Intelligent AI-based Healthcare Cyber Security System using Multi-Source Transfer Learning Method

CHINMAY CHAKRABORTY, Electronics and Communication Engineering, Birla Institute of Technology, India
SENTHIL MURUGAN NAGARAJAN, Department of Mathematics, Université du Luxembourg, Luxembourg
GANESH GOPAL DEVARAJAN, Department of Computer Science and Engineering, SRM Institute of Science and Technology Delhi-NCR Campus, India
T V RAMANA, Department of Computer Science and Engineering, Jain University, India
RAJANIKANTA MOHANTY, Department of Computer Science - Software Engineering, Jain University, India

Cyber-security intelligence have made a great impact over healthcare industry where several researchers are developing new techniques to improve security for healthcare systems. Besides, Artificial Intelligence (AI) become the tremendous technology in recent decades to improve the existing methods to be more intelligent. In this paper, we proposed cyber attack detection system for healthcare sector with centralized and federated transfer learning mode. Edge of Things (EoT) framework is developed in connection with cloud and healthcare sectors to transmit the data efficiently and the proposed Centralized with Multi-Source Transfer Learning (CMTL) algorithm which is used for detection and classification of various threats such as information gathering, DoS/DDoS attacks, Malware attacks, Injection attacks, and Man in the Middle attacks. Performance of the proposed framework is evaluated using various datasets such as EMNIST, X-IIoTID, and Federated TON_IoT. Our framework outperforms with the analysis of execution time and obtains high level accuracy when compared with different algorithms.

CCS Concepts: • **Artificial Intelligent System** → **Embedded systems**; • **Computer systems organization** → *Redundancy*; Robotics; • **Networks** → Network reliability.

Additional Key Words and Phrases: Cyber Security, Healthcare System, Edge of Things (EoT), Transfer Learning, Centralized System.

1 INTRODUCTION

Smart healthcare technology have become one of the most important field of research due to its rapid growth of biomedical data and healthcare communities. The integration of cloud computing and Internet of Things (IoT) paradigms stimulated the development of smart healthcare systems which can diagnose, monitor, and aggregate

Authors' addresses: Chinmay Chakraborty, Electronics and Communication Engineering, Birla Institute of Technology, Mesra, Jharkhand, India, cchakrabarty@bitmesra.ac.in; Senthil Murugan Nagarajan, Department of Mathematics, Université du Luxembourg, Avenue de la Fonte, Esch-sur-Alzette, Luxembourg, senthil.nagarajan@uni.lu; Ganesh Gopal Devarajan, Department of Computer Science and Engineering, SRM Institute of Science and Technology Delhi-NCR Campus, Meerut Road, Modinagar, Ghaziabad, UttarPradesh, India, 201204, dganeshgopal@gmail.com; T V Ramana, Department of Computer Science and Engineering, Jain University, Jayanagara 9th Block, District Fund Road, Bangalore, India, Venkataramana.t@gmail.com; Rajanikanta Mohanty, Department of Computer Science - Software Engineering, Jain University, Jayanagara 9th Block, District Fund Road, Bangalore, India, rkm.bbs@gmail.com.

1550-4859/2023/5-ART $15.00
https://doi.org/10.1145/3597210

large amount of health data and provide reliable analytical tools for processing. Cyber-security community has worked considerably in developing sophisticated security techniques for securing and preventing users data in healthcare industry [10, 35]. Furthermore, existing approaches are insufficient in addressing the novel threats that regularly breaches IoT based healthcare systems. These approaches are developed to investigate and detect malicious behavior that are broadly applied to prevent from contaminated devices and investigate network traffics which participates in major cyber attacks [32, 44]. CPS is one of the engineering and physical systems in which its operations were coordinated, integrated, and monitored by communication, computation, and control. Various critical fields such as intelligent transportation systems, healthcare monitoring, and smart grids have been obtained this CPS. At initial conditions, CPS will be highly sensitive which makes chaos control which makes more predictable and stable [7, 16]. The location of sensor nodes were estimated using different techniques based on several localization algorithms such as Kalman Filter, multi-dimensional scaling, and semi-definite programming approach [6, 23].

A new computing paradigm known as Edge of Things (EoT) that mainly represents the middle computing layer between cloud and IoT devices that helps to utilize computing power for getting closer to the devices of IoT. The basic usefulness of EoT is transmitted functionality but it can also perform smart decision-making and real-time analytical services for local smart community domain [24, 45]. The global data processing of health records is sent through EoT-layer to cloud computing when transmitting occurs. The EoT based healthcare framework allows early treatment and detection of various disease that can potentially reduces harmfulness caused due to diseases and increasing living possibilities [15, 39, 43]. Cyber-security community have done major contribution towards the development of reliable techniques and security tools for preserving the data ans users information in traditional IT systems [8, 42].

The healthcare cyber physical system (H-CPS) is used to built a overall smart healthcare environment. The H-CPS is integration of electronic health record (EHR) and IoMT which is essentially artificial intelligence (AI) and e-health that collected from the EHR as well as sensor data. Various entities such as biosensors, implantable medical device (IMD), traditional healthcare, information and communication technology (ICT), wearable devices, communication mechanisms, and artificial intelligence were used as the combination in H-CPS to develop smart healthcare [28, 38, 41].

The patients body motion is monitored using wearable devices effectively and directly which helps in identifying human behavior and this replicates as the integral part of Cyber Physical Systems (CPS). Systems are integrated by the CPS to control physical process based on adapting and feedback of real-time conditions. Information is exchanged through CPS communication between humans and objects. Based on bandwidth, reliability, and latency the interaction through the communication is analyzed [14]. Therefore, advance implementation of IoT environment is considered when the interaction between objects and computations were occurred. Control components and computation is combined in CPSs to advance efficiency and connectivity of IoT devices while it enables communication between devices by monitoring, exchanging of data, and optimization [4, 26].

1.1 Motivation

CPSs were used heavily in industries, distribution systems, healthcare, manufacturing, buildings, and transportation, etc. Over the last three years, a report has been mentioned that worldwide the connected wearable devices has been doubled. More than 19% of Americans use wearable fitness trackers and it will increase more in the next few years which leads to development in IMoT [1]. The introduction of edge based CPSs that requires an emphasis on dependability and trustworthiness. We know that both dependability and trustworthiness represents multifaceted properties which are strongly related to CPS, human perception, and security of trust. In the context of trustworthy Artificial Intelligence (AI), researchers develop various methodologies for addressing the challenges of future CPS [34].

Various healthcare surveillance models are developed by different researchers but still some limitations are existing for cloud enabled systems which prevents from using in real-world applications. These issues mainly occurs in communication overhead, latency, and privacy concerns between cloud computing and healthcare entities regarding the aggregation of sensitive data. Currently, various malicious attacks were optimized due to growing number of IoT-based healthcare networks. The privacy of IoT nodes, smart phones, and computer systems over the internet [3, 8].

Our main contributions in this research work are as follows:

- We developed a secure EoT based healthcare system for aggregating, monitoring, and analysis of real-time health data.
- We use three main datasets such as EMNIST, X-IIoTID, and Federated TON_IoT data for analyzing the performance of the proposed model.
- The proposed CMTL model is compared with other existing approaches with the help of various performance metrics.

The rest of the article is organized as follows. Segment 2 comprises the recent state-of-the-art carried out by various researchers, segment 3 describes the proposed framework for AI based CPS systems in healthcare. Section 4 discusses the experimental analysis and results. We summarized the conclusion of work in segment 5.

2 RELATED WORK

The next generation technology is meant to be the integration of cloud computing and Internet of Things (IoT) that gives impact over daily living aspects. Convenient solutions can be provided for various applications such as industrial control, smart grid, and healthcare using interconnection between smart devices and objects with the help of internet infrastructure [9]. We focus mainly on healthcare IoT applications due to paradigm of cloud and IoT that has the potential to regularly improve healthcare technology and early detection of diseases. Several framework have proposed by various researchers to improve the healthcare system and provide secure data transmission by using different deep learning techniques to classify and predict cyber attacks [22, 36].

Salahuddin et al., [29] used edge gateway devices for developing smart healthcare system which interconnects between Wireless Sensor Networks (WSN) and public connected networks. Data-driven decisions are supported by using this smart gateways and emergency cases are notified to the medical practitioners. Mohapatra and Rekha [20] proposed a hybrid model for healthcare system by integrating cloud computing resources for uploading aggregated medical data through IoT sensors which provides on-demand access towards caregivers and patients. However, Park and Park [25] developed a model for healthcare which can aggregate the medical data with the help of health devices using Bluetooth, USB, and ZigBee.

Yang and Gerla [40] used a gateway known to be smart phones for personal health monitoring which help in sending and aggregating medical data to the processing servers with the well known technology named Bluetooth. The medical equipements are attached with senors present in the proposed model for collecting the data and it sent to cloud for providing ubiquitous access. Janjua et al., [12] investigated the supervise machine learning techniques and its efficiency for identifying the insider attacks. Authors used behavior traces dataset of 24 users for the proposed model over five days spam. Authors obtained Adaboost to be performing well as it got 98.3% accuracy when compared with other existing algorithms.

Adil et al., [1] proposed a hybrid model based on Cryptographic Parameter based Encryption and Decryption (CPBE&D) scheme with lightweight authentication method for validating the wearable devices of legal patients over the wireless communication channel for secure transmission. Authors minimized authentication time, communication overhead, and computation cost with the help of supervised machine learning (SML) technique. Authors in [17] proposed cost efficient blockchain task scheduling (CBTS) with different heuristics for cyber physical system in order to process costs associated with deadline and security. The cyber security data validation

is reduced by 33% and 50% for security execution. Authors in [30] discussed interesting facts on edge computing for cyber physical systems. Authors in [13] proposed cipher data sharing and secure remote monitoring for IoT which used Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP).

Kang-Di Lu et al., [19] proposed a model for detecting cyber attacks using deep belief network with population extreme optimization (PEO) for SCADA-based IACS data. For aggregating process, authors introduce ensemble learning scheme to improve the performance of model to detect cyber attacks. Authors in [27] proposed Deep BlockIoTNet to improve the performance of analyzing the cyber attacks in the network. The deep learning operation is carried out in the network edge nodes at the edge-layer in a secure and decentralized manner. Authors in [11] proposed a consolidated framework for the early detection of distributed denial of service (DDoS) attacks such as botnets using deep convolution neural networks (DCNN). Authors in [37] proposed recurrent neural network for networking and IoT malware threats detection where this model evaluates the incoming information and decision is forwarded back for firewall to consider necessary actions.

Lin et al., [18] designed a system function module for dealing the resource consuming attacks that occurs in three layer architecture of edge computing. Authors designed an attack model by combining the mean field-game for transforming the security-defense problem in edge-cloud devices of large terminals. The mean coupling equations is approximated using self-organizing neural network. Furthermore, authors proposed AI-driven resource consuming attack security defense (ARASD) algorithm for improving the anti-attacks ability in the system. Yimin Shi et al., [33] proposed a novel privacy-aware and energy efficient decomposition framework or improving the privacy requirements and user-side FL efficiency. Authors also used software decomposition and mobile edge computing (MEC) as a combination for improving the privacy with more efficient. Fisayo et al., [31] presented a framework for preserving the data from privacy issues. Authors achieved better data utility compared to other traditional anonymization techniques. Table 1 shows the research gap based on previous findings.

Table 1. Research Gap on Previous Findings

Author	Limitations		Preservation Mode	Computation Type	Technique
	is CPS	is Computational			
[29]	No	Yes	Fog and Cloud	Machine Learning	Decision Fusion
[20]	No	No	Clou	Not used	Service authentication
[12]	No	No	Not used	Machine Learning	Naive Bayes, LR, KNN, and Adaboost
[17]	Yes	Yes	Blockchain	Machine Learning	Task Scheduling
[19]	Yes	Yes	NA	Machine Learning and Deep Learning	Population extreme optimization
[33]	No	Yes	Mobile Edge Computing	Deep Learning	Federated Learning
[31]	Yes	Yes	Privacy	Database	PAD
[27]	Yes	Yes	Blockchain	Deep Learning	DeepBlockIoTNet

The main research gap addressed in this proposed work is highlighted below:

- The proposed work will have an impact of both computational and CPS based analysis.
- The developed framework based on Edge of Things (EoT) in connection with cloud is more efficient.
- We proposed CPSs with federated transfer learning mode for healthcare sector.
- The detection and classification of different attacks is analyzed based on Centralized with Multi-Source Transfer Learning Method.

3 PROPOSED EOT-TL HEALTHCARE SYSTEM

In this section, the proposed EoT based healthcare system architecture is provided. We then detailed the each process that are applied in this framework which is shown in Fig. 1. There are various testbed consisted in the proposed framework which includes wearable devices, patient/hospital data, edge computing server, IoT

gateway, Blockchain technology, cloud computing storage, Decision Model, and Receiver End. We mainly used three datasets namely, EMNIST, X-IIoTID, and Federated TON_IoT dataset for analyzing the performance of the proposed model.

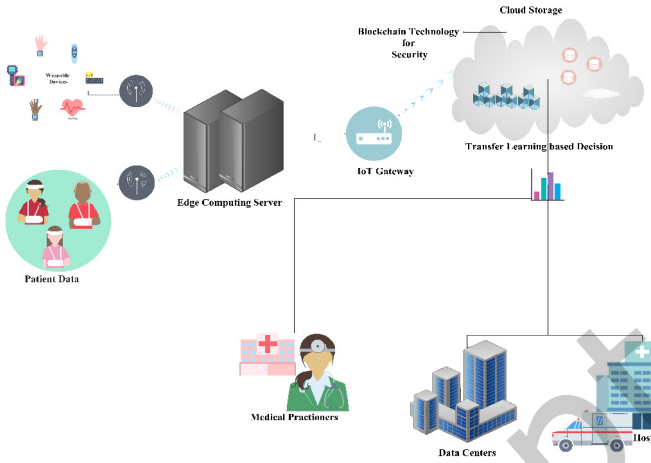

Fig. 1. Proposed Framework for Healthcare System

3.1 Novelty of this Research Work

The main novelty of this research work is presented below:

- Developed a novel framework that replicate the workflow for Edge of Things with cloud based healthcare service based on CPS.
- We introduced centralized based multi source transfer learning method for the analysis of real-time data collected from IoT devices.
- We have shown the performance of proposed model by using Federated TON_IoT, X-IIoTID, and EMNIST dataset.

3.2 Wearable Devices and Patient Data

This is were the collection of health related data are processed using different wearable senor devices and direct patient data gathered from hospitals. The real-time data can also be processed directly from the patients using smart wearable devices which can forward the health information such heart rate, blood pressure, and stress etc., to the edger server for fast processing. Electronic Health Records (EHR) collected from different hospitals is sent through edge server for further analysis. Some of the wearable devices related to health care which are used for the research are ECG Sensors, Smart Clothing, and CGM Sensors.

3.3 Edge Computing

This is an important layer which is very close to the sensor devices as well as to the hospital zones that can process and analyze the data sources instead of sending it to cloud server directly. This edge computing server will helps in prioritizing the data properly at local source which leads to traffic flow minimization and sent to the cloud directly. It also reduces the bandwidth, fewer possibility of failures, and optimizing network latency.

3.4 IoT Gateway

This IoT gateway will process the data to cloud with a secure manner using the Blockchain technology in order to prevent from various cyber attacks. The main motive of this gateway is to connect the IoT devices, sensors, and other smart equipment through physically or virtually to transfer the information or data to the cloud.

3.5 Blockchain Technology

Blockchain technology is most reliable and powerful technique that used recently for cyber security. The central authorities present in the blockchain between two parties have made discontinuation so that they can use blockchain reliably, incorruptible, and as a decentralized public ledger. The use of blockchain technology in this proposed work is to rely on outside third parties for ensuring the safety of data transmission or interactions with different users. The blockchain technology has the capability of ensuring the protection and privacy at all times when data transmission is occurred from edge server to the cloud.

3.6 Cloud Computing

The cloud computing will not be deployed in the working lab as it only acts as a provider for different resources and services like data storage, IoT platforms, and computing power. The major operations which occur in cloud computing is that data storage, visualization, device management, and processing for all applications. Internet will be the source to access towards this cloud computing layer and some access is made locally using the wireless routers.

3.7 Centralized Multi Source Transfer Learning based Detection of Cyber Attacks

In this subsection, we discussed about the centralized with multi-source transfer learning model which is illustrated in Fig. 2.

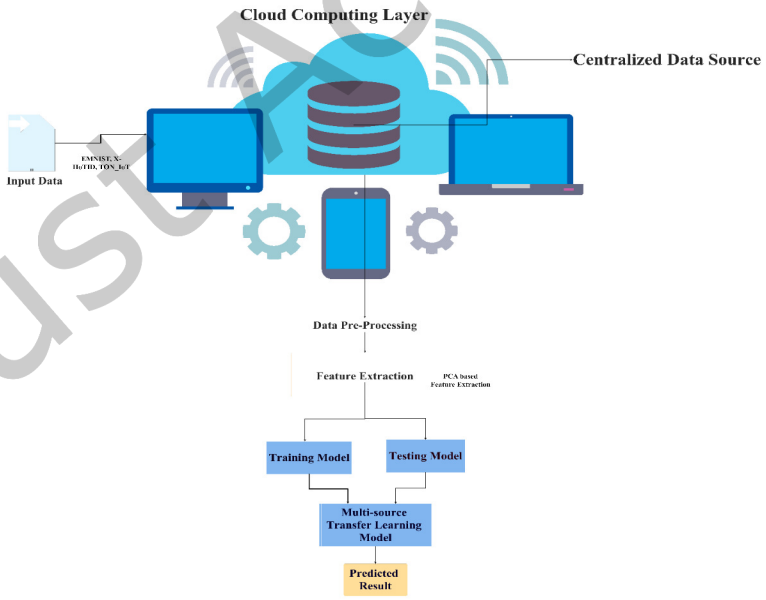

Fig. 2. Proposed Centralized Multi-Source Transfer Learning Process

Firstly, we collected three different datasets namely Federated TON_IoT [21], X-IIoTID [2], and EMNIST [5] data for analyzing the performance of proposed model. Various algorithms such as Decision Tree (DT), Random Forest (RF), Deep Convolution Neural Network (DCNN), and Support Vector Machine (SVM) are used to analyze the dataset and compared the results with proposed model in which our technique outperforms well for these large-scale and heterogeneous dataset. Table 2 shows the parameter settings for the Centralized with Multi-Source Transfer Learning (CMTL) model.

Table 2. Parameter Settings for CMTL Model

Method	Parameters	Value
Centralized	Batch-Size	1000
	Total-Epochs	32
Transfer Learning	Training Data	Testing Data

However, we started with the usual process of analysis such as pre-processing of data in which we removed unwanted and null features from the all three datasets. We dropped unnecessary features using normalization and data imputation methods. Furthermore, we use principal component analysis (PCA) for feature scaling in which certain features are obtained based on the component variance factor and we used label encoding method to map the categorical features to numeric values. Table 3 describes the statistics of attacks and normal flow in the dataset which used for the analysis.

Table 3. Selected Features Statistics for Proposed Model

Classes	Total-Data	Training-Data	Testing-Data
Normal	23201	19081	4120
Attack-Backdoor	11195	7992	3203
Attack-DDoS_HTTP	10261	8196	1999
Ransomware-attack	10955	7721	3234
Attack-DDoS_ICMP	14290	10177	2719
Attack-Fingerprinting	1051	702	201
MITM-attack	1214	286	72
Password-attacks	9789	7878	1894
Port_Scanning-attacks	10171	7167	1804
DDoS_TCP-attack	11247	8698	2549
SQL_injection-attacks	10411	8325	2086
DDoS_UDP-attacks	15498	11998	3200
Uploading-attacks	10269	8271	214

We have conducted the experiment using binary and 13-class classification of different cyber threats and attacks. The multi-source transfer learning based on centralized method is mainly aimed to build a centralize multi-source distribution of data. It measure the relationship based on dependability and similarity. The Kullback–Leibler (KL) divergence is used to measure the difference or relative entropy in information or data associated by two distributions during the transmission of data. The probablity or uniform distirbution of informaiton is analzyed using the KL divergence. Algorithm 1 defines the centralized multi-source transfer learning method.

Algorithm 1 Centralized MTL Algorithm

Input: Dataset collection
Output: Detection of Normal or Attack

Processing Raw Data (RD)
One Edge Server (E):
D← Split(A,B)
for i=1,2,...,S **do**
  for d∈D **do**
    E←E-$\eta\forall f_e(E,d)$
  end for
end for
Data Processed through no. of Edge Server
Data Pre-processing
Feature Selection (Datasets)
Model←PCA(Datasets)
while PCA(Dataset Features) **do**
  Compute Covariance Matrix
  Obtain eigenvectors and eigenvalues
end while
Reduced feature set R
Dividing old data into two sources R1 and R2
$R1^{old} = R1_i^{old^n}{}_{i=1}$
$R2_i^{old} = R1_i^{old_L} \cup R1_i^{old_U}$
Map the samples of R1 and R2 into RM
for i=1,2,....,n **do**
  Compute w^i by MMD
  Train the learner $\hat{l}_i$ on the w^i weighted to $R1^{old}$
end for
Compute relation matrix RM for source target RM_{ij} by

$$RM_{ij} = \begin{cases} \frac{exp(\alpha\hat{\epsilon})_{D_i^{old}}(\hat{h_j})}{\sum_{j^{'}\in[N^{old}]} exp(\alpha\epsilon_{D_i^{old}}(\hat{h_j})} & , i \neq j \end{cases}$$

Compute similarities for source-target θ $\theta = \frac{exp(-\delta.(y_j^i)^\rho)}{\sum_{i=1}^n exp(-\delta.(y_j^i)^\rho)}$
Source similarity and dependability parameterization using ϑ $\vartheta = \theta.[\sigma E_n + ((1-\sigma)M)]$
for m=1,.....,C **do**
  Compute samples proportion with true values $\varsigma_i^{(l)} = \frac{D_i^{old_L}}{\sum_i D_i^{old_L}}$
  Compute KL-divergence between uniform distribution and proportion $R1_{KL}(\varsigma^{(l)} \| uniform) = \sum_{i=1}^n \varsigma^{(l)} log\frac{\varsigma^{(l)}}{uniform}$
  Obtain Bernoulli random variable $BV^{(t)}$
  if $BV^{(t)}$ **then**
    Compute similarity and dependability
  else
    Let $\omega^{(t)} = \frac{1}{\Gamma^{(t)}}$
  end if
  Based on current distribution
  Samples are selected without true values
  Update old sample with new distribution
  Update old data
  Update learner $\hat{l}_i$
end for
Prediction of attack or normal based on the learner

The centralized multi-source transfer learning is computed based on multi source learning method, which has the weights are considered b=from multiple domains that are different from each other. The dependability and source similarity are considered fully or simultaneously that calculating the weight for individual domains. The formula for calculating weight of the particular source is given in Eqn. 1.

$$W = \delta.[\sigma I_n + ((1-\sigma)MS)] \tag{1}$$

Where, the trade-off between domain dependability and source similarity is controlled by the coefficient σ. Identity matrix is represented as $I_n \in M^{n*n}$. In order to evaluate the similarity between target to source domain, the parameter δ is used in a pairwise manner. The δ parameter can be measured using MMD based on the distribution difference as mentioned in Eqn. 2.

$$\delta = \frac{exp(-\Theta.(w_j^i)^\rho)}{\sum_{i=1}^{n} exp(-\Theta.(w_j^i)^\rho)} \tag{2}$$

Where, manually specified parameter is denoted as ρ for regulating the value of δ. The source domain will be more similar to target when the value of MMD is smaller. Therefore, ω is used to measure the weight of each source domain. The Maximum Mean Discrepancy (MMD) is the statistical indicator which is used for measuring the similarity between target and source domain to achieve reasonable transfer learning effect. The value of MMD can be calculated using Eqn. 3.

$$MMD(f_m, SD_i^{old}, SD^{new}) = min \top w^i | \sum_{j=1}^{n_i^{old}} w_j^i f_m(SD_i^{old}) - \frac{1}{n^{new}} \sum_{i=1}^{n^{new}} f_m(SD^{new}) | \tag{3}$$

Where, feature mapping is represented as $f_m(x)$ and weights are denoted as w_j^i for the sub-domain data of i^{th} source. Furthermore, the relation between various source domains is also an important factor and a relation matrix is computed using Eqn. 4.

$$RM_{ij} = \begin{cases} \frac{exp(\vartheta \hat{\epsilon}_{SD_i^{old}}(\hat{l}_j))}{\sum_{j` \in [N^{old}]} exp(\vartheta \hat{\epsilon}_{SD_i^{old}}(\hat{l}_j)^`)}, & ß \neq j \\ j` \neq i \\ 0, otherwise \end{cases} \tag{4}$$

Where, the learner trained is represented as $\hat{l}_j$ which is based on source domain of j^{th} element. The control parameter is denoted by ϑ which is used for retaining predictive error propagation. The empirical error is denoted as $\hat{\epsilon}$ that generated by the learner. R-square statistic is obtained for generating the learner and it is given in Eqn. 5.

$$\hat{\epsilon}_{SD_i^{old}}(\hat{l}_j) = 1 - \frac{\sum(z_i^{old\_L} - \hat{z})^2}{\sum(z_i^{old\_L} - z_i^{-old\_L})^2} \tag{5}$$

4 EXPERIMENTAL ANALYSIS

This section discusses about the performance analysis for the proposed EoT based CMTL method. We have used three main datasets namely EMNIST, X-IIoTID, and Federated TON_IoT data for evaluating the performance of proposed model. The standard benchmark dataset is EMNIST which is considered mainly for analyzing AI-based computer vision systems. Special NIST 19 database is taken to obtain the handwritten character digits which is included in EMNIST dataset. It is the federated version where the dataset is partitioned as single clients where each is assigned with corresponding character/number set of records. The X-IIoTID dataset is used for evaluating and training Intrusion Detection System (IDS) based deep learning or machine learning models for IoT connected systems. The dataset includes 422,317 normal records and 398472 malicious attacks, a total of 67 variables present in it which collected from device sources, alert/devices logs, and network traffic. This dataset is mainly used for centralized learning models in order to provide evaluations of IDS. The federated TON_IoT dataset is collected from three main sources such as operating systems, network traffic, and IoT services telemetry.

This dataset includes attacks traffic and normal which contains 115000 normal records and 6980 attacks. The federated TON_IoT includes a total of nine attack categories such as backdoor, XSS, Man-in-the-Middle (MITM) attack, DDoS/DoS, ransomware, password, scanning, and injection.

4.1 Performance Metrics

We have evaluated the proposed model by splitting the data into training and testing with following performance metrics:

4.1.1 Accuracy. The proportion of correct number for normal or attack classification is determined based on the total number of observations is known as accuracy and it is calculated using Eqn. 6.

$$Accuracy(A) = \frac{TP(Attack) + TN(Normal)}{TP(Attack) + TN(Normal) + FP(Normal) + FN(Attack)} \tag{6}$$

4.1.2 Precision. It is defined as the proportion to the classification of attack classes correctly to the whole amount of attack results that are predicted and it given in Eqn. 7.

$$Precision(P) = \frac{TP(Attack)}{TP(Attack) + FP(Normal)} \tag{7}$$

4.1.3 Recall. It is defined as the proportion of classified proper attacks to the relative count of overall samples that defined as attacks and it is calculated using Eqn.8.

$$Recall(RC) = \frac{TP(Attack)}{TP(Attack) + FN(Attack)} \tag{8}$$

4.1.4 F1-Score. It is defined as the harmonic mean between RC and P which is calculated as given in Eqn. 9.

$$F1_Score = 2.\frac{P.RC}{P + RC} \tag{9}$$

4.2 Model Evaluation

We conducted evaluation of our proposed model using 13-class and Binary classification to understand both detection and traffic predictability of different threats and cyber attack models. However, we used centralized based multi-source transfer learning model for evaluating the detection accuracy while considering heterogeneity, availability of data issues, and privacy. The availability of rich data using centralized learning promotes higher detection possibilities against unknown large-scale attacks.

Various machine learning and deep learning techniques are used in this research for the comparative analysis with the proposed model. The same datasets are used for the performance evaluation of all models based on four main steps and these are processing and analysis of dataset, centralized learning, feature selection, and classification of data using transfer learning model. Figure 3 shows the performance of the centralized based multi-source transfer learning technique which is compared with existing methods such as Random Forest (RF), Decision Tree (DT), Support Vector Machine (SVM), and Deep Convolution Neural Network (DCNN).

From Fig. 3, we can see the analysis of various algorithms with proposed work for different class classification based on 2-class, 6-class, and 13-class. From the results, it is evident that highest accuracy is obtained using the proposed CMTL technique with 96.89% for 13-class classification, 98.45% for 6-class classification, and 99.24% for 2-class classification. The lowest accuracy is obtained by DT technique with 68.46% for 13-class, 75.6% for 6-class, and 82.68% for 2-class classification. SVM classifier obtained 78.2% for 13-class, 82.35% for 6-class, and 88.68% for 2-class classification. For RF classifier, 81.83% for 13-class, 86.89% for 6-class, and 91.65% for 2-class classification.

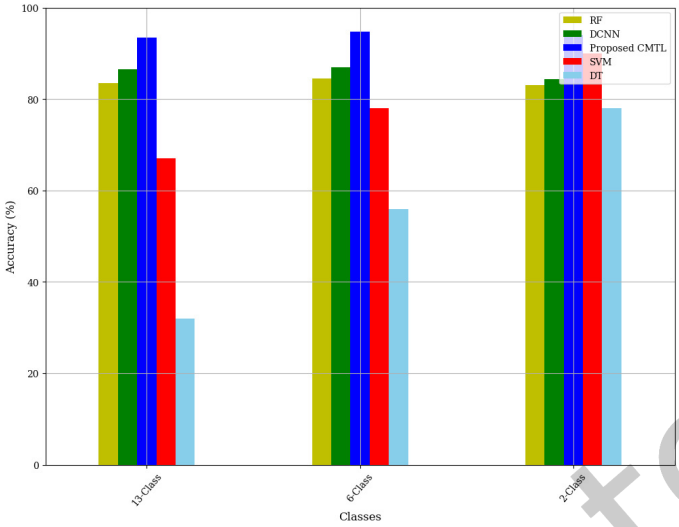

Fig. 3. Comparative Results based on 13-Class, 6-Class, 2-Class Classification

For DCNN technique, 93.68% is achieved for 13-class, 95.68% for 6-class, and finally DCNN obtained 98.67% for 2-class classification. Table 4 shows the performance of various machine learning techniques with proposed centralized multi-source transfer learning model for 6-class classification based Precision, Recall, and F1-Score.

Table 4. Proposed vs Existing Classification Report for 6-Classes

Algorithm	Metrics	Normal-Attack	DDoS-Attack	Injection-Attack	MITM-Attack	Malware-Attack	Scanning-Attack
DT	Pr	1.00	0.36	0.65	1.00	0.85	0.82
	Rc	1.00	0.44	0.49	0.45	0.69	0.62
	F1	1.00	0.38	0.60	0.49	0.76	0.71
RF	Pr	0.978	0.97	0.68	1.00	0.73	0.76
	Rc	0.98	0.84	0.85	1.00	0.72	0.80
	F1	0.99	0.91	0.77	1.00	0.73	0.78
SVM	Pr	0.992	0.96	0.67	1.00	0.97	0.74
	Rc	0.991	0.83	0.91	1.00	0.68	0.92
	F1	0.98	0.89	0.77	1.00	0.80	0.82
DNN	Pr	0.982	0.92	0.66	1.00	0.97	0.96
	Rc	0.99	0.99	0.90	0.94	0.48	0.74
	F1	0.986	0.95	0.76	0.97	0.64	0.84
CMTL	Pr	0.991	0.88	0.63	0.99	0.93	0.82
	Rc	0.97	0.90	0.86	1.00	0.73	0.58
	F1	0.98	0.89	0.73	0.99	0.82	0.68

Table 4 shows the results obtained using various machine learning techniques such as SVM, RF, DT, and DNN for other performance metrics such as Recall (RC), Precision (P), and F1-Score for 6-class classification. Furthermore, Table 4 also shows the results obtained using proposed CMTL technique for same metrics. Therefore, it can seen that the proposed model outperforms well in prediction of various attacks and the difference between normal ones. Different types of attacks such as Backdoor attack (BA), DDoS_HTTP attack, Ransomware attack (RW-A), DDoS_ICMP attack, Fingerprint attack (FP-A), MITM (Man-in-the-Middle) attack, Password attack (PW-A),

Port_Scanning attack (PS-A), DDoS_TCP attack, SQL_Injection attack (SOL-I), DDoS_TCP attack, and Uploading attack (UP-A). The normal class is well determined by the proposed model due to proper data distribution which helps in enhancing the efficiency and effectiveness for the detection of various attacks in real-time capabilities.

Table 5. Proposed vs Existing Classification Report for 13-Classes

Algorithm	Metrics	Normal	B-A	DDoS-HTTP	DDoS-ICMP	DDoS-TCP	DDoS-UDP	FP-A	MITM-A	PD-A	PS-A	RW-A	SQL-A	UP-A
DT	P	1.00	0.87	0.54	0.99	0.76	0.99	0.00	0.99	0.80	0.91	0.78	0.44	1.00
	RC	1.00	0.78	0.63	1.00	1.00	1.00	0.00	1.00	0.00	0.48	0.86	0.96	0.02
	F1-Score	1.00	0.82	0.52	1.00	0.80	1.00	0.00	1.00	0.00	0.58	0.83	0.50	0.04
RF	P	1.00	0.99	0.64	0.96	1.00	1.00	0.77	1.00	0.41	0.63	0.96	0.76	0.66
	RC	1.00	0.92	0.82	1.00	0.60	1.00	0.10	1.00	0.81	1.00	0.93	0.21	0.51
	F1-Score	1.00	0.95	0.72	0.98	0.75	1.00	0.18	1.00	0.54	0.77	0.95	0.33	0.58
SVM	P	1.00	0.96	0.69	1.00	0.76	1.00	0.79	0.97	0.45	0.74	0.95	0.50	0.63
	RC	1.00	0.77	0.60	0.99	0.59	1.00	0.66	1.00	0.23	1.00	0.51	0.82	0.40
	F1-Score	1.00	0.69	0.71	0.99	0.74	1.00	0.72	1.00	0.34	0.78	0.59	0.55	0.50
DNN	P	1.00	0.95	0.76	1.00	0.82	1.00	0.59	1.00	0.55	1.00	0.73	0.47	0.67
	RC	1.00	0.86	0.92	0.99	1.00	1.00	0.64	1.00	0.38	0.50	0.85	0.71	0.48
	F1-Score	1.00	0.90	0.83	1.00	0.90	1.00	0.61	1.00	0.45	0.66	0.79	0.57	0.56
Proposed-CMTL	P	0.96	0.97	0.92	0.93	0.98	0.97	0.95	0.99	0.97	0.98	0.94	0.96	0.98
	RC	0.94	0.96	0.90	0.91	0.97	0.95	0.93	0.97	0.96	0.97	0.91	0.94	0.97
	F1-Score	0.97	0.98	0.94	0.99	0.98	0.98	0.97	0.99	0.99	0.96	0.95	0.97	0.99

Table 5 shows the obtained results for multi-class classification of 13-classes. The machine learning techniques such as RF, DT, SVM, and DNN were used for this multi-class classification based on various performance metrics such as F1-Score, Recall, and Precision. It can be seen that the proposed CMTL technique obtains high accuracy rate for Normal which it gets 96% for precision, 94% for recall, and 97% for F1-Score. Furthermore, our model obtains more than 98% of RC, P, and F1-Score for various attacks such as uploading, password, DDoS-UDP, DDoS-TCP, DDoS-ICMP,Backdoor, and MITM attacks. The SVM and RF gives reasonable accuracy rate for various attacks such as backdoor, DDoS-ICMP, DDoS-UDP, FP-A, and MITM-A. The DT classifier seems to be not obtaining good results when considering multi-class classification and very low accuracy rate is obtained for various attacks. However, the DNN classifier seems to get little higher accuracy for five attack types such as HTTP-A 93%, TCP-SYN 98%, UDP attack 98%, Password 92%, and MITM 99% for multi-class classification of 13-classes. Overall, compared to other existing techniques our proposed model outperforms all the models and obtains high detection/accuracy rate for 13-class classification.

Figure 4 shows the local analysis performance for proposed model on varying edge IoT devices with different number of patients. In this process, we have used Intel i7-3200 CPU of 3 cores with virtual machine having 32GB RAM and 3.2GHz for local processing and globally with EOT framework. When data size is increasing, linear speedup is achieved for proposed model when using real heart disease dataset. Based on VMs number, the global and local processing stages reduced significantly for performance overhead in distributed approach. The reason for used varying Edge IoT devices is to find out how much time difference between single, 4, and 8 devices for certain number of patients. Figure 5 shows the performance analysis of synthetic dataset for varying edge IoT devices.

Figure 6 shows the analysis of accuracy for the synthetic datasets for different number of data points. The execution time is little lesser for distributed based analysis when compared to centralized. The accuracy is varied based on the dataset size. Moreover, VMs with the range between 1% to 17.8% can be affected.

5 LIMITATIONS OF PROPOSED MODEL

The main limitations which should be considered for this proposed work is that parameters while training the model which will affect the performance. Furthermore, the distribution of Edge IoT devices is limited and cannot

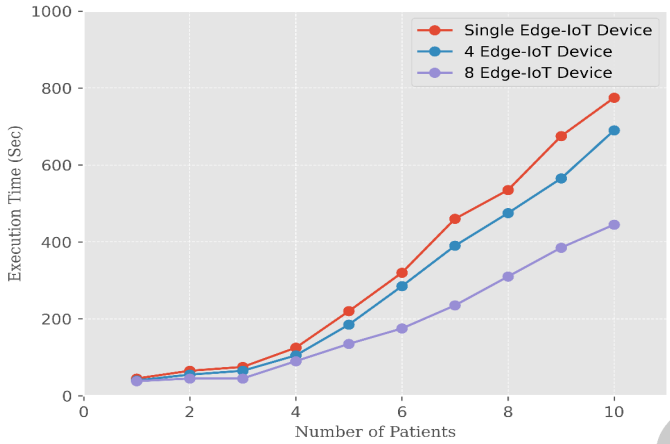

Fig. 4. Local Analysis for Varying Edge-IoT Devices for Proposed Model

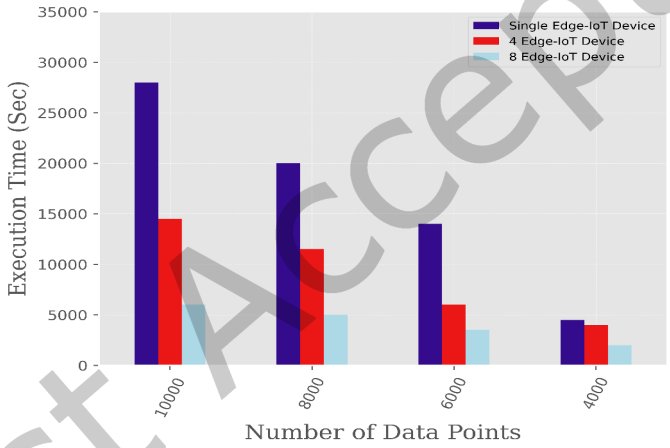

Fig. 5. Data Analysis Performance for Local Analysis on Varying Edge-IoT Devices

get different distributions due to time consumption. Execution time is increases when the increase in patients data to our model. However, we would like take this work to improve the limitation as a future problem.

6 CONCLUSION

In this research, a new paradigm known as Edge of Things (EoT) based Centralized Multi-Source Transfer Learning framework is proposed for analyzing the cuber security attacks during the data processing in healthcare system. The centralized mode is mainly considered in this proposed model for evaluating various machine learning techniques based intrusion detection systems. The main layers of the proposed framework are wearable/patient data, edge computing, IoT gateway, Blockchain technology, cloud computing, and centralized multi-source transfer learning, and finally medical practitioners. Three main datasets such as EMNIST, X-IIoTID, and Federated TON_IoT were used for analyzing the performance of proposed CMTL model. We have used principal component

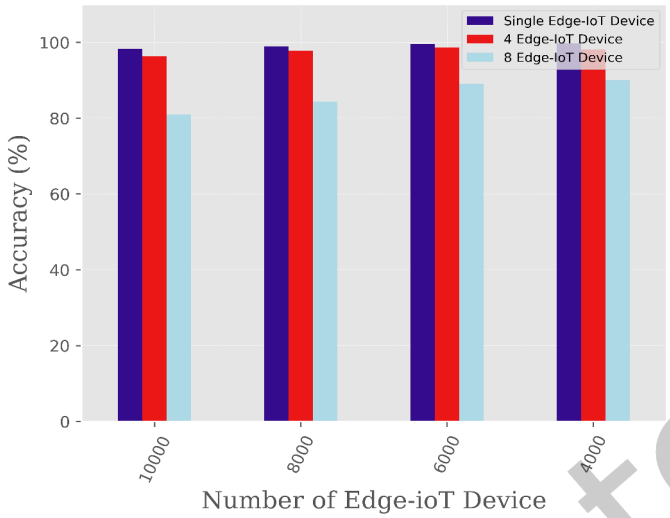

Fig. 6. Accuracy Analysis for Synthetic Dataset

analysis for feature selection and obtained 13 main features from the three datasets which used for analyzing the accuracy, precision, recall, and F1-Score for the proposed model. Moreover, the simulation results of proposed work is compared with existing different machine learning techniques. The CMTL model seems to outperform well by obtaining more than 98% of accuracy for various attack detection when compared with other models. As a future work, we planned to conduct more datasets and different feature selection techniques to analyze the performance for multi-class classification.

REFERENCES

[1] Muhammad Adil, Muhammad Khurram Khan, Muhammad Mohsin Jadoon, Muhammad Attique, Houbing Song, and Ahmed Farouk. 2022. An AI-enabled hybrid lightweight Authentication scheme for intelligent IoMT based cyber-physical systems. *IEEE Transactions on Network Science and Engineering* (2022).

[2] Muna Al-Hawawreh, Elena Sitnikova, and Neda Aboutorab. 2021. X-IIoTID: A Connectivity-and Device-agnostic Intrusion Dataset for Industrial Internet of Things. *IEEE Internet of Things Journal* (2021), 1–1. https://doi.org/10.1109/JIOT.2021.3102056

[3] Abdulatif Alabdulatif, Ibrahim Khalil, Xun Yi, and Mohsen Guizani. 2019. Secure edge of things for smart healthcare surveillance framework. *IEEE Access* 7 (2019), 31010–31021.

[4] Kun Cao, Shiyan Hu, Yang Shi, Armando Walter Colombo, Stamatis Karnouskos, and Xin Li. 2021. A survey on edge and edge-cloud computing assisted cyber-physical systems. *IEEE Transactions on Industrial Informatics* 17, 11 (2021), 7806–7819.

[5] Gregory Cohen, Saeed Afshar, Jonathan Tapson, and André van Schaik. 2017. EMNIST: Extending MNIST to handwritten letters. In *2017 International Joint Conference on Neural Networks (IJCNN)*. 2921–2926. https://doi.org/10.1109/IJCNN.2017.7966217

[6] Zhihua Cui, Bin Sun, Gaige Wang, Yu Xue, and Jinjun Chen. 2017. A novel oriented cuckoo search algorithm to improve DV-Hop performance for cyber–physical systems. *J. Parallel and Distrib. Comput.* 103 (2017), 42–52.

[7] Hongjun Dai, Shulin Zhao, and Kang Chen. 2017. A chaos-oriented prediction and suppression model to enhance the security for cyber physical power systems. *J. Parallel and Distrib. Comput.* 103 (2017), 87–95.

[8] Mohamed Amine Ferrag, Othmane Friha, Djallel Hamouda, Leandros Maglaras, and Helge Janicke. 2022. Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning. (2022).

[9] Vangelis Gazis. 2016. A Survey of Standards for Machine-to-Machine and the Internet of Things. *IEEE Communications Surveys & Tutorials* 19, 1 (2016), 482–511.

[10] Daojing He, Ran Ye, Sammy Chan, Mohsen Guizani, and Yanping Xu. 2018. Privacy in the internet of things for smart healthcare. *IEEE Communications Magazine* 56, 4 (2018), 38–44.

[11] Bilal Hussain, Qinghe Du, Bo Sun, and Zhiqiang Han. 2021. Deep Learning-Based DDoS-Attack Detection for Cyber–Physical System Over 5G Network. *IEEE Transactions on Industrial Informatics* 17, 2 (2021), 860–870. https://doi.org/10.1109/TII.2020.2974520

[12] Faisal Janjua, Asif Masood, Haider Abbas, and Imran Rashid. 2020. Handling insider threat through supervised machine learning techniques. *Procedia Computer Science* 177 (2020), 64–71.

[13] Yong Jin, Masahiko Tomoishi, and Nariyoshi Yamai. 2021. Secure Remote Monitoring and Cipher Data Sharing for IoT Healthcare System with Privacy Preservation. In *Proceedings of the 2021 5th International Conference on Cloud and Big Data Computing*. 46–51.

[14] Ying Ju, Mingjie Yang, Chinmay Chakraborty, Lei liu, Qingqi Pei, Ming Xiao, and Keping Yu. 2023. Reliability-Security Tradeoff Analysis in mmWave Ad Hoc Based CPS. *ACM Transactions on Sensor Networks* (2023).

[15] Gerd Kortuem, Fahim Kawsar, Vasughi Sundramoorthy, and Daniel Fitton. 2009. Smart objects as building blocks for the internet of things. *IEEE Internet Computing* 14, 1 (2009), 44–51.

[16] Randhir Kumar, Prabhat Kumar, Rakesh Tripathi, Govind P Gupta, Sahil Garg, and Mohammad Mehedi Hassan. 2022. A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network. *J. Parallel and Distrib. Comput.* 164 (2022), 55–68.

[17] Abdullah Lakhan, Mazin Abed Mohammed, Jan Nedoma, Radek Martinek, Prayag Tiwari, and Neeraj Kumar. 2022. Blockchain-Enabled Cybersecurity Efficient IIOHT Cyber-Physical System for Medical Applications. *IEEE Transactions on Network Science and Engineering* (2022).

[18] Kai Lin, Jiayi Liu, and Guangjie Han. 2022. AI-Based Mean Field Game against Resource-Consuming Attacks in Edge Computing. *ACM Transactions on Sensor Networks (TOSN)* (2022).

[19] Kang-Di Lu, Guo-Qiang Zeng, Xizhao Luo, Jian Weng, Weiqi Luo, and Yongdong Wu. 2021. Evolutionary Deep Belief Network for Cyber-Attack Detection in Industrial Automation and Control System. *IEEE Transactions on Industrial Informatics* 17, 11 (2021), 7618–7627. https://doi.org/10.1109/TII.2021.3053304

[20] Subasish Mohapatra and K Smruti Rekha. 2012. Sensor-cloud: a hybrid framework for remote patient monitoring. *International Journal of Computer Applications* 55, 2 (2012).

[21] Nour Moustafa, Marwa Keshk, Essam Debie, and Helge Janicke. 2020. Federated TON_IoT Windows datasets for evaluating AI-based security applications. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 848–855.

[22] Senthil Murugan Nagarajan, Ganesh Gopal Deverajan, Kumaran U, Thirunavukkarasan M, Mohammad Dahman Alshehri, and Salem Alkhalaf. 2021. Secure Data Transmission in Internet of Medical Things using RES-256 Algorithm. *IEEE Transactions on Industrial Informatics* (2021), 1–1. https://doi.org/10.1109/TII.2021.3126119

[23] Gia Nhu Nguyen, Nin Ho Le Viet, Mohamed Elhoseny, K Shankar, BB Gupta, and Ahmed A Abd El-Latif. 2021. Secure blockchain enabled Cyber–physical systems in healthcare using deep belief network with ResNet model. *J. Parallel and Distrib. Comput.* 153 (2021), 150–160.

[24] Xirong Ning and Jin Jiang. 2021. Design, Analysis and Implementation of a Security Assessment/Enhancement Platform for Cyber-Physical Systems. *IEEE Transactions on Industrial Informatics* 18, 2 (2021), 1154–1164.

[25] KeeHyun Park and JuGeon Pak. 2012. An integrated gateway for various PHDs in U-healthcare environments. *Journal of Biomedicine and Biotechnology* 2012 (2012).

[26] Ishaani Priyadarshini, Rohit Sharma, Dhowmya Bhatt, and M Al-Numay. 2022. Human activity recognition in cyber-physical systems using optimized machine learning techniques. *Cluster Computing* (2022), 1–17.

[27] Shailendra Rathore and Jong Hyuk Park. 2021. A Blockchain-Based Deep Learning Approach for Cyber Security in Next Generation Industrial Cyber-Physical Systems. *IEEE Transactions on Industrial Informatics* 17, 8 (2021), 5522–5532. https://doi.org/10.1109/TII.2020.3040968

[28] Muneeb Ahmed Sahi, Haider Abbas, Kashif Saleem, Xiaodong Yang, Abdelouahid Derhab, Mehmet A Orgun, Waseem Iqbal, Imran Rashid, and Asif Yaseen. 2017. Privacy preservation in e-healthcare environments: State of the art and future directions. *Ieee Access* 6 (2017), 464–478.

[29] Mohammad A Salahuddin, Ala Al-Fuqaha, Mohsen Guizani, Khaled Shuaib, and Farag Sallabi. 2017. Softwarization of Internet of Things Infrastructure for Secure and Smart Healthcare. *Computer* 50, 07 (2017), 74–79.

[30] José Manuel Gaspar Sánchez, Nils Jörgensen, Martin Törngren, Rafia Inam, Andrii Berezovskyi, Lei Feng, Elena Fersman, Muhammad Rusyadi Ramli, and Kaige Tan. 2022. Edge computing for cyber-physical systems: A systematic mapping study emphasizing trustworthiness. *ACM Transactions on Cyber-Physical Systems (TCPS)* 6, 3 (2022), 1–28.

[31] Fisayo Caleb Sangogboye, Ruoxi Jia, Tianzhen Hong, Costas Spanos, and Mikkel Baun Kjærgaard. 2018. A framework for privacy-preserving data publishing with enhanced utility for cyber-physical systems. *ACM Transactions on Sensor Networks (TOSN)* 14, 3-4 (2018), 1–22.

[32] Jayasree Sengupta, Sushmita Ruj, and Sipra Das Bit. 2020. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *Journal of Network and Computer Applications* 149 (2020), 102481.

[33] Yimin Shi, Haihan Duan, Lei Yang, and Wei Cai. 2022. An Energy-efficient and Privacy-aware Decomposition Framework for Edge-assisted Federated Learning. *ACM Transactions on Sensor Networks (TOSN)* (2022).

[34] Fatemeh Esmaeilnezhad Tanha, Aliakbar Hasani, Saqib Hakak, and Thippa Reddy Gadekallu. 2022. Blockchain-based cyber physical systems: Comprehensive model for challenge assessment. *Computers and Electrical Engineering* 103 (2022), 108347.
[35] Nandor Verba, Kuo-Ming Chao, Anne James, Daniel Goldsmith, Xiang Fei, and Sergiu-Dan Stan. 2017. Platform as a service gateway for the Fog of Things. *Advanced Engineering Informatics* 33 (2017), 243–257.
[36] Yulong Wang, Qixu Wang, Xingshu Chen, Dajiang Chen, Xiaojie Fang, Mingyong Yin, and Ning Zhang. 2022. ContainerGuard: A Real-Time Attack Detection System in Container-Based Big Data Platform. *IEEE Transactions on Industrial Informatics* 18, 5 (2022), 3327–3336. https://doi.org/10.1109/TII.2020.3047416
[37] Marcin Woźniak, Jakub Siłka, Michał Wieczorek, and Mubarak Alrashoud. 2021. Recurrent Neural Network Model for IoT and Networking Malware Threat Detection. *IEEE Transactions on Industrial Informatics* 17, 8 (2021), 5583–5594. https://doi.org/10.1109/TII.2020.3021689
[38] Yirui Wu, Haifeng Guo, Chinmay Chakraborty, Mohammad Khosravi, Stefano Berretti, and Shaohua Wan. 2022. Edge computing driven low-light image dynamic enhancement for object detection. *IEEE Transactions on Network Science and Engineering* (2022).
[39] Geng Yang, Li Xie, Matti Mäntysalo, Xiaolin Zhou, Zhibo Pang, Li Da Xu, Sharon Kao-Walter, Qiang Chen, and Li-Rong Zheng. 2014. A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box. *IEEE transactions on industrial informatics* 10, 4 (2014), 2180–2191.
[40] Sungwon Yang and Mario Gerla. 2011. Personal gateway in mobile health monitoring. In *2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*. IEEE, 636–641.
[41] Xiaokang Zhou, Wei Liang, I Kevin, Kai Wang, and Laurence T Yang. 2020. Deep correlation mining based on hierarchical hybrid networks for heterogeneous big data recommendations. *IEEE Transactions on Computational Social Systems* 8, 1 (2020), 171–178.
[42] Xiaokang Zhou, Xuesong Xu, Wei Liang, Zhi Zeng, Shohei Shimizu, Laurence T Yang, and Qun Jin. 2021. Intelligent small object detection for digital twin in smart manufacturing with industrial cyber-physical systems. *IEEE Transactions on Industrial Informatics* 18, 2 (2021), 1377–1386.
[43] Xiaokang Zhou, Xuesong Xu, Wei Liang, Zhi Zeng, and Zheng Yan. 2021. Deep-learning-enhanced multitarget detection for end–edge–cloud surveillance in smart IoT. *IEEE Internet of Things Journal* 8, 16 (2021), 12588–12596.
[44] Yingying Zhu, Nandita M Nayak, and Amit K Roy-Chowdhury. 2012. Context-aware activity recognition and anomaly detection in video. *IEEE Journal of Selected Topics in Signal Processing* 7, 1 (2012), 91–101.
[45] Maede Zolanvari, Marcio A Teixeira, Lav Gupta, Khaled M Khan, and Raj Jain. 2019. Machine learning-based network vulnerability analysis of industrial Internet of Things. *IEEE Internet of Things Journal* 6, 4 (2019), 6822–6834.