Soft Computing (2021) 25:12319–12332
https://doi.org/10.1007/s00500-021-05926-8

FOCUS

Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques

Ahmad Ali AlZubi[1] · Mohammed Al-Maitah[1] · Abdulaziz Alarifi[1]

Accepted: 31 May 2021 / Published online: 26 June 2021

Abstract
Cyber-physical systems have been extensively utilized in healthcare domains to deliver high-quality patient treatment in multifaceted clinical scenarios. The medical device' heterogeneity involved in these systems (mobile devices and body sensor nodes) introduces enormous attack surfaces and therefore necessitates effective security solutions for these complex environments. Hence, in this study, the cognitive machine learning assisted Attack Detection Framework has been proposed to share healthcare data securely. The Healthcare Cyber-Physical Systems will be proficient in spreading the collected data to cloud storage. Machine learning models predict cyber-attack behavior, and processing this data can offer healthcare specialists decision support. This proposed approach is based on a patient-centric design that safeguards the information on a trusted device like the end-users mobile phones and end-user control data sharing access. Experimental results demonstrate that our suggested model achieves an attack prediction ratio of 96.5%, an accuracy ratio of 98.2%, an efficiency ratio of 97.8%, less delay of 21.3%, and a communication cost of 18.9% to other existing models.

Keywords Cyber-physical system · Machine learning · Attack or malicious detection · Healthcare system

1 Overview of cyber-physical system in healthcare

Cyber-Physical Systems (CPSs) arise as engineered systems that provide integrations of computing, networking, and physical processes, allowing seamless connectivity between cyber services and physical devices (Qiu et al. 2020). A device that controls and monitors a process using computer-based algorithms is a cyber-physical system. Physical and software elements are highly interconnected in cyber-physical structures that can work on various spatial and time scales, show many and distinct behaving modalities, and communicate in different contexts. CPS includes transdisciplinary approaches, cybernetics, mechatronics and philosophy of design, and process science. Embedded systems are often referred to as process management. They describe a developed system as a component combination that works together to perform a useful function collectively. Thus, the components' growth, integration, and ongoing management are influenced by the dynamic interactions and effects of the device process. Healthcare networks as a modern context-aware cyber-physical system (CPS) incorporates integrated devices, Internet of Things technologies, and cloud storage (Shuwandy et al. 2020). The focus of modern business models is customer satisfaction. Social responsibility can be gained by retaining a profit. It survives to embrace all facets of human culture. It considers modern business to be a socioeconomic organization that is often socially responsible. Context sensitivity applies in ICT to the ability to take account, however not limited to, of the situation of individuals that might be users or devices. Even the most obvious factor in this situation is place. Context knowledge is therefore generalized for the position, which is narrowly specified for mobile devices. Health cloud computing improves market productivity, thus lowering prices. Medical records are shared faster and safer; cloud storage

Communicated by Vicente Garcia Diaz.

✉ Ahmad Ali AlZubi
aalzubi@ksu.edu.sa

Mohammed Al-Maitah
malmaitah@ksu.edu.sa

Abdulaziz Alarifi
abdulazizalarifi@ksu.edu.sa

[1] Computer Science Department, Community College, King Saud University, Riyadh, Saudi Arabia

automates back-end operations and makes it easier for telehealth applications to be created and maintained. With mobile terminal systems' intellectualization, a mobile healthcare network is automatically created and can deliver easy healthcare facilities and real-time connectivity (Farivar et al. 2019). A mobile (MDT) or digital mobile (MDC) data terminal is a mechanical interface used to communicate with a central office in the field of public transit vehicles, taxi cabs, delivery vehicle, service trucks, commercial fleets, military logistics, fishing fleets, wire stock control and emergency vehicles, such as police cars. The mapping and details related to the vehicle's tasks and activities, such as CAD drawings, diagrams, and safety information, are shown. Mobile data terminals feature a screen where information and a keyboard or keyboard can be viewed for entry of information and linked to different peripheral devices. In the SearchUnified Communications context, real-time communications involve an almost simultaneous information exchange from sender to the recipient over any telecommunications service about neglectable latency. Though two issues in the cyber-physical system necessary to be addressed (Shakeel et al. 2018). The first concern is the mitigation of mobile terminal computing and storage expenses (Hassan et al. 2019). The second issue is a solution to cyber-physical data security and privacy (Khan et al. 2020). An electronic or electromechanical device is a computer terminal that shows exactly the data into a computer or a computer system and then transcribes data. The Display was an example of a hardcopy early in the day and used a computer screen decades ago. Using a terminal, we can send simple text commands to a machine to do things such as navigate a directory, copy a file and build the foundation for many more complex automation and programming capabilities. The cost of storage means the amount of money spent on inventory storage or inventory keeping. Costs for storage will be a subset of holding product costs, including costs that are not limited. Medical equipment with cyber capabilities is located in Mobile Health Systems to contact patients to capture and monitor diagnostic data (Kurde et al. 2019). Any device designed for medical use is a medical device. Patients receive benefits from the diagnosis and treatment of patients and the management and quality of life improvements to patients' healthcare systems. Significant hazard potential is inherent in using a device for medical purposes, and medical devices must be shown to be safe and reliable with fair assurance before the regulatory authorities permit their country to sell the device. This option starts Monitor Diagnostics, which is used to check LCD and CRT displays for their capabilities and display efficiency. Such instruments may be autonomous, semi-conductor-embedded sensors inserted within the patient's body to quantify the real-time symptoms (Abdali-Mohammadi et al. 2020). Personal devices relay private medical data in electronic health records for diagnostic information to storage centers that process these data (Verma et al. 2020). Today, several cloud providers provide realistic medical information systems, such as IBM Cloud Services, Google Cloud, and Azure (Wang et al. 2016). Cloud-based healthcare systems are useful because they offer a wide range of healthcare equipment, global accessibility, and effective storage-saving (Weerakkody et al. 2017). However, personal information migration through a cloud server potentially not trusted raises concerns about the patient's privacy (Wang et al. 2020). Therefore, it is imperative to provide fine-grained access control on the patient's data to protect patients' details (Sliwa 2019). Healthcare CPS (HCPS) presents several security and privacy problems regarding their various advantages (Wu et al. 2020). The heterogeneity of MCPS and increased usage of web and wireless technology leads to new surface areas and vulnerabilities (Gupta et al. 2020). Sensitive health and personal health records may be unauthorized access to security attacks on HCPS (Iqbal et al. 2020). Malicious attacks may lead to misdiagnosis and improper treatment that can destroy lives (Poongodi et al. 2020). For example, a defective medical device, such as a cardiac pacemaker, could alter or completely shut down, leading to catastrophic consequences (Al-Mhiqani et al. 2019). One of the key causes of vulnerabilities in HCPS is the growing connectivity to other systems and networks while they are intended to be isolated (Gopalakrishnan et al. 2020). With compounded heterogeneous and ad hoc nature of HCPS, security solutions are limited and often lack interoperability (Qi et al. 2020). Besides potential injuries and liability flaws in medical equipment, backdoor access to the rest of the network is conceivable (Haghighi et al. 2020).

Artificial Intelligence (AI) offers learning capability and software flexibility to assist humans in combat cybercrimes (Marques et al. 2020). Several nature-inspired computing techniques of artificial intelligence have been progressively playing a significant role in cybercrime prediction and avoidance (Wazid et al. 2019). Specific Internet security experts support a Cybersecurity Ventures study and predict that cybercrime financial harm would exceed $6 trillion by the end of this year. "Experts for cybersecurity forecast that every 11 s in 2021, a cyber attack will take place. The area of natural computation combines computing with expertise from various fields of science, such as physics, chemistry, biology, mathematics, and engineering. It enables the creation of new computational tools, such as algorithms, hardware, or wetware. The NIC is interdisciplinary. AI allows us to design autonomic computing resolutions proficient in adapting to their utilization and applying self-tuning, self-management, selfdiagnosis, self-configuration, and self-healing (Sivakumar 2020). When it comes to information security, artificial intelligence techniques seem a very encouraging research area that enhances the security measurement for cyberspace (Elhoseny et al. 2018). Data science, and Cognitive machine Learning, have been employed to reduce operating costs, streamline back-end processes, and implement analytics efficiently to produce better forecasts in the healthcare sector. The term cognitive computing is used to describe AI systems designed to simulate human thinking. Several AI technologies are necessary to construct mental models to develop human processes such as machine learning, profound learning, neural networking, NLP, and sentiment analysis in a computer system. Machine Learning is a machine learning algorithm that builds on this data. Cognitive computing is systems that learn on a scale, usefulness, and naturally interact with people. Three ways to integrate the business can be streamlined. Precise figures for shipment and accessibility. Incorporating the e-commerce ERP ensures that ERP is communicated during shopping phases, customer travel, and streamlined management via the e-commerce platform. For enhanced decision-making, machine learning algorithms sincerely rely on Internet of Things (IoT) data produced and transmitted from the IoT devices. Because of CPS's heterogeneity, it is incredible to construct every device in a secure setting, making all the measurements from the systems impracticable for training the ML algorithm (Shu et al. 2020). Thus, the initial step is to model the abstract device behavior, contingent upon its difficulty, to produce the data for training the ML algorithms. Within a CPS and IoT context, diverse IoT layers, such as transportation, perception, and application layers, are vulnerable to cyber-attacks. Data are information used to train a learning algorithm or computer to predict the results that the model is designed to predict. If they use supervised learning or some combination that requires this method, the data are enriched with an annotation or data marking. One thing is an individual or physical object with a unique identifier, a built-in device, and the ability to transmit data over a network within the Internet of Things (IoT). For instance, node tampering, malicious code injection, Denial of Service Attacks, impersonation, Data Transit attacks (man-in-the-middle attack, sniffing), and Routing Attacks are some of the cases of cyber-attacks in an IoT and CPS system model (Vijayakumar et al. 2019).

The significant contribution of the study is,

- Designing the CML-ADF model for securing the healthcare data based on a Cyber-physical system.

  Adopting advanced cognitive machine learning techniques for cyber-attack and anomaly detection for CPS device embedded in a medical health monitoring system. The identification of threats means the analysis of a safe environment to recognize malicious activities that could damage the network. If a threat is discovered, attempts must be made to mitigate the danger properly before taking advantage of any existing vulnerabilities. The alignment of cybersecurity and patient safety policies would not alone support the protection of patient safety and privacy by your company and ensure that high-quality treatment continues effectively by mitigating disruptions that can adversely affect the clinical outcome.
- The simulation results have been performed, and the proposed method enhances the detection accuracy, attack prediction, efficiency, minor delay, and communication cost compared to other existing methods.

The remainder of the study is organized as follows: Sect. 1 and Sect. 2 discussed the cyber-physical system's overview of healthcare and existing methods. In Sect. 3, the CML-ADF model has been proposed. In Sect. 4, the simulation analysis has been performed. Finally, Sect. 5 concludes the research paper.

2 Background study and the features of this research paper

Dan tang et al. (Tang et al. 2020) proposed the LDoS attack detection method based on multiple features of network traffic and an improved Adaboost algorithm (MF-Adaboost). They create a network feature collection to quantify components and select traffic data from networks. The calculation function will derive the most valuable data from network traffic and decrease the network data size. The list of parts is used to choose the best classification functionality to guarantee efficient training for the detection algorithm. This approach uses a classification algorithm in the machine learning field, the Adaboost algorithm. The findings show that their system can effectively detect LDoS attacks.

SEO JIN LEE et al. (AlZubi 2019) suggested the IMPersonation Attack deteCTion using deep auto-encoder and feature abstraction (IMPACT). Deep learning uses the gradient-based SVM to organize and operate on a resource-constrained system by decreasing the number of functions using a stacked autoencoder (SAE), shared knowledge C4.8 wrapper for extraction collection. The Effect is trained on the Aegean Wi-Fi Interference Dataset. The proposed IMPACT findings reveal that 98.22% accuracy was reached with 97.6% identification and 1.2% false alarm, and the new state-of-the-art benchmark methods met the norm amount. The investigation of the AWID database features for further production of IDS is another critical contribution in this study.

Xu et al. (Lee et al. 2020) introduced the Certificateless Signature Scheme (CLS) based on NTRU lattice for the medical cyber-physical system. The latter is based on small integer solutions on NTRU grids and is proven to be resilient to the quantum attack. Protection analyses and performance tests reveal that our proposed method's coordination and measurement costs are substantially lower than two other rival quantum resiliency systems, thus delivering quantum assault resiliency. However, as quantum computers become a reality, quantum survival protection solutions must be planned.

Meng et al. (Xu et al. 2020) initialized a trust-based intrusion detection approach (TBIDA) based on behavioral profiling. The node's reputation is to be judged when the disparity between two behavioral profiles in Euclidean can be established. Our method is tested in a specific MSN setting by interacting with a realistic center in the assessment. Experimental findings indicate that our approach is more rapid than other similar approaches when identifying malicious MSN nodes. MSN nodes can be extracted by defining the disparity between two behavioral profiles in Euclidean distance. They have examined their performance in an actual MSN environment by working with a functional medical center. Experimental data reveal that our mechanism is more potent than other related steps to detect malicious MSN nodes.

AlZubi et al. (Meng et al. 2020; Al-Maitah 2019) discussed the artificial intelligence-based heuristic health management system (AI-HHMS). This system improves patients' live databases' security and privacy and the combination of medical care through multiple points of view incredibly closely. These programs include experts, experts, supervisors, and staff to make sound decisions more efficiently. Furthermore, protection and data quality should be part of any event, task, or arrangement of IoT usage by configuration. The health data sets with IoT-assistant sensors improve and minimize the safety risk using the IoT-sponsored artificial intelligence heuristic health system. The experimental findings indicate positive results concerning multiple success variables. The device reaches 99,75% of precision, 0,0646 error rate, and 98,46% of positive conditions, 98,6% of details, and 99,66% of accuracy.. The system is implemented with the application MATLAB.

In this paper, the CML-ADF model has been suggested to detect anomaly and attack behavior in healthcare networks to secure patient data to overcome these issues. Healthcare is still typical in malware, cryptography, data robbery, phishing, and threats to insiders. Consumers are now more concerned that their PHI is being jeopardized by high-profile violations such as Anthem and Allscripts. Disagreements in cybersecurity: Cyber criminals may lock their machines, servers, or even entire networks by using malware and ransomware, a cloud threat: malware and restitution: There are more and more secure in the cloud health data saved. The following section, 3, discusses the proposed CML-ADF model briefly.

3 Cognitive machine learning assisted attack detection framework (CML-ADF)

Cyberphysical systems (CPS) are the future of automated medicine. They will ensure high-quality real-time care, reliability, and speed to save our patients' lives 24 h a day in terms of their patients' privacy. In cyber-physical systems, real-world physical and automated computational process integrations are combined. CPS are dynamic engineering structures that relate to the convergence of physical process equations and communication processes. Medical automation is described as the controlled operation by mechanical or electronic means of a diagnostic or therapeutic procedure or system, which increases people's observer, effort, and decision-making skills. High-quality care with compassion, integrity, and respect should be as healthy and prosperous as possible. In addition to clinical quality and protection, quality means personalized treatment for every individual. Cyber-physical systems interacting with the physical environment must be ready for unforeseen circumstances and flexible to subsystem failure. Healthcare cyber-physical (HCPS) systems allow the smooth incorporation of physical and computational elements into life-critical, medical device' context-aware networked systems. HCPS provides a promising forum for improving patient treatment effectiveness and providing high-quality healthcare in recent innovations on the internet, including wireless sensors, connected medical equipment, and mobile healthcare. HCPS continuously monitors, evaluates, and detects the patient's diagnostic health and delivers timely treatment through direct input from healthcare professionals or through automated treatments using the medical sensor and actuators. This paper proposed the CML-ADF model for detecting cyber-attacks in healthcare networks to secure patient data using CPS and cognitive ML models.

Cognitive machine-learning models can be used to model decisions of adversaries and network events. A noticeable or dangerous patient should not be allowed to make a medical mistake ("iatrogenesis"). It can include an incorrect or unfinished condition, accident, syndrome, stomach, cancer, or other disease diagnosis or treatment. Data security is a data protection tool against unauthorized access and corruption over its entire life cycle. Protection of data encryption, hacking, tokenization, and critical management operations, identity protection on all applications and platforms. The Health Information System is a technology-driven system that makes it truly easy for organizations and providers to share safe health information (PHI). Besides, patients may receive seamless, organized treatment from healthcare providers because of this scheme.

Figure 1 shows the healthcare cyber-physical system. CPS consists of the following methods: a computing system to monitor and control the physical process, and sensors and actuators to interfere with the physical process and manage the biological approach. Using a communication network to link these modules within each system and even the scenarios individually, remote monitoring and control, scalability, stability, and decentralization of authorities give many advantages. The suggested method provides many physical systems to be associated with cyber systems. Thus, the communication protocol enables physical system formations and uninterrupted, continuous data transmission for real-time application. The communication cost has been minimized utilizing the proposed CML-ADF model.

Figure 2 shows the adversarial attack detection in an intelligent healthcare system. An innovative healthcare system contains a single or a collection of intelligent medical devices (implantable devices, wireless, wearables devices.) to gather data from a patient's body to deliver enhanced handlings and real-time tracking. The Smart Health System considers different medical criteria (vitals of the patient) and non-medical (physical position, status) and offers real-time monitoring to understand the patient's overall condition. Intelligent medical devices use an analog signal to use vital signs, transform them into a digital signal, send data through wireless technology (Zigbee, Bluetooth, etc.), make up a laptop, smartphone, etc., smartwatch a network packet to an individual digital assistant. Personal digital assistant functions like an interface to use and transfer data to a database (local servers, cloud servers, etc.). The database sends data to a Data Processing model, which utilizes Machine Learning to choose and extract features from the dataset. The Central Data Processing Unit uses an ML model. Central Data Processing Unit runs the ML model to detect the patient condition, regular patient activity, and SHS threats. Next, automatic measures are taken to provide improved patient treatment (e.g., change of medicine, pushing a new dose of the drug, etc.) and sending analyzed data to the approved entity (doctor or hospital).

In conclusion, the doctor sends the patient an updated health status management plan. Intelligent health care equipment connected to the patient body, e.g., EEG, ECG, pulse oximeter, etc., collects data about various vital signs (e.g., oxygen in the blood, nervous activity, heart rate, etc.). As different smart medical devices produce various data sets, adversaries can know that machines are partly distributed with data. On that basis, a data value can be changed in a certain threshold to alter the patient's condition or regular pattern of activity. An adversary will know about the SHS architecture in its entirety or part, including the number of devices, device correlations, etc. An adversary can know the ML model's performance labels to trigger an attack, such as disease conditions and standard activity patterns. For disease and user activity identification, various ML models will be used. An

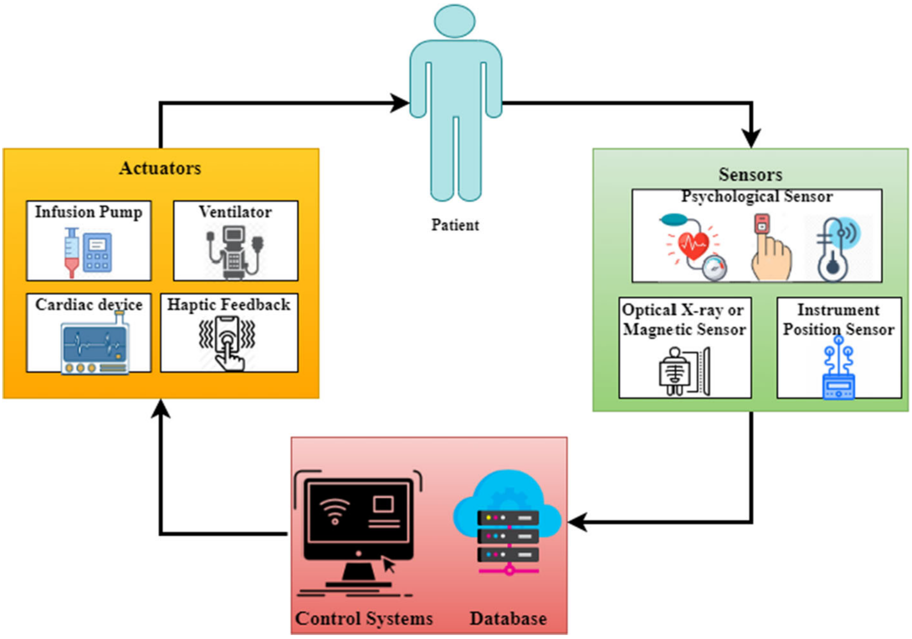


Fig. 1 Healthcare cyber-physical system

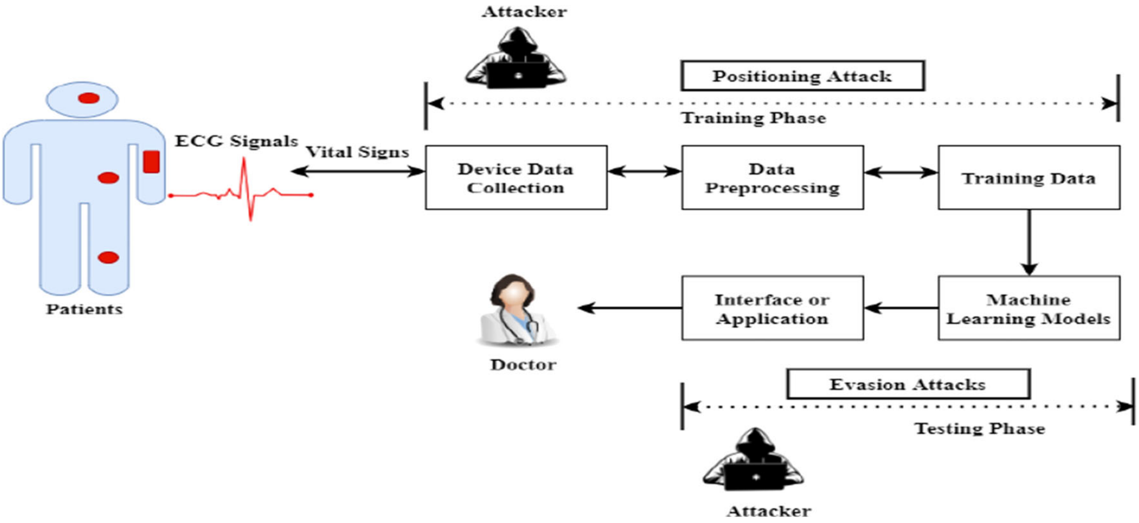


Fig. 2 Adversarial attack detection in an innovative healthcare system

adversary should know the underlying ML model for classifying the status of the patient. The ML-based healthcare system can be regarded as a data processing pipeline to analyze patients' vital signs for disease diagnosis and treatment. A device data collector model gathers data from the various intelligent medical devices representing the patient's vital signs and status and transmits them into the pre-processing data model. A data pre-processing model samples and saves the data consistent with the respective sample frequencies as a range. The sampled data are utilized for training machine learning for the monitoring and detection of diseases in real-time. The training data are marked with various diseases and benign conditions to understand the multiple scenarios' data patterns. Patients' physiological data in the testing phase shall be analyzed based on the formerly learned machine learning model to identify various diseases or patient conditions. In the context of the data processing pipeline, our attack methodology can be defined here. An adversary effort either to deploy data gathering or processing to change the original ML model. A Cyber-physical system (CPS) is a computing and networking integration of physical systems. It can make social life more intelligent. Wireless sensor networks (WSN), a significant driving force behind the CPS applications, may be vital to the CPS. The medical device protection solution must safeguard firmware against tampering, protect stored data from the device, secure communication, and prevent cyber attacks.

Even by building safety from the early stages of construction, can this be accomplished. Cloud storage is a cloud model that stores data on the Web through a cloud-based provider who administers and uses data storage as a service. It is on-demand with just-in-time capacity and costs and removes the acquisition and management of your own data storage facilities. Cyberpsychology is an examination of the human mind and comportment and its effects on the culture of technology, particularly virtual reality and social media. Mainstream research studies concentrate on the psychology of individuals and communities across the internet and cyberspace. Clinical Decision Assistance (CDS) offers healthcare and wellness services, intelligently filtered or delivered at an appropriate time to physicians, staff, patients, and other persons with experience and personal information. CDS includes a range of instruments to improve clinical workflow decision-making.

A standard feedback control system has four elements: (1) the physical occurrences of interest, (2) sensors to perceive the physical system and send a period sequence x_l indicating the physical measurement value at period l. (3) based on the sensor measurements received x_l, the controller sends a control command v_l And (4) actuator that changes the control commands to actual physical changes. Common security tracking framework for a control system that looks into the physics of the systems requires an anomaly prediction system that receives as inputs the sensor measure x_l from the physical systems and the control command v_l sent to the physical systems, and then utilizes them to determine any distrustful sensor or control command. The notion of monitoring sensor measure x_l and control command v_l and to utilize them to recognize issues with sensors, controllers, or actuators.

Physical model prediction Let's consider the sensor x_l and control command v_l, a model of the physical systems will detect anticipated future measurements $\hat{x}_{l+1}$. Auto-Regressive (AR) model has been employed for prediction.

$$\hat{x}_{l+1} = \sum_{j=l-M}^{l} \beta_j x_j + \beta_0 \tag{1}$$

As inferred from Eq. (1) where β_j denotes the coefficient learned via system credentials and x_j indicates the final M sensor dimensions, where the number of factors to learn M can be computed to avoid the model's overfitting. It is probable to determine the coefficients β_j by addressing a problem of optimization that reduces residues.

This paper calculates the inputs (control command v_l) and outputs (sensors measurement x_l) for subspace model identification approaches, generating the subsequent model,

$$\begin{aligned} y_{l+1} &= By_l + Av_l + \varepsilon_l \\ x_l &= Dy_l + Cv_l + \varepsilon_l \end{aligned} \tag{2}$$

As shown in Eq. (2), where B, C, D, and C denotes matrices modeling the physical system dynamics. Biological systems are strictly causal and then, thus, generally $C = 0$. The control command $v_l \in \mathbb{R}^q$ affect the next period step of the system state $x_l \in \mathbb{R}^m$ and sensor measurements $x_l \in \mathbb{R}^p$ are modeled as a linear combination of these hidden states. e_l and ε_l are perturbation and sensor noise and are presumed to be a random progression with 0 means.

Anomaly detection Given a time sequence of residuals r_l (the variance between the received sensor extent x_l and the expected/predicted measurement x_l), the anomaly detection test necessities to identify when to increase the alarm. Anomaly detection policies depend on enduring can be separated into two major types: Stateful and Stateless. Patient-Centered Design (PCD) is a particular type of User-Centered Design (UCD) in which the end-user is a patient who uses ICT for healthcare. In addition to a health specialist's clinical consultations and recommendations, the patient-oriented approach includes delivering special care services to address a patient's unique values, needs, and desires. The healthcare system is changing its paradigm. Patient-Centered Design (PCD) is a particular type of User-Centered Design (UCD) where the end-user is a patient who uses ICT for healthcare. In addition to a health specialist's clinical consultations and recommendations, the patient-oriented approach includes delivering special care services to address a patient's unique values, needs, and desires. The healthcare system is changing its paradigm. The standard format for manuscripts of short stories, novels, poetry, and other literary works is the formatting style.

In a Stateful test, this paper computes a supplementary statistic W_l that retains monitor of the past changes of r_l and make an alert if $W_l \geq \tau$, that is, if there is a persistent deviation across manifold period-steps. Countless tests can retain monitor of the past behavior of the enduring r_l such as taking a mean over a time window utilizing change discovery statistics like the nonparametric Cumulative sum statistic. In a Stateless test, it raises the alarm for each significant deviation at period l: that is, if $|x_l - \hat{x}_l| = r_l \geq \tau$, where τ is a threshold.

Figure 3 shows the proposed CML-ADF. Our proposed attack detection framework is a physical-domain method. It makes attack detection at the physical layers by monitoring and modeling the healthcare physical device's physical behavior or procedure. Monitoring and modeling are accomplished utilizing machine learning methods. The physical measurements obtained for modeling can be tremendously high as the cyber-physical system becomes progressively complex; monitoring and modeling the plan depend on the physical extents become complex. Our effort in emerging the suggested attack detection framework concentrates on originating salient signature or feature from the noise measurement. The produced features capture the dynamic relationship between the measures enormously well and, more significantly, have more discriminant power in unprecedented standard attack and operation events, permitting us to attain more precise and robust prediction performance.

For Healthcare cyber-physical system attack detection, this paper concentrates on producing features that can be improved capture the cyber-physical system asset and are good in acute attack from usual activities. Though our feature can be any signatures computed from any physical measurements, the suggested attack detection framework utilizes three types of features: physics, learning, and statistics-based, to seizure both temporal and spatial possessions of the physical systems. In spatial calculation, this study calculates features on multiple (multivariate) and distinct (univariate) measurements, correspondingly. This paper executes our features computing over the sliding window to capture the whole system's dynamics or temporal possessions. Let's presume m physical measurements, $w^{(1)}, w^{(2)}, \ldots w^{(M)}$, cover actuator measurements, sensor measurement, and potentially period-changing control constraints, and the window width for the sliding window is s. The network delay has been reduced using the proposed CML-ADF model.

For every individual measurement, $w^{(j)}$, its window segment of measurement at period t is $n_t^j = \mathrm{w}_{t-s}^{(j)}, \mathrm{w}_{t-s+1}^{(j)}, \ldots \mathrm{w}_t^{(j)}$. Many statistical descriptions can be computed for the segment of measurements, $n_t^{(j)}$ for instance,

$$f_1^{(j)} = \text{median}\left(n_t^{(j)}\right) \tag{3}$$

$$f_2^{(j)} = \text{std}\left(n_t^{(j)}\right) \tag{4}$$

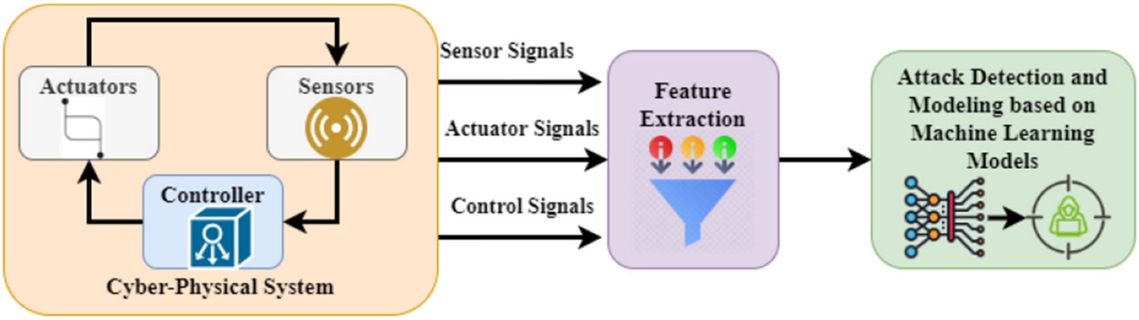


Fig. 3 Proposed CML-ADF

$$f_3^{(j)} = \max\left(n_t^{(j)}\right) \tag{5}$$

$$f_4^{(j)} = \max\left(n_t^{(j)}\right) - \min\left(n_t^{(j)}\right) \tag{6}$$

$$f_5^{(j)} = w_t^{(j)} \tag{7}$$

Besides, for every measurement, this paper calculates the extreme rate-of-variation of the measurements segment, $n_t^{(j)}$.

$$f_6^{(j)} = \max\left(\text{abs}\left(\text{diff}\left(n_t^{(j)}\right)\right)\right) \tag{8}$$

An autoencoder (AE) has two portions: a decoder and an encoder. The encoding function maps an input $y \in \mathbb{R}^{o_y}$ to hidden representation $h(y) \in \mathbb{R}^{o_g}$ that is, $g(y) = w_f\left(Sy + a_g\right)$, where w_f denotes a nonlinear activation function, usually a logistic sigmoid function. The process of decoding map hidden depiction g rear to a reconstruction $w_h(S'g + a_x)$, where w_h indicates the decoder's activation function, usually a sigmoid function.

Autoencoder training includes finding variable $\theta = \left\{S, a_g, a_x\right\}$ that reduce the rebuilding error on a training sets of instances, O, $\underset{\theta}{\text{again}}\left(\sum_{y \in O} y - x^2\right)$. To avoid trivial hidden depictions, some regularization processes are required. Denoising autoencoder (DAE) including corrupting input y during training the autoencoder and corrupting the input y in the encoder restructuring the version of y in the decoder stage. Supporting denoise as a portion of the training measures guarantees the extracted feature to have improved illustration abilities. Considering all the estimated features: the univariable function, the remaining physical model, and the learned feature provide us with the last collection of components to input our attack detection system.

The intense learning machine demonstrates in Fig. 4. As our model for detection, this paper adopts controlled classification approaches. The Extreme Learning Machine (ELM) is used for its many special functions as a detection model. Extreme Learning Machine is a unique type of neural feed network. In the conventional feed-forward neural network where training the networks includes discovering every connection weight and bias, in Extreme Learning Machine, the association between hidden and input neurons is randomly produced and fixed. They do not require to be trained. Therefore, teaching an Extreme Learning Machine develops finding association among output and hidden neuron, which is merely a linear least-square issue whose solution can be systematically resolved by the comprehensive converse of the hidden layer output matrices. Due to such a superior intention of the network, Extreme Learning Machine training suits very efficiently. Moreover, Extreme Learning Machine has good simplification performance than other ML algorithms involving support vector machine and is more effective and efficient for both regression tasks and classification.

Let's consider the datasets $\left\{\left(y_j, x_j\right)\right\}_{j=1}^{M}, y_j \in \mathbb{R}^o, x_j \in \mathbb{R}^l$ with l class and a network with K hidden neurons. The network output for an input y is evaluated as,

$$f(y) = \sum_{j=1}^{K} \alpha_j g_j(y) = g(y)\alpha \tag{9}$$

As discussed in Eq. (9) where $g_j(y) = H\left(s_j, a_j, y\right), s_j \in \mathbb{R}^o, a_j \in \mathbb{R}^1$ denotes the output of jth hidden neuron concerning the input y; $H(s, a, y)$ denotes the nonlinear piecewise continuous function sustaining Extreme Learning Machine universal estimation capability theory; α_j indicates the output weight vector among jth hidden neurons to the $l \geq 1$ output node $g(y) = [g_1(y), \ldots g_K(y)]$ denotes a random feature mapping the data.

For the equivalence optimization restraints-based Extreme Learning Machine, the undefined variable is determined via the subsequent optimization:

$$\text{Minimize: } K_q = \tfrac{1}{2}\alpha^2 + \tfrac{1}{2}D\sum_{j=1}^{M}\xi_j^2$$

$$\text{Subject to : } g\left(y_j\right)\alpha = x_j^T - \xi_j^T, j = 1, \ldots M \tag{10}$$

As shown in Eq. (10) where $\xi_j = \left[\xi_{j,1}, \ldots \xi_{j,l}\right]^T$ denotes the training error vector of the l output node concerning the

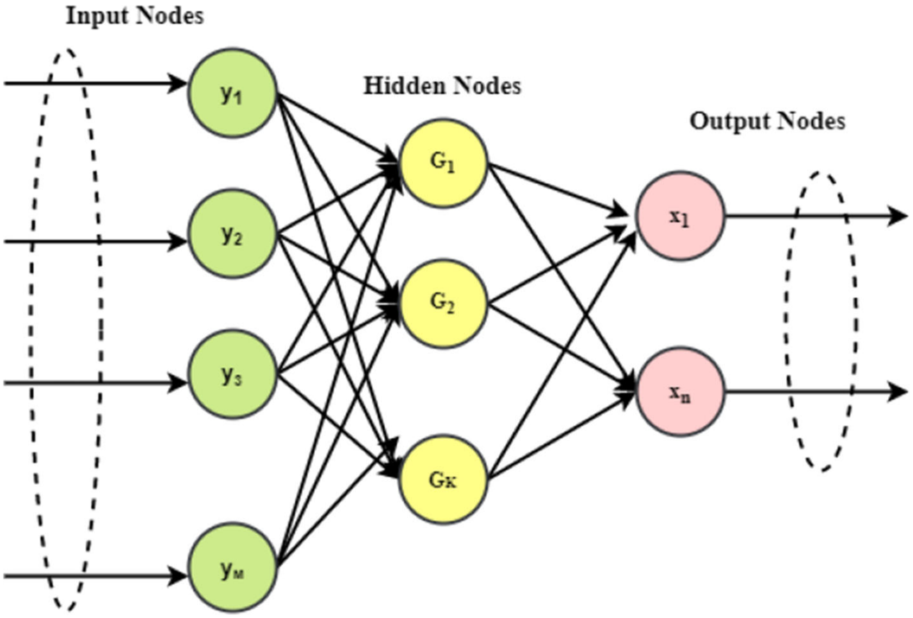


Fig. 4 Extreme learning machine

training samples y_j and the constant D control the tradeoffs among the training error and output weight. The attack detection accuracy has been improved based on these expressions.

The comparable double optimization target function of Eq. (10) is

$$K_d = \frac{1}{2}\alpha^2 + \frac{1}{2}O\sum_{j=1}^{M}\xi_j^2 - \sum_{j=1}^{M}\sum_{i=1}^{l}\beta_{j,i}\left(g\left(y_j\right)\alpha_i - x_{j,i} + \xi_{j,i}\right) \tag{11}$$

Depending on the Karush–Kuhn–Tucker statement, this paper considers the resolution for the Extreme Learning Machine output function $f(y)$,

$$f(y) = g(y)\alpha = g(y)G^T\left(\frac{J}{D} + GG^T\right)^{-1}X \tag{12}$$

As inferred from Eq. (12), where G output matrix of the hidden layer.

$$G = \begin{bmatrix} g(y_1) \\ \vdots \\ g(y_M) \end{bmatrix}\begin{bmatrix} g_1(y_1) & \cdots & g_K(y_1) \\ \vdots & \vdots & \vdots \\ g_1(y_M) & \cdots & g_K(y_M) \end{bmatrix} \tag{13}$$

The expected class labels for the input considers more than two-class classification,

$$\text{label}(y) = \underset{j\in 1,2,\ldots l}{\text{argmax}}[f_1(y), f_2(y), \ldots f_l(y)]. \tag{14}$$

When the objective class, X, is one class, the only α suits a linear calculation mapping from $g(y)$ to X is a hyperplane estimation. Now the distance of test samples, $\bar{y}$, to the hyperplane built by the Extreme Learning Machine is stated as:

$$o(\bar{y}) = \left|g(\bar{y})^T\alpha - x\right| = \left|g(\bar{y})^T G^T\left(\frac{J}{D} + GG^T\right)^{-1} - 1\right|. \tag{15}$$

The distance can suitably attend as the anomaly value; i.e., the higher space is, the more probable the sample is an abnormality. The execute abnormality prediction, this paper applies a threshold to the abnormality scores. $\bar{y}$ is anomalous if $o(\bar{y}) \geq T_g$ Else, it is regular. By cross-validation, the threshold could be identified because of the distance spreading for every standard sample. The proposed CML-ADF method achieves high attack prediction, accuracy, efficiency, minor delay, and communication cost compared to other existing methods.

4 Simulation analysis

The proposed CML-ADF method's experimental results have been performed based on the performance metrics such as attack prediction ratio, detection accuracy, communication cost, delay, and efficiency ratio.

(1) Attack Prediction Ratio
Adversaries in ML-based healthcare schemes aim to change the multi-layer machine learning classifier's data distribution to change the forecast condition. Some of these attacks are directed at medical images to reverse the disease predicted. The change the expected labels with high confidence, universal adversarial problems may be applied to a medical image. The proposed method to identify susceptible locations in a medical time chain using adverse

attacks on deep predictive models. ML-based classification for disease diagnosis and real-time patient tracking. This paper takes the view that the devices are working well, and the machine has no compromise. In this post, a new attack against the adversary will be added to reap brilliant healthcare system benefits and alter a patient's condition to provide the wrong treatment. The carry out the ML model adversarial attack, this paper introduces the positioning attack and evasion attack. Figure 5 shows the attack prediction ratio.

(2) Detection Accuracy Ratio

This paper's primary goal is to design and develop an attack detection system with high accuracy, low communication cost, common false positives, scalability and flexibility, and the Healthcare CPS environment. Explicitly, this study explores a machine learning model (using Extreme Learning Machine) to deliver robust attack detection in HCPS, as shown in Fig. 6. The prediction accuracy is based on an initial training phase, where the model learns how to predict the output based on a set of training data, which involves known input–output pairs. With the generated features, this study can cause better seizure of the dynamic, nonlinear relationship of the physical system when collecting the elements with the supervised ML detection model, extreme learning machine, and high accuracy in the early detection of malicious and attack behaviors.

(3) Efficiency Ratio

Incorporating machine learning to detect and analyze clinical parameters has surely enhanced healthcare efficiency and quality. The feature extraction from the dataset in machine learning can make possible patient-centric therapy and help, ultimately leading to a decrease in medical expense and creating an improved patient-doctor relationship. Our method is effective and can defend confidentiality and integrity. The design architecture, idea, security definition, formal definition, communication protocols of our approach are provided in the study. Widespread analysis and assessment show that our efficient and secure method has excessive practicability in Healthcare cyber-physical systems. Figure 7 shows the detection accuracy ratio.

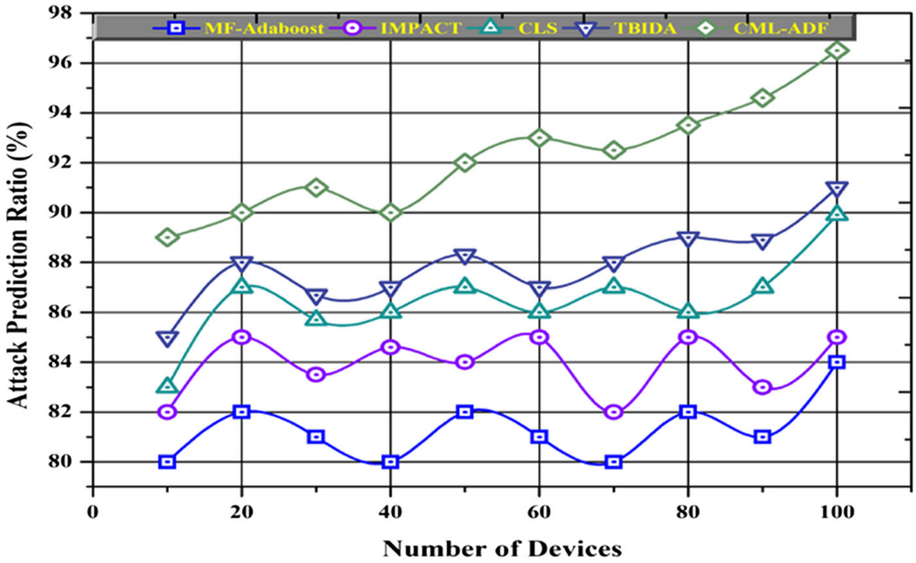
(4) Delay Ratio

Communication failures occur most frequently during shift changes, as patient treatment is shifted to some other caregiver. When the changeover is made with incorrect, inaccurate, or ambiguous information, it increases medical mistakes. Incorrect or unpublished call scheduling and uncertainty about the delivery of one-way communication may be due to decapitated mobile phone facilities inside a hospital, charging for the provider's wrong level, awaiting calls and change. The consistency and timeliness of medical care are compromised when contact is postponed. It can result in medical complications, lengthy periods to wait, delayed releases, poor decision-making, and heightened tension. A fast, seamless, and complete communication system is essential to ensure effective and reliable patient care. Figure 8 shows the delay ratio.

(5) Communication Cost Ratio

Significant cost metrics like a medical bill and compensation for insuring health are created by medical behaviors that are not traditional health data and can be used to analyze and calculate medical

Fig. 5 Attack prediction ratio



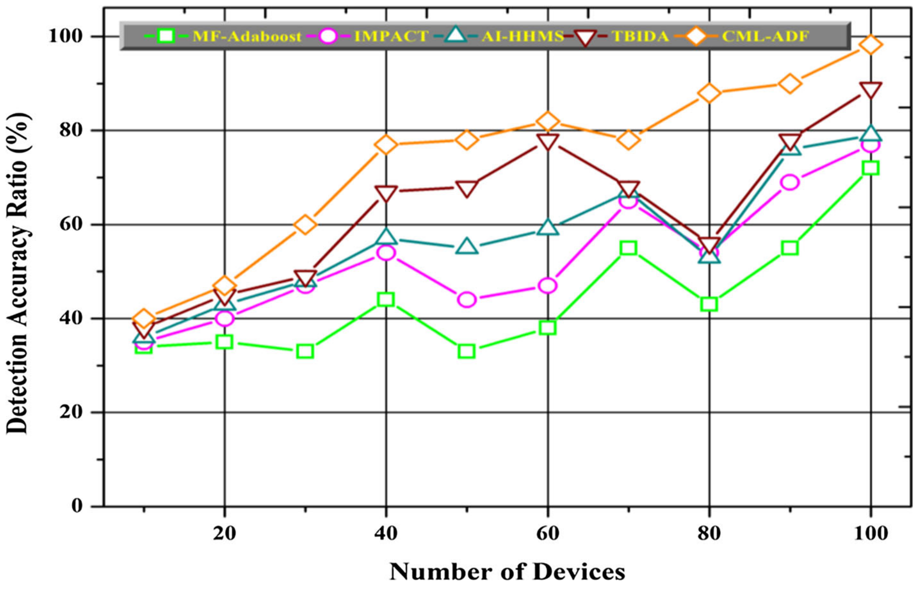


Fig. 6 Detection accuracy ratio

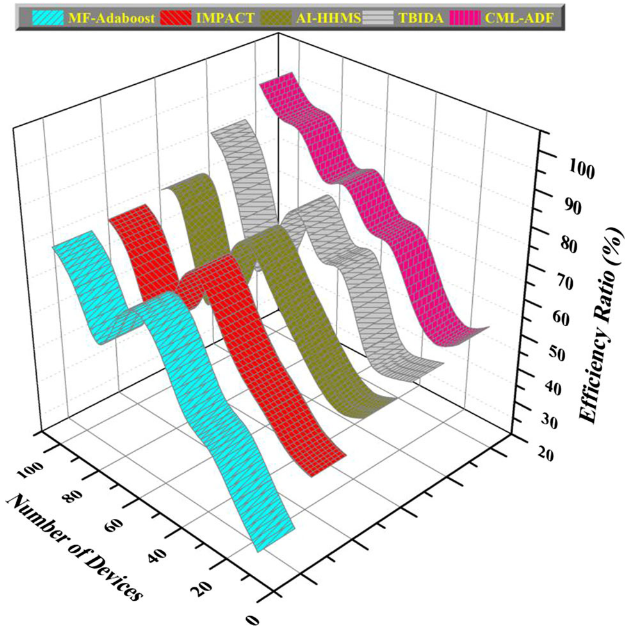


Fig. 7 Efficiency ratio

expenditures. These are usually stored in various medical institutions' databases, dispersed geographically, and unified. Machine learning algorithms for data fusion, pre-processing, and resource complexity are preventive in implementing it in the MCPS environment. This paper aims to design and build a high-accuracy, low false favorable, low communication costs, and flexibility and scalability system suitable for the MCPS environment with these constraints. The dispersion system is used for storing information in a secure position, such as the end-user personal computer and retrieval of the small encrypted subset of data. The remaining datasets are saved for cost-saving purposes on cloud servers. Figure 9 shows the communication cost ratio.

The proposed CML-ADF method secures the patient data in the healthcare network. The experimental results showed that the Certified Signature Schema's IMPersonation Attack Detection Systems (IMPACT) improved high-attack predictions, precision, effectiveness, reduced delays and communication compared to other existing network traffic mitigation features, and enhanced Adaboost algorithms.

5 Conclusion

This paper presents the model for patient data security and privacy in healthcare networks. This study includes a brief analysis and the related research challenges to secure cyber-physical system development on security threats at various cyber-physical system levels and their corresponding threat models. This paper offers a comparative study of the most advanced, static, and adaptive identification and prevention methods and their related limitations to address these challenges. ML-based security techniques against a range of identified attacks on several CPS layers are discussed, and open research issues in developing smart CPS security protocols are established at the end of the paper. The CML-ADF scheme guarantees the CPS security of healthcare information and decreases the local load from the effectiveness analysis and numerical outcomes. The proposed model achieves an attack prediction ratio of

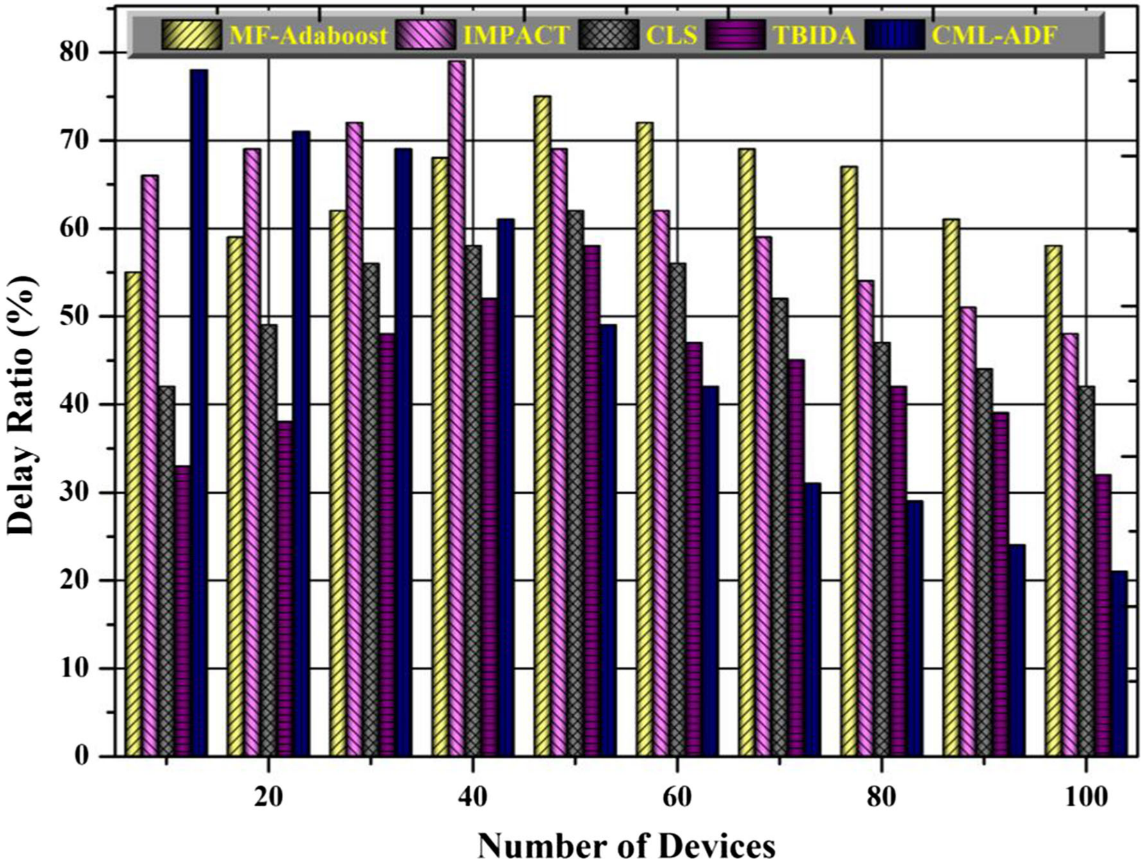


Fig. 8 Delay ratio

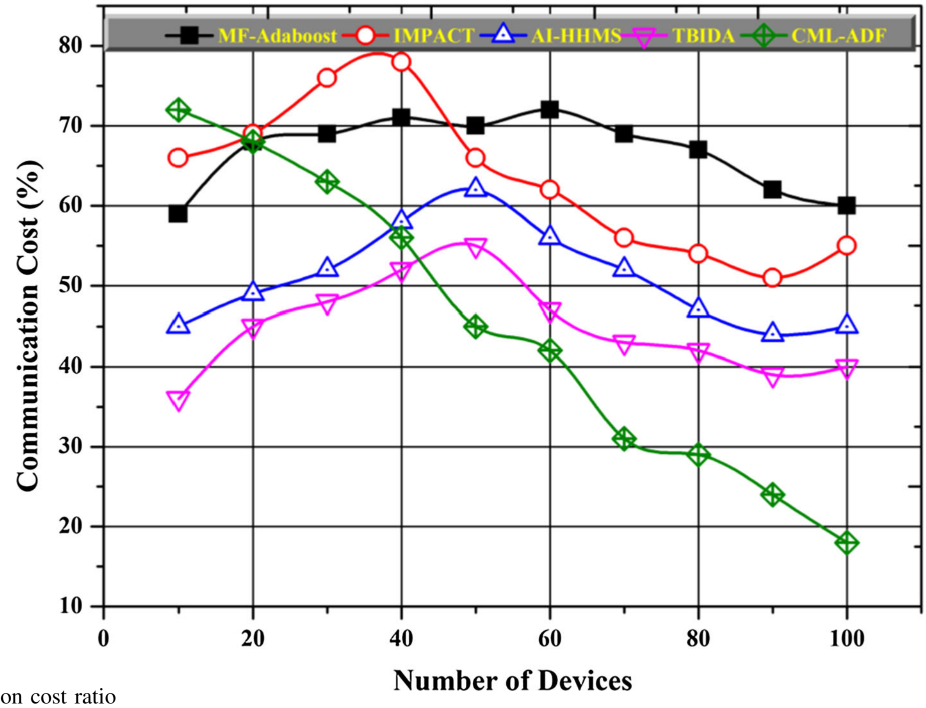


Fig. 9 Communication cost ratio

96.5%, and accuracy ratio of 98.2%, an efficiency ratio of 97.8%, less delay of 21.3%, and a communication cost of 18.9% compared to other existing models.

Acknowledgements The authors extend their appreciation to the Deanship of Scientific Research at King Saud University for funding this work through research group No. (RG-1439-053).

Compliance with ethical standards

Conflicts of interest The authors declare that they have no conflict of interests.

References

Abdali-Mohammadi F, Meqdad MN, Kadry S (2020) Development of an IoT-based and cloud-based disease prediction and diagnosis system for healthcare using machine learning algorithms. Int J ArtifIntell ISSN 2252(8938):8938

Al-Maitah M, AlZubi AA, Alarifi A (2019) An optimal storage utilization technique for IoT devices using sequential machine learning. Comput Netw 152:98-105

Al-Mhiqani MN, Ahmad R, Abidin ZZ, Ali NS, Abdulkareem KH (2019) Review of cyber attacks classifications and threats analysis in cyber-physical systems. Int J Technol Secur Trans 9(3):282–298

AlZubi AA (2019) An optimal sensor placement algorithm (O-SPA) for improving tracking precision of human activity in real-world healthcare systems. Comput Commun 148:98–105

Elhoseny M, Ramírez-González G, Abu-Elnasr OM, Shawkat SA, Arunkumar N, Farouk A (2018) Secure medical data transmission model for IoT-based healthcare systems. IEEE Access 6:20596–20608

Farivar F, Haghighi MS, Jolfaei A, Alazab M (2019) Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber-physical systems and industrial IoT. .IEEE Trans Ind Inform 16(4):2716–2725

Gopalakrishnan T, Ruby D, Al-Turjman F, Gupta D, Pustokhina IV, Pustokhin DA, Shankar K (2020) Deep learning enabled data offloading withcyberattack detection model in mobile edge computing systems. IEEE Access 8:185938–185949

Gupta R, Tanwar S, Al-Turjman F, Italiya P, Nauman A, Kim SW (2020) Smart contract privacy protection using AI in cyber-physical systems: tools, techniques and challenges. IEEE Access 8:24746–24772

Haghighi MS, Farivar F, Jolfaei A, Tadayon MH (2020) Intelligent robust control for cyber-physical systems of rotary gantry type under denial of service attack. J Supercomput 76(4):3063–3085

Hassan MU, Rehmani MH, Chen J (2019) Differential privacy techniques for cyber physical systems: a survey. IEEE Commun Surv Tutor 22(1):746–789

Iqbal R, Doctor F, More B, Mahmudand S, Yousuf U (2020) big data analytics and computational intelligence for cyber–physical systems: recent trends and state of the art applications. Future Gener Comput Syst 105:766–778

Khan F, Ahamed J, Kadry S, Ramasamy LK (2020) Detecting malicious URLs using binary classification through ada boost algorithm. Int J Electr Comput Eng (2088–8708) 10

Kurde S, Shimpi J, Pawar R, Tingare B (2019) Cyber physical systems (CPS) and design automation for healthcare system: a new era of cyber computation for healthcare system. Structure 6(12)

Lee SJ, Yoo PD, Asyhari AT, Jhi Y, Chermak L, Yeunand CY, Taha K (2020) IMPACT: Impersonation attack detection via edge computing using deep autoencoder and feature abstraction. IEEE Access 8:65520–65529

Marques G, Miranda N, Kumar Bhoi A, Garcia-Zapirain B, Hamrioui S, de la Torre Díez I (2020) Internet of things and enhanced living environments: measuring and mapping air quality using cyber-physical systems and mobile computing technologies. Sensors 20(3):720

Meng W, Li W, Wang Y, Au MH (2020) Detecting insider attacks in medical cyber–physical networks based on behavioral profiling. Futur Gener Comput Syst 108:1258–1266

Poongodi M, Vijayakumar V, Al-Turjman F, Hamdi M, Ma M (2020) Intrusion prevention system for DDoS attack on VANET Withre CAPTCHA controller using information based metrics. IEEE Access 7:158481–158491

Qi L, Chen Y, Yuan Y, Fu S, Zhang X, Xu X (2020) A QoS-aware virtual machine scheduling method for energy conservation in cloud-based cyber-physical systems. World Wide Web 23(2):1275–1297

Qiu H, Qiu M, Liu M, Memmi G (2020) Secure health data sharing for medical cyber-physical systems for the healthcare 4.0. IEEE J Biomed Health Inform 24(9):2499–2505

Shakeel PM, Baskar S, Dhulipala VS, Mishra S, Jaber MM (2018) Maintaining security and privacy in health care system using learning based deep-Qnetworks. J Med Syst 42(10):186. https://doi.org/10.1007/s10916-018-1045-z

Shu H, Qi P, Huang Y, Chen F, Xie D, Sun L (2020) An efficient certificateless aggregate signature scheme for blockchain-based medical cyber physical systems. Sensors 20(5):1521

Shuwandy ML, Zaidan BB, Zaidan AA, Albahri AS, Alamoodi AH, Albahri OS, Alazab M (2020) mHealth authentication approach based 3D touchscreen and microphone sensors for real-time remote healthcare monitoring system, comprehensive review, open issues methodological aspects. Comp Sci Rev 38:100300

Sivakumar R (2020) Cyber victimization: healthcare cyber-physical systems (H-Cpss) vulnerability issues and challenges. Criminol Victimol Through Look Glass 155

Sliwa J (2019) Assessing complex evolving cyber-physical systems (case study: smart medical devices). Int J High Perform Comput Networking 13(3):294–303

Tang D, Tang L, Dai R, Chen J, Li X, Rodrigues JJ (2020) Mf-adaboost: Ldos attack detection based on multi-features and improved adaboost'. Futur Gener Comput Syst 106:347–359

Verma P, Sood SK, Kaur H (2020) A fog-cloud based cyber physical system for ulcerative colitis diagnosis and stage classification and management. Microprocess Microsyst 72:102929

Vijayakumar V, Priyan MK, Ushadevi G, Varatharajan R, Manogaran G, Tarare PV (2019) E-health cloud security using timing enabled proxy re-encryption. Mobile Netw Appl 24(3):1034–1045

Wang S, Lei T, Zhang L, Hsu CH, Yang F (2016) Offloading mobile data traffic for QoS-aware service provision in vehicular cyber-physical systems. Futur Gener Comput Syst 61:118–127

Wang S, Guo Y, Li Y, Hsu CH (2020) Cultural distance for service composition in cyber–physical–social system. Futur Gener Comput Syst 108:1049–1057

Wazid M, Reshma Dsouza P, Das AK, Bhat KV, Kumar N, Rodrigues JJ (2019) RAD-EI: a routing attack detection scheme for edge-based internet of things environment. Int J Commun Syst 32(15):e4024

weerakkody s, ozel o, mo y, sinopoli b (2017) resilient control in cyber-physical systems: countering uncertainty, constraints, and adversarial behavior. Found Trends® Syst Control 7(1–2):1–252

Wu D, Zhu H, Zhu Y, Chang V, He C, Hsu CH, Huang Z (2020) Anomaly detection based on RBM-LSTM neural network for

CPS in advanced driver assistance system. ACM Trans Cyber-Phys Sys 4(3):1–17

Xu Z, He D, Vijayakumar P, Choo KKR, Li L (2020) Efficient NTRU lattice-based certificateless signature scheme for medical cyber-physical systems. J Med Syst 44(5):1–8

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.