International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Cyber-Physical System and AI Strategies for Detecting Cyber Attacks in Healthcare

[1]Priyanka Chandani, [2]Smitha Rajagopal, [3]Amit Kumar Bishnoi, [4]Vikas Verma

Submitted:21/04/2023 **Revised:**11/06/2023 **Accepted:**24/06/2023

Abstract: There is a rising need for adequate cybersecurity safeguards to protect patient data, medical equipment, and crucial infrastructure as healthcare systems become more digitized. Effective security solutions are required for these intricate settings because of the range of medical equipment used within this system, i.e., Mobile Devices (MD) and Body Sensor Nodes (BSN). Healthcare facilities may utilize artificial intelligence (AI) techniques and cyber-physical systems (CPS) to identify and thwart cyberattacks. A novel machine learning threat detection framework for safe healthcare data transfer has been suggested in this research. Smart Healthcare Cyber-Physical Systems (SHCPS) can distribute the gathered data to cloud storage. Cyberattack patterns may be predicted using AI models, and this information is processed to aid healthcare professionals in making decisions. The proposed system begins with a medical record and preprocesses it using a normalization method. The novel jellyfish-optimized weighted dropped binary long short-term memory (JFO-WDB-LSTM) technique ultimately distinguishes between valid and erroneous healthcare data. Compared to other models, our suggested model achieves attack prediction ratios of 98%, detection accuracy ratios of 88%, delay ratios of 50%, and communication costs of 67%, according to experimental results.

Keywords: *Cyber-physical system (CPS), artificial intelligence (AI), healthcare, data normalization, jellyfish optimized weighted dropped binary long short-term memory (JFO-WDBLSTM) approach*

1. Introduction

The SHCPS, a system for the future, would help the medical industry effectively handle a pandemic disaster. These systems include the patient's actual environment, medical tools and equipment, externally controlled and monitored medical care, and connected techniques that use communication networks to transfer and exchange physiological data with the internet to analyze it for feedback and control signals [1]. CPS allows for the seamless integration of the physical and digital worlds using computer-based algorithms. A process is managed and controlled by a CPS [2]. The CPS can withstand data assaults like Man in the Middle attacks, tampering with medical data, ransomware attacks like Wannacry, etc. By storing medical data on the blockchain and analyzing it using cutting-edge techniques like convolution neural networks, this system may enhance the privacy and preservation of such data [3]. CPS seeks to combine data processing, networking, and physical techniques. A CPS comprises linked computational things collaborating with the cosmos and its processes [4]. The fourth industrial revolution (4IR), too identified as Industry 4.0 or CPS, has changed business and technology and is now an essential component of daily life. They are currently employed in various application fields, including smart environments and buildings, autonomous vehicles, industrial control systems, medical monitoring, military defense technologies, and physical security systems [5]. Industry 4.0 advanced internet technologies like Internet Of Things (IoT), Service Delivery Networks (SDN), and cloud computing have made it possible to implement smart security (SS), smart homes (SH), smart healthcare systems (SHS), and cloud computing (CC), to name a few [6]. Smart city design and implementation have been greatly facilitated by the rapid growth of IoT, cloud computing, communication technologies, CPS, and other software technologies [7]. CPS are cutting-edge technologies that link computation and network infrastructure with activities in physical reality. CPS focuses on connecting many devices with integrated components, often designed to perform as standalone devices [8].

2. Related Works

The research [9] covered several helpful, logical operators for network connections, increasing performance, decreasing latency, disclosing the optimal pathways, high-speed and secure processor communication, and many

1Associate Professor and HOD, Department of Data Science (DS), Noida Institute of Engineering and Technology, Greater Noida, Uttar Pradesh, India, Email id: priyanka.chandani@niet.co.in
2Assistant Professor, Department of Computer Science and IT, Jain(Deemed-to-be University), Bangalore-27, India, Email Id: smitha.rajagopal@jainuniversity.ac.in
3Assistant Professor, College of Computing Science and Information Technology, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India, Email id: amit.vishnoi08@gmail.com
4Assistant Professor, Department of Computer Science & Engineering, Vivekananda Global University, Jaipur, India, Email Id: vikash.verma@vgu.ac.in

heterogeneous sensing devices. The research [10] decided to put forward the Self-tuned Fuzzy Logic-based Hidden Markov Model (SFL-HMM) with Heuristic Multi-Swarm Optimization (HMS-ACO) method to identify cyberattacks. The article [11] suggested Supervised Machine Learning (SML) along with a Cryptographic Parameter-Based Encryption and Decryption (CPBE&D) scheme as a hybrid lightweight authentication solution to meet the verification as well as data privacy problems (DPP) in Smart Healthcare (SH). This program guarantees that only authorized patient wearables are sent securely across wireless communication channels. The effects of the most recent cyberattacks on CPS are surveyed in [12]. The research [13] discusses recent research using CPS and Artificial Intelligence (AI) in several fields. The author [14] explored the intricacies of Cyber-Physical Systems, one of the most significant technological revolutions, and the growing importance of artificial intelligence approaches in these systems. The research [15] suggested a federated learning (FL) architecture for healthcare-based CPSs that is blockchain-enabled. The article [16] offered several insightful observations on the security examination of CPS using machine learning. The author [17] thoroughly analyzed the many CPS security circumstances, assaults, distinct modeling approaches for assaults, and the need for CPS testbeds. The IoT Device Network System in terms of CPS was motivated by the necessity for in-depth acquaintance with IoT Device Applications to be explored from a parameters point of view [18]. The article [19] proposed that detecting Distributed Denial of Service (DDoS) assaults should be the Medical Cyber-Physical System's (MCPS) primary objective. The author [20] studied the Attack Isolation (AI) and Attack Location (AL) issues for a CPS, where the actual control system at the physical layer is a nonlinear complex network system, using the H-infinity observer and the zonotope theory.

3. Proposed Method

Cyber-Physical Systems (CPS) methodology designates a systematic approach or framework for creating, advancing, and deploying intricately linked systems that include both computational and physical aspects. The CPS technique aims to ensure the effective and efficient integration of biological processes, computer systems, and networking infrastructure to provide dependable, secure, and high-performance cyber-physical systems.

3.1. Data accumulation using NSL-KDD

The Network Security Laboratory - Knowledge Discovery in Databases (NSL-KDD) dataset will be used instead of the KDD Cup 99 dataset for this study's evaluation of network intrusion detection system performance. Since 1999, Knowledge Discovery and Data Mining (KDD'99) has been the most widely used data set for assessing anomaly detection methods. This data collection was created using information from the DARPA IDS assessment program in 1998. More than 5 million connection records with an average size of around 100 bytes each may be found in the more than 4 gigabytes of raw (binary) compressed TCP dump data from 7 weeks of network activity that make up DARPA'98. The test data covers a two-week period and includes more than 2 million connection records. About 4,900,000 single connection vectors are in the KDD training dataset, each classified as either standard or an attack with a specified attack type and includes 41 characteristics. The mock attacks have been divided into four categories:

- **Denial of Service attack (DoS):** Only authorized users are permitted access to a system during a DOS attack, and computational or memory resources are overloaded or rendered too busy to process legitimate requests.
- **User to Root attack (U2R):** A specific kind of vulnerability known as U2R allows an attacker to first access a user account on the system (perhaps by password sniffing, a dictionary attack, or social engineering), then use that access to exploit a hole and get root access to the system.
- **Remote to Local attack (R2L):** When a hacker who is not permitted to use a system but who can transmit network packets to it takes advantage of a flaw to get user-level local access to the device, this is known as remote-access-by-loan (R2L).
- **Probing attack:** Getting past a computer network's security protections is the aim of this effort to understand it better.

The work is more realistic since the test data includes several assault kinds that weren't included in the training data. Understanding that the training and test data originate from separate probability distributions is crucial. There are 38 attacks in the training datasets, with 16 attack types for testing and 22 for training. The idea behind these 14 new assaults is to see how well IDS can adapt to new threats. According to KDD 99 study, the duplicate data in the train and test sets is around 78% and 75%, respectively. This substantially impacts the tested systems' efficacy and leads to a very subpar assessment of anomaly detection methods. These problems were solved by creating the superior dataset known as NSL-KDD by reducing the dataset's size and eliminating all redundant and duplicate occurrences. But there is still a significant imbalance in the NSL-KDD dataset.

3.2. Preprocessing

Preprocessing describes the procedures or methods performed on unprocessed data before it is utilized for further analysis or modeling.The NSLKDD dataset's

records are each characterized by a vector of 41 characteristics. These attributes comprise thirty-eight continuous or discrete numerical features and three category categories. Since neural networks only need numerical values, we preprocess our data in two stages as follows:.

a. Numbering of symbolic elements

A dataset's suggestive features are first translated into numerical values. The service type, protocol type, and TCP status flag are examples of these extended properties.

b. Data Normalization

Normalization is a crucial step in data preparation after converting all symbolic qualities into numerical values. Data normalization is scaling each attribute's value into a proportionate range, removing the bias in the dataset toward features with higher values. Like equation 1, we first normalized the dataset by subtracting the mean from each part, truncating it to +/-3 standard deviation (S.D.), and scaling it from 0 to 9. This preserved the dataset's sparseness structure. Then, using max-min normalization (equation 2), we climbed these characteristics to have a range of 0 to 1. This method will also be used to transmit and normalize test data.

$$V_j' = \frac{V_j - \mu}{\sigma} \quad (1)$$

$$V_{norm,j} = \frac{V_j' - V_{min}}{V_{max} - V_{min}} \quad (2)$$

v_{max} is the feature's maximum value, v_{min} is its lowest value, vnorm, j is the last step toward normalization, and v_j is the feature that still needs to be normalized. The mean and standard deviation are provided in (3) and (4).

$$\mu = \frac{1}{M}\sum_1^M V_j \quad (3)$$

$$\sigma^2 = \frac{1}{M-1}\sum_{j=1}^{M}(\mu - V_j)^2 \quad (4)$$

The letter M indicates the dataset's sample count.

3.3 Classification using Jelly Fish Optimized Weighted Dropped Binary LSTM (JFO-WDBILSTM)

The phrase JFO-WDBILSTM combines several ideas about neural networks and optimization methods. It combines regularization and optimization methods with LSTM-based binary classification.

3.3.1 Weighted Dropped Binary Long Short-Term Memory (WDBILSTM)

According to WDBILSTM, a binary classification LSTM model would be combined with class weights and dropout regularization. The term WDBILSTM, refers to a Long Short-Term Memory (LSTM) network that has been specifically trained for binary classification tasks. This WDBILSTM, architecture application, designed to gather and interpret sequential input, involves making binary predictions or judgments. U is the fully-connected layer weights, b is a nonlinear activation function, N is a binary weight mask, and U is each cell input. The procedure modestly influences training speed since it is only carried once during forward and backward propagation.

$$q = b\big((N * U)x\big) \quad (5)$$

Consequently, Smaller weights are encouraged, simplifying the model and lowering overfitting. Fig. 1 illustrates the use of DropConnect in an LSTM network. Each input feature is analyzed using an LSTM network, then a DropConnect layer is applied. While the outcome moves to the next set of layers, some information is transmitted for the subsequent recurrent LSTM network. A thick layer towards the end of the layers combines the nodes to create a single output.

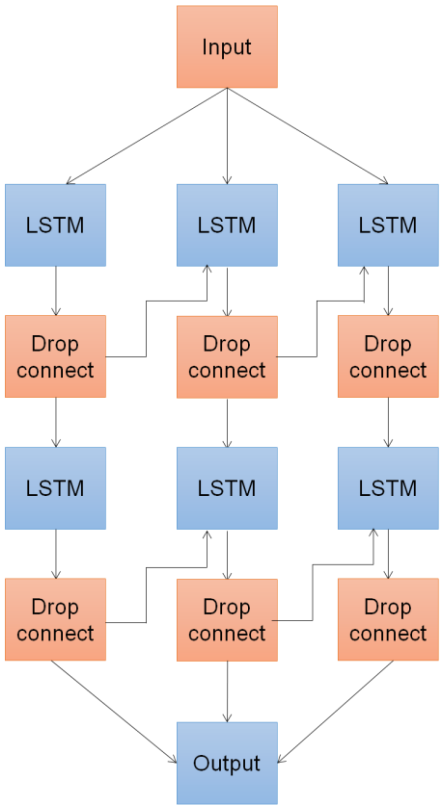

Fig. 1. Weight-Dropped LSTM Network

3.3.2 Jellyfish optimization

The metaheuristic algorithm known as the jellyfish optimization (JFO) technique was partly developed due to jellyfish activity. Chou and Troung suggested the JFO in 2021.

The following actions are included in the jellyfish's food-finding process:

•Within the swarm, the jellyfish's movement.

•Developing a jellyfish bloom by following the water circulation.

•The time control mechanism alternates between the jellyfish's two progressive motions.

•Where there is greater food availability, jellyfish are more attracted to that location.

•The amount of food present depends on the place and its target function.

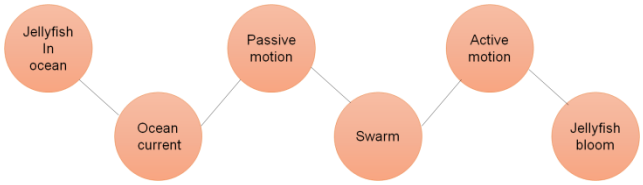

Figure. 2. Behavior of jellyfish in the ocean

Implementing the JFO approach first entails random initialization to disperse the solutions over the issue's search span. After carefully examining each response, the area with the highest fitness value is chosen to serve as a plentiful food supply (fig. 2). The movement of each jellyfish is then updated, depending on the time control factor, either toward the ocean flow or toward progress within the swarm.

a. Ocean current

Ocean currents that carry a lot of nutrients attract jellyfish to them. By averaging the vectors of each jellyfish in the ocean to the jellyfish that now occupies the optimal spot, the ocean current's (i.e., drift's) path is managed. Drift may be calculated mathematically as follows:

$$\overrightarrow{\text{drift}} = \frac{1}{M}\sum\overrightarrow{\text{drift}_l}$$

$$= \frac{1}{M}\sum(v^* - b_d v_l)$$

$$= v^* - b_d \frac{\sum v_l}{M}$$

$$= v^* - b_d \mu' \qquad (8)$$

Where V^* is the jellyfish in the population currently in the best, M position represents the overall number of jellyfish, b_d represents the strength of the attraction, and μ' represents the area where the swarm often congregates. Let:

$$CE = b_d \times \mu' \qquad (9)$$

Here, CE is the distance between the jellyfish of interest's optimal position right now and the swarm's median location. It was predicated on the jellyfish's typical spatial distribution across all dimensions, which gives the likelihood of any jellyfish location. Each jellyfish site is within this distribution's tolerance of $\pm\beta\sigma$. Here, β stands for the distribution coefficient, which is assumed to be "3" according to the analysis provided and stands for the standard deviation for the distribution under consideration, which may be calculated using Equation (11) at the swarm's mean position .

$$CE = \beta \times \text{rand}^{\alpha}(0,1) \times \sigma \qquad (10)$$

$$\sigma = \text{rand}^{\gamma}(0,1) \times \mu' \qquad (11)$$

Drift may thus be described mathematically as:

$$\overrightarrow{\text{drift}} = v^* - \beta \times \text{rand}(0,1) \times \mu' \qquad (12)$$

Drift may thus be formally defined as:

$$v_l(s+1) = v_l(s) + \text{rand}(0,1) \times \overrightarrow{\text{drift}} \qquad (13)$$

The current position of the l^{th} jellyfish is shown by $v_l(s)$. Iteration in the algorithm is indicated by the notation time,s.

b. Jellyfish swarm

The word "swarm" refers to a vast group of drifting jellyfish. In a swarm, jellyfish move in one of two ways: passively (type A) or aggressively (type B). Jellyfish move in type A (passive) way as the swarm forms. Equation (14), which describes this motion, states that the jellyfish circle their location before updating each jellyfish's position separately. The jellyfish also mimic type B movement.

$$v_l(s+1) = v_l(s) + \gamma \times \text{rand}(0,1) \times (WA - KA) \qquad (14)$$

Where γ is chosen as (0.1) by the results of the mathematical analysis, and γ refers to the movement coefficient, which impacts how far a jellyfish moves around its location. The letters (WA) and (KA) denote the search zone's bottom and top bounds, respectively.

In type B motion, a jellyfish (n) different from the one now being studied is randomly picked. The path the jellyfish takes from the one of interest (l) to the jellyfish chosen at random (n) is then shown as a vector. The quantity of food available where the jellyfish (n) is located dictates the movement's direction. In contrast, if there is less food at the jellyfish position (nth), the lth jellyfish travels away from the first jellyfish. Jellyfish position (l) travels toward jellyfish position (n) if there is more food at the latter than at the former. Thus, as shown in Figure 10, each jellyfish moves this way to find the perfect feeding spot inside the swarm. Equations (15) and (18) display a jellyfish's travel direction and most recent position, respectively.

$$\overrightarrow{\text{direction}} = \begin{cases} v_n(s) - v_l(s); ee\left(v_n(s)\right) \geq ee\left(v_n(s)\right) \\ v_n(s) - v_n(s); ee\left(v_n(s)\right) \geq ee\left(v_n(s)\right) \end{cases}$$
(15)

Where 'ff' stands for the fitness function.

$$\overrightarrow{step} = \text{rand}(0,1) \times \overrightarrow{\text{direction}}$$
(16)

Since,

$$\overrightarrow{step} = v_l(s+1) - v_l(s)$$
(17)

$$v_l(s+1) = \overrightarrow{step} + v_l(s)$$
(18)

c. Time Control Component

A temporal control system controls the kind of motion that jellyfish engage in. Both type A and type B motion, or the ability of jellyfish to move away from the flow of the water and inside the swarm, are governed by the time component. Figure 11 displays a schematic representation of the time control system.

The movement selection is controlled by the time control method, which makes use of a threshold constant (l_o) and a time control function (d_e (t)) that varies arbitrarily between 0 and 1. Equation (19) uses arithmetic to describe the time control element.

$$d_e(s) = \left|\left(1 - \frac{s}{j_{max}}\right) \times \left(\left(2 \times \text{rand}(0,1)\right) - 1\right)\right|$$
(19)

Where J_{max} is the maximum number of iterations.

4. Result and Discussion

Experimental findings for the suggested technique (JFO-WDBILSTM) were given based on Performance measures, including Attack Prediction Ratio (APR), Detection Accuracy (DA), Communication Cost (CC), and Efficiency Ratio (ER).

4.1. Attack Prediction Ratio (APR)

Attackers try to alter the data distribution of the multi-layer machine learning classifier to alter the scenario for predictions for ML-based HCS. Attacks against medical imagery that would be used to treat fictitious ailments are among them. Universal adversarial concerns may be successfully used to alter the predicted labels in a medical image with high accuracy. The suggested strategy uses destructive assaults on deep prediction models to identify weak links in a medical time chain. APR uses machine learning to detect illnesses and keep track of patients in real time. The ratio for forecasting assaults is shown in Figure 3. The attack prediction ratio for the JFO-WDBILSTM is (98%), MF-Adaboost is (88%), CLS is (90%), and CML-ADF is (82%).

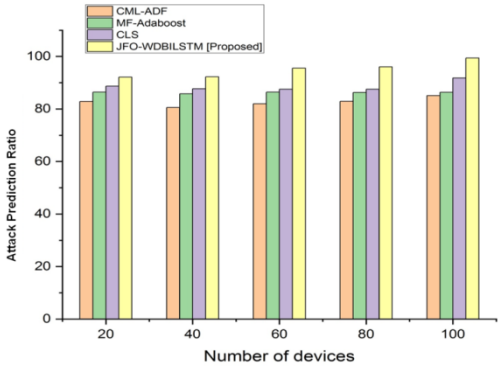

Fig. 3. Attack prediction ratio

4.2. Detection Accuracy Ratio (DAR)

Using a collection of training data that includes recognized input-output pairs, the model learns to predict the output during the initial training phase, defining the detection accuracy ratio. The detection accuracy ratio is shown in Figure 4. The detection accuracy for the JFO-WDBILSTM is (88%), MF-Adaboost is (72%), CLS is (86%), and CML-ADF is (70%).

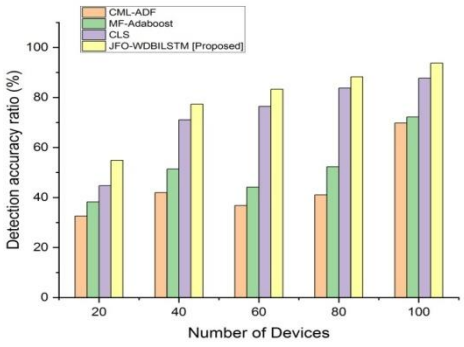

Fig.4. Detection accuracy ratio

4.1. 4.3. Delay Ratio

Medical interventions could be more consistent and timely when communication is delayed. Health problems, lengthy wait times, postponed discharges, faulty judgment, and increased stress might all occur. A robust communication infrastructure must be in place to provide high-quality and dependable patient care. The delay ratio is shown in Figure 8. Comparative analysis of delay ratios for JFO-WDBILSTM is (50%) and the MF-Adaboost is (68%), CLS (72%), and CML-ADF is (80%).

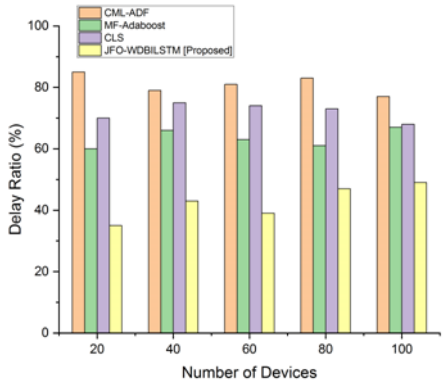

Fig. 5. Efficiency ratio

4.2. 4.4. Communication Cost Ratio

Medical treatments not often considered part of the health data gathering may result in significant cost indicators like medical bills and insurance payments. For instance, the little encrypted portion of the data might be extracted and evaluated, and medical data could be computed on the end-user computer. We store the remaining datasets on cloud servers to save money. The ratio of communication costs is shown in Figure 6. Analysis of the JFO-WDBILSTM is (67%), MF-Adaboost is (57%), CLS is (62%), and CML-ADF is (50%) communication cost ratios were evaluated.

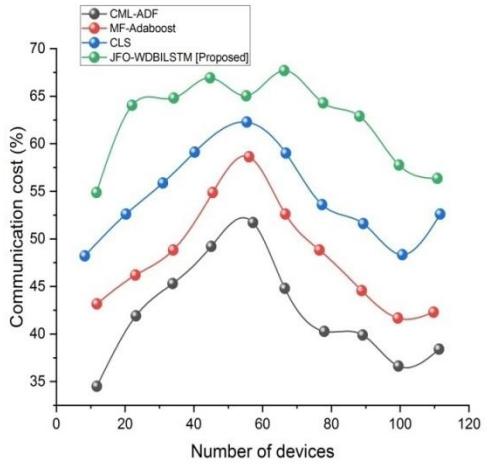

Fig. 6. Communication Cost Ratio

4.5 Discussion

Three proposals for cyber detection in healthcare have been made. Three modern systems that may be compared for performance are the Cognitive Machine Learning Assist Attack Detection Framework (CML-ADF), Multiple Features of Network Traffic with an updated Adaboost (MF-ADABOOST), and Certificateless Signature Scheme (CLS). Cognitive machine learning frameworks often use complex algorithms that need much processing power. When working with many variables or training samples, the MF-ADABOOST approach's computing cost may rise. The ability to create changeable keys using certificate signature systems (CLS) has made several key management strategies possible. The test findings showed that in terms of high attack predictions, accuracy, efficacy, lower latency, and communication, the JFO-WDBILSTM beat other existing networks, such as the CML-ADF, MF-ADABOOST, and CLS algorithms.

5. Conclusion

This research presents a paradigm for patient data privacy and security in healthcare networks. The security risks at different cyber-physical system levels and research problems linked to developing safe CPS and their respective threat models are briefly analyzed. The JFO-WDBILSTM technology lowers the local workload associated with effectiveness analysis and numerical findings while ensuring CPS confidentiality of healthcare information. When compared to other current models, the suggested model achieves Attack prediction ratios of (98%)and detection accuracy ratio(88%), a delay ratio (50%) and a communication cost (67%). CPS may benefit significantly from AI methods like deep learning and machine learning. Future research should focus on creating AI algorithms to improve control schemes, learn from sensor data, and make wise judgments in real-time. By providing autonomous decision-making, adaptive control, and predictive maintenance, AI may improve the capabilities of CPS.

References

[1] Verma, R., 2022. Smart city healthcare cyber-physical System: characteristics, technologies, and Challenges. Wireless personal communications, 122(2), pp.1413-1433.

[2] 2Kumar, C.V., 2022. A real-time health care cyber attack detection using an ensemble classifier. Computers and Electrical Engineering, 101, p.108043. Ch, R., Srivastava, G., Nagasree, Y.L.V., Ponugumati, A. and Ramachandran, S., 2022. Robust Cyber-Physical System Enabled Smart Healthcare Unit Using Blockchain Technology. Electronics, 11(19), p.3070.

[3] 3Ch, R., Srivastava, G., Nagasree, Y.L.V., Ponugumati, A. and Ramachandran, S., 2022. Robust Cyber-Physical System Enabled Smart Healthcare Unit Using Blockchain Technology. Electronics, 11(19), p.3070.

[4] Alowaidi, M., Sharma, S.K., AlEnizi, A. and Bhardwaj, S., 2023. Integrating artificial intelligence in cyber security for cyber-physical systems. Electronic Research Archive, 31(4), pp.1876-1896.

[5] Valeev, N., 2022. Systematic Literature Review of the Adversarial Attacks on AI in Cyber-Physical Systems.

[6] Patil, S. D. ., & Deore, P. J. . (2023). Machine Learning Approach for Comparative Analysis of De-Noising Techniques in Ultrasound Images of Ovarian Tumors. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2s), 230–236. https://doi.org/10.17762/ijritcc.v11i2s.6087

[7] Latif, S.A., Wen, F.B.X., Iwendi, C., Li-li, F.W., Mohsin, S.M., Han, Z. and Band, S.S., 2022. AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber-physical systems. Computer Communications, 181, pp.274-283.

[8] Rani, S., Kataria, A., Chauhan, M., Rattan, P., Kumar, R. and Sivaraman, A.K., 2022. Security and privacy challenges in the deployment of cyber-physical systems in smart city applications: state-of-art work. Materials Today: Proceedings, 62, pp.4671-4676.

[9] Hamzah, M., Islam, M.M., Hassan, S., Akhtar, M.N., Ferdous, M.J., Jasser, M.B. and Mohamed, A.W., 2023. Distributed Control of Cyber-Physical Systems on Various Domains: A Critical Review. Systems, 11(4), p.208.

[10] Shaikh, T.A., Rasool, T., Malla, Y.A. and Sofi, S., 2022. An AI-Based Cyber-Physical System for 21st-Century-Based Intelligent Health Care. In Cyber-Physical Systems (pp. 233-250). Chapman and Hall/CRC.

[11] Almajed, R., Ibrahim, A., Abualkishik, A.Z., Mourad, N. and Almansour, F.A., 2022. Using machine learning algorithm for detection of cyber-attacks in cyber-physical systems. Periodicals of Engineering and Natural Sciences, 10(3), pp.261-275.

[12] Adil, M., Khan, M.K., Jadoon, M.M., Attique, M., Song, H. and Farouk, A., 2022. An AI-enabled hybrid lightweight Authentication scheme for intelligent IoMT-based cyber-physical systems. IEEE Transactions on Network Science and Engineering.

[13] Duo, W., Zhou, M. and Abusorrah, A., 2022. A survey of cyber attacks on cyber-physical systems: Recent advances and challenges. IEEE/CAA Journal of Automatica Sinica, 9(5), pp.784-800.

[14] Sharma, R. and Sharma, N., 2022. Applications of Artificial Intelligence in Cyber-Physical Systems. In Cyber-Physical Systems (pp. 1-14). Chapman and Hall/CRC.

[15] Girdhar, K., Singh, C. and Kumar, Y., 2023. AI and Blockchain for Cybersecurity in Cyber-Physical Systems: Challenges and Future Research Agenda. In Blockchain for Cybersecurity in Cyber-Physical Systems (pp. 185-213). Cham: Springer International Publishing.

[16] Faris, W. F. . (2020). Cataract Eye Detection Using Deep Learning Based Feature Extraction with Classification. Research Journal of Computer Systems and Engineering, 1(2), 20:25. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/7

[17] Liu, Y., Yu, W., Ai, Z., Xu, G., Zhao, L. and Tian, Z., 2022. Blockchain-empowered federated learning in healthcare-based cyber-physical systems. IEEE Transactions on Network Science and Engineering.

[18] Jamal, A.A., Majid, A.A.M., Konev, A., Kosachenko, T. and Shelupanov, A., 2023. A review on security analysis of cyber-physical systems using Machine learning. Materials Today: Proceedings, 80, pp.2302-2306.

[19] Lydia, M., Prem Kumar, G.E. and Selvakumar, A.I., 2022. Securing the cyber-physical system: A review. Cyber-Physical Systems, pp.1-31.

[20] Rajawat, A.S., Bedi, P., Goyal, S.B., Shaw, R.N. and Ghosh, A., 2022. Reliability Analysis in Cyber-Physical System Using Deep Learning for Smart Cities Industrial IoT Network Node. AI and IoT for Smart City Applications, pp.157-169.

[21] Gupta, B.B., Chui, K.T., Arya, V. and Gaurav, A., 2023, May. A Novel Approach of Securing Medical Cyber-Physical Systems (MCPS) from DDoS Attacks. In Big Data Intelligence and Computing: International Conference, DataCom 2022, Denarau Island, Fiji, December 8–10, 2022, Proceedings (pp. 155-165). Singapore: Springer Nature Singapore.

[22] Zhang, X., Zhu, F., Zhang, J. and Liu, T., 2022. Attack isolation and location for a complex network cyber-physical system via zonotope theory. Neurocomputing, 469, pp.239-250.