Retraction Notice

The Editor-in-Chief and the publisher have retracted this article, which was submitted as part of a guest-edited special section. An investigation uncovered evidence of compromised peer review. The Editor and publisher no longer have confidence in the results and conclusions of the article.

PU disagrees with the retraction. NR either did not respond or could not be reached.

Blockchain enabled secure image transmission and diagnosis scheme in medical cyber-physical systems

Padmavathi Udayakumar and Narendran Rajagopalan*
National Institute of Technology Puducherry, Department of Computer Science and Engineering, Karaikal, Puducherry, India

Abstract. Medical cyber-physical systems (MCPSs) are life critical, context aware, networked systems of medical devices that are increasingly used in hospitals to achieve seamless high-quality healthcare. The design of the MCPS for the healthcare sector necessitates significant attention to achieving security. As the medical images need to be communicated regularly for timely and accurate diagnosis, medical images need to be secured by encryption and blockchain technologies. In this aspect, we present a blockchain enabled secure image transmission and diagnosis (BESITD) for the MCPS environment. The BESITD technique encompasses an image acquisition process that enables the wearable devices to capture the medical images. Then, the presented model executes an intrusion detection system using recurrent neural network to determine the presence of intruders in the MCPS. In addition, the block-wise encryption process takes place in which the medical image is partitioned into n blocks, each of which is individually encrypted using the signcryption technique. Moreover, a consortium blockchain technology is used to store the encrypted image along with the hash value of the original medical image to accomplish integrity and traceability. At the cloud server side, the disease diagnosis process takes place in different stages, namely, multilevel thresholding-based segmentation, MobileNet-based feature extraction, and optimal kernel extreme learning machine (OKELM)-based classification. Furthermore, a multiobjective political optimizer is designed for effective selection of threshold values and KELM parameters. A wide range of simulations was performed on two benchmark medical image datasets, and the experimentation results highlighted the promising performance of the BESITD technique over the recent techniques with the maximum accuracy of 0.9816. © *2022 SPIE and IS&T* [DOI: 10.1117/1.JEI.31.6.062002]

Keywords: medical cyber-physical systems; healthcare; blockchain; security; image encryption; disease diagnosis; deep learning.

Paper 210554SS received Aug. 19, 2021; accepted for publication Dec. 29, 2021; published online May 11, 2022; retracted Sep. 13, 2023.

1 Introduction

A cyber-physical system (CPS) is a structural model associated with communication technology and pervasive sensing that offers several advantages to society and the economy. In another words, it is an engineered scheme in which the physical process/system is increased with cyber modules, such as a communication network and computational hardware.[1] These components are very strongly incorporated with one another, that is, the performance of a single component is based on the other components. In recent years, CPSs have seen a considerable increase in the fields of health, energy, industrial Internet of Things, and transportation. In developing this system to be flexible, smart, and efficient, the significant fields of research are reliability, stability, security, privacy, and robustness.[2] However, rapid advancement in the enabling techniques has exposed this system to profound and serious threats.

The medical CPS (MCPS)[3] is a specific kind of CPS that depends on the application background of the smart medical fields that include cyber space and physical space. User space includes nurses, doctors, etc., and physical space consists of medical diagnostic equipment and

*Address all correspondence to Narendran Rajagopalan, narendran@nitpy.ac.in

1017-9909/2022/$28.00 © 2022 SPIE and IS&T

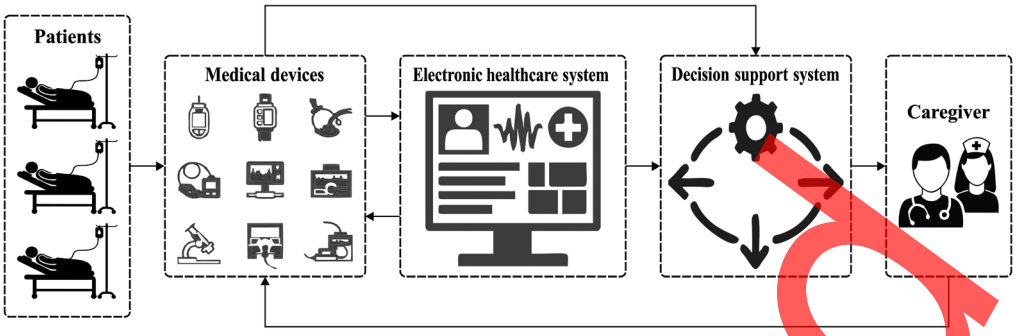

Fig. 1 Overview of the MCPS.

wearable devices. Cyber space is the headquarters of MCPSs. It obtains sensing data from a physical space via transmission networks. Later, the cyber space stores, recognizes, processes, analyses, and generates feedback control data. Finally, it transmits control data to the physical space via transmission networks. MCPSs constantly gather a patient's physical sign data via different medical and wearable devices, so the patient's physical condition is detected better.[4] To offer the patients a timely and more accurate diagnosis, various medical institution needs to share a significant amount of physical information gathered by the medical staff and sensors.[5] Figure 1 shows the overview of the MCPS.

Simultaneously, patient privacy must be secured. Therefore, blockchain is essential for using cryptography technology and peer-to-peer networks to attain non-forgeable, tamper proof, verifiable, and nonrepudiating healthcare records. The combinations of blockchain and MCPS[6] promote the sharing of healthcare resources and services. However, the block capability limit is the major factor that affects the efficiency improvements of the blockchain. MCPSs control the embedded medical equipment via a wireless network, which monitors and senses patient physical data in real-time. Once a patient has an abnormal condition, the medical equipment sends the earlier warning data to the clinical institutions. If the MCPS is under a cyberattack, such as unauthorized access, data breach, and data inconsistency,[7] the patients' health and lives would be at a serious risk. Practically, healthcare institutions need to check the integrity and accuracy of sensed and shared healthcare information before making a medical diagnosis.

In this case, blockchain can be used. It is an underlying technique for enabling decentralization and plays a significant part in the CPS field. At first, the blockchain technique was initially used to protect smart contracts, financial transactions, notary information, and storage systems. However, its advantages soon were recognized for use in other applications, such as healthcare, supply chain, energy, and transportation fields, as these industries realized that it is capable of improving efficacy by adapting blockchain.[8] Blockchain provides a distributed framework that utilizes cryptography as a security tool to create immutable blocks including data ordered and transactions in a chain. This block, when added to the chain, cannot be modified/altered and is secured using timestamps and hash functions on transaction data. Each block in the chain has a similar size.[9] Additionally, the mining process helps validating the transaction blocks and assists in securing the blockchain networks from malicious attack. Smart contracts are simply programs saved on a blockchain which executes upon the fulfillment of predefined conditions.

This paper presents a new blockchain enabled secure image transmission and diagnosis (BESITD) for secure medical image transmission and diagnosis in the MCPS environment. The BESITD technique designs a recurrent neural network (RNN) model for the detection of intrusions in the MCPS. In addition,, a block-wise encryption process is derived in which the medical image is partitioned into n blocks, each of which is individually encrypted using the signcryption technique. Also, a consortium blockchain technology is used for storing the encrypted image and the hash value of the original medical image to achieve integrity and traceability. Next, the disease diagnosis process is performed at the cloud server using different stages of operations, such as multilevel thresholding-based segmentation, MobileNet-based feature extraction, and optimal kernel extreme learning machine (OKELM)-based classification. Finally, a multiobjective political optimizer (MOPO) is designed for effective selection of

threshold values and KELM parameters. To ensure the enhanced performance of the BESITD technique, a comprehensive experimental analysis is conducted on two benchmark datasets.

The remainder of the paper is organized as follows. Section 2 offers the related works, Sec. 3 introduces the proposed model, and Sec. 4 provides the experimental validation. Finally, Sec. 5 draws the conclusion.

2 Literature Review

In Cheng et al.,[10] the blockchain technology is employed to describe the security requirement in a verification model, and the network model of the MCPS that depends on a blockchain is presented. Using the analysis of the healthcare data storage model, it ensures that the information is not traceable or tampered with. In the security verification stage, intractable problems and bilinear mapping are applied for solving the security threats in the verification model of medicinal data users and providers. It prevents the credibility problems of the trusted third party and realizes two-way authentications among the blockchain nodes and hospitals. Next, body area network (BAN) logic is utilized for analyzing the security protocol, and formal analyses and comparison of the security protocols are carried out. The experimental result shows that the MCPS that depends on blockchain realizes medicinal treatment data sharing, and meets the different security needs in the security verification stage. Zhou et al.[11] proposed the integration of consortium and private blockchains that could realize data sharing and defend data security. In this method, the healthcare records of all of the nodes are kept in the private blockchain.

Qiu et al.[12] proposed a sharing and secure data storage approach consisting of an elective encryption approach integrated with dispersion and fragmentation for protecting the data privacy and safety while broadcasting medias (for example the cloud server) and keys are compromised. Shu et al.[13] described a two-phase system in which healthcare records are shared on-blockchain and stored off-blockchain. Moreover, multitrapdoor hash functions were also presented. The aim was to realize the verification of interrelated medicinal equipment, apps, and staff to guarantee the integrity of the healthcare records and assists in secure sharing and storage of healthcare data. In Chen et al.,[14] a lightweight verification system was developed for gateway nodes, execution or sensor devices, and users in the MCPS. The security analyses and stimulation result show that the system is capable of resisting an attack with improved performance; therefore, this presented method could be effectively used for healthcare fields. Vangipuram et al.[15] used an off-chain distributed storage solution to load huge medical datasets and a blockchain execution to safely transfer the data from the diseased patient to the healthcare scheme with an edge framework and called it CoviChain. The COVID19 statistic is loaded on to the edge and shifted to the InterPlanetary File System (IPFS) storage to retrieve the hash value of the data files. When the hash is attained, it is shifted to the blockchain through a smart contract.

Zhang et al.[16] proposed an identity-based proxy-oriented outsourcing using public auditing system in a cloud-based MCPS. Xu et al.[17] proposed a certificate less signature system, according to an N-th degree Truncated polynomial Ring Units (NTRU) lattice. The performance evaluation and security analyses demonstrate that the presented method attains considerably decreased computation and communication cost. In AlZubi et al.,[18] the cognitive machine learning (ML)-supported attack detection architecture was presented for sharing medical data safely. The MCPS was capable of spreading the gathered data to cloud storage. The ML model predicts cyberattack behavior, and processing this data provides medical specialist decision support. This presented method is a patient centric model that safeguards the data on trusted devices such as end user smartphones and controls data sharing access. In Nguyen et al.,[19] a secure intrusion detection system (IDS) scheme via blockchain-based data transmission using a classification method for a CPS in the medical field was proposed. The presented models perform IDS with a deep belief network (DBN) approach. Additionally, the proposed method employs an multiple share creation (MSC) approach to create many shares of the gathered image and thus attains security and privacy. Also, the blockchain technologies are employed to secured data transmission for the cloud servers that execute the ResNet method to find the existence of the diseases. Though various models exist in the literature, designing an effective security-based solution with a disease diagnosis model for the MCPS environment is needed.

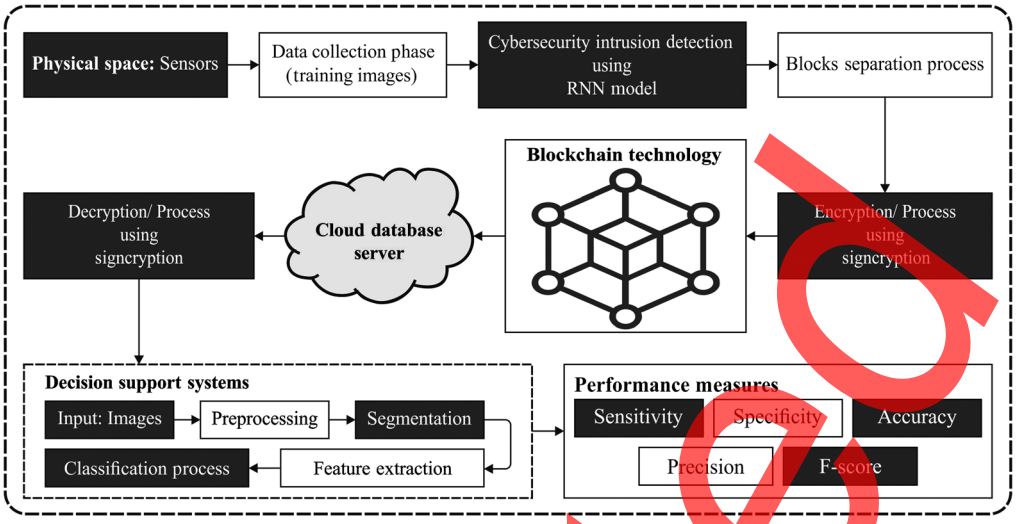

Fig. 2 Block diagram of the BESITD technique.

3 Proposed Model

In this study, an innovative BESITD technique is derived for secure image transmission and diagnosis in the MCPS environment. The proposed model involves different subprocesses, namely, image acquisition, RNN-based intrusion detection, signcryption-based block-wise encryption, blockchain-based secure transmission, and disease diagnosis. The proposed model initially enables the wearable devices, such as smartphones, smart watches, and Internet of Medical Things (IoMT) devices, to collect the medical images of the patient. Then, the RNN model is executed to determine the existence of intrusions in the network. Next, the medical images are divided into n blocks, and the block-wise encryption process is carried out using the signcryption approach. Finally, the encrypted image along with the hash value is stored in the blockchain and is transmitted securely to the cloud server, where the actual disease diagnosis process takes place. Figure 2 shows the overall block diagram of BESITD model.

3.1 *RNN-Based Intrusion Detection*

At the initial stage, the RNN model is used for the detection of intrusions in the MCPS environment. The RNN is a familiar type of DL model that uses past output to estimate the succeeding outcome. The network has repetitive loops, which are the hidden neurons. It enables the storage of past input data and thereby predicts the forthcoming output. The outcome of the hidden layer is resent t times to the hidden layer. The outcome of the recursive neuron is passed to the succeeding layers upon the completion of maximum iterations.[20] Finally, the errors are provided backward for updating weights. The RNN consists of a set of NN organized altogether, in which every NN transmits a message to the other NNs. They hold a memory for storing knowledge regarding the known data; however, the memory is short-term and cannot handle long-term data. The RNN encompasses an internal memory h_t, as defined in the following:

$$h_t = g(Wx_t + U_f h_{t-1} + b), \tag{1}$$

where $g()$ represents an activation function, U and W are weight matrices of the h layer, b is a bias, and X indicates the input vector.

3.2 *Block-Wise Encryption Technique*

In the block-wise encryption technique, the medical images are divided into a set of n individual blocks. Every block is encrypted by the use of the signcryption technique. Signcryption is an effective technique used to satisfy the components of a digital signature and key encryption.

The characteristics of signcryption are confidentiality, non-forgeability, integrity, and non-repudiation. Some signcryption approaches hold extra attributes, namely, public verifiability and forward secrecy of message confidentiality. In this study, the signcryption technique encompasses three stages, namely, key generation, signcryption, and unsigncryption. It defines a public-key primitive that offers privacy and security. It concurrently executes the process of digital signature and encryption. The process begins with the initialization of the prime number, hash function, and key. For improving the security level, the signcryption technique uses ideal private keys.

Initialization: L_P large prime number, L_f large prime factor, I integer with order L_f modulo L_P, chosen randomly from $[1, \ldots L_P - 1]$, *Hash* One way hash function, with an output of at least 128 bits, L_P keyed one way hash function, and D value.

The sender key pair $((M_{k1}, N_{k1}))$ of the signcryption technique is defined as follows:

$$M_{k1} = Q^{A_{k1}} \bmod L_P. \tag{2}$$

In addition, , the receiver key pair $((M_{k1}, N_{k1}))$ of the signcryption technique isresented using Eq. (3)

$$N_{k2} = Q^{A_{k2}} \bmod L_P. \tag{3}$$

3.3 *Blockchain-Based Secure Transmission*

At this stage, the encrypted block of images and the hash value of the input medical image are securely sent to the cloud via blockchain technology. Blockchain relates to a collection of records that are chronologically chained together with cryptography. It can be categorized into two main classes: permissioned chain and public chain. A public chain is similar to the Internet; all users of this record systems can detect this chain and access it. Alternatively, a permissioned chain permits validated entity to add to and read the records. In addition, a consortium blockchain is a hybrid type among permissioned and public chains; however, it is similar to a private chain. It is supervised and permissioned by a predefined set of entities. The chain structure ensures the immutability of blockchain record systems. When blocks exist in this chain, one cannot make a change in prior blocks. Traditional databases are similar to an individual screenshot of data; however, the blockchain is like a chain of time-stamped screenshots. There exists a continuity in time and degree of freedom that allows the blockchain to trace the history of these record systems.

In general, a blockchain employs "consensus" for adding a new data record (not replacing them). But conventional database uses "permission" to handle data. It has centralized maintenance and administration. In the Bitcoin scheme, i.e., one of the familiar applications of public blockchain, proof-of-work (PoW) is employed for reaching this consensus. PoW is a type of arithmetical "puzzle." The secret of these puzzles (e.g., nonce) is difficult to recognize; however, it is easier to prove. The procedure for detecting the nonce is known as "mining." The initial miner who discovers the secret adds the blocks to a longer chain and is rewarded through a Bitcoin. In these decentralized systems, complete duplicate files of transaction records are placed with distinct network miners.[21] The confirmation and verification of every transaction are treated according to the consensus approach. Not even an individual third party entity can completely control the procedure in this peer-to-peer network. Unlike, a distributed system also processes transactions in distinct places; however, it might remain in the control of an individual entity.

Specifically, there are major differences among decentralized and distributed schemes. To reiterate, blockchain is a decentralized scheme that shifts the right of governance from a centralized third entity to a single entity in these records. In contrast to the Bitcoin networks, Ethereum embraces smart contracts, a type of performable script kept on the blockchain. Rather than PoW, Ethereum employs proof-of-stake as its consensus method. This consensus approach chooses the blocks validator randomly, with the one having extra stakes having a higher possibility of being elected. These blockchain nodes are significant and consume more energy.

In this study, a consortium blockchain system in which the users in the blockchain network are trusted users is utilized. For example, hospital authorities and health research institutes can develop a consortium blockchain for medical data transmission between them. In addition, the consortium blockchain is a proper solution that does not involve any untrusted party to connect the blockchain network and attain access to the private healthcare data. The encrypted medical image is saved in the database of the hospital (say A). A transaction block is created and is included in the blockchain. If any user needs to access the shared medical data, they need to verify the integrity of the shared data at the receiving side. The user determines the hash value of the received image and undergoes comparison with the blockchain to ensure the integrity. This blockchain technology can be realized with any familiar blockchain frameworks, such as Hyperledger Fabric and Ethereum.

3.4 *Design of Disease Diagnosis Module*

At the cloud server side, the disease diagnostic process gets executed using different subprocesses, namely, multilevel thresholding-based segmentation, MobileNet-based feature extraction, and OKELM-based classification. In addition, an MOPO technique is designed to fine-tune the threshold values and parameters involved in the KELM model.

3.4.1 *Overview of political optimizer*

The PO is stimulated from the western political procedure of optimization, involving two processes. The initial consideration is that every citizen attempts to optimize their tendency to win the election. The next consideration is that every party tries to attain many seats in the parliament. The general process of political optimizer (PO) includes five levels, namely, party formation and constituency allocation, election campaign, party switching, interparty election, and parliamentary affair.[22] The detailed working of PO is mathematically defined here. The whole population is separated into n political parties, as given in Eq. (4)

$$P = \{P_1, P_2, P_3, \ldots, P_n\}. \tag{4}$$

Each part includes n party members, as follows:

$$P_i = \{p_i^1, p_i^2, p_i^3, \ldots, p_{\text{in}}\}. \tag{5}$$

Every party member comprises d dimensions, as shown in Eq. (6)

$$p_i^j = [p_{i,1}^j, p_{i,2}^j, p_{i,3}^j, \ldots, p_{i,d}^j]^T. \tag{6}$$

Every individual solution represents an election candidate. Let there be n electoral districts, as follows:

$$C = \{C_1, C_2, C_3, \ldots, C_n\}. \tag{7}$$

Let n members be present in every constituency, as follows:

$$c_j = \{p_1^j, p_2^j, p_3^j, \ldots, p_n^j\}. \tag{8}$$

The party leader is represented by the member with the greatest influence in a party, as follows:

$$q = \text{argmin}_{1\le j\le n} f(p_1^j), \qquad \forall\ i\varepsilon\{1, \ldots, n\}, \tag{9}$$

$$p_i^* = p_i^q.$$

Every individual party leader is defined as follows:

$$P^* = \{p_1^*, p_2^*, p_3^*, \ldots, p_n^*\}. \tag{10}$$

The victors of the diverse constituencies are known as parliament members, as shown in Eq. (11)

$$C = \{c_1^*, c_2^*, c_3^*, , c_n^*\}. \tag{11}$$

At the time of the election campaign, Eqs. (12) and (13) are applied to upgrade the location of the significant solutions

$$p_{i,k}^j(t+1) = \begin{cases} \text{if } p_{i,k}^j(t-1) \le m^* \le p_{ik}^j(t) \text{ or } p_{i,k}^j(t-1) \ge m^* \ge p_{i,k}^j(t) \ge m^*, \\ m^* + r(m^* - p_{i,k}^j(t)); \\ \text{if } p_{i,k}^j(t-1) \le m^* \le p_{ik}^j(t) \text{ or } p_{i,k}^j(t-1) \ge m^* \ge p_{i,k}^j(t) \ge (t), \\ m^* + (2r-1)|m^* - p_{i,k}^j(t)|; \\ \text{if } m^* \le p_{i,k}^j(t-1) \le m^* \le p_{ik}^j(t) \text{ or } m^* p_{i,k}^j(t-1) \ge m^* \ge p_{i,k}^j(t), \\ m^* + (2r-1)|m^* - p_{i,k}^l(t-1)| \end{cases} \tag{12}$$

$$p_{i,k}^j(t+1) = \begin{cases} \text{if } p_{i,k}^j(t-1) \le p_{ik}^j(t) \le m^* \text{ or } p_{i,k}^j(t-1) \ge p_{i,k}^j(t) \ge m^*, \\ m^* + (2r-1)|m^* - p_{i,k}^j(t)|; \\ \text{if } p_{i,k}^j(t-1) \le m^* \le p_{ik}^j(t) \text{ or } p_{i,k}^j(t-1) \ge m^* \ge p_{i,k}^j(t) \ge (t), \\ p_{i,k}^j(t-1) + r p_{ik}^j(t) - p_{i,k}^j(t-1); \\ \text{if } m^* \le p_{i,k}^j(t-1) \le p_{ik}^j(t) \text{ or } m^* \ge p_{i,k}^j(t-1) \ge m^* \ge p_{i,k}^j(t), \\ m^* + (2r-1)|m^* - p_{i,k}^j(t-1)| \end{cases} \tag{13}$$

For balancing the exploration as well as exploitation, party switching is used. An adaptive parameter λ is employed that is linearly reduced from 1 to 0. Every individual candidate is chosen based on the probability λ and replaced with a worse member of an arbitrarily selected party, as formulated below:

$$q = \underset{i \le j \le n}{\text{argmax}} f(p_i^j). \tag{14}$$

During the election phase, the winner in a constituency is attained using Eq. (15)

$$q = \underset{i \le j \le n}{\text{argmin}} f(p_i^j), \tag{15}$$

$$c_j^* = p_q^j.$$

3.4.2 *Multilevel thresholding-based image segmentation*

During image segmentation, the medical image is segmented using the multilevel thresholding technique. In multilevel thresholding, the original images are separated into nc number of classes with $nc - 1$ number of thresholds of $\{T_1, T_2, \ldots, T_{nc-1}\}$. This threshold acts as separators among the successive classes of $\{C_1, C_2, \ldots, C_{nc}\}$ in the interval of threshold value of $\{[0, \ldots, T_1], [T_1 + 1, \ldots, T_2], [T_{nc-1} + 1, \ldots, L]\}$, where L denotes the maximum pixel intensity values of the grayscale images. In the proposed model, every individual is determined as the threshold level, and the self-adaptive parameter is decision variable in the vector formation as defined below

$$I_i = [\, T_i^1, T_i^2, \ldots, T_i^{nc-1}, s_i, a_i, c_i, f_i, e_i, \gamma_i, \omega_i]. \tag{16}$$

The proposed model searches for an optimum threshold value using PO by increasing a fitness function F, based on the threshold value.[23] The objective function of Kapur's entropy algorithm, nc dimension functions of increasing the total entropy, is deliberated as fitness function (FF)

$$\text{Maximize } F = \sum_{k=1}^{nc} H_k, \tag{17}$$

where H_k represents the k'th entropy and is evaluated by

$$\begin{matrix} H_1 \sum_{i=0}^{T_1} \frac{p_i}{X_1} \ln\left(\frac{p_i}{X_1}\right); & X_1 \sum_{i=0}^{T_1} p_i \\ H_2 \sum_{i=1+T_1}^{T_2} \frac{p_i}{X_2} \ln\left(\frac{p_i}{X_2}\right) & X_2 \sum_{i=1+T_1}^{T_2} p_i \\ \vdots & \vdots \\ H_{nc} \sum_{i=1+T_{nc-1}}^{L} \frac{p_i}{X_{nc}} \ln\left(\frac{p_i}{X_{nc}}\right) & X_{nc} = \sum_{i=1+T_{nc}-1}^{L} p_i \end{matrix} \tag{18}$$

where p_j signifies the likelihood distribution at the i'th intensity level of the image as follows:

$$p_j = \frac{h_i}{np}; i \in \{0,1,\ldots,L\}, \tag{19}$$

where h_i means the pixel count representing the i'th intensity levels, np represents the overall pixel count in the image, and χ_j represents the likelihood of set C_i. To determine the threshold value of the segmentation technique, the MOPO algorithm is applied.

3.4.3 *MobileNet-based feature extraction*

Next to image segmentation, the features are extracted by the MobileNet model, which is an efficient framework that employs depth-wise separable convolution for constructing lightweight deep convolution neural network (DCNN) and provides a streamlined architecture for embedded and mobile vision applications.[24] The MobileNet model offers reduced network size, a fewer number of parameters, faster performance, and low latency. The architecture of MobileNet depends upon a depth-wise separable filter, as shown in Fig. 3. The depth-wise separable convolutional filter is made up of a depth-wise convolutional filter and a point convolutional filter. The depth-wise convolutional filters perform a single convolutional on every input channel, and the point convolutional filter combines the output of depth-wise convolutions consecutively with 1×1 convolution.

The MobileNet architecture is a network method utilizing depth-wise separable convolutions as its fundamental units. Its depth-wise separable convolutions contain two layers: depth-wise and point convolutional layers. The Dense1-MobileNet method considers the depth-wise convolutional layers and the point convolutional layers to be two separate convolutional layers, viz., the input feature map of every depth-wise convolutional layer in the dense blocks is the superposition of the output feature map in the prior convolutional layers and hence the input feature map of every deep convolutional layer. Since the depth-wise convolutional layer is a single channel convolution, the number of output feature map of the middle depth-wise convolutional layers is similar to the input feature map, i.e., the amounts of output feature map of all prior convolutional layers.

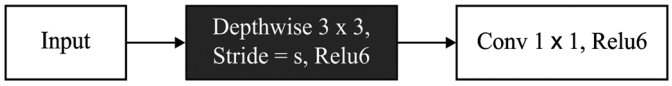

Fig. 3 Structure of MobileNet.

3.4.4 *OKELM-based image classification*

The OKELM model receives the feature vectors as input to perform the classification process. The KELM is an extension approach of the single hidden layer feedforward neural network (SLFN) algorithm that is employed on clustering, regression, and classification methods.[25] As opposed to the conventional artificial neural network (ANN), ELM has a stochastic nature. It arbitrarily assigns the input weight and the hidden layer bias, and retains them fixed without tuning iteratively. The KELM was presented to attain an optimal predictive stability and performance compared with the ELM model with a lower computation cost. The output of ELM for normalized SLFN is given by

$$F_t = \sum_{i=1}^{N} \beta_i h(a_i \cdot x_j + b_i)_j, \qquad j = 1, \ldots, N, \tag{20}$$

where a_i signifies the weight vector connecting the i'th hidden nodes and input node; β_i represents the weight vector linking the j'th hidden nodes and the output node; b_i denotes the threshold of the i'th hidden nodes; and h indicates the feature mapping of the hidden node. The training goal is to detect an optimal output weight β, which is calculated using the least-square approach

$$\beta = H^{\dagger} T, \tag{21}$$

where $H^{\uparrow}$ represents the Moore–Penrose (MP) normalized inverse of the hidden layer outputs and $T = [t_1, t_2, \ldots, t_N]^T$ represents the target vector. For difficult predictive tasks, the hidden layer feature map is usually not known. Therefore, the kernel functions are presented for replacing the feature mapping functions. Based on the orthogonal prediction technique, the MP normalized inverse matrix $H^{\dagger}$ is computed as $H^{\dagger} = H^T(HH^T)^{-1}$, and the output weight β is evaluated by including a positive constant, $1/C$. Therefore, the output functions of KELM is described briefly as follows:

$$F(x) = h\beta = h(x)H^{\dagger}\left(\frac{\mathrm{I}}{C} + HH^{\dagger}\right)^{-1} T = \begin{Bmatrix} K(x_1, x) \\ \vdots \\ K(x_N, x) \end{Bmatrix} \left(\frac{J}{C} + \Omega_{\mathrm{ELM}}\right)^{-1} T, \tag{22}$$

where $K(x_i, x)$ denotes the kernel function and needs to fulfil the Mercer conditions. In this work, Gaussian kernels are employed as . Hence, the key variables of KELM are standardization variable C and kernel parameter γ, which need to be optimally tuned using PO. The PO derives a fitness function based on 10-fold cross validation, in which the training dataset is split into 10 mutually exclusive subsets of approximately equivalent size. Among them, nine sets are employed for training the model, and the final set is applied for testing the model. This process is iterated 10 times, and thereby only one set is utilized for testing. The fitness function is represented as $1 - CA_{\mathrm{validation}}$ of the 10-fold cross validation technique. In addition, the solution with maximum $CA_{\mathrm{validation}}$ has a lower fitness value

$$\mathrm{Fitness} = 1 - CA_{\mathrm{validation}}, \tag{23}$$

$$CA_{\mathrm{validation}} = 1 - \frac{1}{10}\sum_{i=1}^{10}\left|\frac{y_c}{y_c + y_f}\right| \times 100, \tag{24}$$

where y_c and y_f denote the total number of true and false classification outcomes.

4 Performance Validation

This section validates the performance of the BESITD technique with different dimensions. First, the security performance of the BESITD technique is investigated against the NSL-KDD2015 and CIDDS-001 datasets. The NSL-KDD2015 dataset includes 125,973 instances with 41 attributes, and the CIDDS-001 dataset has 1,018,950 instances with 14 features. The results are

Table 1 Results analysis of the BESITD technique on intrusion detection.

Measures	NSL-KDD 2015	CIDDS-001
Precision	98.99	99.09
Recall	99.43	98.90
Accuracy	99.24	99.03
F-score	98.76	98.98

examined in terms of different measures, such as accuracy, precision, recall, and *F*-score.[26] Table 1 and Fig. 4(b) shows the intrusion detection results of the BESITD technique on the applied two datasets.

With the NSL-KDD 2015 dataset, the BESITD technique resulted in an increased precision of 98.99%, recall of 99.43%, accuracy of 99.24%, and *F*-score of 98.76%. In addition, on the CIDDS-001 dataset, the BESITD approach accomplished an improved precision of 99.09%, recall of 98.90%, accuracy of 99.03%, and F-score of 98.98%.

Table 2 and Fig. 5 illustrate the accuracy analysis of the BESITD technique with existing techniques. The figure shows that the CS-PSO (2019) and gradient boosting (2018) models

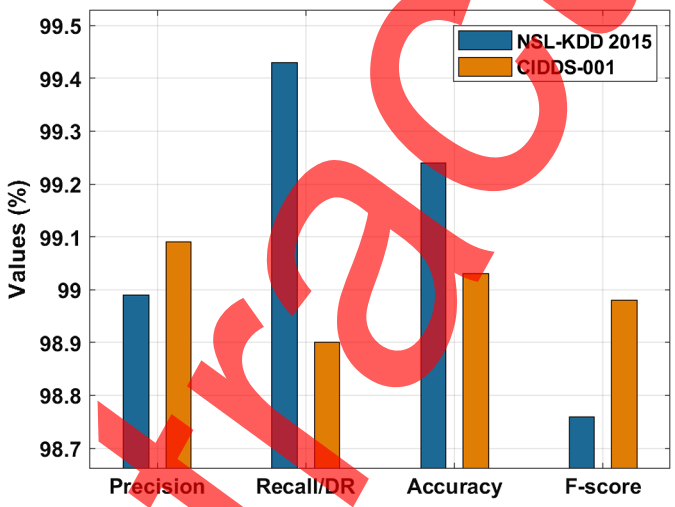

Fig. 4 Result analysis of the BESITD model with different measures.

Table 2 Accuracy analysis of the BESITD technique with existing techniques.

Methods	Accuracy
BESITD	99.24
DBN model	98.95
Cuckoo optimization	96.88
CS-PSO	75.51
Behavior-based IDS	98.89
Gaussian process	91.06
DNN + SVM	92.03
GA + fuzzy	96.53
Fuzzy C-means	95.30
Gradient boosting	84.25

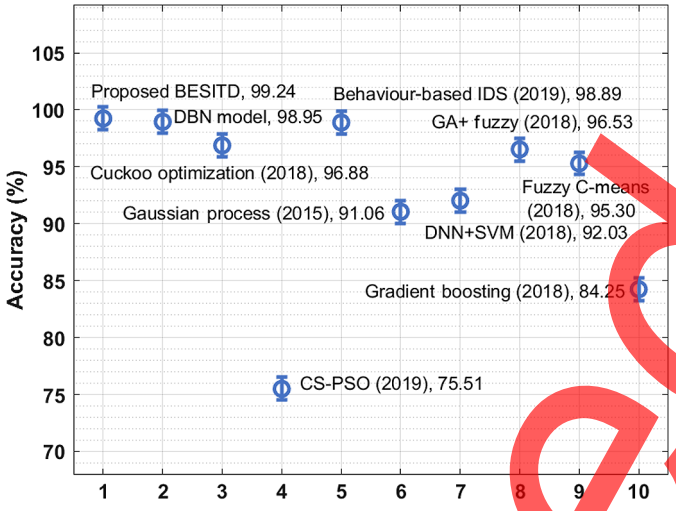

Fig. 5 Accuracy analysis of the BESITD model with existing techniques.

obtained a lower accuracy of 75.51 and 84.25, respectively. In addition, the Gaussian process (2015) and deep neural network (DNN) + support vector machine (SVM) (2018) techniques obtained a slightly enhanced accuracy of 91.06 and 92.03, respectively. Likewise, the fuzzy c-means (FCM) (2018) and genetic algorithm (GA) + Fuzzy (2018) techniques accomplished close accuracy values of 95.30 and 96.53, respectively. Similarly, the cuckoo optimization (2018), behavior-based IDS (2019), and DBN models demonstrate superior accuracy of 96.88, 98.89, and 98.95, respectively. However, the BESITD technique resulted in a superior performance with the maximum accuracy of 99.24.

The performance of the BESITD technique is validated using the ISIC dataset.[27] The BESITD technique includes a number of instances in different classes, namely, angioma, nevus, lentigo NOS, solar lentigo, melanoma, seborrheic keratosis, and basal cell carcinoma. Figure 6 shows the sample images.

Figure 7 shows the results of the analysis of the BESITD technique. Figure 7(a) shows the sample input images, and the corresponding encrypted versions are given in Fig. 7(b). The figures ensure that the input images are completely encrypted and are not meaningful.

The performance of the BESITD technique with existing techniques in terms of PSNR and CC is given in Table 3. Figure 8 shows the PSNR analysis of the BESITD technique for different images. The figure shows that the BESITD technique accomplished an effective outcome with

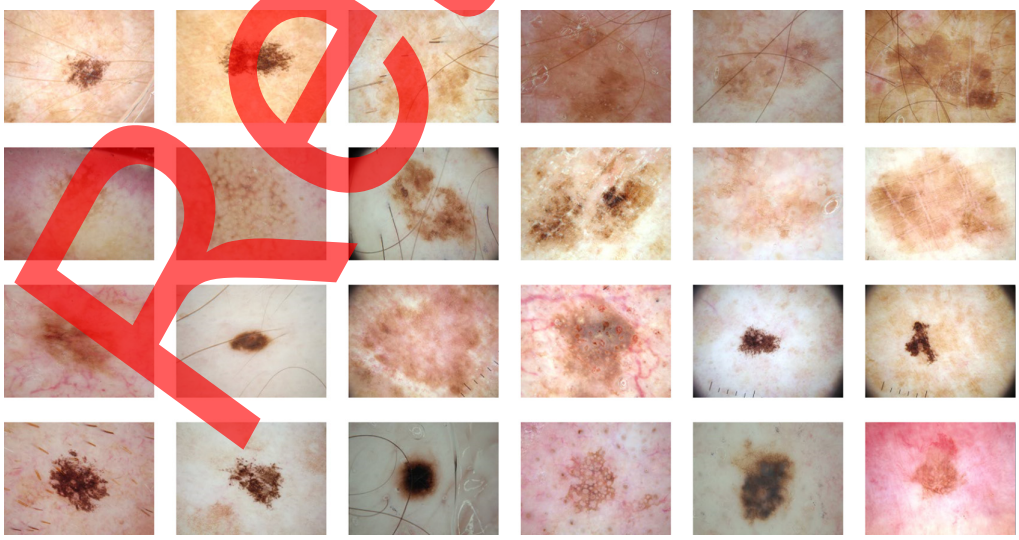

Fig. 6 Sample images.

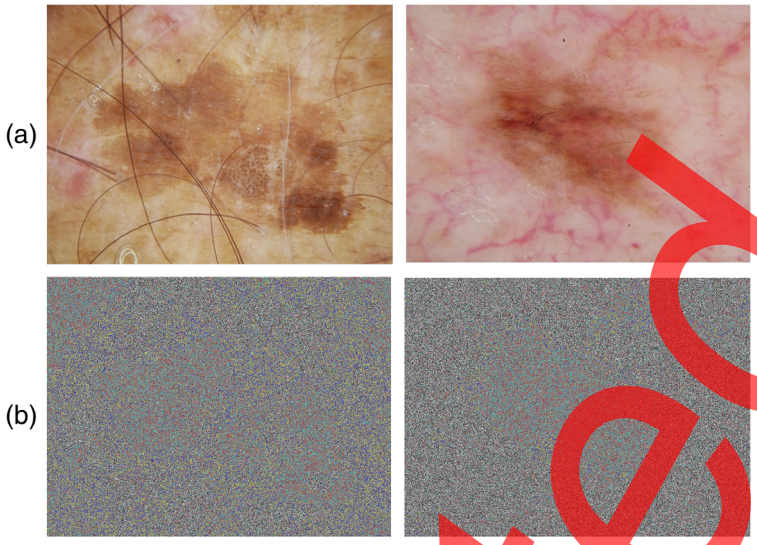

Fig. 7 Sample output: (a) original images and (b) encrypted images.

Table 3 Result analysis of BESITD with existing methods in terms of PSNR and CC.

	PSNR (dB)				Correlation coefficient			
Samples	BESITD	MSC-SC	PSO	GWO	BESITD	MSC-SC	PSO	GWO
Image 1	55.87	54.89	50.98	51.52	99.90	99.90	99.70	99.80
Image 2	56.32	53.87	49.32	50.90	99.90	99.80	99.50	99.60
Image 3	53.90	51.65	50.57	50.98	99.90	99.70	99.60	99.70
Image 4	55.29	52.41	49.41	50.04	99.80	99.70	99.40	99.50

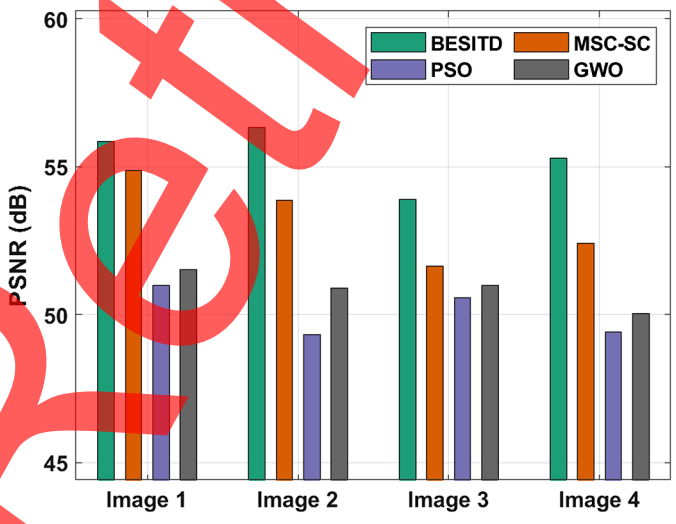

Fig. 8 PSNR analysis of the BESITD model with different measures.

the maximum PSNR value. For instance, with image 1, the BESITD technique resulted in a higher PSNR of 55.87 dB, whereas the MSC-SC, PSO, and GWO techniques obtained a lower PSNR of 54.89, 50.98, and 51.52 dB, respectively. Also, with image 2, the BESITD technique resulted in an increased PSNR of 56.32 dB, whereas the MSC-SC, PSO, and GWO techniques

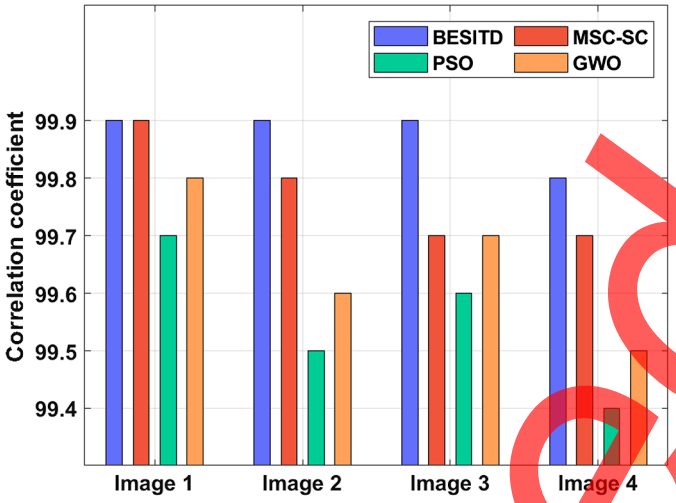

Fig. 9 CC analysis of the BESITD model with distinct images.

reached a lower PSNR of 53.87, 49.32, and 50.90 dB, respectively. In addition, with image 3, the BESITD algorithm resulted in a higher PSNR of 53.90 dB, whereas the MSC-SC, PSO, and GWO methods obtained a lower PSNR of 51.65, 50.57, and 50.98 dB, respectively. Finally, with image 4, the BESITD approach resulted in an increased PSNR of 55.29 dB, whereas the MSC-SC, PSO, and GWO methods attained a lesser PSNR of 52.41, 49.41, and 50.04 dB, respectively.

Figure 9 shows the CC analysis of the BESITD technique for different images. The figure stated that the BESITD technique accomplished an effectual outcome with the maximum CC value. For instance, with image 1, the BESITD technique resulted in a higher CC of 99.90, whereas the MSC-SC, PSO, and GWO techniques obtained a lower CC of 99.90, 99.70, and 99.80, respectively. Also, with image 2, the BESITD technique resulted in a higher CC of 99.90, whereas the MSC-SC, PSO, and GWO methods obtained a lower CC of 99.80, 99.50, and 99.60, respectively.

In addition, with image 3, the BESITD technique resulted in a higher CC of 99.90, whereas the MSC-SC, PSO, and GWO techniques gained a lower CC of 99.70, 99.60, and 99.70, respectively. Moreover, with image 4, the BESITD technique resulted in a higher CC of 99.80, whereas the MSC-SC, PSO, and GWO algorithms obtained a lesser CC of 99.70, 99.40, and 99.50, respectively.

Table 4 shows a brief comparative analysis of the BESITD technique with existing techniques. Figure 10 shows the sensitivity analysis of the BESITD technique with existing techniques. The figure shows that the MD-DLN and DF-RCN models obtained a lower sensitivity of 0.8200 and 0.8540, respectively, followed by the ResNet-50 and C-YOLO-GC approaches,

Table 4 Comparison of BESITD with existing techniques.

Methods	Sensitivity	Specificity	Accuracy
Proposed BESITD	0.9843	0.9897	0.9816
CNN-ResNet 101	0.9612	0.9802	0.9485
VGG-19	0.9500	0.6800	0.8120
ResNet-50	0.9000	0.6100	0.7550
MD-DLN	0.8200	0.9780	0.9320
DF-RCN	0.8540	0.9669	0.9403
C-YOLO-GC	0.9082	0.9268	0.9339

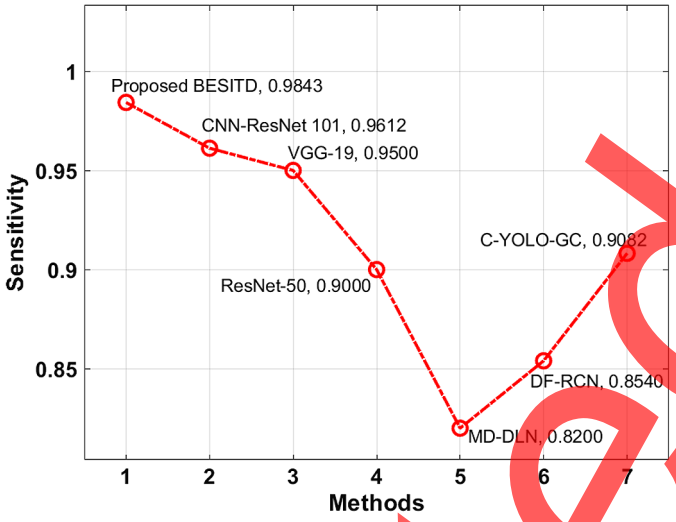

Fig. 10 Sensitivity analysis of the BESITD model with existing techniques.

which reached a slightly improved sensitivity of 0.9000 and 0.9082, respectively. Concurrently, the VGG-19 and CNN-ResNet 101 techniques accomplished close sensitivity values of 0.9500 and 0.9612, respectively. However, the BESITD technique resulted in a higher performance with the maximum sensitivity of 0.9843.

Figure 11 shows the specificity analysis of the BESITD technique with existing techniques. The figure shows that the ResNet-50 and VGG-19 models obtained a lower specificity of 0.6100 and 0.6800, respectively, and the C-YOLO-GC and DF-RCN techniques achieved a slightly improved specificity of 0.9268 and 0.9669, respectively. At the same time, the MD-DLN and CNN-ResNet 101 techniques accomplished close specificity values of 0.9780 and 0.9802, respectively. Finally, the BESITD methodology resulted in a higher performance with the maximum specificity of 0.9897.

Figure 12 shows the accuracy analysis of the BESITD technique with existing techniques. The figure shows that the VGG-19 and ResNet-50 models obtained a lower accuracy of 0.8120 and 0.7550, respectively, followed by the MD-DLN and C-YOLO-GC techniques, which obtained a slightly enhanced accuracy of 0.9320 and 0.9339, respectively. Simultaneously, the CNN-ResNet 101 and DF-RCN techniques accomplished close accuracy values of 0.9485 and 0.9403, respectively. However, the BESITD technique resulted in a superior performance with the maximum accuracy of 0.9816.

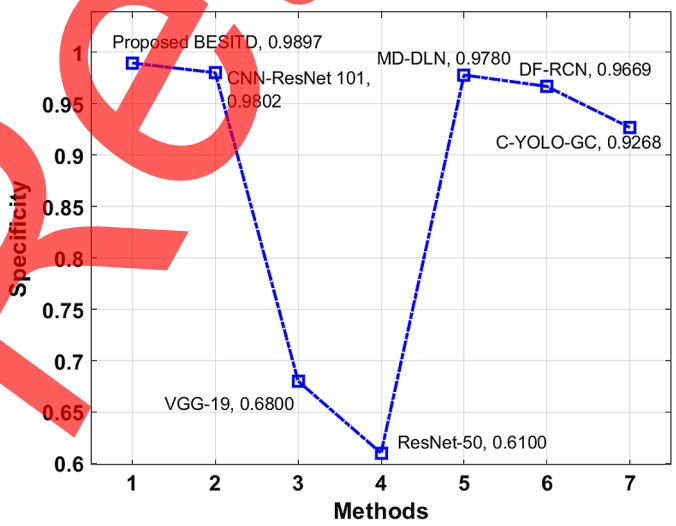

Fig. 11 Specificity analysis of the BESITD model with existing techniques.

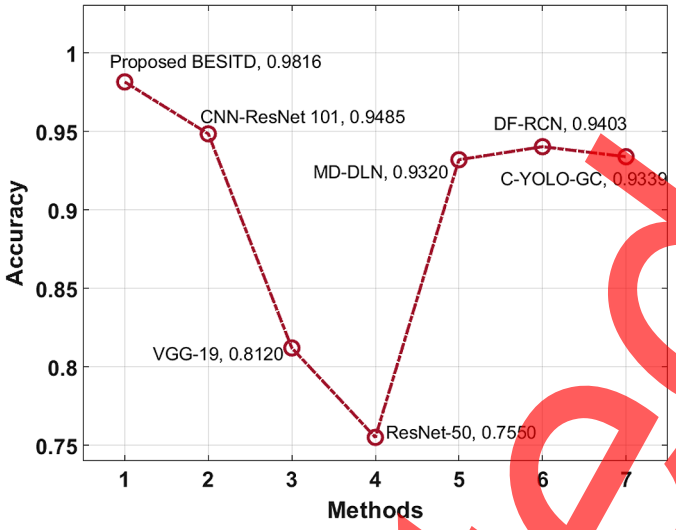

Fig. 12 Accuracy analysis of the BESITD model with existing techniques.

From the detailed results and discussion, it can be seen that the BESITD technique has superior performance over the other methods for all aspects. The enhanced performance of the BESITD technique is due to the inclusion of the MOPO algorithm for the optimal threshold selection and parameter tuning of the KELM model. Therefore, the BESITD technique can be employed as an effective tool for secure image transmission and disease diagnostic processes in the MCPS environment.

5 Conclusion

In this study, an innovative BESITD technique is derived for secure image transmission and diagnosis in the MCPS environment. The proposed model involves different subprocesses, namely, image acquisition, RNN-based intrusion detection, signcryption-based block-wise encryption, blockchain-based secure transmission, and disease diagnosis. In addition, the disease diagnosis process involves several subprocesses, such as multilevel thresholding-based segmentation, MobileNet-based feature extraction, and OKELM-based classification. In addition, the design of MOPO for the optimal threshold selection and parameter tuning of the KELM model considerably increases the diagnostic performance. To ensure the enhanced performance of the BESITD technique, a comprehensive experimental analysis was conducted on two benchmark datasets, and the results are inspected in terms of different evaluation metrics. The experimentation results highlight the promising performance of the BESITD technique over the recent techniques with the maximum accuracy of 0.9816. The enhanced performance of the BESITD technique makes it possible to apply the BESITD technique for secure image transmission and disease diagnostic processes in the MCPS environment. As a part of future work, image steganography and data hiding techniques can be designed to further increase the level of security in the MCPS environment.

References

1. H. Rathore, A. Mohamed, and M. Guizani, "A survey of blockchain enabled cyber-physical systems," *Sensors* **20**(1), 282 (2020).
2. K. T. Smith, M. Smith, and J. L. Smith, "Case studies of cybercrime and its impact on marketing activity and shareholder value," *Acad. Mark. Stud. J.* **15**, 67 (2011).
3. I. Lee and O. Sokolsky, "Medical cyber physical systems," in *Proc. CPS Demystified Session*, Anaheim, CA, pp. 743–748 (2010).
4. X. J. Zhang, et al., "Identity-based proxy-oriented outsourcing with public auditing in cloud-based medical cyber-physical systems," *Pervasive Mob. Comput.* **56**, 18–28 (2019).

5. C. Yi et al., "Blockchain-based medical records secure storage and medical service framework," *J. Med. Syst.* **43**, 5–13 (2019).
6. A. D. Liu et al., "Research progress of blockchain technology and its application in information security," *J. Software* **29**, 270–293 (2018).
7. J. Sengupta, S. Ruj, and S. Das Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *J. Network Comput. Appl.* **149**, 102481–102500 (2020).
8. B. Adanur, B. Bakir-Güngör, and A. Soran, "Blockchain-based fog computing applications in healthcare," in *28th Signal Process. and Commun. Appl. Conf.*, pp. 1–4 (2020).
9. S. P. Mohanty et al., "PUFchain: a hardware-assisted blockchain for sustainable simultaneous device and data security in the Internet of Everything (IoE)," *IEEE Consum. Electron. Mag.* **9**(2), 8–16 (2020).
10. X. Cheng et al., "Design of a secure medical data sharing scheme based on blockchain," *J. Med. Syst.* **44**(2), 1–11 (2020).
11. X. Zhou et al., "A threshold signature scheme without trusted center for blockchain-based medical cyber-physical systems," in *Telecommunication Systems*, pp. 1–9 (2021).
12. H. Qiu et al., "Privacy-preserving health data sharing for medical cyber-physical systems," arXiv:1904.08270 (2019).
13. H. Shu et al., "An efficient certificateless aggregate signature scheme for blockchain-based medical cyber physical systems," *Sensors* **20**(5), 1521 (2020).
14. F. Chen et al., "Blockchain-based efficient device authentication protocol for medical cyber-physical systems," *Secur. Commun. Networks* **2021**, 5580939 (2021).
15. S. L. Vangipuram, S. P. Mohanty, and E. Kougianos, "CoviChain: a blockchain based framework for nonrepudiable contact tracing in healthcare cyber-physical systems during pandemic outbreaks," *SN Comput. Sci.* **2**(5), 1–16 (2021).
16. X. Zhang et al., "Identity-based proxy-oriented outsourcing with public auditing in cloud-based medical cyber-physical systems," *Pervasive Mob. Comput.* **56**, 18–28 (2019).
17. Z. Xu et al., "Efficient NTRU lattice-based certificateless signature scheme for medical cyber-physical systems," *J. Med. Syst.* **44**(5), 1–8 (2020).
18. A. A. AlZubi, M. Al-Maitah, and A. Alarifi, "Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques," *Soft Comput.* **25**, 12319–12332 (2021).
19. G. N. Nguyen et al., "Secure blockchain enabled cyber-physical systems in healthcare using deep belief network with ResNet model," *J. Parallel Distrib. Comput.* **153**, 150–160 (2021).
20. H. Apaydin et al., "Comparative analysis of recurrent neural network architectures for reservoir inflow forecasting," *Water* **12**(5), 1500 (2020).
21. M. H. Rehmani, "Blockchain fundamentals and working principles," in *Blockchain Systems and Communication Networks: From Concepts to Implementation*, pp. 23–59, Springer, Cham (2021).
22. A. Zhu et al., "Political optimizer with interpolation strategy for global optimization," *PLoS One* **16**(5), e0251204 (2021).
23. R. K. Sambandam and S. Jayaraman, "Self-adaptive dragonfly based optimal thresholding for multilevel segmentation of digital images," *J. King Saud Univ.-Comput. Inf. Sci.* **30**(4), 449–461 (2018).
24. W. Wang et al., "A novel image classification approach via dense-MobileNet models," *Mob. Inf. Syst.* **2020**, 7602384 (2020).
25. S. Chen et al., "Prediction, monitoring, and interpretation of dam leakage flow via adaptative kernel extreme learning machine," *Measurement* **166**, 108161 (2020).
26. J. Uthayakumar, T. Vengattaraman, and P. Dhavachelvan, "Swarm intelligence based classification rule induction (CRI) framework for qualitative and quantitative approach: an application of bankruptcy prediction and credit risk analysis," *J. King Saud Univ.-Comput. Inf. Sci.* **32**(6), 647–657 (2020).
27. V. Rotemberg et al., "A patient-centric dataset of images and metadata for identifying melanomas using clinical context," *Sci. Data* **8**, 34 (2021).

Padmavathi Udayakumar received her ME degree in computer science and engineering from Annamalai University, Chidambaram, India, in 2011. Currently, she is pursuing her PhD at National Institute of Technology Puducherry, Karaikal, India. Her research interests include blockchain, networks, and security.

Narendran Rajagopalan received his PhD from NIT Tiruchirappalli in 2013 and is currently serving as an assistant professor and head in the Department of Computer Science and Engineering, National Institute of Technology Puducherry, India. His research interests include networking, security, and quality of service.