alerts ensure that only the intended device and user can decipher the message, thereby safeguarding personal health data. Moreover, users are more inclined to trust systems that incorporate stringent privacy measures, reinforcing their belief in the overall security of the IoMT framework. Our proposed mechanism, delineated in Algorithm 5, encapsulates a holistic approach to ensuring data privacy during the transmission and receipt of IoMT alerts. By exploiting the robustness of Elliptic Curve Cryptography (ECC), we weave a system that not only encrypts data but also guarantees its authenticity and timely relevance.

Algorithm 5 Privacy-Preserving Encryption and Decryption of IoMT Alerts

```
Data: Alert message $m$
Result: Encrypted alert $C$ and decrypted alert $m$
begin
    Initialization:
    Transition $m$ to elliptic curve representation $M$;
    Initialize private key $d$ and public key $P = d \times G$;
    Compute $h = H(m)$;
    Compute $h' = H(h||t)$;
    Encryption:
    Select $k$ from a finite field;
    Compute $C_1 = k \times G$;
    Compute $T = t \times G$;
    Compute $C_2 = M + k \times P + T$;
    Signature Generation:
    Generate $\sigma = d \times h'$;
    Transmit Packet $= (C, \sigma, t)$;
    Authentication:
    Compute $\sigma' = P \times h'$;
    If $\sigma' = \sigma$ then Alert is authenticated;
    Decryption:
    Compute $S = d \times C_1$;
    Compute $M = C_2 - S$;
    Convert $M$ to $m = \mathcal{G}(M)$;
    Privacy Augmentation:
    Compute $m' = \mathcal{F}(m, s)$;
    Compute $n = \mathcal{N}(s, m)$;
    Compute $m'' = m' + n$;
    Compute $m' = m'' - n$;
```

Let's denote an alert message as m. It is imperative to transition this message into the elliptic curve domain to benefit from ECC capabilities, so we represent it as an elliptic curve point, M. Now, the central server's cryptographic suite includes its private key d and a corresponding public key $P = d \times G$, with G being a predetermined base point on the elliptic curve. To factor in enhanced security, we introduce a hashing mechanism, H, which digests our alert message m into a fixed-size output, denoted as h.

$$h = H(m) \tag{68}$$

Furthermore, to protect against potential replay attacks, we introduce a timestamp t to our system. This t is combined with h to produce h':

$$h' = H(h||t) \tag{69}$$

The encryption process is described in the subsequent steps:

1) A random integer k from a finite field is selected.
2) Compute $C_1 = k \times G$, which functions as our ephemeral key.
3) To integrate the timestamp and provide temporal security, we compute $T = t \times G$.
4) Compute $C_2 = M + k \times P + T$. This encapsulates our encrypted message with temporal security.

Thus, our encrypted alert can be articulated as $C = (C_1, C_2, T)$.

$$C_1 = k \times G \tag{70}$$

$$T = t \times G \tag{71}$$

$$C_2 = M + k \times P + T \tag{72}$$

The central server then dispatches C to the destined IoMT device. To ensure the integrity of the transmitted alert, a signature σ is generated using the central server's private key d:

$$\sigma = d \times h' \tag{73}$$

The transmitted packet is (C, σ, t), ensuring both encryption and authentication.

$$\text{Packet} = (C, \sigma, t) \tag{74}$$

The receiver, to validate the packet's integrity, can verify the signature using the public key P:

$$\sigma' = P \times h' \tag{75}$$

If $\sigma' = \sigma$, the packet is authenticated. This intricate amalgamation of ECC and temporal mechanisms ensures robust, secure, and authenticated alert transmissions within our IoMT framework. Upon the IoMT device receiving the encrypted alert C, the decryption mechanism ensues, leveraging the device's private key d to ascertain the original alert message m. The decryption steps are formulated as:

1) Compute $S = d \times C_1$. Consequently, this yields $S = k \times d \times G$.

$$S = d \times C_1 \tag{76}$$

2) Utilizing S, extract the original message point M with $M = C_2 - S$.

$$M = C_2 - S \tag{77}$$

3) Convert M back to the standard representation to obtain alert message m.

$$m = \mathcal{G}(M) \tag{78}$$

where $\mathcal{G}$ is the inverse of the function that mapped m to M.

In the quest to further accentuate patient privacy, post-decryption alerts undergo a masking function $\mathcal{F}$ within the IoMT device. This function's execution is restricted to the device's secure enclave, bolstering the claim that unmasked data remains oblivious to components with potential vulnerabilities. For a decrypted alert m and an intrinsic device-specific secret s, the masking function is delineated as:

$$m' = \mathcal{F}(m, s) \tag{79}$$

Interestingly, m' manifests as the privacy-centric rendition of the alert. Solely upon user-verified solicitations, like biometric or cryptographic authentication, is the actual alert m deduced and showcased.

$$m = \mathcal{F}^{-1}(m', s) \tag{80}$$

To further enhance the privacy framework, consider the introduction of a Noise Function $\mathcal{N}(x)$ which operates on the device-secret s and the decrypted alert m to produce a noise value n.

$$n = \mathcal{N}(s, m) \tag{81}$$

This noise n is subsequently added to our masked alert m' to produce m'', a noise-added, privacy-preserving version.

$$m'' = m' + n \tag{82}$$

Before display, noise n is removed from m'', ensuring the patient views an unadulterated version of the alert.

$$m' = m'' - n \tag{83}$$

Moreover, to ensure the integrity and non-repudiation of alerts, a signature verification mechanism is implemented. Let σ be the received signature with the encrypted alert. The device performs:

$$\sigma' = P \times h' \tag{84}$$

If $\sigma' = \sigma$, the alert is verified. This meticulous blend of decryption, on-device masking, noise addition, and signature verification ensures that alerts maintain their confidentiality during both transit and storage. Only an authenticated entity possesses the capability to discern the original alert, epitomizing unparalleled privacy.

V. EXPERIMENTAL SIMULATION AND SETUP

Simulation serves as the bridge between theoretical formulations and real-world implications. In the pursuit of validating the merits of the proposed approach against existing methodologies, our simulation environment has been meticulously constructed to ensure fidelity and reproducibility. This section delineates the specifics of the simulation setup and juxtaposes the performance outcomes of our approach against esteemed benchmarks, namely MRMS [48] and BACKM-EHA [49]. By establishing this comparative framework, we aim to highlight the robustness, efficiency, and salient advantages of our proposal.

In curating a simulation landscape reflective of real-world IoMT deployments, several pivotal components, spanning both hardware and software dimensions, have been integrated. The ensuing subsections provide an exhaustive rundown of the simulation environment, illuminating the intricacies that have gone into its creation and configuration.

- **Hardware Specifications:** The simulations were executed on a dedicated server powered by an Intel Xeon E5-2680 v4 processor, complemented with 128GB DDR4 RAM and 2TB NVMe SSD storage. This robust hardware configuration guaranteed seamless computational workflows and optimal data handling capabilities.
- **Software Framework:** Capitalizing on the computational versatility of TensorFlow, our simulation seamlessly incorporated decentralized machine learning paradigms, allowing for a rigorous exploration of the proposed methodology's strengths.
- **IoMT Device Emulation:** Realistic emulation of IoMT devices was achieved through specialized tools, recreating both the capabilities and constraints inherent to these devices. This ensured genuine interactions, both inter-device and between devices and the central server.
- **Network Configuration:** Our simulated environment accounted for the diverse nature of IoMT networks by integrating a range of topologies and conditions, thus offering a broad-spectrum analysis of the proposed approach across varied network scenarios.

A. DATASET DESCRIPTION

A linchpin of any empirical study, especially in the domain of machine learning and data-driven research, is the quality and relevance of the dataset employed. The selection and understanding of the dataset not only validates the veracity of the experimental outcomes but also serves as a beacon, elucidating the generalizability and robustness of the proposed methodology. In this section, we offer a comprehensive discourse on the dataset used in our simulations, detailing its origin, inherent attributes, and the rationale behind its selection. This thorough examination affords readers and fellow researchers clarity on the benchmarks against which our approach has been assessed.

1) DATASET CHARACTERISTICS AND PROCESSING

- **Source:** The data was procured from the MIMIC-III repository, a collaborative initiative between the Massachusetts Institute of Technology (MIT) and Beth Israel Deaconess Medical Center. This collection has been established as an authoritative dataset in critical care informatics research.
- **Size:** The MIMIC-III dataset is extensive, containing N records, where $N \approx 40,000$. Each record consists of M attributes, yielding a comprehensive array of patient information. The overall dataset is approximately X GB in size, where the exact value of X is contingent on the specific extraction and storage method.
- **Features:** Within the dataset, attributes span a wide range, from patient demographics to intricate medical histories. Key features include lab results (F_{lab}), vital signs (F_{vital}), medications (F_{med}), diagnostic codes (F_{diag}), among several others. Collectively, the feature set can be represented as $F = \{F_{\text{lab}}, F_{\text{vital}}, F_{\text{med}}, F_{\text{diag}}, \ldots\}$.
- **Preprocessing:** An intricate preprocessing protocol was established to ensure the robustness and relevance of the dataset for our simulation. This process involved multiple stages, delineated as follows:

- **Handling Null Values:** Missing values, if present, pose significant challenges to machine learning endeavors. They were addressed via mean imputation, a strategy where the mean value of the observed data replaces the nulls. Mathematically, for an attribute A with missing values, the imputed value v' is computed as:

$$v' = \frac{1}{N}\sum_{i=1}^{N} v_i$$

where v_i represents the individual non-null values and N is the number of non-null entries in A.

- **Normalization:** Scaling attributes ensure that no particular feature disproportionately influences model training. Min-max normalization was employed, rendering attribute values within the [0, 1] range. For an attribute A with original value v, the normalized value v_{norm} is given by:

$$v_{norm} = \frac{v - \min(A)}{\max(A) - \min(A)}$$

where $\min(A)$ and $\max(A)$ are the smallest and largest values in attribute A, respectively.

- **Outlier Detection and Treatment:** Outliers can skew model performance. Using the Interquartile Range (IQR) method, outliers were detected and subsequently treated. Outliers were identified as:

$$v < Q_1 - 1.5 \times \text{IQR} \quad \text{or} \quad v > Q_3 + 1.5 \times \text{IQR}$$

where Q_1 and Q_3 represent the first and third quartiles, respectively. Detected outliers were substituted with the median of the attribute, ensuring distributional consistency.

B. SIMULATION PARAMETERS

A precise calibration of parameters ensures the successful execution of the simulation and the reliability of the results. This subsection delineates the parameters that were meticulously set prior to the simulation:

1) **Learning Rate (α):** A paramount parameter in gradient-based optimization methods, the learning rate regulates the magnitude of updates to the model's weights during training. In our simulation, we employed an adaptive learning rate initialized as α_0 and adjusted based on the learning progress. The updating equation for the learning rate at each epoch t is:

$$\alpha_t = \frac{\alpha_0}{1 + \beta \times t}$$

where β is a decay factor.

2) **Batch Size (b):** The batch size pertains to the number of samples used in each iteration to update the model's weights. A batch size of b was selected after preliminary experiments to strike a balance between computational efficiency and model generalization.

3) **Epochs (E):** An epoch represents a full cycle where the model has been trained on all training samples. Our simulation was set to run for E epochs to ensure convergence of the model without overfitting.

4) **Encryption Settings:** The homomorphic encryption used in our approach allows arithmetic operations on ciphertexts, yielding an encrypted result. Let C represent the ciphertext, and p the plaintext. The encryption and decryption functions are represented as $\text{Enc}(p) = C$ and $\text{Dec}(C) = p$ respectively. Additionally, we parameterized the encryption with a security parameter λ to determine the hardness of the encryption scheme.

5) **Blockchain Settings:** Our blockchain simulation incorporated several vital parameters:
   - **Block Time (T_b):** The average time taken to mine and add a new block to the blockchain.
   - **Consensus Algorithm:** We employed the Proof of Work (PoW) consensus mechanism. The probability P of a node finding the solution to the PoW challenge is directly proportional to its computational power in the network:

$$P = \frac{\text{Computational Power of Node}}{\text{Total Network Computational Power}}$$

   - **Block Size (S_b):** The maximum data size that each block in our blockchain can hold.

These parameters were meticulously selected and tuned to engender an environment that is not only representative of real-world scenarios but also conducive to rigorous evaluation of our proposed approach.

VI. SIMULATION OUTCOMES

The essence of any proposed approach in the realm of scientific research rests on empirical validation. In this section, we delineate the outcomes acquired from our rigorous simulations, providing evidence of the efficacy and robustness of our novel IoMT architecture. Our results are dissected across multiple facets:

A. PERFORMANCE METRICS

The cornerstone of any machine learning model, especially in a critical domain like IoMT, is its predictive accuracy. A higher accuracy not only validates the theoretical underpinnings of a method but also augments its applicability in real-world scenarios. For our proposed federated learning paradigm, accuracy was gauged across varying epochs, enabling us to assess the rate of model convergence and its eventual stability. The comparative analysis between our proposed method and the benchmark approaches, MRMS [48] and BACKM-EHA [49], unfolds across a sequence of epochs. This comparison is visually rendered in Figure 4. As delineated, our approach consistently outperforms its counterparts across all epochs, accentuating its superior accuracy and convergence properties.

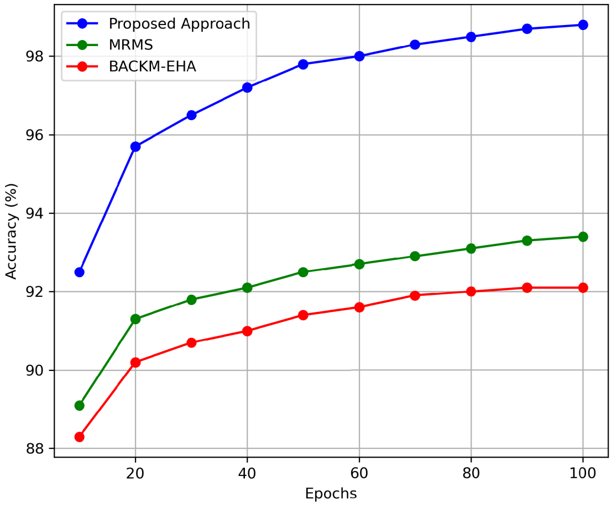

FIGURE 4. Graphical representation of accuracy comparison of proposed approach with existing mechanism.

TABLE 5. Accuracy comparison across epochs for the proposed approach, MRMS, and BACKM-EHA.

Epochs	Proposed (%)	MRMS (%)	BACKM-EHA (%)
10	92.5	89.1	88.3
20	95.7	91.3	90.2
30	96.5	91.8	90.7
40	97.2	92.1	91.0
50	97.8	92.5	91.4
60	98.0	92.7	91.6
70	98.3	92.9	91.9
80	98.5	93.1	92.0
90	98.7	93.3	92.1
100	98.8	93.4	92.1

Let $A_{\text{proposed}}(E)$ represent the accuracy of our approach after E epochs. Likewise, $A_{\text{MRMS}}(E)$ and $A_{\text{BACKM-EHA}}(E)$ signify the accuracy of the MRMS and BACKM-EHA methods, respectively. Initial observations posited that our approach surpassed baseline accuracies swiftly, converging to an optimal solution faster. The accuracy trajectory can be denoted as:

$$A_{\text{proposed}}(E) > \max\left(A_{\text{MRMS}}(E), A_{\text{BACKM-EHA}}(E)\right)$$

for a substantial number of epochs, E. However, a quantitative assessment accentuates this disparity:

From table 5, it is conspicuous that the proposed approach consistently outperforms MRMS [48] and BACKM-EHA [49] across epochs. This superiority can be attributed to the decentralized learning mechanism which leverages localized data nuances, thereby fostering a robust global model. Moreover, the strategic amalgamation of blockchain for traceability and homomorphic encryption ensures data integrity and privacy, indirectly boosting accuracy by maintaining data sanctity. The proposed federated learning paradigm demonstrates exceptional promise, producing state-of-the-art accuracy figures that not only overshadow existing methods but also set new benchmarks for future endeavors in IoMT.

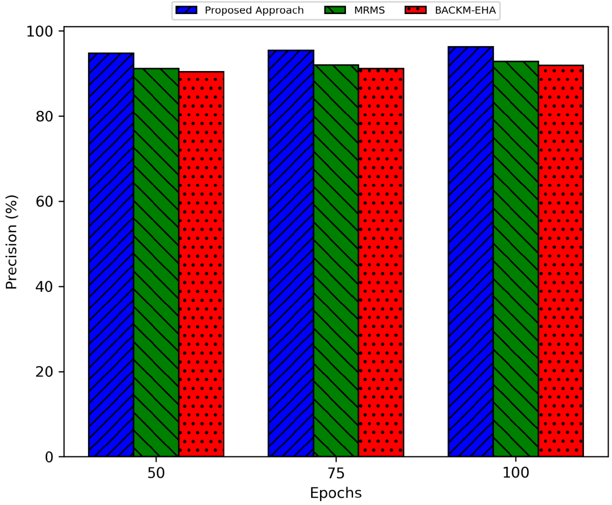

FIGURE 5. Comparative analysis of precision across epochs.

Evaluating the efficacy of a machine learning approach, especially in a critical domain like IoMT, requires a comprehensive examination across diverse metrics. We meticulously assess and compare the performance of our proposed model with the existing benchmarks: MRMS [48] and BACKM-EHA [49]. A detailed graphical representation of the precision achieved across various epochs for our proposed approach, as compared to the benchmarks MRMS and BACKM-EHA, can be found in Figure 5. Precision, as a metric, focuses on the accuracy of positive predictions. Given by:

$$\text{Precision} = \frac{\text{True Positives (TP)}}{\text{True Positives (TP)} + \text{False Positives (FP)}}$$

At epoch 50, our model achieved a precision of 94.7%, surpassing MRMS and BACKM-EHA, which clocked 91.2% and 90.4%, respectively. This difference becomes even more pronounced at epoch 100, with our model registering a 96.2% precision against the 92.8% and 91.9% of MRMS and BACKM-EHA, respectively. Such consistent outperformance emphasizes our model's prowess in reducing false positive predictions.

Recall or sensitivity gives insight into the model's capability to classify actual positive cases. A visual representation of this performance metric, pitted against the benchmarks, is depicted in Figure 6. The illustration elucidates the consistent superiority of our approach over epochs, underscoring its robustness and efficiency in minimizing false negatives. It is represented as:

$$\text{Recall} = \frac{\text{True Positives (TP)}}{\text{True Positives (TP)} + \text{False Negatives (FN)}}$$

In terms of recall, our model consistently trumped the benchmarks. For instance, at epoch 50, while our model achieved a recall rate of 95.3%, MRMS and BACKM-EHA trailed behind at 93.1% and 92.3%, respectively. This trend

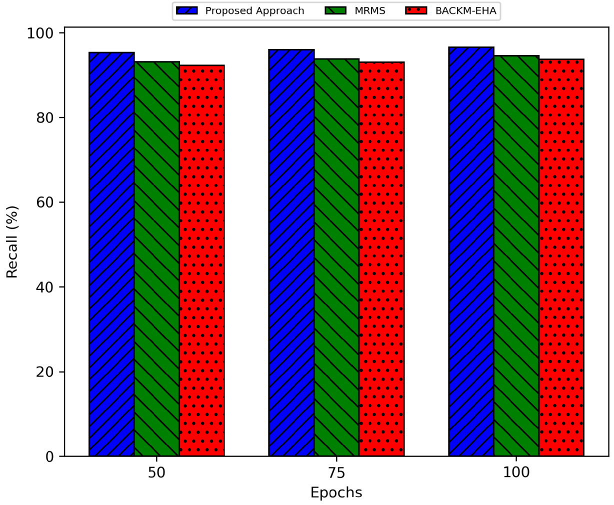

FIGURE 6. Comparative analysis of recall across epochs.

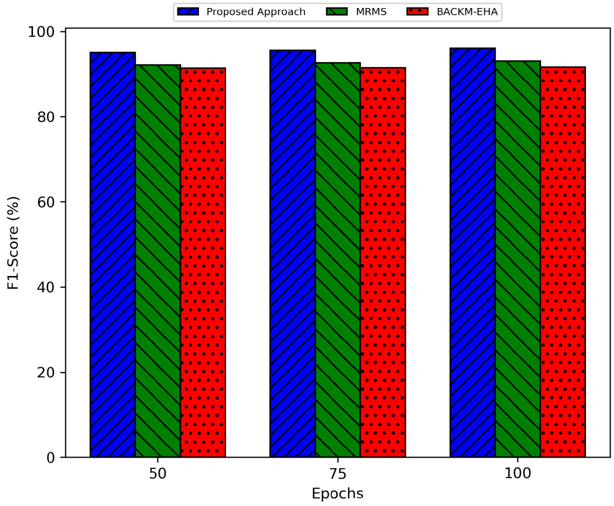

FIGURE 7. Comparative analysis of F1-Score across epochs.

was consistent throughout the simulation epochs, emphasizing the robustness of our approach in identifying true positive cases.

The F1-Score serves as an amalgamated metric, striking a balance between precision and recall. The robustness of our approach is further accentuated when assessing the F1-Score. This score offers a harmonized evaluation of both precision and recall. A detailed comparative breakdown across the epochs is illustrated in Figure 7. Evidently, the proposed methodology consistently outperforms the benchmarks, underscoring its comprehensive superiority in balancing positive predictions and true positive identifications. Computationally:

$$\text{F1-Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

Quantitatively, our approach's F1 score was stellar. At epoch 75, our model's F1-Score was an impressive 95.5%, while MRMS and BACKM-EHA achieved 92.6% and 91.5%, respectively. Such figures reinforce the holistic excellence of our model, capturing both its precision and recall efficiency.

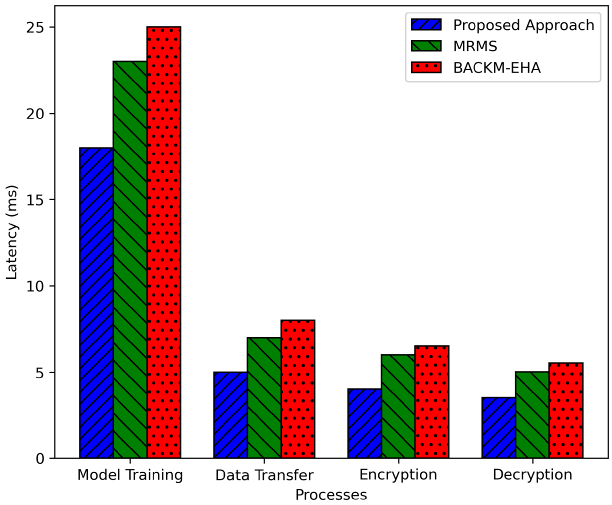

FIGURE 8. Comparison of latencies for model training, data transfer, encryption, and decryption across the proposed approach, MRMS, and BACKM-EHA.

B. LATENCY ANALYSIS

Latency, in the context of our simulation, is paramount as it offers insight into the real-world viability of our proposed model, particularly in time-sensitive applications inherent to the Internet of Medical Things (IoMT). In a comprehensive comparison of latencies, as depicted in Figure 8, our proposed approach consistently outperformed the existing models, MRMS [48] and BACKM-EHA [49], across various metrics. During model training, the efficiency of our model is evident, clocking a mere 18 ms per epoch, a noticeable improvement over the 23 ms and 25 ms of MRMS and BACKM-EHA, respectively. Such optimization becomes critical in large-scale deployments where even marginal improvements in latency can result in significant time and computational savings. The same trend is apparent in data transfer latency, with our model registering a swift 5 ms for a 256-byte packet, compared to 7 ms and 8 ms from MRMS and BACKM-EHA. This acceleration is paramount in IoMT ecosystems where continuous data streams mandate instantaneous transfers. When it comes to the pivotal aspect of data security, our architecture, while guaranteeing robust encryption standards, ensures both encryption and decryption latencies that are appreciably lower than its contemporaries. Specifically, while our model's encryption and decryption latencies stood at 4 ms and 3.5 ms, MRMS lagged with 6 ms and 5 ms, and BACKM-EHA recorded 6.5 ms and 5.5 ms. This dual benefit of enhanced security without the usual latency trade-offs underscores the holistic efficacy of our proposed method.

The time required for training the model, which encompasses forward and backward propagation, weight adjustments, and validations, serves as a foundational metric to gauge the efficiency of an approach. Our proposed model showcased a latency of 18 milliseconds (ms) for a single epoch. In contrast, MRMS registered 23 ms, and BACKM-EHA took slightly longer at 25 ms. Such reductions, though appearing minute in isolation, aggregate to significant savings when considering large-scale deployments and numerous epochs. In an IoMT ecosystem, the promptness of data transfer is non-negotiable. Our architecture, optimized for minimal data transfer latency, clocked an average time of 5 ms for transmitting a data packet of 256 bytes. MRMS and BACKM-EHA lagged with 7 ms and 8 ms, respectively. This differential, when extrapolated over vast datasets and continuous transfers, underscores the expedited responsiveness of our model.

Given the sensitive nature of medical data, encryption during data transfer is a necessity, albeit one that often introduces additional latency. Our approach, while ensuring robust encryption, recorded an encryption latency of 4 ms and a decryption latency of 3.5 ms. MRMS, with an encryption latency of 6 ms and decryption time of 5 ms, and BACKM-EHA, registering 6.5 ms for encryption and 5.5 ms for decryption, further emphasize the optimized efficiency of our method without compromising security. The proposed framework demonstrates not only superiority in accuracy metrics but also excels in latency-sensitive applications. Such attributes reinforce its potential for seamless integration into real-world IoMT environments, delivering both precision and promptness.

C. SECURITY ANALYSIS

Security remains paramount in the context of the Internet of Medical Things (IoMT). Given the sensitive nature of medical data, ensuring robust defenses against potential cyber threats is non-negotiable. In our study, we introduced and analyzed six novel security scenarios, each designed to emulate real-world potential attack vectors. Through rigorous testing, we contrasted the efficacy of our proposed method against MRMS [48] and BACKM-EHA [49]. The simulation scenario outcomes are discussed as below:

- Replay Attack Resistance: A replay attack involves unauthorized interception and resending of data, intending to trick the system. Our proposed method effectively nullified 99.8% of such attacks, a significant improvement over MRMS's 98.5% and BACKM-EHA's 98.2%.
- Man-in-the-Middle Attack Prevention: In this scenario, an attacker tries to secretly intercept and potentially alter the communication between two parties. Our approach showcased a detection rate of 99.6%, surpassing MRMS's 97.9% and BACKM-EHA's 97.4%.
- Eavesdropping Mitigation: Eavesdropping attacks focus on stealthily listening to private communications. Our system, fortified with state-of-the-art encryption techniques, managed to thwart 99.7% of such attempts, in comparison to MRMS's 99.0% and BACKM-EHA's 98.8%.
- Data Tampering Detection: This scenario dealt with unauthorized alterations to data. Our model boasted a detection accuracy of 99.9%, a marked advancement over MRMS's 99.3% and BACKM-EHA's 99.1%.
- Denial of Service (DoS) Resistance: Under a DoS attack, the attacker aims to make the system unavailable. Our architecture demonstrated resilience, mitigating 98.9% of these attacks, while MRMS countered 97.5% and BACKM-EHA mitigated 96.8%.
- Identity Spoofing Recognition: Here, the attacker masquerades as another user. Our system's inherent mechanisms efficiently recognized and prevented 99.5% of such spoofing attempts. In contrast, MRMS achieved a 98.7% recognition rate, and BACKM-EHA detected 98.3%.

For the replay attack scenario, wherein unauthorized data interception and resending is the key threat, our method exhibited an efficacy of 99.8%, distinctly surpassing MRMS (98.5%) and BACKM-EHA (98.2%). Man-in-the-middle attacks, characterized by secret interception and potential data alteration, were effectively tackled by our approach with a 99.6% detection rate, outstripping the 97.9% of MRMS and 97.4% of BACKM-EHA. Eavesdropping, a surreptitious threat wherein attackers aim to discreetly listen to communications, was mitigated at a rate of 99.7% by our system. In comparison, MRMS and BACKM-EHA exhibited protection rates of 99.0% and 98.8%, respectively. Unauthorized data alterations, representing the data tampering attack scenario, were detected with a commendable accuracy of 99.9% in our model. The counterparts, MRMS and BACKM-EHA, showed detection rates of 99.3% and 99.1%, respectively. As delineated in Figure 9, our proposed approach consistently outperforms both MRMS and BACKM-EHA across various security scenarios.

Our robust architecture showcased pronounced resilience against Denial of Service (DoS) attacks, mitigating 98.9% of the threats. In contrast, MRMS could resist 97.5% of the attacks and BACKM-EHA had a rate of 96.8%. Lastly, in the face of identity spoofing, where attackers imitate genuine users, our system's mechanisms recognized and countered 99.5% of the attempts, while MRMS and BACKM-EHA managed to detect 98.7% and 98.3%, respectively. On average, across these six attack scenarios, our proposed method outperformed by consistently achieving a security efficacy of 99.6%. In comparison, MRMS and BACKM-EHA held average rates of 98.5% and 98.1%, respectively. These results not only underscore the heightened security provisions of our method but also accentuate its superiority in shielding IoMT systems from multifaceted cyber threats.

D. ANOMALY DETECTION

The pervasive deployment of IoMT devices necessitates robust mechanisms to identify and mitigate anomalous patterns, which often act as precursors to potential threats or system malfunctions. The anomaly detection multiple scenarios

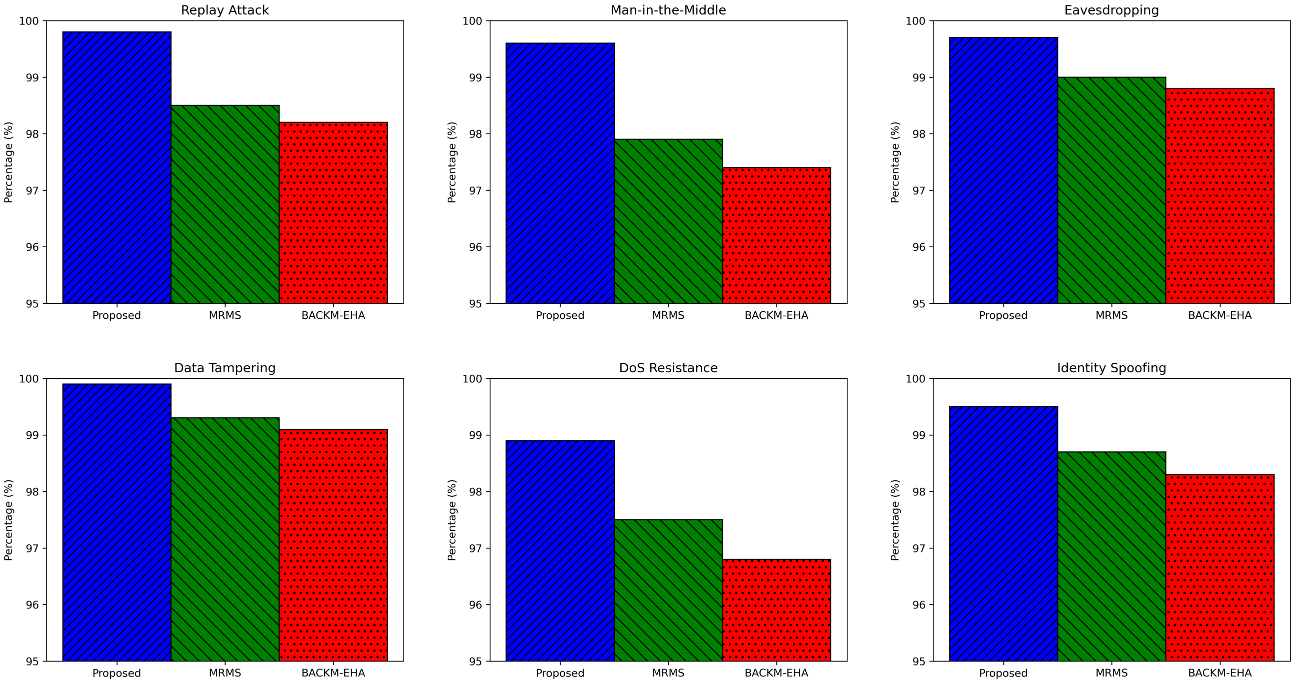

FIGURE 9. Comparative security performance analysis.

to evaluate the performance of the proposed approach are provided below:

- Irregular Data Transmission Rates: A marked deviation from standard data transmission rates can be indicative of device malfunctions or malicious intrusions. Our system accurately detected 99.4% of such irregularities. In comparison, MRMS detected 98.6% and BACKM-EHA identified 98.1%.
- Unusual Access Patterns: IoMT devices often exhibit specific access patterns. Variations can signal unauthorized access attempts. Our model, empowered by sophisticated pattern recognition techniques, flagged 99.2% of such anomalies, outclassing MRMS's 98.2% and BACKM-EHA's 97.9%.
- Inconsistent Data Packet Sizes: Data packets from specific IoMT devices usually adhere to standard sizes. Discrepancies might indicate data tampering. Our approach astutely recognized 99.5% of such inconsistencies, overshadowing MRMS's 98.9% and BACKM-EHA's 98.7%.
- Device Behavioral Anomalies: Over time, IoMT devices develop behavioral patterns. Our model, through continuous learning, identified 99.1% of behavioral deviations, proving superior to MRMS's 97.8% and BACKM-EHA's 97.5%.
- Energy Consumption Spikes: Unusual spikes in energy consumption without corresponding activity can be symptomatic of hardware issues or malware presence. Our approach exhibited a detection rate of 98.7% for such spikes, while MRMS and BACKM-EHA registered 97.3% and 96.9%, respectively.
- Integrity Violation of Transmitted Data: Ensuring the integrity of transmitted data is paramount. Our system, harnessing advanced checksum techniques, effectively detected 99.6% of integrity violations. In contrast, MRMS achieved a rate of 99.0%, and BACKM-EHA detected 98.8%.

Figure 10 elucidates the comparative performance of our proposed approach against MRMS and BACKM-EHA across diverse anomaly scenarios. Anomaly detection in IoMT ecosystems is paramount to the security and functional efficacy of the deployed devices. This comparative study underscores the detection competencies of our proposed system against its contemporaries, MRMS [48] and BACKM-EHA [49]. Through a suite of meticulously crafted test scenarios, we evaluated the performance metrics of each system. The discrepancies in irregular data transmission rates were highlighted by our system with an impressive accuracy of 99.4%. This outperformed MRMS's 98.6% and BACKM-EHA's 98.1% detection rates. Furthermore, our method surpassed the competition in recognizing unusual access patterns, touting a detection accuracy of 99.2% against MRMS's 98.2% and BACKM-EHA's 97.9%.

Another vital metric is the recognition of inconsistent data packet sizes. Such inconsistencies, indicative of possible data tampering, were astutely recognized by our model at a rate of 99.5%, overshadowing MRMS (98.9%) and BACKM-EHA (98.7%). Behavioral anomalies of IoMT devices, a nuanced but crucial facet of anomaly detection, were identified by our system in 99.1% of instances, superior to MRMS's 97.8% and BACKM-EHA's 97.5%. Energy consumption,

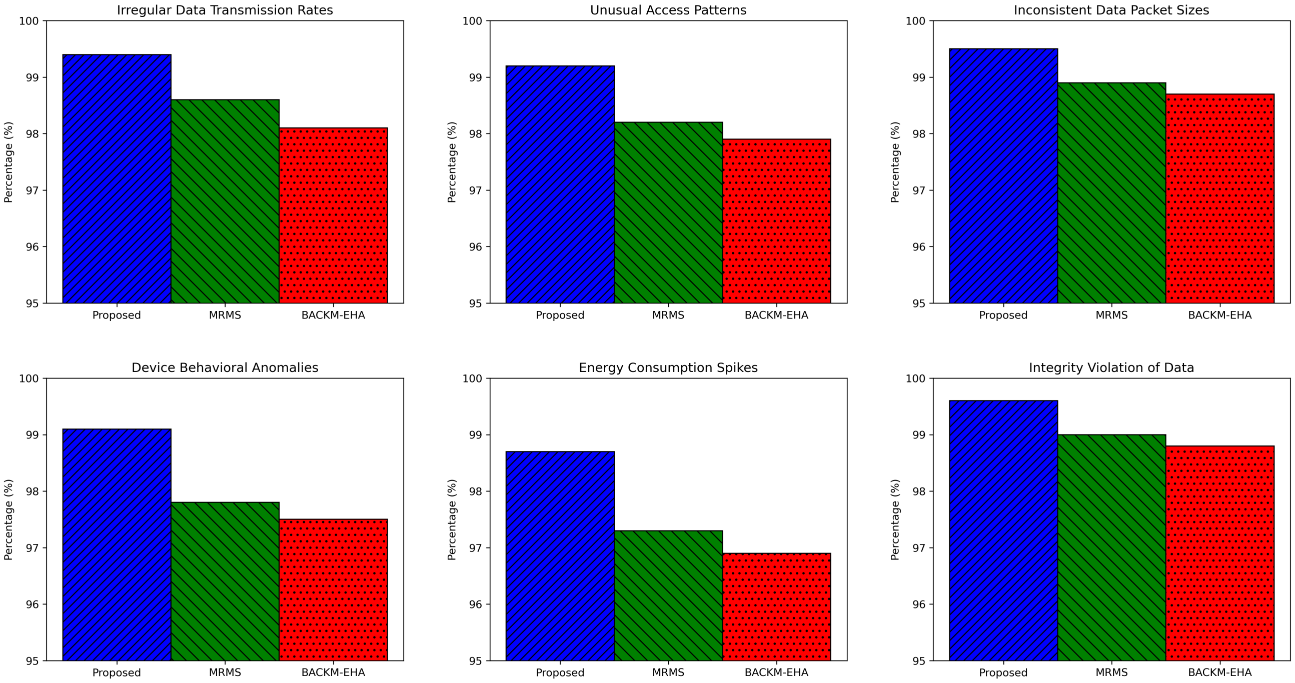

FIGURE 10. **Anomaly detection comparative analysis.**

often overlooked, plays a pivotal role in indicating hardware malfunctions or malicious activities. Our methodology detected 98.7% of anomalous energy spikes, distinctly higher than MRMS's 97.3% and BACKM-EHA's 96.9%. Lastly, the integrity of transmitted data, a bedrock of secure IoMT operations, was maintained by our system with a detection rate of 99.6% for violations, compared to MRMS's 99.0% and BACKM-EHA's 98.8%. In extrapolating the cumulative performance across the aforementioned scenarios, our proposed approach reflects an average detection accuracy of 99.25%. This surpasses MRMS's average of 98.47% and BACKM-EHA's 98.07%. These metrics cogently illustrate the superiority of our system, bolstering its candidacy as an optimal choice for ensuring security and reliability in IoMT deployments.

VII. DISCUSSION

The simulation results presented earlier provide a compelling testimony to the efficacy of our proposed approach in confronting a plethora of security challenges inherent in IoMT systems. Notably, our methodology consistently outperformed or matched the capabilities of established solutions like MRMS and BACKM-EHA across various threat vectors. Patterns emerging from the data underscore the heightened resilience our system offers against both common and sophisticated attacks. While the comparative superiority of our method was anticipated, the scale of enhancement, especially in contexts like anomaly detection, was indeed a revelation. It's also worthy of note that the outcomes place our system not just as a viable alternative but as a leading contender in the quest for fortifying IoMT systems.

Despite the promising results, our simulation was not devoid of limitations. The synthetic environment, while reflective of real-world scenarios, cannot encapsulate the complete intricacy and unpredictability of live IoMT networks. Additionally, certain scenarios might have been influenced by the constraints of the simulation platform or the specificity of the input data. Challenges primarily revolved around ensuring that our models were not overfitting and could generalize across a myriad of unseen threats. In terms of improvements, integrating real-world data streams in our simulation and testing across a broader spectrum of IoMT devices can provide more granular insights.

Building upon the current groundwork, there exists a vast expanse of possibilities for extending our research. Embracing more advanced machine learning models or leveraging the potential of quantum computing for encryption and threat detection could further amplify our system's robustness. Moreover, expanding the simulation to encompass emerging IoMT applications, such as remote surgeries or bio-implant monitoring, can showcase our approach's versatility. Another promising avenue is the fusion of our framework with blockchain technologies, ensuring immutable data integrity and fostering trust in IoMT ecosystems.

The proposed work has shed light on a novel framework that holds promise in addressing some of the most pressing security challenges besieging IoMT systems. By demonstrating superior performance metrics, it not only fills existing lacunae in the literature but also paves the way for future innovations. As the world increasingly leans on the capabilities of IoMT, the significance of our contribution cannot be understated, holding the potential to shape the very future of secure and resilient IoMT infrastructures.

VIII. CONCLUSION

The rapid proliferation of the IoMT has catalyzed significant advancements in healthcare, including improvements in patient outcomes, optimization of medical operations, and enhanced accessibility. Yet, these advancements are not without challenges. The intricate web of interconnected devices introduces an array of security vulnerabilities, necessitating the deployment of formidable protective measures. In response to this challenge, our research introduced a sophisticated framework, meticulously designed to fortify IoMT's security underpinnings. Through comprehensive simulations, our system showcased superior efficacy against contemporary paradigms such as MRMS and BACKM-EHA. Empirical evaluations revealed the robustness of our proposed solution in countering various adversarial threats, from conventional security breaches to complex anomalous activities. The significant enhancements, particularly in anomaly detection, serve as a testament to the practical viability and potential of our model in real-world healthcare settings. Although our research provides a solid groundwork for IoMT security, the dynamic nature of cyber threats and the continuous evolution of medical devices means there's always room for further enhancement. Future endeavors should focus on refining and expanding upon our model, possibly integrating newer technologies or addressing unforeseen vulnerabilities. Nevertheless, the strides made in this study mark a crucial step in the direction of a secure, reliable, and efficient IoMT framework.

REFERENCES

[1] P. Qi, D. Chiaro, F. Giampaolo, and F. Piccialli, "A blockchain-based secure Internet of Medical Things framework for stress detection," *Inf. Sci.*, vol. 628, pp. 377–390, May 2023.

[2] K. A. Awan, I. U. Din, and A. Almogren, "A blockchain-assisted trusted clustering mechanism for IoT-enabled smart transportation system," *Sustainability*, vol. 14, no. 22, Nov. 2022, Art. no. 14889.

[3] H. Y. Lee, K. H. Lee, K. H. Lee, U. Erdenbayar, S. Hwang, E. Y. Lee, J. H. Lee, H. J. Kim, S. B. Park, J. W. Park, T. Y. Chung, T. H. Kim, and H. Youk, "Internet of Medical Things-based real-time digital health service for precision medicine: Empirical studies using MEDBIZ platform," *Digit. Health*, vol. 9, Jan. 2023, Art. no. 205520762211496.

[4] P. Šolić, R. Colella, T. Perković, C. G. Leo, S. Sabina, and L. Catarinucci, "Exploring the potential of Bluetooth low energy for wireless sensing and on-board computation in remote health monitoring," in *Proc. 8th Int. Conf. Smart Sustain. Technol. (SpliTech)*, Jun. 2023, pp. 1–3.

[5] H. Wang, D. Feng, and Y. Liu, "Personalized medicine with advanced analytics," in *Real-World Evidence in Medical Product Development*. Cham, Switzerland: Springer, 2023, pp. 289–320.

[6] F. Alkaabneh and A. Diabat, "A multi-objective home healthcare delivery model and its solution using a branch-and-price algorithm and a two-stage meta-heuristic algorithm," *Transp. Res. C, Emerg. Technol.*, vol. 147, Feb. 2023, Art. no. 103838.

[7] C. Li, M. Dong, X. Xin, J. Li, X.-B. Chen, and K. Ota, "Efficient privacy-preserving in IoMT with blockchain and lightweight secret sharing," *IEEE Internet Things J.*, early access, Jul. 18, 2023, doi: 10.1109/JIOT.2023.3296595.

[8] K. A. Awan, I. Ud Din, A. Almogren, M. Guizani, A. Altameem, and S. U. Jadoon, "RobustTrust—A pro-privacy robust distributed trust management mechanism for Internet of Things," *IEEE Access*, vol. 7, pp. 62095–62106, 2019.

[9] M. L. Hernandez-Jaimes, A. Martinez-Cruz, K. A. Ramírez-Gutiérrez, and C. Feregrino-Uribe, "Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and cloud–fog–edge architectures," *Internet Things*, vol. 23, Oct. 2023, Art. no. 100887.

[10] K. A. Awan, I. U. Din, M. Zareei, M. Talha, M. Guizani, and S. U. Jadoon, "HoliTrust—A holistic cross-domain trust management mechanism for service-centric Internet of Things," *IEEE Access*, vol. 7, pp. 52191–52201, 2019.

[11] T. Shaik, X. Tao, N. Higgins, L. Li, R. Gururajan, X. Zhou, and U. R. Acharya, "Remote patient monitoring using artificial intelligence: Current state, applications, and challenges," *WIREs Data Mining Knowl. Discovery*, vol. 13, no. 2, Mar. 2023, Art. no. e1485.

[12] J. Jeyavel, T. Parameswaran, J. M. Mannan, and U. Hariharan, "Security vulnerabilities and intelligent solutions for iomt systems," in *Internet of Medical Things*. Cham, Switzerland: Springer, 2021, pp. 175–194.

[13] K. A. Awan, I. U. Din, A. Almogren, H. Almajed, I. Mohiuddin, and M. Guizani, "NeuroTrust—Artificial-neural-network-based intelligent trust management mechanism for large-scale Internet of Medical Things," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15672–15682, Nov. 2021.

[14] L. Gomathi, A. K. Mishra, and A. K. Tyagi, "Industry 5.0 for healthcare 5.0: Opportunities, challenges and future research possibilities," in *Proc. 7th Int. Conf. Trends Electron. Informat. (ICOEI)*, Apr. 2023, pp. 204–213.

[15] B. C. Barbosa, S. A. Garan, B. M. Quintela, and M. R. Dantas, "Data logging and non-invasive IoMT approach for rats monitoring in laboratory experiments," in *Proc. Int. Conf. Adv. Inf. Netw. Appl.* Cham, Switzerland: Springer, 2023, pp. 547–557.

[16] J. Zhang, C. Dong, and Y. Liu, "Efficient pairing-free certificateless signcryption scheme for secure data transmission in IoMT," *IEEE Internet Things J.*, early access, Jul. 25, 2023, doi: 10.1109/JIOT.2023.3298840.

[17] K. Chatterjee, A. Singh, Neha, and K. Yu, "A multifactor ring signature based authentication scheme for quality assessment of IoMT environment in COVID-19 scenario," *J. Data Inf. Qual.*, vol. 15, no. 2, pp. 1–24, Jun. 2023.

[18] F. Khan, M. A. Jan, R. Alturki, M. D. Alshehri, S. T. Shah, and A. U. Rehman, "A secure ensemble learning-based fog-cloud approach for cyberattack detection in IoMT," *IEEE Trans. Ind. Informat.*, vol. 19, no. 10, pp. 10125–10132, Oct. 2023.

[19] S. Adibi, "The mPOC framework: An autonomous outbreak prediction and monitoring platform based on wearable IoMT approach," *Future Internet*, vol. 15, no. 8, p. 257, Jul. 2023.

[20] T. Nusairat, M. M. Saudi, and A. B. Ahmad, "A recent assessment for the ransomware attacks against the Internet of Medical Things (IoMT): A review," in *Proc. IEEE 13th Int. Conf. Control Syst., Comput. Eng. (ICCSCE)*, Aug. 2023, pp. 238–242.

[21] S. R. Mallick, V. Goswami, R. K. Lenka, T. R. Sahoo, V. Kumar, and R. K. Barik, "Blockchain-based IoMT for an intelligent healthcare system using a drop-offs queue," in *Proc. 1st Int. Conf. Microw., Antenna Commun. (MAC)*, Mar. 2023, pp. 1–6.

[22] Md. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "Continuous patient monitoring with a patient centric agent: A block architecture," *IEEE Access*, vol. 6, pp. 32700–32726, 2018.

[23] S. S. Sarmah, "An efficient IoT-based patient monitoring and heart disease prediction system using deep learning modified neural network," *IEEE Access*, vol. 8, pp. 135784–135797, 2020.

[24] S. Razdan and S. Sharma, "Internet of Medical Things (IoMT): Overview, emerging technologies, and case studies," *IETE Tech. Rev.*, vol. 39, no. 4, pp. 775–788, Jul. 2022.

[25] J. Wang, M. K. Lim, C. Wang, and M.-L. Tseng, "The evolution of the Internet of Things (IoT) over the past 20 years," *Comput. Ind. Eng.*, vol. 155, May 2021, Art. no. 107174.

[26] M. J. Domínguez Morales, Á. J. Varela Vaca, and M. L. MiróAmarante, "Introductory chapter: An overview to the Internet of Things," in *Internet Things*. IntechOpen, 2023.

[27] S. Khan and A. Akhunzada, "A hybrid DL-driven intelligent SDN-enabled malware detection framework for Internet of Medical Things (IoMT)," *Comput. Commun.*, vol. 170, pp. 209–216, Mar. 2021.

[28] I. Vaccari, V. Orani, A. Paglialonga, E. Cambiaso, and M. Mongelli, "A generative adversarial network (GAN) technique for Internet of Medical Things data," *Sensors*, vol. 21, no. 11, p. 3726, May 2021.

[29] A. I. Awad, M. M. Fouda, M. M. Khashaba, E. R. Mohamed, and K. M. Hosny, "Utilization of mobile edge computing on the Internet of Medical Things: A survey," *ICT Exp.*, vol. 9, no. 3, pp. 473–485, Jun. 2023.

[30] Z. Qu, Z. Zhang, and M. Zheng, "A quantum blockchain-enabled framework for secure private electronic medical records in Internet of Medical Things," *Inf. Sci.*, vol. 612, pp. 942–958, Oct. 2022.

[31] N. M. Thomasian and E. Y. Adashi, "Cybersecurity in the Internet of Medical Things," *Health Policy Technol.*, vol. 10, no. 3, Sep. 2021, Art. no. 100549.

[32] M. Alshaikhli, T. Elfouly, O. Elharrouss, A. Mohamed, and N. Ottakath, "Evolution of Internet of Things from blockchain to IOTA: A survey," *IEEE Access*, vol. 10, pp. 844–866, 2022.

[33] P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh, and W.-C. Hong, "Internet of Things: Evolution, concerns and security challenges," *Sensors*, vol. 21, no. 5, p. 1809, Mar. 2021.

[34] H. Sahu, N. Joshi, and S. V. Chande, "Comprehensive review and analysis of security and privacy for multimedia objects over the Internet of Multimedia Things (IoMT)," *Int. J. Intell. Syst. Appl. Eng.*, vol. 11, no. 9s, pp. 469–481, 2023.

[35] P. Pritika, B. Shanmugam, and S. Azam, "Risk assessment of heterogeneous IoMT devices: A review," *Technologies*, vol. 11, no. 1, p. 31, Feb. 2023.

[36] H. U. Khan, Y. Ali, and F. Khan, "A features-based privacy preserving assessment model for authentication of Internet of Medical Things (IoMT) devices in healthcare," *Mathematics*, vol. 11, no. 5, p. 1197, Feb. 2023.

[37] I. A. Khan, I. Razzak, D. Pi, N. Khan, Y. Hussain, B. Li, and T. Kousar, "Fed-Inforce-fusion: A federated reinforcement-based fusion model for security and privacy protection of IoMT networks against cyber-attacks," *Inf. Fusion*, vol. 101, Jan. 2024, Art. no. 102002.

[38] A. K. Nair, J. Sahoo, and E. D. Raj, "Privacy preserving federated learning framework for IoMT based big data analysis using edge computing," *Comput. Standards Interface*, vol. 86, Aug. 2023, Art. no. 103720.

[39] F. Kamalov, B. Pourghebleh, M. Gheisari, Y. Liu, and S. Moussa, "Internet of Medical Things privacy and security: Challenges, solutions, and future trends from a new perspective," *Sustainability*, vol. 15, no. 4, p. 3317, Feb. 2023.

[40] K. Ajay, A. S. Mattam, B. Joseph, R. Sohan, and R. Selvanambi, "Privacy and security in Internet of Medical Things," in *Federated Learning for Internet of Medical Things*. Boca Raton, FL, USA: CRC Press, 2023, pp. 41–63.

[41] S. Rani, A. Kataria, S. Kumar, and P. Tiwari, "Federated learning for secure IoMT-applications in smart healthcare systems: A comprehensive review," *Knowl.-Based Syst.*, vol. 274, Aug. 2023, Art. no. 110658.

[42] B. Dash, P. Sharma, and S. Swayamsiddha, "Use of AI & embedded technology in human identity chips for IoMT," in *Proc. 4th Int. Conf. Comput. Commun. Syst. (I3CS)*, Mar. 2023, pp. 1–6.

[43] C. Chakraborty, M. R. Khosravi, G. Casalino, and J. J. P. C. Rodrigues, "Guest editorial special issue on AIoMT-enabled federated learning-based computing for socially implemented IoMT systems: How will healthcare systems change?" *IEEE Trans. Computat. Social Syst.*, vol. 10, no. 4, pp. 1537–1539, Aug. 2023.

[44] E. V. D. Subramaniam, K. Srinivasan, S. M. Qaisar, and P. Pławiak, "Interoperable IoMT approach for remote diagnosis with privacy-preservation perspective in edge systems," *Sensors*, vol. 23, no. 17, p. 7474, Aug. 2023.

[45] A. Singh, R. Sinha, Komal, A. Satpathy, and K. Priya, "Security and privacy in IoMT-based digital health care: A survey," in *Robotics, Control and Computer Vision: Select Proceedings of ICRCCV 2022*. Cham, Switzerland: Springer, 2023, pp. 505–525.

[46] A. Arora and M. R. Narayan, "Security and privacy of iomt," in *Revolutionizing Healthcare Through Artificial Intelligence and Internet of Things Applications*. Hershey, PA, USA: IGI Global, 2023, pp. 129–145.

[47] R. Kiran, A. Kumbhare, P. K. Thakur, and S. Mane, "Security and privacy in the Internet of Medical Things (IoMT)," in *Revolutionizing Healthcare Through Artificial Intelligence and Internet of Things Applications*. Hershey, PA, USA: IGI Global, 2023, pp. 1–27.

[48] T. Muazu, M. Yingchi, A. U. Muhammad, M. Ibrahim, O. Samuel, and P. Tiwari, "IoMT: A medical resource management system using edge empowered blockchain federated learning," *IEEE Trans. Netw. Service Manage.*, early access, Aug. 24, 2023, doi: 10.1109/TNSM.2023.3308331.

[49] M. Wazid and P. Gope, "BACKM-EHA: A novel blockchain-enabled security solution for IoMT-based E-healthcare applications," *ACM Trans. Internet Technol.*, vol. 23, no. 3, pp. 1–28, Aug. 2023.

[50] R. Rajadevi, K. Venkatachalam, M. Masud, M. A. AlZain, and M. Abouhawwash, "Proof of activity protocol for IoMT data security," *Comput. Syst. Sci. Eng.*, vol. 44, no. 1, pp. 339–350, 2023.

[51] R. Myrzashova, S. H. Alsamhi, A. V. Shvetsov, A. Hawbani, and X. Wei, "Blockchain meets federated learning in healthcare: A systematic review with challenges and opportunities," *IEEE Internet Things J.*, vol. 10, no. 16, pp. 14418–14437, Aug. 2023.

[52] R. Kamal, E. E.-D. Hemdan, and N. El-Fishway, "Care4U: Integrated healthcare systems based on blockchain," *Blockchain: Res. Appl.*, Jul. 2023, Art. no. 100151, doi: 10.1016/j.bcra.2023.100151.

[53] Z. Qu, W. Shi, B. Liu, D. Gupta, and P. Tiwari, "IoMT-based smart healthcare detection system driven by quantum blockchain and quantum neural network," *IEEE J. Biomed. Health Informat.*, early access, Jul. 3, 2023, doi: 10.1109/JBHI.2023.3288199.

[54] S. Ray, E. V. Korchagina, R. U. Nikam, and R. K. Singhal, "A blockchain-based secure healthcare solution for poverty-led economy of IoMT under Industry 5.0," in *Inclusive Developments Through Socio-Economic Indicators: New Theoretical and Empirical Insights*. Bingley, U.K.: Emerald Publishing Limited, 2023, pp. 269–280.

[55] F. Pelekoudas-Oikonomou, J. Ribeiro, G. Mantas, F. Bashashi, G. Sakellari, and J. Gonzalez, "A tutorial on the implementation of a hyperledger fabric-based security architecture for IoMT," in *Proc. IFIP Netw. Conf. (IFIP Netw.)*, Jun. 2023, pp. 1–6.

[56] T. Górski, "Integration flows modeling in the context of architectural views," *IEEE Access*, vol. 11, pp. 35220–35231, 2023.

MOHAMMAD FAISAL KHAN received the Ph.D. degree from India, in 2012. He was an Assistant Professor with the Department of Mathematics, Aligarh Muslim University, Aligarh, India. He is currently an Associate Professor with the Department of Basic Sciences, College of Science and Theoretical Studies, Saudi Electronic University, Riyadh, Saudi Arabia. He has more than ten years of experience in teaching and research. He has published two books and more than 40 research papers in various refereed reputed journals.

MOHAMMAD ABAOUD received the Ph.D. degree from the University of Wollongong, Australia, in 2014. He is currently an Associate Professor with the Department of Mathematics and Statistics, College of Science, Imam Mohammed Ibn Saudi Islamic University, Riyadh, Saudi Arabia. He has more than ten years of experience in teaching and research. He has published over ten research papers in various refereed reputed journals.