IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 6 February 2024, accepted 7 March 2024, date of publication 13 March 2024, date of current version 21 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3377561

SURVEY

Deep Learning-Assisted Security and Privacy Provisioning in the Internet of Medical Things Systems: A Survey on Recent Advances

RAMBOD PAKROOH, ABDOLLAH JABBARI, AND CAROL FUNG
Concordia Institute for Information Systems Engineering, Concordia University, Montreal, QC H3G 1M8, Canada
Corresponding author: Rambod Pakrooh (rambod.pakrooh@concordia.ca)

This work was supported by the Gina Cody Foundation under Grant 300010031.

ABSTRACT Internet of Medical Things (IoMT) are a kind of Internet of Things (IoT) systems which are used in the healthcare domain. Nowadays, there are an abundance of wearable smart devices, either commercial or clinical, which can be used to collect vital signs and transmit the collected data to remote servers for further analysis. Remote patient monitoring, smart diagnostics, and autonomous control of chronic diseases are examples of different healthcare services that can be provided by these systems at a lower cost and higher efficiency compared to traditional healthcare settings. However, as data related to patients' health status and treatment history, transmitted in these systems, are highly confidential and private, security and privacy concerns in their widespread adoption may arise. Deap Learning (DL) algorithms, with their ability in extracting knowledge from big data generated in these systems, can be leveraged to design smart security mechanisms. In this survey study, the recent literature on the DL-assisted security and privacy provisioning frameworks in IoMT systems are categorized and summarized with respect to their main contributions. Finally, some possible future directions are introduced to assist interested researchers to continue research in this domain.

INDEX TERMS Deep learning, Internet of Medical Things, privacy, security, survey.

I. INTRODUCTION

With the recent advancements in communication, computation, and storage technologies, the Internet of Things (IoT) has found its way into many diverse applications in different industrial and non-industrial domains. The aim of IoT is to make human life easier by making conventional human-operated procedures automatic, autonomous, more efficient, and more cost-effective. In the healthcare domain, Healthcare Internet of Things (HIoT), aka Internet of Medical Things (IoMT), have been in the limelight over the past few years because of their potential impact on the general well-being of societies. Throughout this paper, we use the terms HIoT and IoMT interchangeably. Recent years have witnessed the struggle of the traditional healthcare systems in coping with worldwide pandemics such as Covid-19 in a timely fashion. This bitter experience calls for an alternative, more effective solution. In fact, leveraging the benefits of IoT systems in the healthcare industry which marks the beginning of Medicine 4.0 or Health 2.0 era [1], will empower healthcare professionals to provide more personalized, cost-effective, and proactive services to individuals [2].

There are two types of HIoT systems, namely personal HIoT and clinical HIoT [2]. Personal HIoT systems are mainly composed of commercial wearable devices, such as smart watches and smart clothes, which can be used for personal care without a requirement of either a clinical approval or a direct involvement of an expert. In 2017, the greatest market share in the wearable devices industry, comprised of 115.4 million devices, belonged to three companies, namely Apple, Xiaomi, and Fitbit [1]. On the other hand, clinical HIoT systems are those comprised of

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

clinically approved devices, such as connected inhalers and smart continuous glucose monitors, which should be used according to the instructions that are directly provided by practitioners and specialists.

Although IoMTs are very advantageous to healthcare systems, we should pay close attention to the downsides associated with using them, especially with respect to users' privacy and security. As wearable devices gather and transmit sensitive data regarding patients' physical and physiological conditions, these systems are targets of several attacks from malicious hackers and intruders. Based on a report provided by CyberMDX in 2020, half of the IoMT devices are vulnerable to different types of attacks, posing a great risk to patients' privacy and health [3]. Furthermore, it should be noted that healthcare information is 50 times more valuable than credit cards information making it a great asset to be sold in the black market [3].

Apart from resource limitations in terms of computation, communication, and energy, which renders the application of conventional security mechanisms in IoT settings impracticable, the close interaction of the IoT devices with their surrounding environment makes the situation even more complex [4]. For example, IoT systems in the healthcare domain should be designed to avoid any detrimental consequences affecting their users. Deep learning (DL) methods and in general Machine Learning (ML) approaches could be leveraged to provide intelligent security provisioning schemes in IoT systems [5].

DL algorithms are a subset of ML algorithms which try to mimic the function of a human brain in learning from a massive amount of data [4]. A DL model is generally composed of multiple layers of neurons where each neuron at each layer generates a non-linear transformation of its inputs from the previous layer. In this way, DL models are capable of extracting complex features from the raw input data at each layer of abstraction without a need for a separate feature engineering process. In this way, DL methods can find patterns in huge data sets more efficiently compared to traditional ML methods. In IoT systems, a vast number of smart devices generate heterogeneous application and control data in the network. These data can be used to train different ML/DL models in order to enhance several security and privacy protection operations such as encryption, access control, authentication, and regulatory compliance with respect to data protection laws [6]. In the past decade, there have been several attempts from the academia and industry to deploy DL models to boost the performance of IoT systems in providing security and privacy to their users.

Despite the fact that DL algorithms bring so much benefit to the security improvement in critical IoMT applications, surprisingly, we were not able to find any other survey paper that has focused specifically on the application of DL models in boosting the security and privacy provisioning in these systems. Therefore, in this paper, we survey the recent trends in DL-assisted security and privacy provisioning in the IoMT systems. We have selected related papers published since 2020. In the following subsections, after providing a review of related works, first, we elaborate our motivation for doing this survey, and next, we provide the general structure of the paper.

A. RELATED WORKS

There have been several survey studies on the application of ML/DL approaches in enhancing the security and privacy provisioning in different IoT systems. In Table 1, in addition to our current work, we have summarized the recent survey papers that have been published in the literature since 2020 with respect to their contribution and focus for comparison purposes. As you can see, most of them target IoT systems in general, and are not specifically focused on IoMT/HIoT systems. Although Ghubaish et al. [3] have targeted IoMT systems security, their paper mostly discusses various security mechanisms proposed in the literature based on different methodologies other than ML/DL-based approaches. Furthermore, Ali et al. [7] have only focused on the application of Federated Learning (FL) in protecting the privacy of users in HIoT systems. On the other hand, in this study, we have done a comprehensive survey that is focused on DL-based mechanisms for security and privacy protection in HIoT/IoMT systems.

B. MOTIVATION

As mentioned earlier, IoMT systems are in direct contact with patients for continuous monitoring and proactive treatment. Wearable devices continually gather personal sensitive data to be communicated, stored, and processed. Although this brings a huge advantage to healthcare professionals in providing services remotely in a timely and efficient way with reduced costs and resource consumption, it is essential to bear in mind the presence of malicious criminals waiting to take advantage of the valuable data flowing in the system. Furthermore, we already know that IoMT devices are usually resource-constrained which limits the application of conventional resource-intensive security and privacy protection mechanisms in these systems. Therefore, IoMT devices could be easily compromised and put the lives of patients and the general performance of the system in great danger. In order to convince the healthcare authorities to replace the existing inefficient systems with smart IoMT systems, efficient mechanisms should be devised considering the unique characteristics of these systems which ensure the protection of their users' privacy and security.

DL algorithms with their inherent capability in extracting valuable knowledge from a massive amount of data have attracted the security researchers' attention in recent years. In IoMT systems, as in all other IoT systems, an enormous heterogeneous data are generated which could be used to optimize the performance of security and privacy provisioning mechanisms. There have been a lot of research efforts in recent years in proposing different DL-assisted mechanisms to make IoMT systems more secure. To the

TABLE 1. The summary of recent related survey papers.

Ref.	Contribution	Focus
[4]	A comprehensive study on the attack surfaces in IoT systems, different available ML/DL methods, and the application of ML/DL algorithms in securing different network layers	General IoT systems and ML/DL-assisted security mechanisms
[5]	A thorough study on how DL approaches can boost the security of IoT systems, the current security research in different applications of IoT, and the potential future improvements based on technological advancements	General IoT systems and DL-assisted security mechanisms
[8]	A review on Federated Learning (FL)-assisted security and privacy insurance in different IoT applications, the integration of FL and blockchain in IoT systems, vulnerabilities of FL-based systems, along with an experimental analysis	General IoT systems and FL-assisted security mechanisms
[9]	A discussion on the advantages and challenges associated with the application of FL in different IoT applications	FL deployment in General IoT systems
[10]	A survey on the application of ML algorithms in IoT device authentication and identification based on passively collected data	General IoT systems and ML-assisted device authentication and identification
[11]	A systematic and comprehensive survey on IoT vulnerabilities and current solutions, the role of ML/DL approaches in enhancing the IoT security, and the challenges involved	General IoT systems and ML/DL-assisted security mechanisms
[3]	A survey on IoMT systems security requirements, proposed solutions and their resilience against known attacks, along with proposing a security framework combining various available solutions	IoMT systems and general security mechanisms
[12]	A tutorial paper on the application of FL in IoT systems, its evaluation based on defined metrics, taxonomy, and open research challenges	FL deployment in general IoT systems
[6]	A review on the data generated at different layers of IoT systems and how they can be utilized by ML algorithms to improve the privacy protection	General IoT systems and ML-assisted privacy protection
[13]	A literature review on the application of ML algorithms in IoT security, in addition to a discussion on IoT architecture, security requirements, and potential attacks	General IoT systems and ML-assisted security mechanisms
[14]	A review on the application of DL methods in IoT security, their classification from different points of view, and potential future research directions	General IoT systems and DL-assisted security mechanisms
[15]	A review on the IoT architecture, security requirements, and the role of ML, AI, and the blockchain technology in IoT security enhancement	General IoT systems and security provisioning based on ML, AI, and the blockchain technology
[16]	A review on the ML-assisted attack detection and security enhancement in IoT systems in order to identify challenges and future research directions	General IoT systems and ML-assisted attack detection
[17]	A review and discussion on security and privacy threats in IoT, Ml and blockchain-based security and privacy provisioning, current challenges and future directions	General IoT systems, and ML and blockchain-assisted security and privacy provisioning
[18]	A review on DL-assisted anomaly-based intrusion detection systems in IoT, their classification, analysis, challenges, and future directions	General IoT systems and DL-assisted intrusion detection
[19]	A review and discussion on IoT architecture and enabling technologies, vulnerabilities and attack surfaces, ML/DL-based intrusion detection systems, challenges, and future directions	General IoT systems and ML/DL-assisted intrusion detection
[20]	A review on the security vulnerabilities at each layer of IoT systems, AI-based security solutions, open challenges, and future directions	General IoT systems and various AI-based security solutions
[7]	A survey on FL-assisted privacy protection in health-IoT systems, the integration of FL with Deep Reinforcement Learning (DRL), Generative Adversarial Networks (GANs), and the digital twin technology, open challenges, and future directions	Health-IoT systems and FL-assisted privacy protection
[21]	A comprehensive survey on anomaly-based Intrusion Detection Systems (IDS), ML/DL-assisted anomaly detection, eXplainable AI (XAI) methods and their integration in IDS systems designed for IoT environments, current challenges, and potential future directions	General IoT systems and explainable ML/DL-assisted IDS systems
Our Work	A comprehensive survey on the recent literature on DL-assisted security/privacy provisioning in IoMT systems along with their classification into multiple groups and some discussion on existing challenges and potential future directions	HIoT/IoMT systems and DL-assisted security/privacy provisioning mechanisms

best of our knowledge, no other survey paper has focused on the application of DL methods in IoMT security and privacy provisioning. This motivates us to review, discuss, and classify the current literature on this topic in order to pave the way for researchers in this specific domain by introducing the open challenges and possible future directions.

C. PAPER STRUCTURE

This paper is organized as follows. In section II, the reviewed literature is classified, and the contributions of each work in each category are summarized. In section III, a discussion on the current state of the research in this area, open challenges, and some possible future directions are provided. Finally in section IV, the concluding remarks are provided.

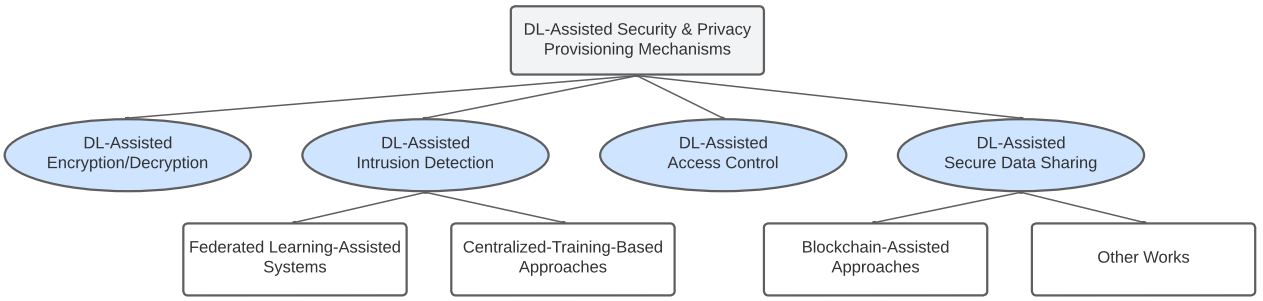

FIGURE 1. An overview of the classification of DL-assisted security & privacy provisioning mechanisms.

II. DL-ASSISTED SECURITY AND PRIVACY PROVISIONING

DL algorithms are able to help in optimizing the performance of different security and privacy protection mechanisms. In this section, based on the optimized security mechanism, the reviewed works in the literature are classified into four broad categories: DL-assisted encryption/decryption, DL-assisted intrusion detection, DL-assisted access control, and DL-assisted secure data sharing. An overview of the classification performed in this study is shown in Fig. 1. In the following subsections, the works presented in each category are summarized with respect to their main contributions.

A. DL-ASSISTED ENCRYPTION/DECRYPTION

DL methods could be leveraged to either encrypt/decrypt messages directly or enhance conventional encryption/decryption mechanisms. Ding et al. [22] propose a deep-learning based approach, based on a Cycle-Generative Adversarial Network (Cycle-GAN), to encrypt and decrypt medical images. They also propose a Region of Interest (ROI)-mining network to extract regions of interest from cyphertexts without decryption. Finally, they evaluate the performance of their proposed approach based on a dataset comprised of X-ray chest images.

In order to improve the spectral and energy efficiency as well as data confidentiality, Wei et al. [23] come up with a privacy-preserving sensing and transmission scheme based on compressed sensing-based encryption and deep-learning-based sparse signal recovery.

In another study, a deep learning-based Ciphertext-Policy Attribute-Based Encryption (CP-ABE) scheme in a fog-assisted mobile health IoT system is introduced [24]. In their proposed scheme, the authors train a deep learning model to learn the pattern of change in values of dynamic attributes to reduce the encryption, decryption, and communication costs.

In summary, DL algorithms with their ability to learn from big data are good candidates to improve the efficiency and robustness of traditional encryption/decryption mechanisms. In this way, we could improve the security by making dynamic encryption algorithms based on context-awareness.

B. DL-ASSISTED INTRUSION DETECTION

Because of their intrinsic capability in extracting valuable information from a large dataset, ML algorithms could be leveraged to analyze the behavior of IoT systems based on the generated data in the network. They can detect any changes in the normal behavior of the system and can adapt efficiently to the dynamic nature of these systems [25]. DL methods, as a subset of ML methods, could deal with the massive amount of data generated in modern IoT systems with a higher accuracy. In recent years, there have been several research attempts to incorporate different DL mechanisms in intrusion detection frameworks in IoMT environments.

1) FEDERATED LEARNING-ASSISTED SYSTEMS

In the 5G/6G era, there are two challenges facing centralized training of ML/DL models [9]; first, a huge amount of frequently generated data puts a high computational and storage burden on the network and the central servers; second, data transmitted to central servers usually contain sensitive and private information of users putting users' privacy in danger.

Federated Learning (FL) has shown a promising solution in overcoming the scalability and privacy challenges. In FL, models are trained in a distributed fashion at each local IoMT network using local data, and only the generated updates are transmitted to the central server for aggregation [7]. In this way, there is no need to transmit raw data from IoMT devices to central servers which protects the data from unauthorized access, and saves the bandwidth. Moreover, harnessing the computational power of clients (either local servers or IoMT devices themselves) to train local models results in boosted training performance. Furthermore, FL helps in training a more accurate model based on data from various sources. However, we should be mindful of the challenges and limitations in deploying the FL mechanism in IoMT and, in general, IoT environments; first, the FL process, non-intuitively, has been shown to be susceptible to different kinds of privacy/security-breaching attacks, such as poisoning attacks, inference attacks, shilling attacks, Byzantine attacks, jamming attacks, and adversarial attacks; second, IoMT devices are usually resource-constrained and are not capable of training complex models, and they might not be willing

to devote their limited resources to the training process [7]. There have been some proposed frameworks in the literature where FL is deployed to train intrusion detection DL models in a distributed fashion.

Otoum et al. [26] use a combination of FL and Transfer Learning (TL) methods to train an intrusion detection model in a privacy-protecting manner. In another study [27], the authors propose a multi-layered federated learning framework to train two deep generative adversarial networks for intrusion detection in medical cyber-physical systems based on two groups of data, namely patient medical data and network traffic data.

Rehman et al. [28] design a blockchain-based federated learning framework for secure and privacy-preserving medical data analysis in IoMT systems. They balance the privacy and accuracy of the federated learning process by introducing a Real-Time Deep Extreme Learning System (RTS-DELM) for disease prediction and intrusion detection.

A privacy-preserving misbehavior detection scheme in IoMT systems based on blockchain and federated learning is introduced in [29]. They use federated learning to train a Bidirectional Long Short Term Memory (BLSTM) model, and utilize the blockchain-enabled smart contract to anonymize and disguise information. Finally, the authors implement an Artificial Pancreas System (APS) controller based on the proposed framework to evaluate its performance.

In another study, Singh et al. [30] propose a Dew-Cloud-based intrusion detection system in IoMT networks using a hierarchical federated learning approach to train a hierarchical Long Short Term Memory (LSTM) model.

Finally, a threat-defense analysis scheme in a partially monitored IoMT environment is introduced in [31]. They utilize a Recurrent Deterministic Policy Gradient (RDPG) approach based on an LSTM model to induce experience-driven False Data Injection Attacks (FDIAs), and train an attack detection module using the privacy-preserving Deep Optimized Attentive Federated Aggregation (DpOptFedAA) method.

As mentioned earlier, FL can protect the privacy by sharing local model parameters, in place of local private data, with the cloud server. However, an attacker intercepting the transmitted updates may also be able to get a sense of the original data by doing some statistical analysis. Moreover, an attacker can inject false updates into the training process. For these reasons, some works have adopted the blockchain technology to secure the training process by securing the local/global model sharing among the involved entities and controlling access to the private information. Considering the benefits of FL, more research is recommended to make it more secure.

2) CENTRALIZED-TRAINING-BASED APPROACHES

Most of the proposed intrusion detection systems in the literature are based on the centralized training of DL models. For example, the authors in [32] investigate the application of Recurrent Neural Networks (RNNs) and some other machine learning algorithms for intrusion detection in IoMT systems. They use the Particle Swarm Optimization (PSO) technique for feature selection in order to improve the performance of the intrusion detection system.

Furthermore, Kumar et al. [33] introduce a hybrid deep-learning model composed of a Convolutional Neural Network (CNN), a BLSTM, and a Gated Recurrent Unit (GRU) to detect botnet attacks in an IoMT environment. On the other hand, Manimurugan et al. [34] design an intrusion detection system based on a Deep Belief Network (DBN).

Moreover, a secure healthcare data sharing framework, composed of a permissioned blockchain and a deep learning model, is designed in [35]. They use the blockchain technology and smart contracts to register, verify, and validate genuine devices to avoid poisoning attacks and data integrity breaches. Furthermore, a deep learning model composed of a Stacked Sparse Variational Autoencoder (SSVAE) and a Self-Attention-based BLSTM (SA-BLSTM) is utilized to encode data (to prevent inference attacks), and to enhance the intrusion detection process.

Haque et al. [36] propose a single deep learning model for both classification and anomaly detection in a timely fashion to counteract adversarial machine learning-based attacks. They design a new training process to avoid training with malicious samples.

In another study [37], a distributed intrusion detection system is designed to improve the training and detection efficiency. In their proposed system, the preprocessing task is distributed among IoT devices to reduce the burden on the remote classifier. Data are preprocessed in IoT devices to remove duplicate features, and to enhance data privacy and security by not sending the raw data to the remote server. Moreover, incremental learning is leveraged to retrain the classifier based on new and unique incoming data features in order to detect novel attacks.

Chaganti et al. [38] design and evaluate a deep learning-based intrusion detection model for detecting attacks in IoMT systems based on a combined dataset of network traffic and patients' sensing data. They use PSO for feature selection to improve the detection performance.

A multidimensional deep learning model for malware detection, malware classification, and CPU architecture classification in an IoMT environment, composed of several IoT devices with different CPU architectures, is proposed in [39]. This hybrid model is composed of a multichannel CNN and a BLSTM. The attention mechanism is used to focus on the most important features to improve the detection accuracy.

The authors in [40] introduce a deep neural network-based anomaly detection framework in IoMT systems. They use both the Principal Component Analysis (PCA) and the Grey-Wolf Optimization (GWO) algorithm to reduce dimensionality in order to decrease the training time, and improve efficiency.

Khan and Akhunzada [41] use a hybrid deep learning model, composed of a CNN and an LSTM, for Software Defined Networking (SDN)-enabled malware detection in an IoMT system, considering the resource constraints of IoT devices.

Recently, Khan et al. [42] utilized an ensemble learning approach, using a series of LSTMs and a decision tree classifier, to create an intrusion detection system in the IoMT environment. They design a fog-cloud architecture for implementing the proposed security system.

In another recent study [43], the authors introduce an online Hardware-supported Malware Detection (HMD) scheme in IoMT systems to detect zero-day malware attacks. In their proposed scheme, multiple deep neural networks are continuously trained, based on various hardware-generated data streams, to detect zero-day malware signatures. Furthermore, a DRL agent is trained to select the best Deep Neural Network-based (DNN-based) detector at runtime, considering their performances.

Nandy et al. [44] propose a novel swarm-Neural Network-based (Swarm-NN-based) intrusion detection system. Their proposed system is used to detect attacks during data transmission in an edge-assisted IoMT system.

A feature extraction and fusion method, based on a multi-modal autoencoder, is proposed in [45]. The authors use a BiLSTM to capture the time-dependent information in the streaming data, and deploy a multi-feature sequence anomaly detection algorithm, based on residual learning, to detect attacks in a blockchain-assisted IoMT network.

Finally, in [46], a hybrid deep learning-assisted SDN-enabled intrusion detection system, using a CNN in combination with a Cuda Deep Neural Network Long Short Term Memory (cuDNNLSTM), is introduced. This hybrid system is designed to detect multivector malware botnets in an IoMT environment.

As we can see, most of the works in the literature have focused on improving the intrusion detection performance. However, it should be noted that sending and storing all data on a central server for training could lead to privacy leakage, especially in the healthcare domain. Moreover, processing all data on a single server could cause scalability issues, and creates a single point of attack.

Finally yet importantly, we should mention the recently risen interest in the so-called eXplainable AI (XAI). Although DL algorithms have been used in modern intrusion detection systems to successfully improve the detection accuracy and performance, these models are often treated as black-box functions [47]. In other words, no explanations or interpretations accompany the decisions made by these models. Therefore, decision-makers and security operators cannot rely solely on the output decisions made by these models as they cannot trust them. Moreover, it is hard to improve the performance of these models since their inner workings are completely vague. Considering the importance of this subject, we review a few recent works in this direction. Interested readers are encouraged to refer to the excellent survey in [21].

Some classical machine learning models are interpretable by nature such as decision trees. However, for more complex and deep models, we usually need some post hoc methods to explain the decision-making process of the model [21]. We have noticed two common post hoc methods in the literature, namely SHapley Additive exPlanations (SHAP) and Local Interpretable Model-Agnostic Explanations (LIME). An explainable bidirectional simple recurrent unit-based recurrent neural network model is introduced in [48] to detect attacks efficiently in an IoMT environment. Skip connections are used to overcome the vanishing gradient problem in deep networks. The authors have used the LIME method to explain the predictions made by their trained model. Hasan et al. [47] integrate LIME and SHAP techniques into an ensemble model of three CNNs and an Extreme Learning Machine (ELM) for explainable intrusion detection in Industrial IoT (IIoT) systems. Moreover, the authors in [49] have also employed the SHAP method in order to make their proposed novel stacked DL model for intrusion detection explainable. They use the term ''cyber-resilient'' to describe their innovative Intrusion Detection System (IDS) as it helps to identify the reason for each anomaly event, and to recover quickly from unwanted situations. Finally, Aljuhani et al. [50] refer to the challenges that arise from treating DL models as black-box, and integrate the SHAP method into their proposed edge-assisted DL-based intrusion detection system to make it trustable as well as understandable. They have leveraged the PSO algorithm for enhanced feature engineering with the aim of bolstering detection capability and computational efficiency. However, it should be noted that they have not used any DL model in their proposed approach. In section III, we provide a brief discussion on integrating XAI methods into ML/DL models.

C. DL-ASSISTED ACCESS CONTROL

The main purpose of access control mechanisms is to prevent unauthorized users from accessing private and sensitive information. As IoMT systems generate highly sensitive data, access control becomes a necessity to protect the privacy of users. We could only find two recent papers that address the application of DL methodologies in optimizing the access control process.

In the first study, Lin et al. [51] introduce an attribute-based secure access control system. By feeding a social graph about users, and each node's features into a Graph Convolutional Network (GCN) which deploys an SIR-based (Susceptible – Infected – Recovered) loss function, they get the corresponding influence and trust values. Furthermore, they use a combination of federated learning and deep reinforcement learning to learn the access control parameters such as the optimal access control threshold.

In the other study, the authors [52] use a CNN model to classify users into normal and abnormal groups, and leverage

a blockchain-integrated cryptography-based FL technique to identify abnormal users and restrict their access to private data.

DL algorithms, with their ability to learn the context from the huge amount of data generated in the network, could be of great help to enhance the access control mechanisms in IoMT systems. Surprisingly, this potential has not been given much attention in the past few years.

D. DL-ASSISTED SECURE DATA SHARING

Because of its ability in creating trust in a trust-less environment, blockchain technology has found its way into many applications including healthcare. The blockchain technology is based on a decentralized ledger which is essentially a chain of blocks managed through a consensus mechanism. The consensus mechanism which is run in a distributed manner by all members of the blockchain, ensures transparency, trust, security, and integrity without a need for a trustworthy third-party involvement. In modern blockchain systems, smart contracts provide a way to automatize certain processes when certain conditions are met. In other words, the blockchain state is updated automatically in predefined circumstances [53].

More than half of the works in this category are based on the blockchain technology as it provides a means for secure sharing of data. However, DL methods could be used to improve the overall performance of the blockchain-based systems as well.

1) BLOCKCHAIN-ASSISTED APPROACHES

A blockchain and edge computing-based health IoT system is proposed in [54] to ensure security and energy efficiency. They leverage an energy harvesting approach to prolong the network lifetime, and use DRL for the joint optimization of the blockchain-based security provisioning and energy efficiency.

In another study, Rakib et al. [55] develop a secure framework for COVID-19 disease management based on the blockchain technology. They store facial images in an off-chain storage, while keeping encrypted profiles and physiological data on the blockchain. In their proposed framework, deep learning-based face recognition along with QR code recognition are used to map facial features of citizens to QR codes that are generated based on their health status. Finally, they develop three distributed apps for citizens, health authorities, and governmental authorities, based on their introduced approach.

Using the benefits of both blockchain and FL, Wang et al. [56] design a privacy-enhanced crowdsensing task assignment strategy in a health IoT environment. They deploy a deep differential privacy method, based on deep convolutional generative adversarial networks, to protect the privacy of data providers by adding noise to their provided data. Moreover, a framework, composed of deep Q-learning, spectral clustering, and federated learning, is used to protect the privacy of task information of data collectors by classifying patients into different access levels. Furthermore, a smart contract-based blockchain technology is utilized to store the published tasks and manage access to them based on patients' assigned levels.

In [57], an intelligent blockchain-based health-IoT system for secure data sharing, between different parties, is designed. They formulate an optimization problem, based on a Markov Decision Process (MDP), to maximize the security and minimize the delay and cost. This optimization problem is solved using the deep Q-learning algorithm.

Finally, in an interesting study, Kumar et al. [58] propose a framework for maintaining data security, privacy, and integrity during data uploading and storage in a cloud-assisted IoMT system. The proposed framework consists of an authentication process, privacy preservation using the K-anonymity algorithm, sensitive vs insensitive data classification using an improved Elman Neural Network (ENN) model, and secure uploading of data to the cloud server leveraging the rooted elliptic curve cryptography with Vigenère cipher encryption mechanism. They use the blockchain technology on the cloud to store the information in order to guarantee integrity.

Blockchain technology establishes the foundation for secure and trustable data sharing in healthcare applications, while DL algorithms add intelligence to the whole process. They are two promising building blocks, among others, toward a secure and efficient framework for future smart healthcare systems.

2) OTHER WORKS

There have been some other works in the literature where the blockchain technology has not been used as a platform to facilitate secure sharing of data. Lin et al. [59] propose an intelligent data fusion approach in an IoMT environment to enhance the privacy of information. They propose a novel task classification, based on k-means classification algorithm, to protect the private information against malicious test subjects. Moreover, a DRL algorithm, called Deep Deterministic Policy Gradient (DDPG), is used to reward/punish test subjects based on their performance, and to validate the data reliability. Furthermore, they design a homomorphic-encryption-based data fusion mechanism to protect the identity of test subjects.

In another study, Allahham et al. [60] design a framework for secure transmission of medical information based on DRL-assisted physical layer security. In their designed framework, an optimization problem is formulated to optimize energy efficiency, signal distortion at the receiver caused by compression at the sender, and QoS requirements. The authors propose two DRL-based algorithms to solve the optimization problem in static and dynamic environments respectively.

In [61], a resource allocation and association optimization problem, in a UAV-assisted IoMT environment, is formulated as a Markov Decision Process (MDP). This problem is solved

using a federated DRL algorithm to ensure the privacy of patients' data.

Finally, in [62], Moqurrab et al. propose a fog-assisted deep learning-based sanitization mechanism, using a CNN and a BLSTM, to maintain the privacy of unstructured health data by medical entity detection and masking, while keeping the data utility at a reasonable level.

Although blockchain is not necessary for secure sharing of information, as evidenced by these works, let us not disregard the trust. One important advantage of the blockchain technology is that its users do not need to make assumptions about the trustfulness of other users and entities. Blockchain, with its inherent features, makes sure that no one can cheat others.

III. DISCUSSION AND FUTURE DIRECTIONS

An overview of the reviewed literature in the previous section is presented in Table 2. As we can see, most of the research efforts in this area have been devoted to designing, implementing, and evaluating DL-assisted intrusion detection systems. Although detecting the presence of anomalies, attacks, and malware in IoMT environments is helpful, there is a need for further investigation to develop DL-assisted techniques for mitigating or even preventing catastrophes that can result from these kinds of intrusions. Especially, in healthcare applications where the lives of patients are at stake, preventing attacks would be much more helpful than detecting them. In recent years, several DL-assisted security provisioning mechanisms for encryption/decryption, controlling access to private information, and secure sharing of data have been proposed which demonstrates the potential of DL methods in enhancing the performance of traditional methods. More research in this direction is recommended.

The main challenges confronting researchers in designing and deploying DL-assisted intrusion detection systems are explainability, data availability, training efficiency, and detection performance. To the best of our knowledge, only one paper in the literature proposes an intrusion detection system, specifically in an IoMT environment, based on the explainable AI framework to provide reasoning for the DL model generated output. In almost all of the proposed systems, DL models are used to detect intrusions without providing any logic behind their decisions. More research is required to make DL-based intrusion detection systems more transparent.

An interpretable model enables non-expert users of the model to understand the relationship between each input and the generated output, whereas an explainable model provides deep explanations about the inner workings of the model which result in producing a certain output [21]. There are several challenges in incorporating either interpretability or explainability in ML/DL models; first, a meticulous feature engineering process is needed to extract the most relevant features from different data sources while removing the redundant ones; second, hyperparameters are often selected by hand, based on some empirical results, which could make the understanding of decisions, made by corresponding trained models, tricky; third, although most researchers are attempting to find the relationship between input features and predictions, they should pay more attention to the data sources and their associated attack surfaces and vulnerabilities; finally and above all, explaining the inner workings of complex and powerful DL models, with a lot of hidden layers and neurons, is not a trivial task. XAI methods can be classified from different points of view [21]. They are either model-specific or model-agnostic, intrinsic or post-hoc, global or local. They can also provide explanations by different means, namely visualization, surrogate models, relevance-based, and example-based approaches.

Using patients' sensitive data along with the control data generated in the network to train DL models to detect anomalies could jeopardize patients' privacy. Moreover, malicious entities could compromise the system by injecting false information. Some works in the literature use federated learning as an approach to train models in a distributed manner while preserving privacy. There are also some proposed frameworks where the blockchain technology is used to provide a secure platform for authentication and data sharing. We were able to find only two papers which have considered the combination of both blockchain and federated learning to enhance security and privacy in the training process. Federated learning could also help in improving the training efficiency and scalability by distributing the training process among several nodes. Most proposed frameworks are based on the central training of models which is not efficient in case of dealing with a huge dataset in IoT systems. Moreover, the decentralized nature of the federated learning approach helps in avoiding the single point of failure problem. Another challenge regarding data availability is how to access a reliable labeled dataset for research purposes. The problem is that most of data generated in real systems are either confidential or private. Generating up-to-date datasets based on real-world IoMT systems in normal and under-attack situations could assist researchers in analyzing the performance of their proposed methods more accurately.

DL-assisted encryption/decryption mechanisms are promising solutions to provide confidentiality in dynamic environments of IoT systems. DL models could be trained dynamically, based on recent available data regarding different types of attacks, to provide the best possible countermeasures. Surprisingly, to the best of our knowledge, only a few number of studies has taken into account the potential of DL algorithms in this regard. One reason for this hesitation could be the limitation of IoT devices with respect to their computing power. Although IoT devices are not powerful enough for training and using sophisticated models, there are several supporting methodologies (as has been seen in other studies in other categories) which assist in improving the training efficiency and scalability. More research in this direction is advisable.

We were able to find only two papers in the recent literature which have investigated the application of DL methods

TABLE 2. An overview of reviewed papers.

Application	Ref.	Supporting Methods and Technologies													DL Models												
		PSO	FL	TL	Blockchain	Attention Mechanism	Incremental Learning	Explainable AI	PCA	GWO	SDN	Ensemble Learning	Swarm-NN	Residual Learning	GAN	DNN	RNN	CNN	LSTM	GRU	DBN	Autoencoder	DELM	DRL	GCN	ENN
Encryption /Decryption	[22]	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	–	–	–	–	–	–	–	–	–	–	–	–
	[23]	–	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	–	–	–	–	–	–	–	–	–	–	–
	[24]	–	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	–	–	–	–	–	–	–	–	–	–	–
Intrusion Detection	[32]	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	–	–	–	–	–	–	–	–	–	–
	[26]	–	✓	✓	–	–	–	–	–	–	–	–	–	–	–	✓	–	–	–	–	–	–	–	–	–	–	–
	[33]	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	✓	✓	–	–	–	–	–	–	–
	[34]	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	–	–	–	–	–	–
	[35]	–	–	–	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–	✓	–	–	✓	–	–	–	–	–
	[36]	–	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	–	–	–	–	–	–	–	–	–	–	–
	[27]	–	✓	–	–	–	–	–	–	–	–	–	–	–	✓	–	–	–	–	–	–	–	–	–	–	–	–
	[37]	–	–	–	–	–	✓	–	–	–	–	–	–	–	–	–	–	✓	–	–	–	✓	–	–	–	–	–
	[38]	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	–	✓	✓	–	–	–	–	–	–	–	–
	[48]	–	–	–	–	–	–	✓	–	–	–	–	–	–	–	–	✓	–	–	–	–	–	–	–	–	–	–
	[28]	–	✓	–	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	–	–	–	–
	[39]	–	–	–	–	✓	–	–	–	–	–	–	–	–	–	–	–	✓	✓	–	–	–	–	–	–	–	–
	[40]	–	–	–	–	–	–	–	✓	✓	–	–	–	–	–	✓	–	–	–	–	–	–	–	–	–	–	–
	[41]	–	–	–	–	–	–	–	–	–	✓	–	–	–	–	–	–	✓	✓	–	–	–	–	–	–	–	–
	[42]	–	–	–	–	–	–	–	–	–	–	✓	–	–	–	–	–	–	✓	–	–	–	–	–	–	–	–
	[29]	–	✓	–	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	–	–	–	–	–	–	–	–
	[30]	–	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	–	–	–	–	–	–	–	–
	[31]	–	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	✓	–	–	–	✓	–	–	–
	[43]	–	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	–	–	–	–	–	–	–	✓	–	–	–
	[44]	–	–	–	–	–	–	–	–	–	–	–	✓	–	–	✓	–	–	–	–	–	–	–	–	–	–	–
	[45]	–	–	–	✓	–	–	–	–	–	–	–	–	✓	–	–	–	–	✓	–	–	✓	–	–	–	–	–
	[46]	–	–	–	–	–	–	–	–	–	✓	–	–	–	–	–	–	✓	✓	–	–	–	–	–	–	–	–
	[47]	–	–	–	–	–	–	✓	–	–	–	✓	–	–	–	–	–	✓	–	–	–	–	–	–	–	–	–
	[49]	–	–	–	–	–	–	✓	–	–	–	–	–	–	–	–	–	–	✓	✓	–	–	–	–	–	–	–
	[50]	✓	–	–	–	–	–	✓	–	–	–	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Access Control	[51]	–	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	✓	–	–
	[52]	–	✓	–	✓	–	–	–	–	–	–	–	–	–	–	–	–	✓	–	–	–	–	–	–	–	–	–
Secure Data Sharing	[54]	–	–	–	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	–	–	–
	[59]	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	–	–	–
	[60]	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	–	–	–
	[55]*	–	–	–	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	[56]	–	✓	–	✓	–	–	–	–	–	–	–	–	–	✓	–	–	–	–	–	–	–	–	✓	–	–	–
	[57]	–	–	–	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	–	–	–
	[61]	–	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	–	–	–
	[62]	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	✓	–	–	–	–	–	–	–	–
	[58]	–	–	–	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	✓

*The model used in this work is not specified. The authors have used a pre-built face recognition model in Python.

in enhancing the performance of traditional access control schemes. Intelligent access control frameworks, based on different DL models, could help us in blocking novel and sophisticated attack vectors from malicious users aiming to get access to personal information, especially sensitive healthcare data. DL models could be trained to reconfigure the system parameters dynamically based on recent trends in attacking behaviors. In other words, DL models should become context-aware by incorporating contextual data in the training process. For example, in [51], the authors argue that in dynamic and distributed healthcare environments, attribute-based authentication and authorization can lead to better privacy insurance by considering different attributes of users in addition to their identity. They train a DL model to calculate trust and influence values based on users' social interactions, and use the generated trust values along with their occupations to grant access to specific medical data. Additionally, they have deployed a DRL to dynamically set the access control threshold based on the ever-changing context.

Finally, DL methods can also be used to optimize the secure data sharing frameworks in general. Most of the proposed frameworks in this category are based on the blockchain technology as a trustable data storage and retrieval

platform. DL models assist the blockchain technology in boosting the security performance of the system. However, some factors should be taken into consideration while designing a DL-assisted secure data sharing mechanism. It should be noted that IoMT/HIoT systems are usually characterized by low availability of communication, computation, and energy resources. Designing a secure system for data sharing, which is also energy-efficient, is challenging [54]. Security/privacy provisioning mechanisms, such as blockchain, are usually computationally demanding, and consume too much energy. On the other hand, although DL algorithms can help us in achieving the optimum performance with respect to security and resource consumption in dynamic environments, the resource-demanding nature of DL algorithms themselves should also be taken into consideration.

Blockchain is not the only way to ensure secure data sharing. There has been some studies on the application of DL in creating intelligent frameworks for secure and privacy-protecting data dissemination. As witnessed in the current literature, encryption is not the only way to secure data transmission. More research is required to come up with more sophisticated, efficient, and intelligent data sharing frameworks for protecting users' privacy.

IV. CONCLUSION

IoMT systems have the potential to make human life easier and to improve the life quality by providing various services such as remote monitoring, remote diagnostics, and remote control. The main motivations for using these systems are cost reduction, treatment efficiency improvement, and autonomous control. However, the main barriers in their wide adoption are security concerns. The data collected, transmitted, and stored in these systems are of highly sensitive nature and should be dealt with carefully. Moreover, any security breach in healthcare IoT systems could put the lives of patients in danger.

DL algorithms, with their capability in extracting knowledge from a huge amount of data, could be leveraged to design smart security and privacy provisioning schemes in the dynamic environment of IoMT networks. In this paper, the recent literature on DL-assisted security and privacy provisioning in IoMT systems is broadly classified into four categories, namely DL-assisted encryption/decryption, DL-assisted intrusion detection, DL-assisted access control, and DL-assisted secure data sharing. Moreover, the works presented in each category are summarized with respect to their main contributions. Finally, a brief discussion on the current state of the literature is provided, and some possible future directions are introduced. We hope this survey study paves the way for fruitful future research in this domain.

REFERENCES

[1] Y. A. Qadri, A. Nauman, Y. B. Zikria, A. V. Vasilakos, and S. W. Kim, "The future of healthcare Internet of Things: A survey of emerging technologies," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1121–1167, 2nd Quart., 2020.

[2] H. Habibzadeh, K. Dinesh, O. Rajabi Shishvan, A. Boggio-Dandry, G. Sharma, and T. Soyata, "A survey of healthcare Internet of Things (HIoT): A clinical perspective," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 53–71, Jan. 2020.

[3] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, "Recent advances in the Internet-of-Medical-Things (IoMT) systems security," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 8707–8718, Jun. 2021.

[4] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for Internet of Things (IoT) security," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1646–1685, 3rd Quart., 2020.

[5] Y. Li, Y. Zuo, H. Song, and Z. Lv, "Deep learning in security of Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 22, pp. 22133–22146, Nov. 2022.

[6] M. Amiri-Zarandi, R. A. Dara, and E. Fraser, "A survey of machine learning-based solutions to protect privacy in the Internet of Things," *Comput. Secur.*, vol. 96, Sep. 2020, Art. no. 101921.

[7] M. Ali, F. Naeem, M. Tariq, and G. Kaddoum, "Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey," *IEEE J. Biomed. Health Informat.*, vol. 27, no. 2, pp. 778–789, Feb. 2023.

[8] M. A. Ferrag, O. Friha, L. Maglaras, H. Janicke, and L. Shu, "Federated deep learning for cyber security in the Internet of Things: Concepts, applications, and experimental analysis," *IEEE Access*, vol. 9, pp. 138509–138542, 2021.

[9] T. Zhang, L. Gao, C. He, M. Zhang, B. Krishnamachari, and A. S. Avestimehr, "Federated learning for the Internet of Things: Applications, challenges, and opportunities," *IEEE Internet Things Mag.*, vol. 5, no. 1, pp. 24–29, Mar. 2022.

[10] Y. Liu, J. Wang, J. Li, S. Niu, and H. Song, "Machine learning for the detection and identification of Internet of Things devices: A survey," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 298–320, Jan. 2022.

[11] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1686–1721, 3rd Quart., 2020.

[12] L. U. Khan, W. Saad, Z. Han, E. Hossain, and C. S. Hong, "Federated learning for Internet of Things: Recent advances, taxonomy, and open challenges," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1759–1799, 3rd Quart., 2021.

[13] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): A survey," *J. Netw. Comput. Appl.*, vol. 161, Jul. 2020, Art. no. 102630.

[14] L. Aversano, M. L. Bernardi, M. Cimitile, and R. Pecori, "A systematic review on deep learning approaches for IoT security," *Comput. Sci. Rev.*, vol. 40, May 2021, Art. no. 100389.

[15] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet Things*, vol. 11, Sep. 2020, Art. no. 100227.

[16] R. Ahmad and I. Alsmadi, "Machine learning approaches to IoT security: A systematic literature review," *Internet Things*, vol. 14, Jun. 2021, Art. no. 100365.

[17] N. Waheed, X. He, M. Ikram, M. Usman, S. S. Hashmi, and M. Usman, "Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures," *ACM Comput. Surveys*, vol. 53, no. 6, pp. 1–37, Nov. 2021.

[18] M. A. Alsoufi, S. Razak, M. M. Siraj, I. Nafea, F. A. Ghaleb, F. Saeed, and M. Nasser, "Anomaly-based intrusion detection systems in IoT using deep learning: A systematic literature review," *Appl. Sci.*, vol. 11, no. 18, p. 8383, Sep. 2021.

[19] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, "A review of intrusion detection systems using machine and deep learning in Internet of Things: Challenges, solutions and future directions," *Electronics*, vol. 9, no. 7, p. 1177, Jul. 2020.

[20] S. Zaman, K. Alhazmi, M. A. Aseeri, M. R. Ahmed, R. T. Khan, M. S. Kaiser, and M. Mahmud, "Security threats and artificial intelligence based countermeasures for Internet of Things networks: A comprehensive survey," *IEEE Access*, vol. 9, pp. 94668–94690, 2021.

[21] N. Moustafa, N. Koroniotis, M. Keshk, A. Y. Zomaya, and Z. Tari, "Explainable intrusion detection for cyber defences in the Internet of Things: Opportunities and solutions," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 3, pp. 1775–1807, 3rd Quart., 2023.

[22] Y. Ding, G. Wu, D. Chen, N. Zhang, L. Gong, M. Cao, and Z. Qin, "DeepEDN: A deep-learning-based image encryption and decryption network for Internet of Medical Things," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 1504–1518, Feb. 2021.

[23] T. Wei, S. Liu, and X. Du, "Learning-based efficient sparse sensing and recovery for privacy-aware IoMT," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9948–9959, Jun. 2022.

[24] M. Talreja, M. P. Taranath, H. Shanware, M. S. Obaidat, and R. R. Rout, "Deep neural networks for dynamic attribute based encryption in IoT-fog environment," in *Proc. ICC IEEE Int. Conf. Commun.*, May 2022, pp. 5670–5675.

[25] A. Jamalipour and S. Murali, "A taxonomy of machine-learning-based intrusion detection systems for the Internet of Things: A survey," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9444–9466, Jun. 2022.

[26] Y. Otoum, Y. Wan, and A. Nayak, "Federated transfer learning-based IDS for the Internet of Medical Things (IoMT)," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2021, pp. 1–6.

[27] I. Siniosoglou, P. Sarigiannidis, V. Argyriou, T. Lagkas, S. K. Goudos, and M. Poveda, "Federated intrusion detection in NG-IoT healthcare systems: An adversarial approach," in *Proc. ICC IEEE Int. Conf. Commun.*, Jun. 2021, pp. 1–6.

[28] A. Rehman, S. Abbas, M. A. Khan, T. M. Ghazal, K. M. Adnan, and A. Mosavi, "A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique," *Comput. Biol. Med.*, vol. 150, Nov. 2022, Art. no. 106019.

[29] S. Rahmadika, P. V. Astillo, G. Choudhary, D. G. Duguma, V. Sharma, and I. You, "Blockchain-based privacy preservation scheme for misbehavior detection in lightweight IoMT devices," *IEEE J. Biomed. Health Informat.*, vol. 27, no. 2, pp. 710–721, Feb. 2023.

[30] P. Singh, G. S. Gaba, A. Kaur, M. Hedabou, and A. Gurtov, "Dew-cloud-based hierarchical federated learning for intrusion detection in IoMT," *IEEE J. Biomed. Health Informat.*, vol. 27, no. 2, pp. 722–731, Feb. 2023.

[31] B. Tahir, A. Jolfaei, and M. Tariq, "A novel experience-driven and federated intelligent threat-defense framework in IoMT," *IEEE J. Biomed. Health Informat.*, pp. 1–8, 2023.

[32] Y. K. Saheed and M. O. Arowolo, "Efficient cyber attack detection on the Internet of Medical Things-smart environment based on deep recurrent neural network and machine learning algorithms," *IEEE Access*, vol. 9, pp. 161546–161554, 2021.

[33] A. K. Kumar, K. Vadivukkarasi, and R. Dayana, "A novel hybrid deep learning model for botnet attacks detection in a secure IoMT environment *," in *Proc. Int. Conf. Intell. Syst. Commun., IoT Secur. (ICISCoIS)*, Feb. 2023, pp. 44–49.

[34] S. Manimurugan, S. Al-Mutairi, M. M. Aborokbah, N. Chilamkurti, S. Ganesan, and R. Patan, "Effective attack detection in Internet of Medical Things smart environment using a deep belief neural network," *IEEE Access*, vol. 8, pp. 77396–77404, 2020.

[35] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, A. K. M. N. Islam, and M. Shorfuzzaman, "Permissioned blockchain and deep learning for secure and efficient data sharing in industrial healthcare systems," *IEEE Trans. Ind. Informat.*, vol. 18, no. 11, pp. 8065–8073, Nov. 2022.

[36] N. I. Haque, M. A. Rahman, and S. I. Ahamed, "DeepCAD: A stand-alone deep neural network-based framework for classification and anomaly detection in smart healthcare systems," in *Proc. IEEE Int. Conf. Digit. Health (ICDH)*, Jul. 2022, pp. 218–227.

[37] A. Tabassum, A. Erbad, A. Mohamed, and M. Guizani, "Privacy-preserving distributed IDS using incremental learning for IoT health systems," *IEEE Access*, vol. 9, pp. 14271–14283, 2021.

[38] R. Chaganti, A. Mourade, V. Ravi, N. Vemprala, A. Dua, and B. Bhushan, "A particle swarm optimization and deep learning approach for intrusion detection system in Internet of Medical Things," *Sustainability*, vol. 14, no. 19, p. 12828, Oct. 2022.

[39] V. Ravi, T. D. Pham, and M. Alazab, "Attention-based multidimensional deep learning approach for cross-architecture IoMT malware detection and classification in healthcare cyber-physical systems," *IEEE Trans. Computat. Social Syst.*, vol. 10, no. 4, pp. 1597–1606, 2023, doi: 10.1109/TCSS.2022.3198123.

[40] P. K. R. Maddikunta, S. Koppu, T. R. Gadekallu, C. L. Chowdhary, and M. Alazab, "An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture," *Comput. Commun.*, vol. 160, pp. 139–149, Jul. 2020.

[41] 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.

[42] 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, 2023, doi: 10.1109/TII.2022.3231424.

[43] Z. He and H. Sayadi, "Image-based zero-day malware detection in IoMT devices: A hybrid AI-enabled method," in *Proc. 24th Int. Symp. Quality Electron. Design (ISQED)*, Apr. 2023, pp. 1–8.

[44] S. Nandy, M. Adhikari, M. A. Khan, V. G. Menon, and S. Verma, "An intrusion detection mechanism for secured IoMT framework based on swarm-neural network," *IEEE J. Biomed. Health Informat.*, vol. 26, no. 5, pp. 1969–1976, May 2022.

[45] J. Wang, H. Jin, J. Chen, J. Tan, and K. Zhong, "Anomaly detection in Internet of Medical things with blockchain from the perspective of deep neural network," *Inf. Sci.*, vol. 617, pp. 133–149, Dec. 2022.

[46] S. Liaqat, A. Akhunzada, F. S. Shaikh, A. Giannetsos, and M. A. Jan, "SDN orchestration to combat evolving cyber threats in Internet of Medical Things (IoMT)," *Comput. Commun.*, vol. 160, pp. 697–705, Jul. 2020.

[47] M. M. Shtayat, M. K. Hasan, R. Sulaiman, S. Islam, and A. U. R. Khan, "An explainable ensemble deep learning approach for intrusion detection in industrial Internet of Things," *IEEE Access*, vol. 11, pp. 115047–115061, 2023.

[48] I. A. Khan, N. Moustafa, I. Razzak, M. Tanveer, D. Pi, Y. Pan, and B. S. Ali, "XSRU-IoMT: Explainable simple recurrent units for threat detection in Internet of Medical Things networks," *Future Gener. Comput. Syst.*, vol. 127, pp. 181–193, Feb. 2022.

[49] D. Javeed, T. Gao, P. Kumar, and A. Jolfaei, "An explainable and resilient intrusion detection system for industry 5.0," *IEEE Trans. Consum. Electron.*, early access, Jun. 7, 2023, doi: 10.1109/TCE.2023.3283704.

[50] A. Aljuhani, A. Alamri, P. Kumar, and A. Jolfaei, "An intelligent and explainable SaaS-based intrusion detection system for resource-constrained IoMT," *IEEE Internet Things J.*, early access, 2023, doi: 10.1109/JIOT.2023.3327024.

[51] H. Lin, K. Kaur, X. Wang, G. Kaddoum, J. Hu, and M. M. Hassan, "Privacy-aware access control in IoT-enabled healthcare: A federated deep learning approach," *IEEE Internet Things J.*, vol. 10, no. 4, pp. 2893–2902, Feb. 2023.

[52] J. A. Alzubi, O. A. Alzubi, A. Singh, and M. Ramachandran, "Cloud-IIoT-Based electronic health record privacy-preserving by CNN and blockchain-enabled federated learning," *IEEE Trans. Ind. Informat.*, vol. 19, no. 1, pp. 1080–1087, Jan. 2023.

[53] B. Cao, Z. Wang, L. Zhang, D. Feng, M. Peng, L. Zhang, and Z. Han, "Blockchain systems, technologies, and applications: A methodology perspective," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 353–385, 1st Quart., 2023.

[54] L. Liu and Z. Li, "Permissioned blockchain and deep reinforcement learning enabled security and energy efficient healthcare Internet of Things," *IEEE Access*, vol. 10, pp. 53640–53651, 2022.

[55] G. A. Rakib, M. S. Islam, M. A. Rahman, A. M. Syed, M. S. Hossain, N. A. Alrajeh, and A. El Saddik, "DeepHealth: A secure framework to manage health certificates through medical IoT, blockchain and deep learning," in *Proc. IEEE Int. Symp. Med. Meas. Appl. (MeMeA)*, Jun. 2021, pp. 1–6.

[56] X. Wang, M. Peng, H. Lin, Y. Wu, and X. Fan, "A privacy-enhanced multiarea task allocation strategy for healthcare 4.0," *IEEE Trans. Ind. Informat.*, vol. 19, no. 3, pp. 2740–2748, Mar. 2023.

[57] A. Z. Al-Marridi, A. Mohamed, A. Erbad, and M. Guizani, "Smart and secure blockchain-based healthcare system using deep Q-learning," in *Proc. IEEE 7th World Forum Internet Things (WF-IoT)*, Jun. 2021, pp. 464–469.

[58] M. Kumar, S. Verma, A. Kumar, M. F. Ijaz, and D. B. Rawat, "ANAF-IoMT: A novel architectural framework for IoMT-enabled smart healthcare system by enhancing security based on RECC-VC," *IEEE Trans. Ind. Informat.*, vol. 18, no. 12, pp. 8936–8943, Dec. 2022.

[59] H. Lin, S. Garg, J. Hu, X. Wang, M. J. Piran, and M. S. Hossain, "Privacy-enhanced data fusion for COVID-19 applications in intelligent Internet of Medical Things," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15683–15693, Nov. 2021.

[60] M. Saria Allahham, A. Awad Abdellatif, A. Mohamed, A. Erbad, E. Yaacoub, and M. Guizani, "I-SEE: Intelligent, secure, and energy-efficient techniques for medical data transmission using deep reinforcement learning," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6454–6468, Apr. 2021.

[61] A. Mohammed, H. N. Abishu, A. Albaseer, A. Erbad, M. Abdallah, and M. Guizani, "FDRL approach for association and resource allocation in multi-UAV air-to-ground IoMT network," in *Proc. GLOBECOM IEEE Global Commun. Conf.*, Dec. 2022, pp. 1417–1422.

[62] S. A. Moqurrab, N. Tariq, A. Anjum, A. Asheralieva, S. U. R. Malik, H. Malik, H. Pervaiz, and S. S. Gill, "A deep learning-based privacy-preserving model for smart healthcare in Internet of Medical Things using fog computing," *Wireless Pers. Commun.*, vol. 126, no. 3, pp. 2379–2401, Oct. 2022.

RAMBOD PAKROOH received the B.S. degree in information technology engineering from the University of Kurdistan, Kurdistan, Iran, in 2011, and the M.S. degree in information technology engineering–computer networks from the University of Isfahan, Isfahan, Iran, in 2013. He is currently pursuing the Ph.D. degree with Concordia University, Montreal, QC, Canada.

Previously, he was a Lecturer with Islamic Azad University (Sanandaj Branch), Kurdistan, for about five years. His current research interests include the Internet of Things, wireless sensor networks, cyber-physical systems, security, privacy, and applied machine learning.

ABDOLLAH JABBARI received the Ph.D. degree in information technology from Urmia University, Urmia, Iran.

He is currently a Postdoctoral Researcher with Concordia University. He has a track record of publishing impactful works in various journals and conferences. His research interests include applied cryptography and information security.

CAROL FUNG is currently an Associate Professor with Concordia University. Her research interests include collaborative intrusion detection networks, social networks, security issues in mobile networks and medical systems, security issues in next generation networking, and machine learning in intrusion detection.

She serves as an Associate Editor for multiple journals, including IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT and *Computer Networks* (COMNET) (Elsevier).