Cluster Computing (2023) 26:2245–2257
https://doi.org/10.1007/s10586-022-03654-8

Deep learning with metaheuristics based data sensing and encoding scheme for secure cyber physical sensor systems

Ala' A. Eshmawi[1] · Mashael Khayyat[2] · S. Abdel-Khalek[3] · Romany F. Mansour[4] · Umesh Dwivedi[5] · Krishna Kumar joshi[5] · Deepak Gupta[6]

Received: 5 January 2022 / Revised: 6 May 2022 / Accepted: 17 June 2022 / Published online: 17 August 2022

Abstract
Cyber Physical System (CPS) plays an important role in industry 4.0 applications such as smart factories, smart energy, smart transportation, smart buildings, smart healthcare, etc. Similarly, Cyber Physical Sensor System (CPSS) has gained popularity in recent times and is composed of a computing platform linked to an actuator, sensor, and wireless access point. In real-time scenarios, CPSS continuously gathers data from physical objects and conducts real-time control events based on the process algorithm. Then, the gathered data is transferred to the control centre or cloud services via network layer for further processing. In this scenario, there exists a need to identify the way of utilizing the intellect correctly, by designing effective data sensing and fusion schemes for CPSS. With this background, the current paper presents a Deep Learning with Metaheuristics based Data Sensing and Encoding (DLMB-DSE) scheme for CPSS. The aim of the proposed DLMB-DSE technique is to present a prediction-based data sensing and fusion approach to reduce the quantity of data communication and maintain maximum coverage by ensuring security. DLMB-DSE technique involves the design of Optimal Deep Belief Network (DBN) with Adagrad optimizer to primarily predict the data of the succeeding period with minimum number of data items. It also helps in making the primary predicted value, estimate the actual value, with maximum accuracy. Besides, Multi-Key Homomorphic Encryption (MKHE) technique is also applied for useful data encoding and decoding processes, thereby accomplishing security. Moreover, the novelty of the study lies in optimal key generation process, followed in MKHE technique, using Equilibrium Optimizer (EO). This helps in improving the security. A wide range of experiments was implemented to validate the better performance of the proposed DLMB-DSE technique. The experimental results exhibit the promising performance of DLMB-DSE approach over other methods under different measures.

Keywords Cyber physical systems · Security · Sensing process · Data fusion · Encryption · Artificial intelligence · Key generation

1 Introduction

In recent years, the role played by Cyber Physical Systems (CPS) gained much importance in industry 4.0 applications namely, smart energy, smart factory, smart cities, smart healthcare, smart building, and smart transportation. The emergent CPS is a feedback control system-based pervasive sensing method [1]. Therefore, CPS represents a vision of physical devices that include sensor-enabled mobile devices, sensors, and actuators that perform feedback control loops. These actuator devices deliver and receive data from a control system that performs the given applications. In general, the physical devices are assumed to be seamlessly incorporated into day-to-day living objects in the name of 'embedded devices or systems'. The existence of feedback loops, assisted by a pervasive sensing system, is the general feature of each proposal on CPS [2]. In this regard, CPS focuses on various problems like realtime application development that provides customized service in the context of Internet of Things (IoT) and improvement of incorporation levels in embedded device. The conceptual framework of CPS that can manage physical objects, consists of four layers such as networking, applications, security, and Cyber Physical Sensor System (CPSS) [3].

Extended author information available on the last page of the article

The network layers provide the links between application layer and CPSS through distinct IoT transmission systems. The application layers handle user interface services, data processing, storage, visualization, and analysis services [4]. CPSS layers consist of actuators, controllers, single chip computing platforms, and sensors while altogether it communicates with physical objects. The sensing element is developed to provide highly reliable outcomes that require low maintenance cost. Figure 1 illustrates the framework of CPS technique [5].

CPSS gathers the status about physical objects and transmits it to the application layer via network layer [6]. All these layers are susceptible and prone to cyberattack, which creates some disturbance or malfunction that leads to serious impact [7]. The study considers vulnerabilities, CPSS function, and security threats while it also provides feasible solution to the threats found. The data created by sensors at the time of continuous sensing period generally consists of higher temporal coherence. Due to this, certain information exists in the sustaining data sequence which might be wasting the energy and causing redundant transmission of data. Therefore, prediction was introduced based on fusion and data sensing systems to process the original information in sensors and reduce redundant transmission [8]. In order to attain the objective of expanding the network lifetime, the proposed scheme takes full advantage of higher temporal coherence of the sensed data to reduce unwanted transmission and save the energy of sensors [9]. Furthermore, some problems including data leakage at the time of communication remain a major problem in WSN in terms of data security. The presented model organized the sensors into clusters of distinct sizes in a way such that all the clusters can interact with fusion centre in an interleaved manner [10]. For various data fusion and sensing network topologies (for example, tree, chain, and star), the optimum solution is given by determining the amount of communications for all the nodes.

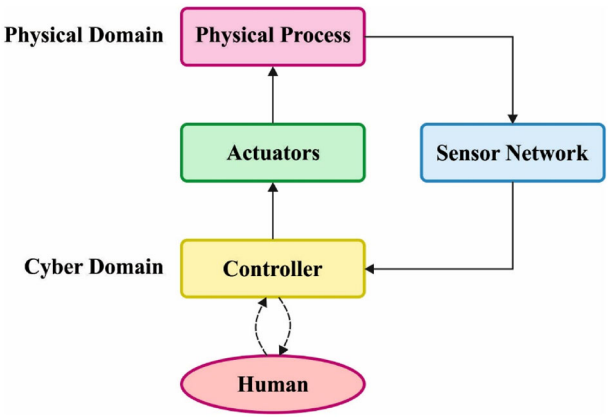


Fig. 1 Sensor-based CPS

The current research paper presents a Deep Learning with Metaheuristics based Data Sensing and Encoding (DLMB-DSE) scheme for CPSS. The aim of the proposed DLMB-DSE technique is to present a prediction-based data sensing and fusion approach to reduce the quantity of data communication and maintain maximum coverage by ensuring security. In addition, DLMB-DSE technique involves the design of Optimal Deep Belief Network (DBN) with Adagrad optimizer to primarily predict the data of succeeding period with less number of data items. Furthermore, Equilibrium Optimizer (EO)-based optimal key generation with Multi-Key Homomorphic Encryption (MKHE) technique is also applied for useful data encoding and decoding processes, thereby accomplishing security. In order to demonstrate the enhanced performance of the proposed DLMB-DSE technique, a series of simulation experiments was conducted on benchmark sensor datasets.

Rest of the paper is planned as follows. Section 2 offers information on related works, Sect. 3 provides the proposed model, Sect. 4 discusses about performance validation, and Sect. 5 concludes the paper.

2 Related works

In Dai et al. [11], a CPS with remote state assessment was considered under DoS attacks in infinite time-horizon. The goal is to frame the policy for selecting local channels in a certain state, so as to transfer the messages and mitigate the overall estimate error covariance, due to energy-saving in an infinite time-horizon. Wu et al. [12], utilized a linear discrete-time state-space system to describe the proposed system, in which a sparse vector is adapted later to attack the models. By collecting sensor measurements and utilizing an iterative model, a novel approach was attained in descriptor procedure that happens to be the basis for assessing system state under unknown input circumstance.

Meleshko et al. [13] presented a method for the detection of anomalous data from sensor nodes in Cyber-Physical Systems in line with water supply system. The method depends upon ML and modelling of technical systems. The basic information for ML was attained on the designed hardware or software prototypes of the water supply system with the help of actuators, microcontrollers, and sensors. Liu et al. [14] proposed a Trust-Based Active Detection (TBAD) system to reduce data redundancy and improve the consistency of gathering data packets. Furthermore, the assessment trust of the node, stored in data packet header, would be identified, once the UAV suspects the storing trust of sensors.

Venkatasubramanian et al. [15] introduced Physiology-based System-wide Information Security (PySIS) system that applies generative model concept in which synthetic

physiological signals are generated to extend PKA so as to assist end-to-end data privacy in CHMS from sensor nodes to PHR. Shin et al. [16] presented a smart sensor attack identification and detection system-based DNN technique, named 'DL model', without the priori knowledge of deception attack that modifies the sensing data over time.

3 The proposed model

In this study, a novel DLMB-DSE technique is presented for the prediction of data sensing and fusion approach to reduce the quantity of data communication and maintain maximum coverage by ensuring security. The proposed DLMB-DSE technique involves a series of operations namely, DBN-based prediction, Adamax-based hyperparameter tuning, MKHE-based encryption, and EO-based optimal key generation process. Adamax and EO techniques are used to accomplish improved security and overall network efficiency. Figure 2 illustrates the working process involved in the proposed method.

3.1 Predictive model for data sensing and fusion process

Initially, optimal DBN model is used in the prediction of data for succeeding period with least number of data items. This model aims at making the initial predicted value, estimate the actual value, with maximum accuracy. DBN is nothing but stacked RBM except the fact that initial RBM has undirected connection. This network structure considerably decreases the training difficulty and creates possible DL outcomes. An easy and effective layer-wise trained technique is presented to DBN by Hinton [17]. It trained the layer consecutively and greedily by tying the weight of unlearned layer. In this study, CD was used to learn the weight of single layer and iterate until every layer gets trained. Afterward, the network weight was fine-tuned by following two-pass up-down technique. This technique almost continuously demonstrated the network learned with no pre-trained models as this stage performs as 'regularizer' and helps in supervision of the optimized issue. The energy, limited from the directed method, is computed with the help of Eq. (1), in which the maximal energy is upper bounded in Eq. (2). Further, it attains equivalence, if the network weight is tied. By equal, the derivatives are equivalent to Eq. (3) and are utilized to resolve the now-simpler maximized issue.

$$E\left(x^0, h^0\right) = -\left(\log p\left(h^0\right) + \log p\left(x^0 | h^0\right)\right) \tag{1}$$

$$\begin{aligned} \log p(x^0) \geq & \sum_{\forall h^0} Q(h^0|x^0)(\log p(h^0) + \log p(x^0|h^0)) \\ & - \sum_{\forall h^0} Q(h^0|x^0) \log Q(h^0|x^0) \end{aligned} \tag{2}$$

$$\frac{\partial \log p(x^0)}{\partial \xi_{n,\mathrm{m}}} = \sum\nolimits_{\forall h^0} Q\left(h^0|x^0\right) \log p\left(h^0\right) \tag{3}$$

After iteratively learning the weight of networks, the up-down technique fine-tunes the weight of the network. The wake-sleep technique is an unsupervised technique which is used for training NN from two stages: the 'wake' stage is executed on feed-forward path to compute the weight whereas 'sleep' stage is implemented on feed-back path. The up-down technique was implemented in the network to reduce the under-fit that is generally detected as greedily-trained network [18]. Especially, in the primary stage (up-pass) of this technique, the weight on directed connection is called 'generative weight' while the parameters are altered by computing wake-phase probability, sampling of the states, and updating the weight using CD. On the other hand, the secondary phase (down-pass) stochastically stimulates the previous layer with top-down connections named after inference weight/parameter. This sleep-phase probability computed the states that are sampled and the resultant was evaluated.

In order to enhance the training efficiency of DBN approach, Adamax optimizer is utilized in this study to adjust the hyperparameter value of DBN technique [19]. It can be an altered version of Adam optimizer in which the distributed variance is proposed to be ∞. Also, the maximized weights are defined through Eq. (4):

$$w_t^i = w_{t-1}^i - \frac{\eta}{v_t + \epsilon} \cdot \widehat{m}_t \tag{4}$$

where:

$$\widehat{m}_t = \frac{m_t}{1 - \beta_1^t} \tag{5}$$

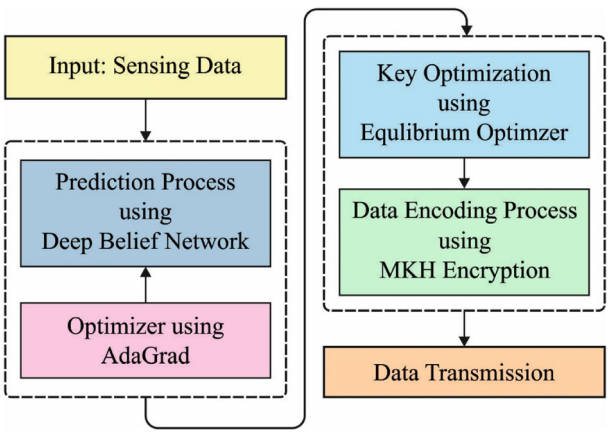


Fig. 2 Process involved in the Proposed Model

$$v_t = max(\beta_2 \cdot v_{t-1}, |G_t|) \tag{6}$$

$$m_t = \beta_1 m_{t-1} + (1 - \beta_1)G \tag{7}$$

$$G = \nabla_w C(w_t) \tag{8}$$

where η implies the learning rate, w_t stands for weight at step t, $C(.)$ denotes the cost function, and $\nabla_w C(w_t)$ signifies the gradient of weight parameter w_t x and equal label y. β_i is utilized to selecting the data required for old upgrade, where $\beta_i \in [0, 1]$. m_t and v_t are referred to as 1st and 2nd moments.

Algorithm 1: Pseudocode of AdaMax

η: Rate of Learning

$\beta_1, \beta_2 \in [0, 1)$: Exponential decompose value to moment candidate

$C(w)$: The cost function with parameter w

w_0: Primary variable vector

$m_0 \leftarrow 0$

$u_0 \leftarrow 0$

$i \leftarrow 0$ (Apply time step)

while w doesn't converge do

$i \leftarrow i + 1$

$m_i \leftarrow \beta_1 \cdot m_{i-1} + (1 - \beta_1) \cdot \frac{\partial C}{\partial w}(w_i)$

$u_i \leftarrow \max(\beta_2 \cdot u_{i-1}, |\frac{\partial C}{\partial w}(w_i)|)$

$w_{i+1} \leftarrow w_i - (\eta/(1 - \beta_1^i)) \cdot m_i/u_i$

end while

show w_i (end parameter)

3.2 Data encoding and decoding process

Once the data is sensed, the next stage is to encode the sensed data to ensure 'secure data transmission process'. An encryption system $E(k, x)$ for a key k and an input x is named as homomorphic if, for the encryption method E and operation f, there is an effective method G. Thus,

$$E(k, f(x_1, \ldots, x_n)) = G(k, f(E(x_1), \ldots, E(x_n))) \tag{9}$$

The above formula only holds for addition or multiplication while the system is named partially as 'homomorphic encryption'. It is known as Fully Homomorphic Encryption (FHE), whether it holds for addition or multiplication. Multi-Key Homomorphic Encryption (MKHE) enables multiple participants to employ distinct keys for encryption [20]. The aggregated ciphertext, attained after conducting polynomial operation on many individual ciphertexts, can only be decrypted together by integrating the corresponding secret keys, related to this ciphertext. While homomorphic multiplication is not involved in federated learning method, the study proposed an additive homomorphism of MKHE. MKHE is a Ring Learning with Errors (RLWE)-based homomorphic encryption system.

$$R = \mathbb{Z}[X]/(X^n + 1) \tag{10}$$

where n represents the power of 2D, $\mathbb{Z}[X]$ denotes the polynomial ring with integer coefficient and the element in R satisfies $X^n = -1$. $R_q = \mathbb{Z}_q[X]/(X^n + 1)$ denotes the residue ring of R with coefficient modulo, an integer q. For parameter $(n, q, \chi, \psi$, assume polynomial of the forms $(a, b = s \cdot a + e) \in R_q^2$, the b is computationally indistinguishable from uniform random elements of R_q whereas a is randomly selected from R_q, s denotes the key distribution χ over R_q, and e represents the error distribution ψ over R. MKHE assumes Common Reference String (CRS) due to which each device shares a random polynomial vector $a \leftarrow U(R_q^d)$, now $U(\cdot)$ is drawn from uniform distribution. Consider $sk_i = (1, s_i)$ represents the secret key s_i, $\overline{sk} = (1, s_1, \ldots s_N)$ for the concatenation of different secret keys. Where $ct_i = (c_0^{d_i}, c_1^{d_i})$ represents the ciphertext of plaintext m_i from remote device $d_i, i = 1, \ldots, N$.

For a variable λ, set the RLWE dimension n, ciphertext modulus q, key distribution χ, and error distribution ψ over R. Create a random vector $a \leftarrow U(R_q^d)$. Return the public variable (n, q, χ, ψ, a). A remote device d_i generates a

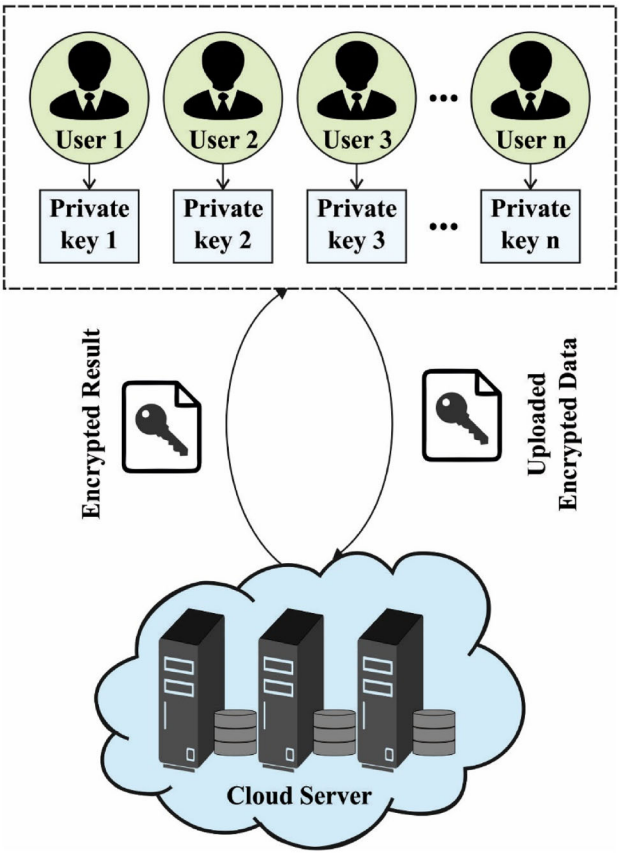


Fig. 3 Process involved in MKHE

secret key $s_i \leftarrow \chi$, and computes the public key as $b_i = -s_i \cdot a + e_i \in R_q^2$, now e_i represents the error vector derived from error distribution ψ through R. Fig. 3 demonstrates the process involved in MKHE technique.

3.3 Encoding and decoding

Before encryption, a complex number is initially extended into a vector and then encrypted as a polynomial of ring R based on complex canonical embedding map. Decryption process changes the polynomial into a complex vector after decoding. After encoding a message vector into a plaintextm_i, viz. an element of a cyclotomic ring , d_i encrypt m_i as a ciphertext $ct_i = (c_0^{d_i}, c_1^{d_i})$ in which $c_0^{d_i} = v_i \cdot b_i + m_i + e_0^{d_i}(modq)$ and$c_1^{d_i} = v_i \cdot a + e_1^{d_i}(modq)$. Now $a = a[0]$ and $b_i = b_i[0]$, $v_i \leftarrow \chi$ and $e_0^{d_i}, e_1^{d_i} \leftarrow \psi$. A small error is injected to guarantee the security and is detached by the rounding process after running homomorphic operation. In MKHE, an additive ciphertext related to N distinct parties are expressed as

$$C_{sum}^{d} \stackrel{\text{def}}{=} \left(\sum_{i=1}^{N} c_0^{d_i}, c_1^{d_1}, c_1^{d_2}, \ldots, c_1^{d_N}\right) \in R_q^{N+1}.$$

In the decoding method, d_i calculates a dot product of $sk_i = (1, s_i)$ and $ct_i = (c_0^{d_i}, c_1^{d_i})$

$$\begin{aligned} &< ct_i, sk_i > (\text{mod}q) = c_0^{d_i} + c_1^{d_i} \cdot s_i(\text{mod}q) \\ &= v_i \cdot b_i + m_i + e_0^{d_i} + v_i \cdot a \cdot s_i + e_1^{d_i} \cdot s_i(\text{mod}q) \\ &= v_i \cdot (-s_i \cdot a + e_i) + m_i + e_0^{d_i} + v_i \cdot a \cdot s_i + e_1^{d_i} \cdot s_i(\text{mod}q) \\ &= m_i + v_i \cdot e_i + e_0^{d_i} + e_1^{d_i} \cdot s_i(\text{mod}q) \\ &\approx m_i \end{aligned} \tag{11}$$

Additive homomorphism. where $ct_i = (c_0^{d_i}, c_1^{d_i})$ and $ct_j = (c_0^{d_j}, c_1^{d_j})$ represents two ciphertexts of plaintext message m_i and m_j from remote devices, d_i and d_j. The amount of the ciphertexts is $C_{sum}^{d} \stackrel{\text{def}}{=} (c_0^{d_i} + c_0^{d_j}, c_1^{d_i}, c_1^{d_j})$. It is decoded by calculating a dot product of C_{sum} and $\overline{sk} = (1, s_i, s_j)$:

$$\begin{aligned} &< C_{sum}, \overline{sk} > ; (modq) = \left(c_0^{d_i} + c_0^{d_j}\right) + c_1^{d_i} \cdot s_i + c_1^{d_j} \cdot s_j (modq) \\ &= (c_0^{d_i} + c_1^{d_i} \cdot s_i) + (c_0^{d_j} + c_1^{d_j} \cdot s_j)(modq) \\ &\approx m_i + m_j \end{aligned} \tag{12}$$

Decoding of the sum. The distributed decoding-based noise flooding is presented in MKHE, because it is not acceptable to consider that any party holds different secret keys. Decryption process contains two processes such as merge and partial decryption.

$MK - CKKS.PartDec(c_1^{d_i}, s_i)$: Assumed a polynomial $c_1^{d_i}$ and a secrets_i, sample an error $e_i^* \leftarrow \varphi$ and return $\mu_i = c_1^{d_i} \cdot s_i + e_i^*(modq)$.

$MK - CKKS.Merge(\sum_{i=1}^{N} c_0^{d_i}, \{\mu_i\}_{1 \le i \le N})$: Calculate and return $= \sum_{i=1}^{N} c_0^{d_i} + \sum_{i=1}^{N} \mu_i(modq) \approx < C_{Sum}, \overline{sk} > (modq)$.

Here, e_i^* is created from error distribution φ that has large variances, when compared to standard error distribution, ψ.

3.4 Optimal Key generation process

In order to improve the efficiency of MKHE technique, an optimal set of keys is generated with the help of EO algorithm. The basic concept of single objective EO was established in 2020. EO depends upon a dynamic mass balance on a control volume where it utilizes a mass balance formula. In terms of eligibility as a fine-tuned technique, EO has several advantages. This attribute has the capability for maintaining a balance between detection and exploitation, for executing them rapidly, and for retaining the flexibility amongst individual solutions. Thus the outcome which addressed the optimization issues with many single objectives, started dealing with real

world issues after which it gained popularity [21]. In the subsequent three stages, the mathematical method of single objective EO technique is explained. During initialization, EO utilizes a specific group, whereas all the particles explain the vector of focus that contains solutions to the problems. A primary focus vector is arbitrarily established using a subsequent equation from search spaces.

$$Y_j^{initial} = lb + rand_j(ub - lb), j = 0, 1, 2, 3, \ldots, n \tag{13}$$

where, $Y_j^{initial}$ refers to vector focus on j^{th} particle, ub and lb imply the upper and lower limits of the variables, $rand_j$ signifies a arbitrary number between 0 and 1and n stands for the amount of particles. EO technique chases the system equilibrium state. But, after attaining the equilibrium state, EO attains near-optimal solutions. It does not recognize the count of concentration, which gains the equilibrium state. So, it allocates equilibrium candidates to four optimum particles from the populations and one more that is composed of average of four optimum particles. During exploitation as well as exploration techniques, these five equilibrium candidates assist EO. The four primary candidates seek optimum exploration, while the 5$^{\text{th}}$ candidate with average value seek alteration from exploitation. These five candidates retain a vector named as 'equilibrium pool'.

$$\vec{C}_{\text{eq,pool}} = \left\{ \vec{C}_{eq(1)}, \vec{C}_{eq(2)}, \vec{C}_{eq(3)}, \vec{C}_{eq(4)}, \vec{C}_{eq(ave)} \right\} \tag{14}$$

The upgrade of concentration permits EO to balance the exploration as well as exploitation equally.

$$\vec{F} = e^{-\vec{\lambda}(t - t_0)} \tag{15}$$

where $\vec{\lambda}$ implies the arbitrary vector that is assumed between 0 and 1, permitting turnover rate fluctuation on a time period, and t has decreased as the iteration count improves as per Eq. (16).

$$t = (1 - \frac{It}{\text{Max\_}it})^{\left(a_2 \frac{It}{\text{Max\_}it}\right)} \tag{16}$$

It and Max_it correspond to present and maximal amount of iterations, and a_2 implies the constants to control the capacity for exploitation. Another variable a_1 is utilized for improving combined of exploration and exploitation and is determined as:

$$\vec{t} = \frac{1}{\vec{\lambda}} \ln\left(a_1 \; sign \; (\vec{r} - 0.5) \left[1 - e^{-\vec{\lambda} t} \right] \right) + t \tag{17}$$

The generation rate has demonstrated as G that increases exploitation and is defined as:

$$\vec{G} = \vec{G}_0 e^{-\vec{l}(t - t_0)} \tag{18}$$

where, $\vec{l}$ signifies the arbitrary vector between zero and one, and the primary generation rate named as $\vec{G}_0$ is expressed as follows.

$$\vec{G}_0 = G\vec{C}P\left(\vec{C}_{\text{eq}} - \vec{\lambda}\vec{C}\right) \tag{19}$$

$$G\vec{C}P = \begin{cases} 0.5 r_1, r_2 \geq GP \\ 0, r_2 < GP \end{cases} \tag{20}$$

where the arbitrary numbers are demonstrated as r_1 and r_2 which differbetween 0 and 1. The vector $\overrightarrow{GCP}$ stands for generation rate control parameter which controls if the rate of generation is implemented to upgrade the phase or not. Eventually, EO is upgraded utilizing in Eq. (21).

$$\vec{C} = \vec{C} + \left(\vec{C} - \vec{C}_{eq}\right) . \vec{F} + \frac{\vec{G}}{\vec{\lambda} V}\left(1 - \vec{F}\right) \tag{21}$$

The value of V is equivalent to 1.

4 Experimental validation

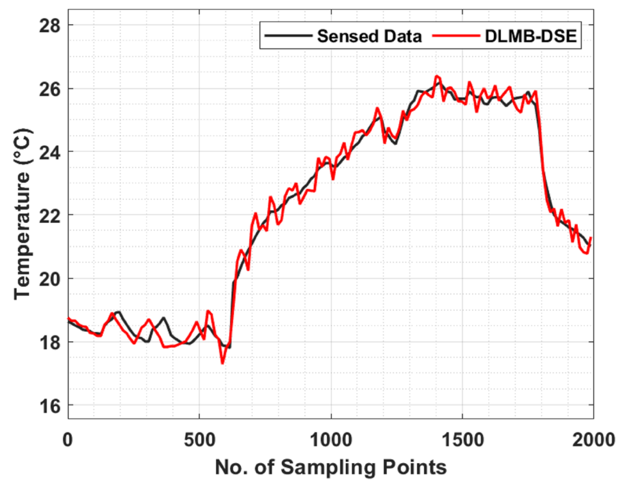


Fig. 4 Predictive analysis results of DLMB-DSE technique on temperature data

This section validates the performance of the proposed DLMB-DSE technique on 3 real-word data namely, temperature data, humidity data, and light data. The results were inspected under varying user threshold values in terms of Successful Prediction Rate (SPR) and Average Error Rate (AER). Figure 4 shows the predictive analysis results accomplished by DLMB-DSE technique on temperature data. The figure demonstrates that the proposed DLMB-DSE technique effectively predicted the values which were almost closer to the actually sensed temperature data.

Table 1 and Fig. 5 offers SPR analysis results accomplished by DLMB-DSE technique with recent methods under distinct threshold values. The experimental results report that the proposed DLMB-DSE technique enhances

Table 1 SPR analysis results of DLMB-DSE technique under distinct threshold on temperature data

User's threshold	GM	GM_OP_ELM	GM_LSSVM	GM_KRLS	DLMB-DSE
0.2	10.62	22.30	23.06	31.18	37.02
0.6	49.46	64.18	66.46	77.38	82.71
1.0	62.40	77.12	77.63	85.75	92.86
1.4	72.30	81.18	82.45	89.05	95.40
1.8	76.36	84.23	84.74	90.57	95.90
2.2	79.66	86.00	87.27	92.60	96.41
2.6	81.18	87.02	88.29	93.11	96.92
3.0	82.96	88.04	90.07	93.37	96.92
3.4	87.27	89.05	90.07	93.62	97.17
3.8	88.29	91.08	92.60	93.62	96.92

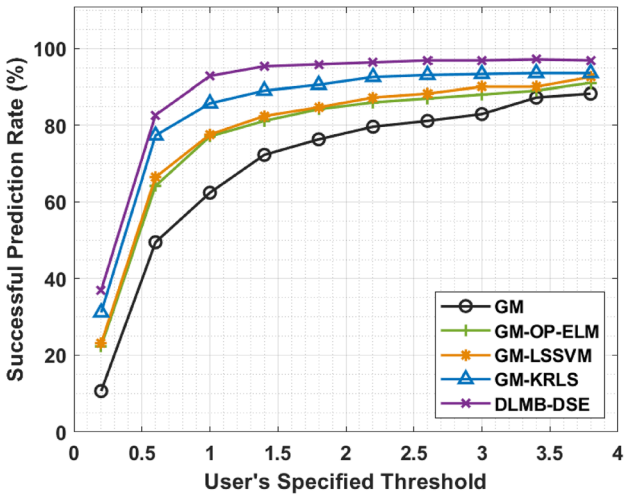


Fig. 5 SPR analysis of DLMB-DSE technique on temperature data

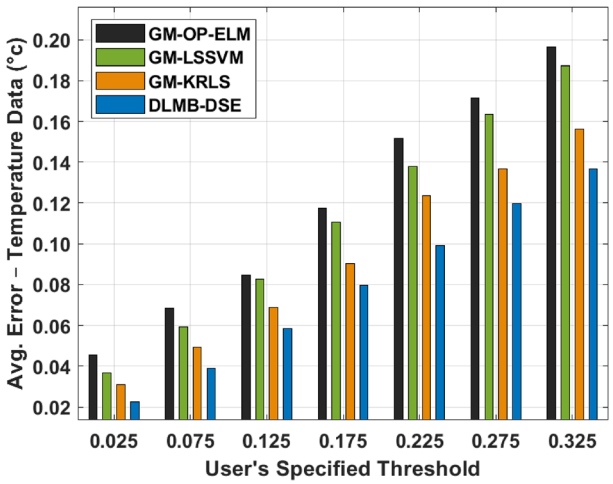


Fig. 6 AER analysis results of DLMB-DSE technique on temperature data

SPR values and indicates better predictive performance. For instance, with a threshold value of 0.2, DLMB-DSE technique offered a high SPR of 37.02%, whereas GM, GM_OP_ELM, GM_LSSVM, and GM_KRLS techniques obtained the least SPR values such as 10.62%, 22.30%, 23.06%, and 31.18% respectively. Meanwhile, with a threshold value of 2.2, the proposed DLMB-DSE approach obtained a maximum SPR of 96.41%, whereas GM, GM_OP_ELM, GM_LSSVM, and GM_KRLS methods obtained the least SPR values such as 79.66%, 86%, 87.27%, and 92.60% correspondingly. Eventually, with a threshold value of 3.8, the proposed DLMB-DSE approach offered a superior SPR of 96.92%, whereas GM, GM_OP_ELM, GM_LSSVM, and GM_KRLS systems achieved minimum SPR values such as 88.29%, 91.08%, 92.60%, and 93.62% correspondingly.

A detailed AER analysis was conducted between DLMB-DSE technique and recent techniques under various threshold values and the results are shown in Fig. 6. The results indicate that the proposed DLMB-DSE technique attained minimal AER values under all thresholds. For instance, with a threshold value of 0.2, DLMB-DSE technique demonstrated the least AER of 0.0225%, whereas GM_OP_ELM, GM_LSSVM, and GM_KRLS techniques exhibited increased ARR values such as

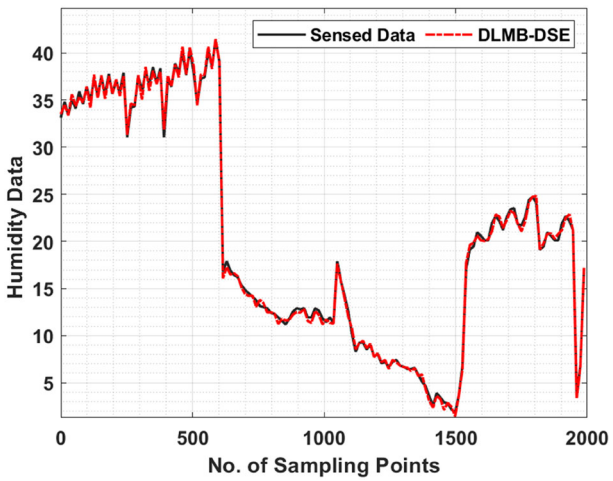


Fig. 7 Predictive analysis results of DLMB-DSE technique on humidity data

Table 2 SPR analysis results of DLMB-DSE technique under distinct threshold on humidity data

User's threshold	GM	GM_OP_ELM	GM_LSSVM	GM_KRLS	DLMB-DSE
0.2	4.76	8.86	9.32	9.09	12.74
0.6	22.09	37.36	41.92	41.01	45.34
1.0	32.57	54.46	58.79	57.65	63.81
1.4	40.55	65.40	67.22	67.22	73.15
1.8	46.71	70.64	72.24	73.38	79.31
2.2	53.32	74.06	76.57	78.17	83.41
2.6	59.93	76.12	78.62	81.13	86.37
3.0	63.12	79.76	81.13	83.18	86.37
3.4	66.77	81.59	82.95	85.46	87.74
3.8	73.15	83.41	85.23	85.92	87.29

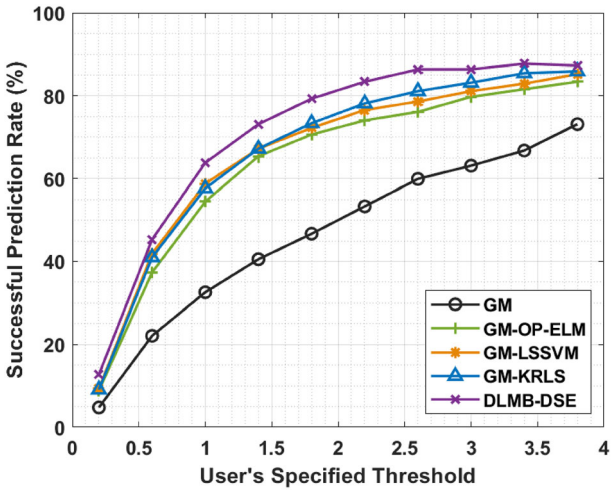


Fig. 8 SPR analysis results of DLMB-DSE technique on humidity data

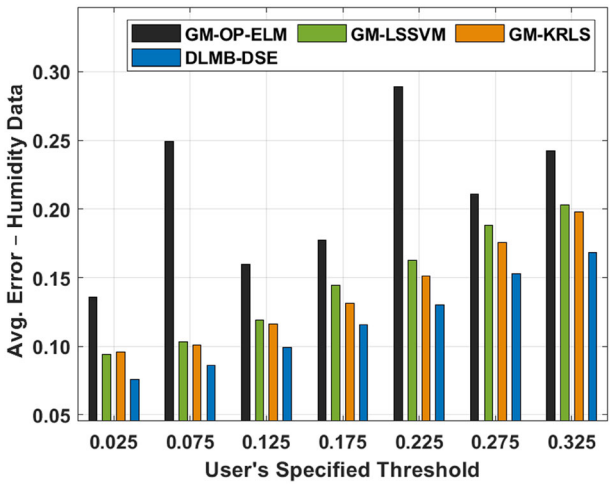


Fig. 9 AER analysis results of DLMB-DSE technique on humidity data

0.0454%, 0.0368%, and 0.0311% respectively. Along with that, with a threshold value of 0.325, DLMB-DSE algorithm demonstrated the least ARR of 0.1368%, whereas GM_OP_ELM, GM_LSSVM, and GM_KRLS methodologies exhibited improved ARR values such as 0.1965%, 0.1873%, and 0.1562% correspondingly.

Figure 7 illustrates the predictive analysis results accomplished by DLMB-DSE technique on humidity data. The figure shows that DLMB-DSE approach outperformed the existing methods in terms of predicting the values and it is almost closer with actually sensed data in humidity data.

Table 2 and Fig. 8 offers SPR analysis results accomplished by DLMB-DSE technique and other recent methods under varying threshold values. The experimental results reported that DLMB-DSE approach reached a enhanced SPR value and indicates better predictive performance. For instance, with a threshold value of 0.2, the proposed DLMB-DSE technique achieved a superior SPR of 12.74%, whereas GM algorithm, GM_OP_ELM system, GM_LSSVM approach, and GM_KRLS techniques obtained less SPR values such as 4.76%, 8.86%, 9.32%, and 9.09% correspondingly. In the meantime, with a threshold value of 2.2, the proposed DLMB-DSE technique offered a high SPR of 83.41%, whereas GM algorithm, GM_OP_ELM system, GM_LSSVM approach, and GM_KRLS systems gained low SPR values such as 53.32%, 74.06%, 76.57%, and 78.17% correspondingly. At last, with a threshold value of 3.8, the proposed DLMB-DSE technique offered a high SPR of 87.29%, whereas GM algorithm, GM_OP_ELM system, GM_LSSVM approach, and GM_KRLS methods obtained the least SPR values such as 73.15%, 83.41%, 85.23%, and 85.92% correspondingly.

A brief AER analysis was conducted between DLMB-DSE algorithm and recent techniques under various threshold values and the results are shown in Fig. 9. The outcomes designate that the proposed DLMB-DSE technique obtained minimal AER values under all the thresholds. For instance, with a threshold value of 0.025, the proposed DLMB-DSE technique achieved a minimum ARR of 0.0756%, whereas GM_OP_ELM approach, GM_LSSVM system, and GM_KRLS techniques achieved high ARR values such as 0.1355%, 0.0939%, and 0.0956% correspondingly. In

addition, with a threshold value of 0.325, the proposed DLMB-DSE technique demonstrated the least ARR of 0.1685%, whereas GM_OP_ELM method, GM_LSSVM system, and GM_KRLS techniques portrayed maximum ARR values such as 0.2423%, 0.2033%, and 0.1981% correspondingly.

Figure 10 portrays the predictive analysis results achieved by DLMB-DSE system on light data. The figure exhibits that the proposed DLMB-DSE approach predicted the values effectively and it is almost closer with actually sensed data in light data.

Table 3 and Fig. 11 provides the SPR analysis results accomplished by DLMB-DSE technique and other recent methods under distinct threshold values. The experimental outcomes infer that the proposed DLMB-DSE technique gained high SPR values indicating better predictive performance. For instance, with a threshold value of 0.2, DLMB-DSE method offered a maximum SPR of 35.43%, whereas GM approach, GM_OP_ELM technique, GM_LSSVM methodology, and GM_KRLS techniques obtained the least SPR values such as 27.36%, 30.35%, 29.44%, and 32.95% correspondingly.

Besides, with a threshold value of 2.0, the proposed DLMB-DSE technique presented a high SPR of 64.20%, whereas GM system, GM_OP_ELM algorithm, GM_LSSVM approach, and GM_KRLS methodologies obtained low SPR values such as 42.07%, 50.79%, 57.69%, and 59.77% correspondingly. Finally, with a threshold value of 4.0, the proposed DLMB-DSE technique accessed a high SPR of 72.66%, whereas GM methodology, GM_OP_ELM system, GM_LSSVM approach, and GM_KRLS techniques reached minimum SPR values namely, 49.75%, 59.38%, 68.10%, and 70.97%.

A detailed AER analysis was conducted between DLMB-DSE technique and recent approaches under different threshold values and the results are portrayed in Fig. 12. The results infer that the proposed DLMB-DSE

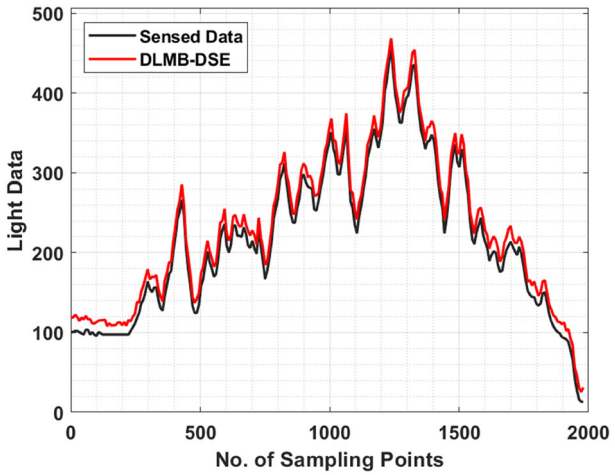


Fig. 10 Predictive analysis results of DLMB-DSE technique on light data

Table 3 SPR analysis results of DLMB-DSE technique under distinct threshold on light data

User's threshold	GM	GM_OP_ELM	GM_LSSVM	GM_KRLS	DLMB-DSE
0.2	27.36	30.35	29.44	32.95	35.43
0.5	31.65	38.42	39.72	42.46	45.58
1.0	36.08	44.15	48.57	50.79	54.69
1.5	38.68	47.92	53.26	55.21	59.90
2.0	42.07	50.79	57.69	59.77	64.20
2.5	45.06	54.56	60.81	63.81	67.97
3.0	46.88	54.82	63.02	66.80	70.18
3.5	48.18	58.34	66.54	69.53	71.75
4.0	49.75	59.38	68.10	70.97	72.66

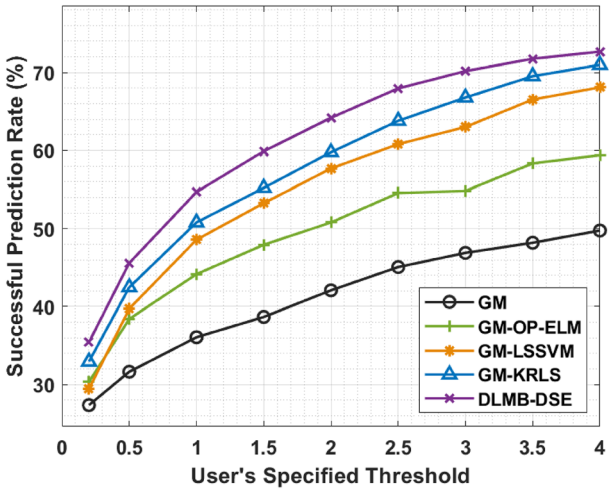


Fig. 11 SPR analysis of DLMB-DSE technique on light data

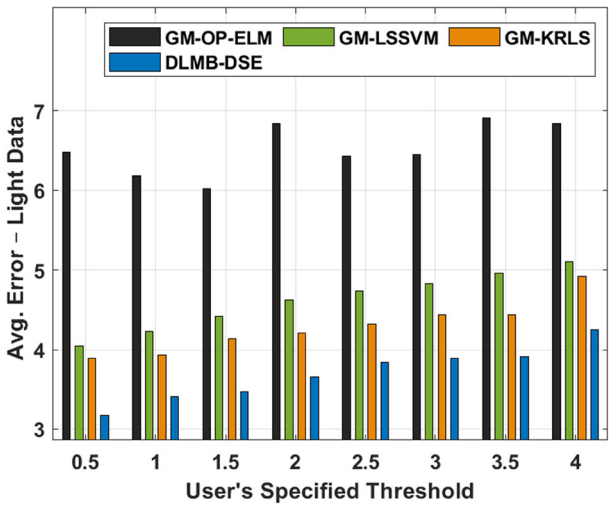


Fig. 12 AER analysis results of DLMB-DSE technique on light data

Table 4 Computation time analysis results of DLMB-DSE technique and existing approaches under three datasets

Methods	GM_OP_ELM	GM_LSSVM	GM_KRLS	DLMB-DSE
Temperature	0.0672	0.0554	0.0830	0.0314
Humidity	1.1073	1.0364	1.5328	0.5824
Light	0.1184	0.0987	0.1184	0.0711

approach obtained the least AER values under all thresholds. For instance, with a threshold value of 0.5, the proposed DLMB-DSE technique demonstrated the least ARR of 3.1786%, whereas GM_OP_ELM system, GM_LSSVM approach, and GM_KRLS techniques demonstrated high ARR values such as 6.4742%, 4.0483%, and 3.8881% respectively. Followed by, with a threshold value of 4.0, the proposed DLMB-DSE system achieved a minimal ARR of 4.2542%, whereas GM_OP_ELM algorithm, GM_LSSVM method, and GM_KRLS techniques demonstrated the maximum ARR values namely, 6.8404%, 5.1010%, and 4.9179%.

Finally, Computation Time (CT) analysis was conducted between DLMB-DSE technique and recent methods on three datasets and the results are given in Table 4. The experimental results infer that the proposed DLMB-DSE technique required the least CT over other methods. For instance, with temperature data, DLMB-DSE technique required a minimal CT of 0.0314 s, whereas GM_OP_ELM system, GM_LSSVM method, and GM_KRLS techniques required the maximum CT such as 0.0672 s, 0.0554 s, and 0.0830 s respectively.

Besides, with humidity data, the proposed DLMB-DSE approach required a low CT of 0.5824 s, whereas GM_OP_ELM algorithm, GM_LSSVM method, and GM_KRLS techniques demanded maximal CT such as 1.1073 s, 1.0364 s, and 1.5328 s correspondingly. In addition, with light data, DLMB-DSE technique required a less CT of 0.0711 s, whereas GM_OP_ELM technique, GM_LSSVM system, and GM_KRLS methodologies required high CT such as 0.1184 s, 0.0987 s, and 0.1184 s correspondingly. From the above discussed tables and figures, it is evident that DLMB-DSE technique has the ability to outperform other methods on three real world datasets namely temperature data, humidity data, and light data. The enhanced performance is due to the utilization of Adamax and EO optimizers which helped in accomplished improved security and overall network efficiency.

5 Conclusion

In this study, a novel DLMB-DSE technique has been presented for the prediction of data sensing and fusion approach so as to reduce the quantity of data communication and maintain maximum coverage by ensuring security. The proposed DLMB-DSE technique involves a series of operations namely, DBN-based prediction, Adamax-based hyperparameter tuning, MKHE-based encryption, and EO-based optimal key generation process. The utilization of Adamax and EO optimizers helped in accomplishing improved security and overall network efficiency. In order to demonstrate the enhanced performance of the proposed DLMB-DSE technique, a series of simulations was conducted on benchmark sensor datasets. The experimental results exhibit the promising performance of DLMB-DSE technique over other methods under different measures. Therefore, DLMB-DSE technique can be used to accomplish effective data sensing and fusion approach for CPSS with maximum security. In future, resource allocation and task scheduling approaches can be designed to improve the performance of CPSS.

Author contributions AAE and MK—Conceptualization. MK, SAK—Data curation and Formal analysis. SAK, RFM—Investigation and Methodology. RFM and DG—Project administration and Resources: Supervision. UD and KKK—Validation and Visualization. AAE—Writing—original draft. AAE and EFM—Writing—review and editing. All authors have read and agreed to the published version of the manuscript.

Funding Taif University Researchers Supporting Project number (TURSP-2020/154), Taif University, Taif, Saudi Arabia.

Data availability Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Conflict of interest The authors declare that they have no conflict of interest. The manuscript was written through contributions of all authors. All authors have given approval to the final version of the manuscript.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

Informed consent Not applicable.

References

1. Wang, W., Harrou, F., Bouyeddou, B., Senouci, S.M., Sun, Y.: A stacked deep learning approach to cyber-attacks detection in industrial systems: application to power system and gas pipeline systems. Clust. Comput. **25**(1), 561–578 (2022)

2. Ammi, M., Adedugbe, O., Alharby, F.M., Benkhelifa, E.: Leveraging a cloud-native architecture to enable semantic interconnectedness of data for cyber threat intelligence. Clust. Comput. **24**, 1–12 (2022)
3. Vangala, A., Das, A.K., Chamola, V., Korotaev, V., Rodrigues, J.J.: Security in IoT-enabled smart agriculture: architecture, security solutions and challenges. Clust. Comput. **16**, 1–24 (2022)
4. Barišić, A., Ruchkin, I., Savić, D., Mohamed, M.A., Al-Ali, R., Li, L.W., Mkaouar, H., Eslampanah, R., Challenger, M., Blouin, D., Nikiforova, O.: Multi-paradigm modeling for cyber–physical systems: a systematic mapping review. J. Syst. Softw. **183**, 111081 (2022)
5. Lakhan, A., Mohammed, M.A., Kozlov, S., Rodrigues, J.J.: Mobile-fog-cloud assisted deep reinforcement learning and blockchain-enable IoMT system for healthcare workflows. Trans. Emer. Telecommun. Technol. **15**, e4363 (2021)
6. Berger, C., Hees, A., Braunreuther, S., Reinhart, G.: Characterization of cyber-physical sensor systems. Procedia CIRP **41**, 638–643 (2016)
7. Lakhan, A., Mohammed, M.A., Kadry, S., Abdulkareem, K.H., Al-Dhief, F.T., Hsu, C.H.: Federated learning enables intelligent reflecting surface in fog-cloud enabled cellular network. PeerJ Comput. Sci. **7**, e758 (2021)
8. Lakhan, A., Mohammed, M.A., Rashid, A.N., Kadry, S., Panityakul, T., Abdulkareem, K.H., Thinnukool, O.: Smart-contract aware ethereum and client-fog-cloud healthcare system. Sensors **21**(12), 4093 (2021)
9. Adil, M., Khan, M.K., Jadoon, M.M., Attique, M., Song, H., Farouk, A.: An AI-enabled Hybrid lightweight Authentication Scheme for Intelligent IoMT based Cyber-Physical Systems. IEEE Trans. Netw. Sci. Eng. **24**, 59–62 (2022)
10. Amma, N.G.: A vector convolutional deep autonomous learning classifier for detection of cyber attacks. Clust. Comput. **16**, 1–12 (2022)
11. Dai, P., Yu, W., Wang, H., Wen, G., Lv, Y.: Distributed reinforcement learning for cyber-physical system with multiple remote state estimation Under DoS attacker. IEEE Trans. Netw. Sci. Eng. **7**(4), 3212–3222 (2020)
12. Wu, C., Hu, Z., Liu, J., Wu, L.: Secure estimation for cyber-physical systems via sliding mode. IEEE Trans. Cybern. **48**(12), 3420–3431 (2018)
13. Meleshko, A.V., Desnitsky, V.A. and Kotenko, I.V.: Machine learning based approach to detection of anomalous data from sensors in cyber-physical water supply systems. In IOP conference series: materials science and engineering (Vol. 709, No. 3, p. 033034). IOP Publishing (2020)
14. Liu, Y., Liu, A., Liu, X., Ma, M.: A trust-based active detection for cyber-physical security in industrial environments. IEEE Trans. Industr. Inf. **15**(12), 6593–6603 (2019)
15. Venkatasubramanian, K.K., Banerjee, A., Gupta, S.K. and Walls, R.J.: August. A cyber-physical approach to trustworthy operation of health monitoring systems. In 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI) (pp. 1–6). IEEE. (2017)
16. Shin, J., Baek, Y., Eun, Y. and Son, S.H.: November. Intelligent sensor attack detection and identification for automotive cyber-physical systems. In 2017 IEEE Symposium Series on Computational Intelligence (SSCI) (pp. 1–8). IEEE. (2017)
17. Hinton, G.: A practical guide to training restricted boltzmann machines. Momentum **9**(1), 926 (2010)
18. Rizk, Y., Hajj, N., Mitri, N., Awad, M.: Deep belief networks and cortical algorithms: a comparative study for supervised classification. Appl. Comput. Inform. **15**(2), 81–93 (2019)
19. Nahhas, F.H., Shafri, H.Z., Sameen, M.I., Pradhan, B., Mansor, S.: Deep learning approach for building detection using lidar–orthophoto fusion. J. Sens. **25**, 8–9 (2018)
20. Chen, H., Dai, W., Kim, M. and Song, Y.: November. Efficient multi-key homomorphic encryption with packed ciphertexts with application to oblivious neural network inference. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 395–412). (2019)
21. Faramarzi, A., Heidarinejad, M., Stephens, B., Mirjalili, S.: Equilibrium optimizer: a novel optimization algorithm. Knowl.-Based Syst. **191**, 105190 (2020)

Ala' A. Eshmawi is an assistant professor in the Department of Cybersecurity, College of Computer Science and Engineering at University of Jeddah, Jeddah, Saudi Arabia. She earned her PhD in computer science from Southern Methodist University, Dallas Texas USA, in 2015. She is currently working as the Deputy supervisor of Cybersecurity Administration at University of Jeddah. Her research interests include information privacy and security, intrusion detection, mobile agents and application of AI and Machine Learning in various fields including the field of Cybersecurity.

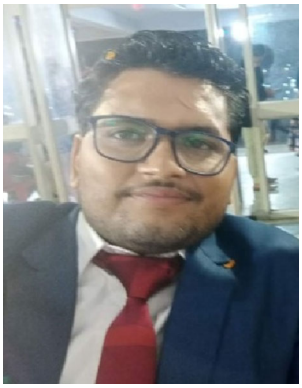
Mashael Khayyat received the bachelor's degree (Hons.) in computer science degree from King Abdul-Aziz University, in 2004, the master's degree in applied information systems (AIS) from the Arab Academy for Science and Technology and Maritime Transport, Alexandria, Egypt, the second master's degree in technology management (MTM) from the University of New South Wales (UNSW), Sydney, Australia, and the Ph.D. degree in computer science and statistics from Trinity College Dublin (TCD), Dublin, Ireland, in 2017. She has been a Supervisor at the Department of Computer and Network Engineering and an Assistant Professor at the Information Systems and Technology Department, College of Computer Science and Engineering, University of Jeddah, since 2017. Prior to that, she worked at the Information Systems Department, King Abdul-Aziz University, as an Assistant Professor. She received

international and distinguished research grants from the University of Jeddah.

S. Abdel-Khalek received a Ph.D. degree in computer science from Azhar University, in 2016. He is a Full Professor in applied mathematics with the Mathematics Department, Faculty of Science, Sohag University, Egypt. He is also an Associate Professor in applied mathematics with the Department of Mathematics, Faculty of Science, Taif University, Taif, Saudi Arabia. He is the author of several articles published in different international scientific journals. His research interests include different directions in quantum information and computer sciences. He is a member of different working groups.

Romany F. Mansour Received the Ph.D. degree from the University of Assiut in 2009, He is currently working as an Associate Professor at Department of Mathematics, Faculty of science, New Valley University, Egypt. His research interests include IOT, Data Analysis, Computer Networks, Soft Computing, Biomedical Image, Bioinformatics and machine learning.

Umesh Dwivedi got his M.Tech. Degree in 2010 and PhD Degree from Dr. A.P.J. Abdul Kalam Technical University, Lucknow, Uttar Pradesh, India in 2020. He is currently working as Associate. Professor in Dept. of Computer Science and Engineering, at Babu Banarsi Das Northern India Institute of Technology, Lucknow, Uttar Pradesh, India. He has more than 15 years of teaching experience and 9 years of research experience in the field of Cloud computing, Artificial Intelligence specially in the field of Deep Learning. He has published several outstanding research publications in national and International Journals. He has one patent also in the field of Cloud Computing. He is a member of Computer Society of India, International Association of Computer Science and Information Technology (IACSIT) and various other bodies engaged in the field of research.



Krishna Kumar joshi got his M.Tech. Degree in 2014 and persuing his PhD from Lucknow University, Lucknow, Uttar Pradesh, India. He is currently working as Assistant. Professor in Dept. of Computer Science and Engineering, at Babu Banarsi das Northern India Institute of Technology Lucknow, India. He has 7 years of teaching experience and 6 years of research experience in the field of Wireless Sensor Network Specially in Data Aggregation in wireless sensor network, energy efficiency in wireless sensor network. He has produced several outstanding research publications. He is a member of Computer Society of India, International Association of Computer Science and Information Technology (IACSIT) and various other bodies engaged in the field of research.

Deepak Gupta received a B.Tech. degree in 2006 from the Guru Gobind Singh Indraprastha University, Delhi, India. He received M.E. degree in 2010 from Delhi Technological University, India and Ph. D. degree in 2017 from Dr. APJ Abdul Kalam Technical University (AKTU), Lucknow, India. He has completed his Post-Doc from National Institute of Telecommunications (Inatel), Brazil in 2018. He has co-authored more than 145 journal articles including 109 SCI papers and 45 conference articles. He has authored/edited 53 books, published by IEEE-Wiley, Elsevier, Springer, Wiley, CRC Press, DeGruyter and Katsons. He has filled four Indian patents. He is convener of ICICC, ICDAM & DoSCI Springer conferences series. Currently he is Associate Editor of Expert Systems (Wiley), and Intelligent Decision Technologies (IOS Press). He is the recipient of 2021 IEEE System Council Best Paper Award. He has been featured in the list of top 2% scientist/researcher database in the world [Table-S7-singleyr-2019]. He is also working towards promoting Startups and also serving as a Startup Consultant. He is also a series editor of "Elsevier Biomedical Engineering" at Academic Press, Elsevier, "Intelligent Biomedical Data Analysis" at De Gruyter, Germany, "Explainable AI (XAI) for Engineering Applications" at CRC Press. He is appointed as Consulting Editor at Elsevier.

Authors and Affiliations

Ala' A. Eshmawi[1] · Mashael Khayyat[2] · S. Abdel-Khalek[3] · Romany F. Mansour[4] · Umesh Dwivedi[5] · Krishna Kumar joshi[5] · Deepak Gupta[6]

✉ Romany F. Mansour
romanyf@sci.nvu.edu.eg

Ala' A. Eshmawi
aaeshmawi@uj.edu.sa

Mashael Khayyat
mmakhayyat@kau.edu.sa

S. Abdel-Khalek
sabotalb@tu.edu.sa

Umesh Dwivedi
umesh2112@bbdniit.ac.in

Krishna Kumar joshi
1990.krishnajoshi@gmail.com

Deepak Gupta
deepakgupta@mait.ac.in

[1] Department of Cybersecurity, College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia

[2] Department of Information Systems and Technology, College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia

[3] Department of Mathematics and Statistics, College of Science, Taif University, Taif 21944, Saudi Arabia

[4] Department of Mathematics, Faculty of Science, New Valley University, El-Kharga 72511, Egypt

[5] Department of Computer Science & Engineering, Babu Banarsi Das Northern India Institute of Technology, Lucknow, Uttar Pradesh, India

[6] Department of Computer Science & Engineering, Maharaja Agrasen Institute of Technology, Delhi, India