The Open Bioinformatics Journal
DOI: 10.2174/0118750362380269250502062754, 2025, 18, e18750362380269

ISSN: 1875-0362
1

RESEARCH ARTICLE **OPEN ACCESS**

iCDRET: A Dynamic Cyber Risk Estimation Technique for Intelligent Cyber-Physical Systems in PCS

Swati Devliyal[1,*], Himanshu Rai Goyal[1] and Sachin Sharma[1]

[1]*Computer Science and Engineering, Graphic Era Deemed to be University Dehradun, India*

Abstract:

Background: To detect cyberattacks and assess risks in cyber-physical systems used in pharmaceutical treatment, this study presents a two-tiered approach that combines machine learning and Internet of Things (IoT) security. By prioritizing risk-based responses and facilitating real-time threat mitigation, it improves system resilience.Drug delivery, patient data management, and healthcare efficiency have all been greatly improved by the incorporation of cyber-physical systems (CPS) into pharmaceutical care services. However, because digital and physical infrastructures are now interconnected, this development has created serious cybersecurity risks. Strong detection and mitigation procedures are necessary because cyberattacks have the potential to compromise patient safety, data integrity, and service reliability. The necessity for a specific cybersecurity architecture for pharmaceutical CPS is highlighted by the fact that current security solutions frequently fall short in addressing real-time threat detection and risk assessment.

Methods: To detect and eliminate cyber threats instantly, the suggested method makes use of sophisticated machine learning models, intrusion detection systems, and Internet of Things security strategies. A risk-estimation system that assesses attacks according to impact, detectability, and risk estimation factor (REF) is included in a two-layered strategy. To evaluate the performance of the proposed method in comparison with existing security frameworks, simulations were conducted. Analysis is performed on important variables such as system resilience, risk quantification, and detection accuracy.

Results: The results of the simulation show that the suggested method improves the accuracy of threat identification and offers a methodical framework for risk evaluation. The strategy demonstrates increased accuracy in detecting cyberattacks and prioritizing mitigation measures when compared to current approaches. By accurately estimating the intensity of an assault, the risk estimation approach guarantees preventative security measures.

Conclusion: A unique cybersecurity architecture for intelligent CPS in pharmaceutical care is presented in this paper. The method improves system resilience, protects patient data, and guarantees the dependable functioning of pharmaceutical services against changing cyber threats by combining real-time threat detection with risk assessment.

Keywords: Pharmaceutical care services, Cyber-physical System, Risk estimation, Internet of things.

* Address correspondence to this author at the Computer Science and Engineering, Graphic Era Deemed to be University Dehradun, India; E-mail: swatidevliyal@gmail.com

Cite as: Devliyal S, Goyal H, Sharma S. iCDRET: A Dynamic Cyber Risk Estimation Technique for Intelligent Cyber-Physical Systems in PCS. Open Bioinform J, 2025; 18: e18750362380269.
http://dx.doi.org/10.2174/0118750362380269250502062754

Received: December 23, 2024
Revised: February 22, 2025
Accepted: March 05, 2025
Published: May 09, 2025

1. INTRODUCTION

Intelligent healthcare technologies make major contributions to daily life by providing electronic healthcare services and have the potential to improve patient care quality. Technology is used in a variety of applications, including smart homes [1, 2], intelligent businesses [3], intelligent neighborhoods [4], mobility [5], intelligent healthcare [6], and satellites. Due to their tiny size and heterogeneity, smart devices and apps have grown fast in recent years, making them very vulnerable to cyberattacks. The integration of advanced technologies has transformed wearable and healthcare devices, leading to the development of intelligent medical systems [7]. Due to the gadgets and wearables, remote monitoring in healthcare is now feasible, keeping patients safe and motivating clinicians to provide the best treatment possible [8]. Patient participation and comfort have increased, and medical interactions have become more efficient [9]. Unfortunately, the connectivity of this large number of IoMT devices has drawn attackers into the healthcare system. The latest cyberattacks highlighted fundamental flaws in the IoMT ecosystem [10]. Inadequate architecture and security methods can allow attackers to intercept such networks. Unauthorized access poses a security risk due to a lack of detection and prevention. An attacker can modify medicine doses remotely and use IoMT sensors as botnets for DDoS assaults [11]. Healthcare organizations have experienced hacking and unauthorized access, such as the 2018 Ransomware cyber-attack that cost Indiana hospitals $55,000 [12]. A cyber-attack aims to ruin and interfere with computer network operation [13]. The numerous cyber-attack categories are denial-of-service (DoS), logical bombs, spam, sniffers, viruses, worms, Trojan horses, and botnets. The DoS attack keeps the system from communicating with other computers or surfing the internet. Attacks might start fast from one or many scattered sources. Protecting networks and data from several kinds of assaults depends on cybersecurity. It is thus important to have a plan for spotting different types of attacks in IoHT. Apart from safety concerns, medical professionals do not openly access databases on cyber-attacks as sensitive material is at risk and can harm and kill people [14]. CPS is an engineering and physical system that relies on communication, computation, and control to coordinate and monitor processes. This CPS has been used in significant industries, including biomedical, smart grids, and ITS (intelligent transportation systems). The Healthcare Cyber-Physical System (H-CPS) generates a smart healthcare environment all around. From sensors, the H-CPS combines e-health data, IoMT (artificial intelligence), and EHR. To build smart healthcare, H-CPS integrates biosensors, implanted medical devices (IMD), conventional healthcare, ICT, wearable devices, communication mechanisms, and artificial intelligence [15-17]. We use a special technique to identify several cyberattacks to reduce the described risks. Cyber-Physical Systems (CPS) automate and regulate industrial processes by combining cyber elements for processing and communication with physical components for sensing and actuation. Important sectors include healthcare, traffic management, industry, and energy infrastructure, all of which are extensively used. These systems use commercial and open-source software as well as common communication protocols to enable interaction with corporate networks and save infrastructure expenses. These technologies have, however, been susceptible to fresh security concerns and cyberattacks, therefore upsetting normal business operations. Recent advanced attacks on systems draw attention to the necessity of methods and instruments to control cybersecurity vulnerabilities [18]. Early in the course of system design, safety and security needs should be noted and taken care of [19]. IT security risk assessment follows recognized international standards, such as those mentioned in a study [20]. This paradigm presents new hazards compared to traditional computer networks. Data loss can have a wide range of consequences, including service disruption and loss of life. To improve efficiency in e-health systems, risk assessment approaches should be updated accordingly. Trustworthiness and patient confidence in e-healthcare security and data protection are crucial for its widespread adoption. To promote the expansion of electronic linked devices in the healthcare industry, firms must balance low transaction costs with effective and efficient data transfers and acceptable hazards. Effective security mechanisms need increased processing expenses. E-health system builders support risk as an indirect cost [21]. In this study, we are providing a cyber-risk estimation technique.

2. MOTIVATION

Among other uses, CPSs were extensively used in sectors like distribution networks, manufacturing, construction, pharmaceutical, and transportation. Advancements in IMoT technology are resulting from the growing number of connected wearable devices and communication *via* PCS as it is emerging. Adoption of edge-based CPSs underlines dependability and credibility. We are aware that dependability and trustworthiness are multifaceted aspects intimately related to CPS, human perception, and trust security. Researchers are developing AI-based approaches to solve future CPS difficulties. Researchers have created many healthcare monitoring models; however, limits remain for cloud-enabled systems, making them unsuitable for real-world applications. Cloud computing and healthcare organizations face communication overhead, latency, and privacy challenges when aggregating sensitive data. As the number of IoT-based healthcare networks grows, hostile assaults have become more sophisticated. Privacy concerns for IoT nodes, smartphones, and computer systems on the internet. Companies, especially pharmaceuticals, are increasingly relying on technology for their operations. Businesses have successfully adapted to remote work, with TCS projecting that by 2025, 75% of their personnel will be working from home. As firms adjust to this new work style, mitigating related risks becomes increasingly important. Effective risk management is essential for

Table 1. Cyber attacks identified.

Cyber Attack Types	Different Attacks	Cyber Risk Types
Social engineering attacks	Baiting Pretexting Tailgating Business Email Compromise Whaling Vishing Watering Hole	Data loss Credential theft Malware and ransomware Financial loss Reputation damage Legal and regulatory consequences Damaged client relationships Legal liabilities Reputation damage
Application attacks,		
Cryptography attacks		
Control Hijacking attacks	Buffer Overflow Attack Integer Overflow Attack Format String Vulnerabilities Reconnaissance attacks	
Computer network attacks	DoS Attacks DDoS Attack Bots and botnets Malware attacks	
Phishing attacks		
Password attacks		
Man-in-the-middle attack		
Spoofing		
Identity-Based Attacks		
Code Injection Attacks		
Supply Chain Attacks		

digital and technological transformation. Digital risk refers to the risks that arise when a firm transitions to digital platforms. Identifying and mitigating possible risks is crucial for all industries. Businesses might experience data loss and theft of crucial information. Privacy breaches occur as a result of digital advancements in business. Businesses may encounter risks associated with automation and compliance. This research analyses the viewpoints and experiences of subject matter specialists in the pharmaceutical sector, coding the data to draw precise findings. In the detailed study, it was found that there are different types of attacks. Our primary accomplishments of this study effort are as follows:

• We developed algorithms that can detect cyberattacks in pharmaceutical care services.

• Introduced a novel risk estimation factor (REF) to quantify attack severity based on impact and detectability.

• Included anomaly detection and IoT security methods to improve the security and dependability of pharmaceutical care services.

• The proposed algorithms are performing better than the existing ones.

The remaining work is organized as follows: starting with the literature review followed by the proposed scheme. The next segment contains a discussion of the experiment. Finally, the conclusion summarizes the work and outlines potential directions for future research.

3. DIFFERENT TYPES OF CYBER ATTACKS

Table **1** lists all the identified attacks and highlights the various types of risks that could occur if any of these attacks were executed on the system. This section contains details about each attack and also describes the different techniques required to detect these attacks.

• Social engineering attacks: When it comes to cyber security, many people feel that they should defend themselves against hackers that use technological flaws to assault data networks. However, there is another method for infiltrating organizations and networks that makes use of people's vulnerabilities. "Social engineering" refers to the process of deceiving someone into disclosing information or getting access to data networks. In short, social engineering is the manipulation of individuals so that they can access or expose information or data. Social engineering, like other cyber-attacks, seeks to circumvent an individual's or organization's security measures. Anyone can fall prey to a social engineering attack. However, elderly individuals with inadequate technical skills, individuals very minimal human connection, along with those susceptible to impetuous behavior are frequent targets. One's own/exclusive information should not be disclosed to avoid potential attacks; anyone attempting to communicate should be investigated; URL/address verification must be undertaken; unreliable sources ought to be ignored. Social engineering assaults use human psychology to deceive people into disclosing critical information. Here are some examples of social engineering assaults and the algorithms they use:

◦ Baiting: This assault, like phishing, takes advantage of a target's greed, temptation, or fear by providing something appealing in exchange for personal information.

◦ Pretexting: This assault employs appealing stories to persuade victims that they are genuine and then exploits their beliefs to obtain personal information.

◦ Tailgating is an exploit that allows hackers to enter restricted regions without appropriate authentication. Corporate Email Compromise (BEC) is an attack in which an individual obtains access to a corporate email account and uses it to send fraudulent emails.

◦ Whaling: Senior executives are the target of this kind of phishing assault, which poses as a genuine email and tempts them to perform a secondary action, such as initiating a wire transfer.

◦ Vishing: This type of targeted assault sends recorded messages over the phone, such as alerting victims that their bank accounts have been hacked. The attacker then gains access to the victims' accounts when they are asked to enter their information on the keypad of their phone.

◦ Attacks known as "watering holes" entail infecting unprotected websites and online sources that the targeted individuals often access. The objective may obtain exposure to the target's infrastructure or infect devices with malware.

• Application attacks: Cybercriminals can access unauthorized sites using an application attack. Often, attackers start scanning the application layer for flaws in code-based services. Numerous apps representing different programming languages are attacked, even if certain programming languages are targeted more frequently than others. There are flaws in commercial software and free frameworks and libraries. Cybercriminals can take advantage of application flaws to attack programs in production. These attacks target open-source frameworks and libraries as well as proprietary programs. Cybercriminals exploit a variety of techniques, including flaws in programming, vulnerabilities brought on by outdated certificates, and vulnerabilities brought on by inadequate authentication.

• Cryptography attacks: The technique of storing and sending data in a certain manner such that only the intended receivers can access and comprehend is known as cryptography. The processes of encryption, which transforms plain text into cipher text, and decryption, which transforms cipher text back into plain text, are used to accomplish this. A cryptographic attack occurs when an attacker looks for weaknesses in the code, cipher, encryption protocol, or key handling system to compromise an encryption system. Such assaults can be split into two distinct categories: passive or aggressive. While active attacks change or start an unauthorized flow of information, passive attacks permit the illegal disclosure of data with no compromising with the exchange of information channels. While active assaults entail altering data without authorization, passive attacks are frequently linked to information theft. The confidentiality and integrity of sensitive data may be jeopardized by any kind of assault.

• Hijacking attacks: Hijacking assaults are a subset of security-related attacks wherein an assailant gains control of computer systems, software applications, and network communications. The majority of cyber attacks depend on some sort of hijacking, and hacking is routinely—if not always—illegal, with grave repercussions for the victim as well as the attacker. Among these incidents are those involving aircraft hijackers or the commandeering of an armored transport truck. There are several varieties of hijack assaults; these are enumerated here: Session, Domain Name System (DNS), browser, clipboard, Internet Protocol (IP) and page hijacking.

• **Computer Network Attacks (CNAs):** These involve gaining unauthorized control over a computer or network to manipulate, delete, reject, or distort data within the system. CNAs can be used to shut down systems, alter data, exploit resources for botnets, or perform any activity that compromises the availability, confidentiality, or integrity of the targeted system. A CNA executes attacks by manipulating data streams. For example, it might transmit malicious code or commands to the central processing unit (CPU), potentially causing hardware malfunctions or forcing system shutdowns. Attackers join the network and scout it before acting to execute a CNA. Discovery helps one to learn the network configuration and choose the best approach to engage in negative behavior.

• Phishing attacks: Computer Network Attacks (CNAs) involve gaining unauthorized control over a computer or network by modifying, deleting, rejecting, or distorting data within the system. These attacks can shut down systems, alter or erase data, exploit system resources for botnets, and perform other actions that compromise the availability, integrity, or functionality of the targeted system.The CNA runs the attack using the data stream. For example, a CNA might send a code or order to a central processing unit forcing system shutdowns. Attackers join the network and scout it before acting to execute a CNA. Discovery enables an attacker to identify the network configuration and determine the most effective method to carry out malicious activities.

• Paying attention and learning will help prevent phishing attacks. Although email monitoring systems can block many regular phishing attempts, employee email security training can help reduce the number of prospective victims by raising an understanding of phishing risk. Simultaneously, one should be careful of website pop-ups and ensure the URL starts with "HTTPS" and features a closed lock icon next to the address bar to stop phishing efforts.

• Malware attacks: Malware, short for malicious software, is designed to compromise computer systems, steal data, or disrupt users through various harmful activities. Among the several instances of this kind of program are Trojan horses, worms, viruses, and rootkits. Though their main classification is as software, they can resemble simple codes. Often referred to as scumware, malware may be distributed in almost any programming or scripting language and written in several file formats. Malware might keep gathering data and spy for a significant length of time without informing the affected computer system. Moreover, it can be used for extortion of money or payments or for damage or disturbance of the system it targets (such as Stuxnet).

• Bots and botnets: Standing for "robot," a "bot" is a piece of software designed to do specified, automated, repeating operations. Bots regularly copy or replace the acts of human users. Being automated, they run significantly faster than human users. They may be used practically for customer service or search engine indexing, or they can be used as malware to seize complete control of a machine. To spread spam, scan contact lists, breach user accounts, and complete other evil activities, one can design or hack malware bots and Internet bots. The term "botnet" combines the words "robot" and "network." A botnet is an assembly of Internet-connected computers interacting with other such devices to achieve goals and repetitive activities. Spam emails are sent using these networks rather often. Under attacker control, a botnet can be as vast as hundreds of thousands of zombie computers or even thousands. Every software agent program also is run remotely.

• Password attacks: One of the most common forms of cyberattacks is the password assault. Both personal and business targets are susceptible to password assaults. By stealing the passwords to any area that needs one, including social media networks, technology, or software that the person or organization uses, the goal is to cause harm to the organization or individuals. Easy passwords are typically preferred by people or organizations to prevent forgetting them. Specifically, social media users can provide a summary of the password text they use on their profiles. For instance, a person's social media profiles provide a wealth of information, like their date of birth, place of residence, spouse or partner's name, years of relationship, and the team they support. For hackers, this knowledge is crucial. As a result, disclosing this information makes it easier for hackers to execute password assaults.

• Man-in-the-middle attack: A "man-in-the-middle" attack is the first type of cybercrime in which a hostile person discreetly meddles with two parties' communication. This hack provides access to and even modification capability for the victim's supplied data. The attacker succeeds by creating a clandestine, phony link between their devices and the victims. Usually aiming to either mimic one of the parties or get passwords, bank information, and personal data, a man-in-the-middle assault is These deeds, regretfully, might include changing login passwords or beginning a money transfer. The optimum locations for an attack to take place are those with free Wi-Fi. The content of unencrypted packets is easily accessible. Attackers use Wi-Fi sites to control network traffic so it flows across them. Consequently, the assailant turns into the traffic conduit for the users of the network. The assailant who intercepts this message may find passwords or personal information.

• DDoS (Distributed DoS): A kind of DoS attack aimed at one system by use of several hacked systems.

• Denial of Service (DoS): An attack that overwhelms a system or network with traffic or requests to make it unavailable to its users

• Reconnaissance attacks: These include techniques such as packet sniffing, ping sweeps, port scanning, and internet information queries, which are used to gather information about a target system or network.

4. CYBER-ATTACK DETECTION TECHNIQUE

• Technique 1: Proof of Source Authenticity (PoSATM) from Memcyco: It employs AI to identify anomalous activity and provides organizations with complete assault information for transparency. Memcyco enhances security by immediately alerting users when they visit a fraudulent website. It provides a comprehensive analysis of the attack and uses a unique, editable watermark to authenticate web pages. As an agentless solution, Memcyco requires no registration or installation from your clients.

• Technique 2: Anomaly Detection: Based on a known pattern in a system, organizations can use tools and procedures to detect anomalous conduct. In this scenario, anomalies are defined as any user or system events that depart from a baseline pattern. Techniques for anomaly detection can be used by businesses to find important incidents.

• Technique 3: Signature-based Detection in Intrusion Detection Systems (IDS): Signature-based detection is a fundamental detection method. By recognizing danger indicators, the approach enables intrusion detection systems (IDS) to identify malicious activity or unauthorized network access. An expert system in cervical dysplasia is a specialized computer-based application designed to assist healthcare professionals, such as gynecologists and pathologists, in the diagnosis and management of cervical dysplasia, a precancerous condition of the cervix [15-17]. This technique combines clinical know-how and artificial intelligence to offer accurate assessments, recommendations, and aid for healthcare practitioners in their choice-making methods.

• Technique 4: Heuristic Analysis Examining code for questionable elements—a technique known as "heuristic analysis"—may also be necessary for threat detection. By enabling security experts to decompile questionable applications and compare them with known malware code stored in a heuristic database, the approach aids in malware identification. If a certain proportion of the program's source code matches a virus in the database, the software is marked as potentially dangerous.

• Technique 5: Sandboxing is the process of executing and examining code in a secure, segregated section of a network. It is best practice to employ a sandbox that replicates the real end-user operating environment for better outcomes.

• Technique 6: Honey Pots and Honey Nets A fascinating security method called a "honeypot" uses virtual or intruder traps to entice hackers. Security experts create a purposefully weak system that makes it easy for attackers to take advantage of vulnerabilities. To strengthen their cybersecurity posture in the meantime, the security team might research the strategies, methods, and practices used by the threat actors.

• Technique 7: Endpoint Detection and Response (EDR) is an essential tool in today's dynamic threat landscape. The adage "time is money" holds particularly true, as the faster you can detect, respond to, and recover from security threats, the more effectively you can protect your system. EDR combines automated detection and response, offering a streamlined approach to managing risks.

• Technique 8: Artificial Intelligence and Machine Learning Prior to AI and machine learning, IT systems could only detect known and tested dangers like viruses and malware using rule and signature-based threat detection methods. Unfortunately, the ability of these conventional security methods to identify complex and changing assaults is limited. Missed security events and delayed discovery were encountered by security analysts. EDR is an integrated security method that combines rule-based analysis and response capabilities with real-time endpoint event monitoring and recording.

5. LITERATURE REVIEW

Cyberspace has evolved into a breeding ground for new types of entrepreneurship, technical developments, the spread of free expression, and new social networks that power our economy and reflect our values. Critical infrastructure is required to ensure the nation's and its economy's safety, health, and well-being. The efficacy of cyberspace is essential to our national security and economy. Cyberspace, which allows all information infrastructures to be available over the Internet outside all geographical boundaries, poses a tremendous danger to our national security, economic prosperity, and public safety and health. Cyberspace has become the most hazardous area in the world, the number one threat to our Homeland, and defending against cyberattacks is exceedingly tough. Salahuddin *et al*. [21] designed edge gateway hardware to build a smart healthcare system combining publicly accessible networks and wireless networks of sensors (WSN). Smart gates alert doctors to crises and offer data-driven decision-making. Janjua *et al*. [22] assessed the insider threat detection capability of many machine-learning techniques. The proposed spam detection algorithm was developed by the authors from a dataset of 24 users' activity traces spanning five days. With 98.3% accuracy, Adaboost excelled among other methods. In a study [23], the authors introduced affordable block chain task scheduling (CBTS) with many techniques for cyber- physical systems to control security costs and deadlines. Data validation in cyber security drops by 33%; security execution drops by 50%. Fisayo *et al*. [24] proposed a framework for protecting data against privacy concerns. The authors achieved higher data usefulness compared to other classic anonymization strategies. Manimurugan *et al*. [25] utilized the CICIDS 2017 dataset to detect various types of attacks—primarily botnet, brute force, DoS, intrusion, and port attacks—using deep belief neural network models. Syed *et al*. [26] noted that Intensive Care Units (ICUs) commonly contain a range of medical devices, such as ECG monitors, glucose meters, syringe pumps, and others. Among the several assaults, these devices can be subjected to include ransomware, man-in-the-middle, and DoS. Several research applied machine learning algorithms on the medical information mart for intensive care (MIMIC) dataset, comprising discrete structured clinical data, physio-logical waveform data, free text documents, and radiology imaging reports, according to the study. T. Mohamed *et al*. [27] defined a security architecture suitable for mobile e-health platforms. It uses computerized personal health records to establish and manage pharmaceutical prescription services in mobility settings. This design uses RFID technology to provide safe and authorized interactions. Wireless Sensor Networks (WSNs) are a weak link in e-health systems, prompting researchers to address security concerns. In Gonçalves *et al*.'s study [28] an end-to-end safe routing using block chain architecture was created and a technique for intrusion prevention in mobile WSNs is offered. The method takes the restricted funds and flexible structure of mobile WSN into account. Table **2** contains a brief overview of the literature review and shows that no technique is available which can identify the cyber- attack as well as the risk can also be estimated. So in this research, our aim is to develop a model that can do both attack detection as well as risk estimation.

Table 2. Research gap identified with existing work.

Author	Limitation				Technique
	PCS	iPCS	Cyber Attack Detection	Cyber Attack Risk Estimation	
[21]	×	×	✓	×	Decision Fusion
[22]	×	×	✓	×	Naive Bayes, LR, KNN, Adaboost
[23]	×	✓	✓	×	Task Schedul- ing
[24]	×	✓	✓	×	PAD
[25]	×	×	✓	×	Deep Learning

Author	Limitation				Technique
	PCS	iPCS	Cyber Attack Detection	Cyber Attack Risk Estimation	
[27]	×	×	✓	×	Random Forest, Neural Network
[29]	×	×	×	✓	Decision-analysis- based
[30]	×	×	✓	✓	Blockchain
[31]	×	✓	✓	✓	Penetration

6. METHOD

6.1. Problem Statement

6.1.1. Notation

This study is related to pharmaceutical care services. There are 10 stakeholders in our research. The stakeholders are as follows. The patient is the main element of the PCS, followed by the Hospital, Staff, Doctors, MR, Retailers, Wholesalers & Raw Material Manufacturers, Investors, Drug Manufacturers and lastly PBM & Governance. For each, the notation is mentioned in Table **3**. Subsequently, different features were selected to design a PCS plan for a patient. The complete features are listed in Table **4**. When a plan is prepared for the patient, many factors must be considered before training and testing.

Table 3. Notations.

Stakeholder's Name	Notation
Patient	N_P
Hospital	N_H
Staff	N_S
Doctor	N_D
Medical Representative	N_{MR}
Retailer	N_R
Wholesalers & Raw material Manufacturer	$N_{W(RM)}$
Investor	N_I
Drug Manufacturer	N_{DM}
Pharmacy Business Management & Governance	$N_{PBM(G)}$

Table 4. Features required for PCS.

Feature	Sub Feature	Patient (Pnt)	Pharmacist (Phst)	Doctor (Dor)	Healthcare Organisation (Horg)
Demographic (Pde)	Name(Pn)	√	×	√	√
	Age(Pa)	√	×	√	√
	Gender(Pg)	√	×	√	√
	DoB(Pdob)	√	×	√	√
Medical (Pme)	Weight & Height(Pwh)	√	×	√	√
	Current Symptoms(Psym)	√	×	√	√
	Past Medical History(Pmh)	√	×	√	√
	Lab Information(Pli)	√	×	√	√
	Allergies and Intolerance(Pai)	√	×	√	√
	Vital Sign(Pvs)	√	×	√	√
Design Therapist Plan (Pdtp)	Prescribe medication(Pme)	√	√	√	√
	Medication used Before(Pmeb)	√	×	√	√
	Medical Regimen(Pmr)	√	×	√	√
	Compliance with therapy(Pct)	√	×	√	√
	Medication allergies and Intolerances(Pme)	√	×	√	√
	Lab Test(Plt)	√	×	√	√

Feature	Sub Feature	Patient (Pnt)	Pharmacist (Phst)	Doctor (Dor)	Healthcare Organisation (Horg)
Lifestyle(Pl)	Diet Exercise(Pde)	√	×	√	√
	Recreation(Pre)	√	×	√	√
	Tobacco/alcohol/caffeine/other substance use or abuse(Pls)	√	×	√	√
	Daily activities(Pda)	√	×	√	√
Implementing Therapeutic Plan(Pitp)	Dosage(Pdo)	√	√	√	√
	Medical Regimen(Pmr)	√	×	√	√
	Diet Exercise(Pde)	√	×	√	√
Monitoring Therapeutic Plan(Pmtp)	Patient Status(Pst)	√	×	√	√
	Patient Condition(Pco)	√	×	√	√
	Medication theraphy(Pmt)	√	×	√	√

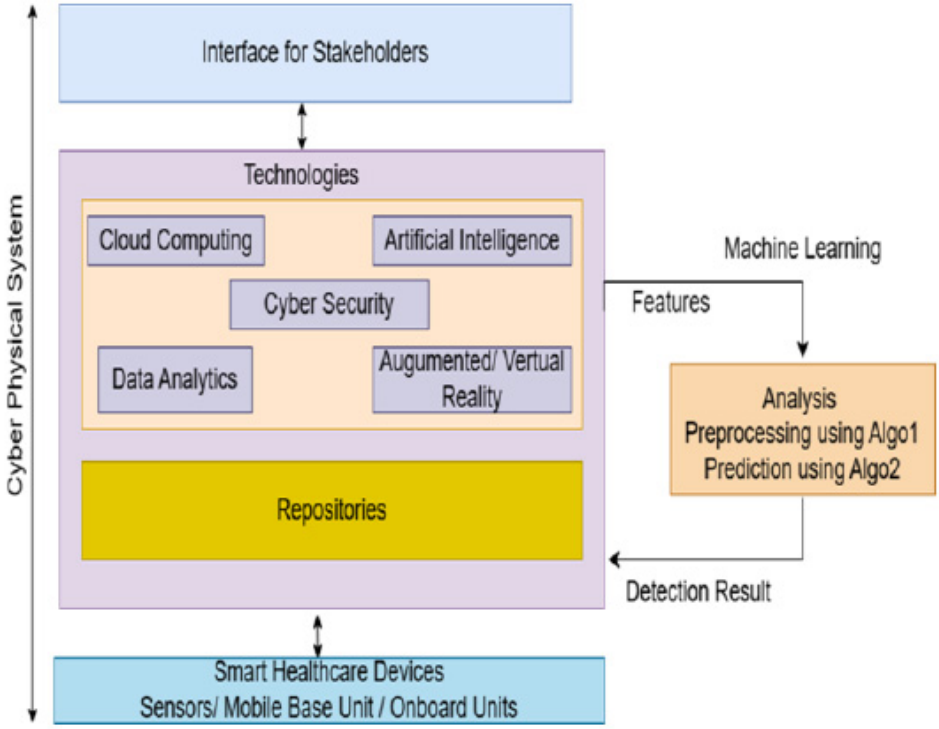

Fig. (1). Proposed model.

6.2.2. Proposed Model

In Fig. (**1**), the suggested model is displayed. Architecture is created with CPS's assistance, with smart medical devices at the bottom that gather the necessary data from the surroundings. Following that, the data is examined using a variety of cutting-edge technologies, each of which is accessed through an interface. This filtered data is available for use by various parties. We have chosen 11 stakeholders: Patient, Hospital, Staff, Doctors, MR, Retailers, Wholesalers, Raw Material Manufacturers, Investors, Drug Manufacturers, and last is the PBM and Governance for our study, and protecting privacy and security is our top priority. For this, we have developed algorithms that can detect different types of cyberattacks on 11 different stakeholders, and after that, risk estimation is also done. For analysis and preprocessing, Algorithm 1 is used. For detection, Algorithm 2 is used.

6.3.3. Problem Formulation

First, we gathered the dataset for analysis of the performance of the suggested approach from many healthcare institutions. For analysis and comparison of the suggested method's performance with the already-existing algorithm, other algorithms are also applied, including Decision tree, Random forest, Diffie-Hellman, Deep convolution network, and Naïve Bayes. To start the investigation, we eliminated null and undesired elements from all three datasets using conventional pre-processing techniques. We applied data computation and normalizing

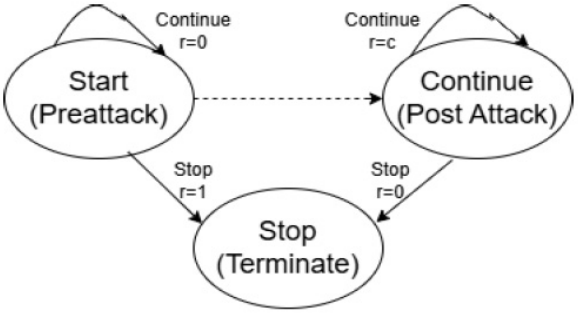

Fig. (2). State transitions.

methods to remove duplicate features. We also scale features using principal component analysis (PCA). Based on the component variance factor, several traits were determined: we mapped category features to numerical values using the label encoding method. We investigated binary and 13-class classifications of different cyber threats and attacks. Aiming to consolidate data distribution, the centralized technique for multi-source transfer learning assesses the relationship depending on consistency and similarity. In data transmission, the Kullback-Leibler (KL) divergence gauges the entropy difference between two different distributions. We examine the likelihood of uniform information distribution using the KL divergence. The first algorithm uses a centralized multi-source transfer learning method. We assume a cyber-attack occurs at an unknown moment (y) and try to find it as soon as possible. The attacker's techniques and talents. This presents the quickest change detection problem for which the objective is to reduce the false alarm rate as well as the average detection latency. Fig. (**2**) explains this issue. Two hidden states exist: suspicious state and preliminary attack due to the unknown attack launch time y: At each time t_i, after collecting the measurement vector y_t, the agent (defender) has two options: halt and announce an attack or proceed to take observations. When the action stop option is selected, the system is assumed to enter a terminal state and remain there permanently.

Under normal operating conditions, the system model can estimate the conditional observation probability associated with the initial state. However, due to unknown attacking strategies, the conditional observation probability for the prevention state is assumed to be completely unknown. The chance of transitioning between the preliminary state and the prevention state is uncertain due to the unknown assault launch time (r). To reduce detection delays and false alarm rates, both false alarm and detection delay events should incur charges. Let $c > 0$ represent the proportional cost of a detection delay v/s a false alarm occurrence. If the true underlying state is the preliminary state and the action to halt is taken, a false alarm occurs, resulting in a penalty of 1 for the defender. If the underlying state is the prevention state and the action to continue is chosen, the defender incurs a cost of *c* due to the detection delay. For all other (hidden) state-action pairings, the cost is set to zero. Once the action halt is chosen, the defender will not incur any more costs while in the terminal state. The defender's goal is to minimize their predicted total cost during this time. The defender's goal is to minimize its predicted overall cost by carefully picking its actions. The defender must identify the appropriate moment to declare an attack depending on their observations. We suggest using a limited history of observations. We suggest employing an RL algorithm to learn an AT(s, a) value, which represents the projected future cost for each observation-action combination (s, a). This value is then kept in an AT-table. After learning the AT-table, the defender's policy will be to select the action a with the lowest AT(s, a) for each observation. To train, a simulation environment is constructed. During the procedure, the defender acts based on their observations and receives a cost from the simulation. Based on this experience, the defender modifies and learns an AT-table.

During the online detection phase, observations are used to select the action with the lowest projected future cost (AT value) based on the previously learned AT-table. The online detection phase continues until the defender chooses the action prevention state. When the preventive state is selected, an attack is declared and the process terminates. After announcing an attack, the online detection phase can be resumed after the system has been restored to normal operating circumstances. That is, once a defender is taught, no more training is required. We summarize the learning and online detection stages of

Algorithm 1: Learning Algorithm

1: Collect Sample Data from the iCPS server for all 10 nodes ($N_{P,}$ $N_{H,}N_{S,}$ $N_{D,}$ $N_{MR,}$ $N_{R,}$ $N_{W(RM),}N_{I,}N_{DM,}N_{PBM(G)}$)

2: Process the primary data for removing unwanted features

3: SD<- split(x,y)

4: for i=1,2....10 do

for sd subset SD do

ES<- ES-ŋ $\dot{V}f_e$(ES,SD)

end inner loop

end outer loop

5.Process data from the server

6.Feature Selected

7. Use PCA (Model dataset)

8. while PCA (DataSet Features) do

Evaluate the covariance matrix

Acquire eigenvalues and values

end loop

9. Represents the reduced feature set obtained after PCA.

10. Divide the data set into D1 and D2

11.$D1^{old}=D1^{old}_{i}$

$D2^{old}_{i=} D2^{oldL}_{i} U D1^{oldU}_{i}$

12. Map D1 D2 into relation matrix

13. for i=1,2,....,N do

compute w^{i} by MMD

Train the learner on a weighted sample from D1

End loop

14. The initial a

Initialize AT(s,a)

for i= 1 to 10 do

for j=1 to 10 do

t ← 0

st ← preliminary

select an initial state 'st' based on the preliminary state and choose initial action a=continue

while st ≠ prevention and t< T do

ti←ti+1

if a= stop then

st← Prevention

r← π{t< r}

AT (s,a) ← AT (s,a)+α(r- AT (s,a))

elseif a=continue then

If ti>= r then

r ←c

st ←suspected

else

r←0

endif

Collect measurements m_t and update the Kalman filter using:

$\hat{e}_{t|t-1}=M1\hat{e}_{t-1|t-1}+M2u_{t-1}$ and

$P_{t|t-1}=M1P_{t-1|t-1}M1^{T}+AT$

Update: Kalman Gain

$K_t=P_{t|t-1}H^{T}(HP_{t|t-1}H^{T}+R)^{-1}$

State Update

$\hat{e}_{t|t}=\hat{e}_{t|t-1}+K_t(m_t-H\hat{e}_{t|t-1})$

Error Covariance Update

$P_{t|t}=(I-K_tH)P_{t|t-1}$

AT(s, a) ← AT(s, a) + α (r + AT(s', a') − AT(s, a))

s ← s', a ← a'

end if

end while

end for

end for

Procedure Risk Estimation (StT,ADT(1 to 10))

1: for each stakholder in StT do

2: AttackList ← IdentifyRelevantAttacks using Algorithm 2

3: for each attack in AttackList ADT do

4: Impact ← Calculate Attack Impact (ADT)

5: Detectability ← Calculate Attack Detectability(ADT)

6: REF ← Impact × Detectability

7: MitigationList ← GetAttackMitigation (FMT)

8: end for

9: end for

10: return AttackLists, Risk Estimation and MitigationLists

11: end procedure

Algorithm 2: Cyber Attack Detection Algorithm

1. Input: Algorithm-learned AT-table 1.

2: Select the initial a = continue and an initial s depending on the prior situation.

3. t ← 0

4: do 5: t → t + 1 while a ≠ stop

Sixth, gather measurements for each item.

7: Find the new s as it appears in Algorithm 1 lines 20–22.

8: a ← arg minaQ(o, a).

9: finish whilst

10: Claim an assault and stop the process.

In Algorithm 1, after detecting an attack, we have also defined a procedure for risk estimation. The approach is to systematically assess risks by identifying attacks for each stakeholder, quantifying their effect and detectability, and suggesting mitigation solutions. Data gathered from the intelligent cyber-physical system (iCPS) server is processed and prepared for cyberattack detection by this algorithm. It starts by dividing the dataset into subsets and eliminating any unnecessary features. Using an evaluation function, superfluous variables are removed as part of the feature selection process. After that, dimensionality is decreased and key features are extracted using Principal Component Analysis (PCA). For additional processing, the dataset is split into two sets (D1 and D2),

guaranteeing an optimal feature representation that improves the effectiveness of attack detection. Impact: It indicates the severity of the effects if the attack is successful. Detectability: This measures how readily the attack may be discovered or detected by the system or security team. The Risk Estimation Factor (REF) combines impact and detectability to provide an overall assessment of the danger presented by an assault. A greater REF signifies a more serious threat. Mitigation refers to the techniques or procedures utilized to lessen the danger or severity of an attack. Algorithm 2 is used to find the stakeholder's relevant attack types and put them in AttackList. Loop through each assault in AttackList that matches one of the attack types mentioned in the ADT. This algorithm uses a reinforcement learning-based methodology to identify cyberattacks. It iteratively adjusts its state depending on gathered measurements after beginning with an initial state and action based on historical data. By reducing the attack risk function, the system detects possible threats and continuously assesses its current state. By adding additional observations to state estimates, the Kalman filter improves detection accuracy. The operation halts and the system marks an assault if an attack is identified. In order to prioritize the required mitigation steps, the risk estimate process then computes the attack impact, detectability, and risk estimation factor (REF). To evaluate the impact of each attack, it is important to consider how damaging it is to the system, the stakeholders, and the overall organizational objectives. Additionally, assess how easily the attack can be detected by factoring in the level of monitoring, auditing, and available defense mechanisms.. The Risk Exposure Factor (REF) is computed by multiplying the attack's impact by its detection probability. This provides an overall risk assessment that accounts for both the harm and the chance of identifying the assault. Viable mitigation measures for each assault using the FMT are determined as below:

Store the mitigation techniques in the MitigationList.

End the loop that processes each attack for the stakeholder.

End the loop that iterates through each stakeholder.

Return the AttackList, RiskEstimationList, and MitigationList.

The final result includes lists of potential attacks, evaluated risks, and recommended mitigations.

7. RESULT AND DISCUSSION

We assessed the suggested model by dividing the data into training and testing sets. About 30% of the data is set aside for testing to evaluate generalization on unobserved data, while the remaining 70% is used for training to ensure that the model captures a variety of attack patterns. This ratio ensures an accurate performance evaluation while preventing underfitting by offering enough training samples. Finding the ideal balance between accuracy and practical applicability is a regular procedure in cybersecurity research. Depending on the size and complexity of the dataset, alternative splits like 60-40 or 90-10 may be utilized. The following are the performance metrics:

• Precision: (Eq.1) calculates the fraction of accurately classified attack classes compared to expected attack results.

$$\text{Precision(P)} = \frac{\text{TruePositive}}{(TruePositive + FalsePositive)} \quad (1)$$

• Recall: The fraction of properly classified assaults compared to the total number of attacks is obtained using (Eq. 2).

$$\text{Recall} = \frac{\text{TruePositive}}{(TruePositive + FalseNegative)} \quad (2)$$

• F1-Score: It is denoted as the mean of the harmonic between RC and P, which is determined as shown in Eq. 3.

$$\text{F1score} = \frac{2\text{P.RC}}{P + RC} \quad (3)$$

We evaluated our suggested model using 16-class and binary classification to analyze threat identification and prediction of various cyber-attack types. We evaluated detection accuracy using a centralized multi-source transfer learning model, taking into account heterogeneity, data availability, and privacy. Centralized learning allows for better identification of unknown large-scale threats due to the abundance of available data. This research compares several machine learning and deep learning approaches to the suggested model. The models' performance is evaluated using the same datasets through four steps: dataset processing and analysis, centralized learning, feature selection, and data classification with a transfer learning model. Fig. (**3**) compares the performance of a centralized multi-source transfer learning system to current techniques, including Random Forest (RF), Decision Tree (DT), Diffie-Hallman, Support Vector Machine (SVM), Naïve Bayes and Deep Convolution Neural Network (DCNN). Fig. (**3**) shows an examination of potential algorithms for 16-class, 8-class, and 4-class classifications. The suggested approach achieves the maximum accuracy at 97.89% for 16-class classification, 98.45% for 8- 8-class classification, and 98.97% for 4-class classification.

Tables **5**-**14** compares machine learning methodologies to the proposed centralized multi-source transfer learning model for 16-class classification, including Precision, Recall, and F1-Score for all 10 stakeholders. Tables **5**-**14** compare the performance parameters of recall (RC), precision (P), and F1-score for 16-class classification utilizing machine learning approaches including SVM, RF, Naive Bayes, DT, Diffie-Hellman, and DCNN. Each table is generated for all 10 stakeholders. Table **5** is for Patients, Table **6** is for the Hospital, Table **7** is for Staff, Table **8** is for Doctors, Table **9** is for MR, Table **10** is for

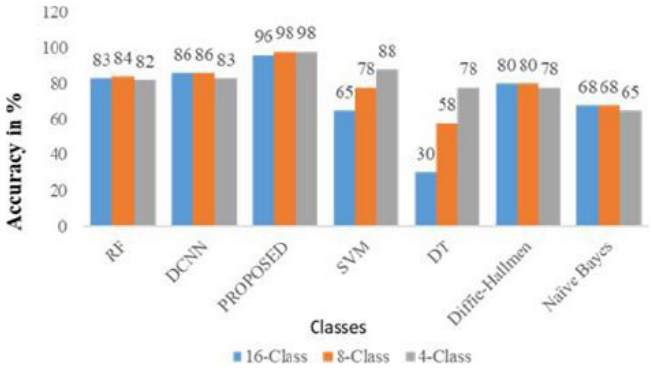

Fig. (3). Comparative result based on 16,8 and 4-class classification.

Table 5. Cyber attack detection table for stakeholder 1.

Algorithm	Matrics	Social Engineering Attacks	Cryptography Attacks	Control Hijacking Attacks	Computer Network Attacks	Phishing Attacks	Malware Attacks	Password Attacks	DDoS Attack	Identity Based Attacks	DoS Attacks
DT	P	0.99891	0.897001	0.69825	0.96864	0.99891	0.89801	0.96864	0.990495	0.893445	0.668325
	RC	0.97485	0.991935	0.59295	0.9447	0.97485	0.87435	0.9447	0.9797	0.991935	0.59295
	F1-Score	0.97485	0.99495	0.603	0.9447	0.97485	0.87435	0.9447	0.9797	0.99495	0.603
RF	P	0.991935	0.891435	0.70149	0.97485	0.991935	0.901485	0.97485	0.99687	0.891435	0.70149
	RC	0.9849	0.903495	0.804	0.95475	0.9849	0.90249	0.95475	0.9898	0.903495	0.804
	F1-Score	0.99495	0.903495	0.7839	0.93465	0.99495	0.903495	0.93465	0.9999	0.903495	0.7839
SVM	P	0.933645	0.833145	0.67335	0.99495	0.933645	0.99294	0.99495	0.93829	0.833145	0.67335
	RC	0.923595	0.823095	0.9045	0.99495	0.923595	0.995955	0.99495	0.92819	0.823095	0.9045
	F1-Score	0.9849	0.8844	0.77385	0.9849	0.9849	0.95475	0.9849	0.9898	0.8844	0.77385
DCNN	P	0.93264	0.93264	0.6633	0.9849	0.93264	0.833145	0.9849	0.93728	0.93264	0.6633
	RC	0.99495	0.99495	0.9045	0.993945	0.99495	0.89445	0.993945	0.9999	0.99495	0.9045
	F1-Score	0.97284	0.97284	0.7638	0.9648	0.97284	0.90048	0.9648	0.97768	0.97284	0.7638
Diffie-Hallman	P	0.923595	0.823095	0.63315	0.99495	0.923595	0.823095	0.99495	0.92819	0.823095	0.63315
	RC	0.97485	0.8844	0.8643	0.97485	0.97485	0.87435	0.97485	0.9797	0.8844	0.8643
	F1-Score	0.9849	0.893445	0.73365	0.97485	0.9849	0.8844	0.97485	0.9898	0.893445	0.73365
Naïve Bayes	P	0.89445	0.993945	0.7638	0.99495	0.89445	0.89445	0.99495	0.8989	0.993945	0.7638
	RC	0.93264	0.9849	0.8844	0.9246	0.93264	0.93264	0.9246	0.93728	0.9849	0.8844
	F1-Score	0.97485	0.99495	0.77385	0.97485	0.97485	0.97485	0.97485	0.9797	0.99495	0.77385
Proposed	P	0.99495	0.95475	0.79395	0.9648	0.99495	0.97485	0.9648	0.9999	0.95475	0.79395
	RC	0.9849	0.89445	0.89445	0.9447	0.9849	0.99495	0.9447	0.9898	0.89445	0.89445
	F1-Score	0.995955	0.99495	0.8844	0.99495	0.995955	0.923595	0.99495	0.991991	0.99495	0.8844

Table 6. Cyber attack detection table for stakeholder 2.

Algorithm	Matrics	Social Engineering Attacks	Cryptography Attacks	Control Hijacking Attacks	Computer Network Attacks	Phishing Attacks	Malware Attacks	Password Attacks	DDoS Attack	Identity Based Attacks	DoS Attacks
DT	P	0.99495	0.893445	0.668325	0.9648	0.99495	0.89445	0.9648	0.9999	0.893445	0.668325
	RC	0.97485	0.991935	0.59295	0.9447	0.97485	0.87435	0.9447	0.9797	0.991935	0.59295
	F1-Score	0.97485	0.99495	0.603	0.9447	0.97485	0.87435	0.9447	0.9797	0.99495	0.603
RF	P	0.991935	0.891435	0.70149	0.97485	0.991935	0.901485	0.97485	0.99687	0.891435	0.70149
	RC	0.9849	0.903495	0.804	0.95475	0.9849	0.90249	0.95475	0.9898	0.903495	0.804
	F1-Score	0.99495	0.903495	0.7839	0.93465	0.99495	0.903495	0.93465	0.9999	0.903495	0.7839

Algorithm	Matrics	Social Engineering Attacks	Cryptography Attacks	Control Hijacking Attacks	Computer Network Attacks	Phishing Attacks	Malware Attacks	Password Attacks	DDoS Attack	Identity Based Attacks	DoS Attacks
SVM	P	0.933645	0.833145	0.67335	0.99495	0.933645	0.99294	0.99495	0.93829	0.833145	0.67335
	RC	0.923595	0.823095	0.9045	0.99495	0.923595	0.995955	0.99495	0.92819	0.823095	0.9045
	F1-Score	0.9849	0.8844	0.77385	0.9849	0.9849	0.95475	0.9849	0.9898	0.8844	0.77385
DCNN	P	0.93264	0.93264	0.6633	0.9849	0.93264	0.833145	0.9849	0.93728	0.93264	0.6633
	RC	0.99495	0.99495	0.9045	0.993945	0.99495	0.89445	0.993945	0.9999	0.99495	0.9045
	F1-Score	0.97284	0.97284	0.7638	0.9648	0.97284	0.90048	0.9648	0.97768	0.97284	0.7638
Diffie-Hallman	P	0.923595	0.823095	0.63315	0.99495	0.923595	0.823095	0.99495	0.92819	0.823095	0.63315
	RC	0.97485	0.8844	0.8643	0.97485	0.97485	0.87435	0.97485	0.9797	0.8844	0.8643
	F1-Score	0.9849	0.893445	0.73365	0.97485	0.9849	0.8844	0.97485	0.9898	0.893445	0.73365
Naïve Bayes	P	0.89445	0.993945	0.7638	0.99495	0.89445	0.89445	0.99495	0.8989	0.993945	0.7638
	RC	0.93264	0.9849	0.8844	0.9246	0.93264	0.93264	0.9246	0.93728	0.9849	0.8844
	F1-Score	0.97485	0.99495	0.77385	0.97485	0.97485	0.97485	0.97485	0.9797	0.99495	0.77385
Proposed	P	0.99495	0.95475	0.79395	0.9648	0.99495	0.97485	0.9648	0.9999	0.95475	0.79395
	RC	0.9849	0.89445	0.89445	0.9447	0.9849	0.99495	0.9447	0.9898	0.89445	0.89445
	F1-Score	0.995955	0.99495	0.8844	0.99495	0.995955	0.923595	0.99495	0.991991	0.99495	0.8844

Table 7. Cyber attack detection table for stakeholder 3.

Algorithm	Matrics	Social Engineering Attacks	Cryptography Attacks	Control Hijacking Attacks	Computer Network Attacks	Phishing Attacks	Malware Attacks	Password Attacks	DDoS Attack	Identity Based Attacks	DoS Attacks
DT	P	0.9999	0.89789	0.67165	0.9696	0.9999	0.8989	0.9696	0.991485	0.89789	0.668325
	RC	0.9797	0.99687	0.5959	0.9494	0.9797	0.8787	0.9494	0.971455	0.99687	0.59295
	F1-Score	0.9797	0.9999	0.606	0.9494	0.9797	0.8787	0.9494	0.971455	0.9999	0.603
RF	P	0.99687	0.89587	0.70498	0.9797	0.99687	0.90597	0.9797	0.988481	0.89587	0.70149
	RC	0.9898	0.90799	0.808	0.9595	0.9898	0.90698	0.9595	0.98147	0.90799	0.804
	F1-Score	0.9999	0.90799	0.7878	0.9393	0.9999	0.90799	0.9393	0.991485	0.90799	0.7839
SVM	P	0.93829	0.83729	0.6767	0.9999	0.93829	0.99788	0.9999	0.930394	0.83729	0.67335
	RC	0.92819	0.82719	0.909	0.9999	0.92819	1.00091	0.9999	0.920379	0.82719	0.9045
	F1-Score	0.9898	0.8888	0.7777	0.9898	0.9898	0.9595	0.9898	0.98147	0.8888	0.77385
DCNN	P	0.93728	0.93728	0.6666	0.9898	0.93728	0.83729	0.9898	0.929392	0.93728	0.6633
	RC	0.9999	0.9999	0.909	0.99889	0.9999	0.8989	0.99889	0.991485	0.9999	0.9045
	F1-Score	0.97768	0.97768	0.7676	0.9696	0.97768	0.90496	0.9696	0.969452	0.97768	0.7638
Diffie-Hallman	P	0.92819	0.82719	0.6363	0.9999	0.92819	0.82719	0.9999	0.920379	0.82719	0.63315
	RC	0.9797	0.8888	0.8686	0.9797	0.9797	0.8787	0.9797	0.971455	0.8888	0.8643
	F1-Score	0.9898	0.89789	0.7373	0.9797	0.9898	0.8888	0.9797	0.98147	0.89789	0.73365
Naïve Bayes	P	0.8989	0.99889	0.7676	0.9999	0.8989	0.8989	0.9999	0.891335	0.99889	0.7638
	RC	0.93728	0.9898	0.8888	0.9292	0.93728	0.93728	0.9292	0.929392	0.9898	0.8844
	F1-Score	0.9797	0.9999	0.7777	0.9797	0.9797	0.9797	0.9797	0.971455	0.9999	0.77385
Proposed	P	0.9999	0.9595	0.7979	0.9696	0.9999	0.9797	0.9696	0.991485	0.9595	0.79395
	RC	0.9898	0.8989	0.8989	0.9494	0.9898	0.9999	0.9494	0.98147	0.8989	0.89445
	F1-Score	0.992982	0.99198	0.8888	0.99198	0.992982	0.920838	0.99198	0.992487	0.99099	0.8844

Table 8. Cyber attack detection table for stakeholder 4.

Algorithm	Matrics	Social Engineering Attacks	Cryptography Attacks	Control Hijacking Attacks	Computer Network Attacks	Phishing Attacks	Malware Attacks	Password Attacks	DDoS Attack	Identity Based Attacks	DoS Attacks
DT	P	0.99198	0.890778	0.674975	0.96192	0.99198	0.89178	0.96192	0.996138	0.890334	0.668325
	RC	0.98455	0.987494	0.59885	0.94047	0.970485	0.870435	0.94047	0.976014	0.988481	0.59295
	F1-Score	0.98455	0.990495	0.609	0.94047	0.970485	0.870435	0.94047	0.976014	0.991485	0.603
RF	P	0.988974	0.888774	0.70847	0.97194	0.988974	0.898794	0.97194	0.993119	0.888331	0.70149
	RC	0.9947	0.912485	0.812	0.96425	0.9947	0.91147	0.96425	0.986076	0.900349	0.804
	F1-Score	0.99198	0.900798	0.7917	0.93186	0.99198	0.900798	0.93186	0.996138	0.900349	0.7839

Algorithm	Matrics	Social Engineering Attacks	Cryptography Attacks	Control Hijacking Attacks	Computer Network Attacks	Phishing Attacks	Malware Attacks	Password Attacks	DDoS Attack	Identity Based Attacks	DoS Attacks
SVM	P	0.942935	0.841435	0.68005	0.990495	0.929465	0.988494	0.990495	0.93476	0.830244	0.67335
	RC	0.932785	0.831285	0.9135	0.990495	0.91946	0.991496	0.990495	0.924698	0.820229	0.9045
	F1-Score	0.9947	0.8932	0.78155	0.9947	0.9947	0.96425	0.9947	0.986076	0.88132	0.77385
DCNN	P	0.94192	0.94192	0.6699	0.9947	0.94192	0.841435	0.9947	0.933754	0.929392	0.6633
	RC	0.99198	0.99198	0.9135	0.990978	0.99198	0.89178	0.990978	0.996138	0.991485	0.9045
	F1-Score	0.98252	0.98252	0.7714	0.9744	0.98252	0.90944	0.9744	0.974002	0.969452	0.7638
Diffie-Hallman	P	0.932785	0.831285	0.63945	0.990495	0.91946	0.81941	0.990495	0.924698	0.820229	0.63315
	RC	0.98455	0.8932	0.8729	0.98455	0.98455	0.88305	0.98455	0.976014	0.88132	0.8643
	F1-Score	0.9947	0.902335	0.74095	0.98455	0.9947	0.8932	0.98455	0.986076	0.890334	0.73365
Naïve Bayes	P	0.90335	0.989495	0.7714	0.990495	0.890445	0.890445	0.990495	0.895518	0.990484	0.7638
	RC	0.94192	0.9947	0.8932	0.9338	0.94192	0.94192	0.9338	0.933754	0.98147	0.8844
	F1-Score	0.98455	0.990495	0.78155	0.970485	0.970485	0.970485	0.970485	0.976014	0.991485	0.77385
Proposed	P	0.99198	0.9519	0.80185	0.96192	0.99198	0.97194	0.96192	0.996138	0.951425	0.79395
	RC	0.9947	0.90335	0.90335	0.9541	0.9947	0.990495	0.94047	0.986076	0.891335	0.89445
	F1-Score	0.992982	0.99198	0.8932	0.99198	0.992982	0.920838	0.99198	0.997144	0.991485	0.8844

Table 9. Cyber attack detection table for stakeholder 5.

Algorithm	Matrics	Social Engineering Attacks	Cryptography Attacks	Control Hijacking Attacks	Computer Network Attacks	Phishing Attacks	Malware Attacks	Password Attacks	DDoS Attack	Identity Based Attacks	DoS Attacks
DT	P	0.99198	0.890778	0.6783	0.96192	0.99198	0.89178	0.96192	0.992475	0.894512	0.668325
	RC	0.9894	0.987197	0.6018	0.940188	0.970194	0.870174	0.940188	0.99425	0.993119	0.59295
	F1-Score	0.9894	0.990198	0.612	0.940188	0.970194	0.870174	0.940188	0.99425	0.996138	0.603
RF	P	0.988974	0.888774	0.71196	0.97194	0.988974	0.898794	0.97194	0.989468	0.892499	0.70149
	RC	0.9996	0.91698	0.816	0.969	0.9996	0.91596	0.969	0.98245	0.904574	0.804
	F1-Score	0.99198	0.900798	0.7956	0.93186	0.99198	0.900798	0.93186	0.992475	0.904574	0.7839
SVM	P	0.94758	0.84558	0.6834	0.990198	0.929186	0.988198	0.990198	0.952225	0.83414	0.67335
	RC	0.93738	0.83538	0.918	0.990198	0.919184	0.991198	0.990198	0.941975	0.824078	0.9045
	F1-Score	0.9996	0.8976	0.7854	0.9996	0.9996	0.969	0.9996	0.98245	0.885456	0.77385
DCNN	P	0.94656	0.94656	0.6732	0.9996	0.94656	0.84558	0.9996	0.9512	0.933754	0.6633
	RC	0.99198	0.99198	0.918	0.990978	0.99198	0.89178	0.990978	0.992475	0.996138	0.9045
	F1-Score	0.98736	0.98736	0.7752	0.9792	0.98736	0.91392	0.9792	0.9922	0.974002	0.7638
Diffie-Hallman	P	0.93738	0.83538	0.6426	0.990198	0.919184	0.819164	0.990198	0.941975	0.824078	0.63315
	RC	0.9894	0.8976	0.8772	0.9894	0.9894	0.8874	0.9894	0.99425	0.885456	0.8643
	F1-Score	0.9996	0.90678	0.7446	0.9894	0.9996	0.8976	0.9894	0.98245	0.894512	0.73365
Naïve Bayes	P	0.9078	0.989198	0.7752	0.990198	0.890178	0.890178	0.990198	0.91225	0.995132	0.7638
	RC	0.94656	0.9996	0.8976	0.9384	0.94656	0.94656	0.9384	0.9512	0.986076	0.8844
	F1-Score	0.9894	0.990198	0.7854	0.970194	0.970194	0.970194	0.970194	0.99425	0.996138	0.77385
Proposed	P	0.99198	0.9519	0.8058	0.96192	0.99198	0.97194	0.96192	0.992475	0.95589	0.79395
	RC	0.9996	0.9078	0.9078	0.9588	0.9996	0.990198	0.940188	0.98245	0.895518	0.89445
	F1-Score	0.992982	0.99198	0.8976	0.99198	0.992982	0.920838	0.99198	0.993478	0.996138	0.8844

Table 10. Cyber attack detection table for stakeholder 6.

Algorithm	Matrics	Social Engineering Attacks	Cryptography Attacks	Control Hijacking Attacks	Computer Network Attacks	Phishing Attacks	Malware Attacks	Password Attacks	DDoS Attack	Identity Based Attacks	DoS Attacks
DT	P	0.990594	0.889533	0.681625	0.960576	0.990594	0.890534	0.960576	0.992475	0.893445	0.668325
	RC	0.970582	0.987592	0.60475	0.940564	0.970582	0.870522	0.940564	0.99425	0.991935	0.59295
	F1-Score	0.970582	0.990594	0.615	0.940564	0.970582	0.870522	0.940564	0.99425	0.99495	0.603
RF	P	0.987592	0.887532	0.71545	0.970582	0.987592	0.897538	0.970582	0.989468	0.891435	0.70149
	RC	0.980588	0.899539	0.82	0.95057	0.980588	0.898539	0.95057	0.98245	0.903495	0.804
	F1-Score	0.990594	0.899539	0.7995	0.930558	0.990594	0.899539	0.930558	0.992475	0.903495	0.7839

Algorithm	Matrics	Social Engineering Attacks	Cryptography Attacks	Control Hijacking Attacks	Computer Network Attacks	Phishing Attacks	Malware Attacks	Password Attacks	DDoS Attack	Identity Based Attacks	DoS Attacks
SVM	P	0.929557	0.829497	0.68675	0.990594	0.929557	0.988593	0.990594	0.952225	0.833145	0.67335
	RC	0.919551	0.819491	0.9225	0.990594	0.919551	0.991595	0.990594	0.941975	0.823095	0.9045
	F1-Score	0.980588	0.880528	0.78925	0.980588	0.980588	0.95057	0.980588	0.98245	0.8844	0.77385
DCNN	P	0.928557	0.928557	0.6765	0.980588	0.928557	0.829497	0.980588	0.9512	0.93264	0.6633
	RC	0.990594	0.990594	0.9225	0.989593	0.990594	0.890534	0.989593	0.992475	0.99495	0.9045
	F1-Score	0.968581	0.968581	0.779	0.960576	0.968581	0.896538	0.960576	0.9922	0.97284	0.7638
Diffie-Hallman	P	0.919551	0.819491	0.64575	0.990594	0.919551	0.819491	0.990594	0.941975	0.823095	0.63315
	RC	0.970582	0.880528	0.8815	0.970582	0.970582	0.870522	0.970582	0.99425	0.8844	0.8643
	F1-Score	0.980588	0.889533	0.74825	0.970582	0.980588	0.880528	0.970582	0.98245	0.893445	0.73365
Naïve Bayes	P	0.890534	0.989593	0.779	0.990594	0.890534	0.890534	0.990594	0.91225	0.993945	0.7638
	RC	0.928557	0.980588	0.902	0.920552	0.928557	0.928557	0.920552	0.9512	0.9849	0.8844
	F1-Score	0.970582	0.990594	0.78925	0.970582	0.970582	0.970582	0.970582	0.99425	0.99495	0.77385
Proposed	P	0.990594	0.95057	0.80975	0.960576	0.990594	0.970582	0.960576	0.992475	0.95475	0.79395
	RC	0.980588	0.890534	0.91225	0.940564	0.980588	0.990594	0.940564	0.98245	0.89445	0.89445
	F1-Score	0.991595	0.990594	0.902	0.990594	0.991595	0.919551	0.990594	0.993478	0.99495	0.8844

Table 11. Cyber attack detection table for stakeholder 7.

Algorithm	Matrics	Social Engineering Attacks	Cryptography Attacks	Control Hijacking Attacks	Computer Network Attacks	Phishing Attacks	Malware Attacks	Password Attacks	DDoS Attack	Identity Based Attacks	DoS Attacks
DT	P	0.99594	0.894334	0.68495	0.96576	0.99594	0.89534	0.96576	0.99297	0.893445	0.668325
	RC	0.97582	0.992922	0.6077	0.94564	0.97582	0.87522	0.94564	0.9991	0.991935	0.59295
	F1-Score	0.97582	0.99594	0.618	0.94564	0.97582	0.87522	0.94564	0.9991	0.99495	0.603
RF	P	0.992922	0.892322	0.71894	0.97582	0.992922	0.902382	0.97582	0.989961	0.891435	0.70149
	RC	0.98588	0.904394	0.824	0.9557	0.98588	0.903388	0.9557	0.98294	0.903495	0.804
	F1-Score	0.99594	0.904394	0.8034	0.93558	0.99594	0.904394	0.93558	0.99297	0.903495	0.7839
SVM	P	0.934574	0.833974	0.6901	0.99594	0.934574	0.993928	0.99594	0.95687	0.833145	0.67335
	RC	0.924514	0.823914	0.927	0.99594	0.924514	0.996946	0.99594	0.94657	0.823095	0.9045
	F1-Score	0.98588	0.88528	0.7931	0.98588	0.98588	0.9557	0.98588	0.98294	0.8844	0.77385
DCNN	P	0.933568	0.933568	0.6798	0.98588	0.933568	0.833974	0.98588	0.95584	0.93264	0.6633
	RC	0.99594	0.99594	0.927	0.994934	0.99594	0.89534	0.994934	0.99297	0.99495	0.9045
	F1-Score	0.973808	0.973808	0.7828	0.96576	0.973808	0.901376	0.96576	0.99704	0.97284	0.7638
Diffie-Hallman	P	0.924514	0.823914	0.6489	0.99594	0.924514	0.823914	0.99594	0.94657	0.823095	0.63315
	RC	0.97582	0.88528	0.8858	0.97582	0.97582	0.87522	0.97582	0.9991	0.8844	0.8643
	F1-Score	0.98588	0.894334	0.7519	0.97582	0.98588	0.88528	0.97582	0.98294	0.893445	0.73365
Naïve Bayes	P	0.89534	0.994934	0.7828	0.99594	0.89534	0.89534	0.99594	0.9167	0.993945	0.7638
	RC	0.933568	0.98588	0.9064	0.92552	0.933568	0.933568	0.92552	0.95584	0.9849	0.8844
	F1-Score	0.97582	0.99594	0.7931	0.97582	0.97582	0.97582	0.97582	0.9991	0.99495	0.77385
Proposed	P	0.99594	0.9557	0.8137	0.96576	0.99594	0.97582	0.96576	0.99297	0.95475	0.79395
	RC	0.98588	0.89534	0.9167	0.94564	0.98588	0.99594	0.94564	0.98294	0.89445	0.89445
	F1-Score	0.996946	0.99594	0.9064	0.99594	0.996946	0.924514	0.99594	0.993973	0.99495	0.8844

Table 12. Cyber attack detection table for stakeholder 8.

Algorithm	Matrics	Social Engineering Attacks	Cryptography Attacks	Control Hijacking Attacks	Computer Network Attacks	Phishing Attacks	Malware Attacks	Password Attacks	DDoS Attack	Identity Based Attacks	DoS Attacks
DT	P	0.99693	0.895223	0.688275	0.96672	0.99693	0.89623	0.96672	0.993465	0.893445	0.668325
	RC	0.97679	0.993909	0.61065	0.94658	0.97679	0.87609	0.94658	0.973395	0.991935	0.59295
	F1-Score	0.97679	0.99693	0.621	0.94658	0.97679	0.87609	0.94658	0.973395	0.99495	0.603
RF	P	0.993909	0.893209	0.72243	0.97679	0.993909	0.903279	0.97679	0.990455	0.891435	0.70149
	RC	0.98686	0.905293	0.828	0.95665	0.98686	0.904286	0.95665	0.98343	0.903495	0.804
	F1-Score	0.99693	0.905293	0.8073	0.93651	0.99693	0.905293	0.93651	0.993465	0.903495	0.7839

Algorithm	Matrics	Social Engineering Attacks	Cryptography Attacks	Control Hijacking Attacks	Computer Network Attacks	Phishing Attacks	Malware Attacks	Password Attacks	DDoS Attack	Identity Based Attacks	DoS Attacks
SVM	P	0.935503	0.834803	0.69345	0.99693	0.935503	0.994916	0.99693	0.961515	0.833145	0.67335
	RC	0.925433	0.824733	0.9315	0.99693	0.925433	0.997937	0.99693	0.951165	0.823095	0.9045
	F1-Score	0.98686	0.88616	0.79695	0.98686	0.98686	0.95665	0.98686	0.98343	0.8844	0.77385
DCNN	P	0.934496	0.934496	0.6831	0.98686	0.934496	0.834803	0.98686	0.96048	0.93264	0.6633
	RC	0.99693	0.99693	0.9315	0.995923	0.99693	0.89623	0.995923	0.993465	0.99495	0.9045
	F1-Score	0.974776	0.974776	0.7866	0.96672	0.974776	0.902272	0.96672	0.971388	0.97284	0.7638
Diffie-Hallman	P	0.925433	0.824733	0.65205	0.99693	0.925433	0.824733	0.99693	0.951165	0.823095	0.63315
	RC	0.97679	0.88616	0.8901	0.97679	0.97679	0.87609	0.97679	0.973395	0.8844	0.8643
	F1-Score	0.98686	0.895223	0.75555	0.97679	0.98686	0.88616	0.97679	0.98343	0.893445	0.73365
Naïve Bayes	P	0.89623	0.995923	0.7866	0.99693	0.89623	0.89623	0.99693	0.92115	0.993945	0.7638
	RC	0.934496	0.98686	0.9108	0.92644	0.934496	0.934496	0.92644	0.96048	0.9849	0.8844
	F1-Score	0.97679	0.99693	0.79695	0.97679	0.97679	0.97679	0.97679	0.973395	0.99495	0.77385
Proposed	P	0.99693	0.95665	0.81765	0.96672	0.99693	0.97679	0.96672	0.993465	0.95475	0.79395
	RC	0.98686	0.89623	0.92115	0.94658	0.98686	0.99693	0.94658	0.98343	0.89445	0.89445
	F1-Score	0.997937	0.99693	0.9108	0.99693	0.997937	0.925433	0.99693	0.994469	0.99495	0.8844

Table 13. Cyber attack detection table for stakeholder 9.

Algorithm	Matrics	Social Engineering Attacks	Cryptography Attacks	Control Hijacking Attacks	Computer network Attacks	Phishing Attacks	Malware Attacks	Password Attacks	DDoS Attack	Identity Based Attacks	DoS Attacks
DT	P	0.99792	0.896112	0.694925	0.96768	0.99792	0.89712	0.96768	0.994455	0.893445	0.668325
	RC	0.97776	0.994896	0.61655	0.94752	0.97776	0.87696	0.94752	0.974365	0.991935	0.59295
	F1-Score	0.97776	0.99792	0.627	0.94752	0.97776	0.87696	0.94752	0.974365	0.99495	0.603
RF	P	0.994896	0.894096	0.72941	0.97776	0.994896	0.904176	0.97776	0.991442	0.891435	0.70149
	RC	0.98784	0.906192	0.836	0.9576	0.98784	0.905184	0.9576	0.98441	0.903495	0.804
	F1-Score	0.99792	0.906192	0.8151	0.93744	0.99792	0.906192	0.93744	0.994455	0.903495	0.7839
SVM	P	0.936432	0.835632	0.70015	0.99792	0.936432	0.995904	0.99792	0.970805	0.833145	0.67335
	RC	0.926352	0.825552	0.9405	0.99792	0.926352	0.998928	0.99792	0.960355	0.823095	0.9045
	F1-Score	0.98784	0.88704	0.80465	0.98784	0.98784	0.9576	0.98784	0.98441	0.8844	0.77385
DCNN	P	0.935424	0.935424	0.6897	0.98784	0.935424	0.835632	0.98784	0.96976	0.93264	0.6633
	RC	0.99792	0.99792	0.9405	0.996912	0.99792	0.89712	0.996912	0.994455	0.99495	0.9045
	F1-Score	0.975744	0.975744	0.7942	0.96768	0.975744	0.903168	0.96768	0.972356	0.97284	0.7638
Diffie-Hallman	P	0.926352	0.825552	0.65835	0.99792	0.926352	0.825552	0.99792	0.960355	0.823095	0.63315
	RC	0.97776	0.88704	0.8987	0.97776	0.97776	0.87696	0.97776	0.974365	0.8844	0.8643
	F1-Score	0.98784	0.896112	0.76285	0.97776	0.98784	0.88704	0.97776	0.98441	0.893445	0.73365
Naïve Bayes	P	0.89712	0.996912	0.7942	0.99792	0.89712	0.89712	0.99792	0.93005	0.993945	0.7638
	RC	0.935424	0.98784	0.9196	0.92736	0.935424	0.935424	0.92736	0.96976	0.9849	0.8844
	F1-Score	0.97776	0.99792	0.80465	0.97776	0.97776	0.97776	0.97776	0.974365	0.99495	0.77385
Proposed	P	0.99792	0.9576	0.82555	0.96768	0.99792	0.97776	0.96768	0.994455	0.95475	0.79395
	RC	0.98784	0.89712	0.93005	0.94752	0.98784	0.99792	0.94752	0.98441	0.89445	0.89445
	F1-Score	0.998928	0.99792	0.9196	0.99792	0.998928	0.926352	0.99792	0.99546	0.99495	0.8844

Table 14. Cyber attack detection table for stakeholder 10.

Algorithm	Matrics	Social Engineering Attacks	Cryptography Attacks	Control Hijacking Attacks	Computer Network Attacks	Phishing Attacks	Malware Attacks	Password Attacks	DDoS Attack	Identity Based Attacks	DoS Attacks
DT	P	0.99891	0.897001	0.69825	0.96864	0.99891	0.89801	0.96864	0.990495	0.893445	0.668325
	RC	0.97873	0.995883	0.6195	0.94846	0.97873	0.87783	0.94846	0.970485	0.991935	0.59295
	F1-Score	0.97873	0.99891	0.63	0.94846	0.97873	0.87783	0.94846	0.970485	0.99495	0.603
RF	P	0.995883	0.894983	0.7329	0.97873	0.995883	0.905073	0.97873	0.987494	0.891435	0.70149
	RC	0.98882	0.907091	0.84	0.95855	0.98882	0.906082	0.95855	0.98049	0.903495	0.804
	F1-Score	0.99891	0.907091	0.819	0.93837	0.99891	0.907091	0.93837	0.990495	0.903495	0.7839

Algorithm	Matrics	Social Engineering Attacks	Cryptography Attacks	Control Hijacking Attacks	Computer Network Attacks	Phishing Attacks	Malware Attacks	Password Attacks	DDoS Attack	Identity Based Attacks	DoS Attacks
SVM	**P**	0.937361	0.836461	0.7035	0.99891	0.937361	0.996892	0.99891	0.97545	0.833145	0.67335
	RC	0.927271	0.826371	0.945	0.99891	0.927271	0.999919	0.99891	0.96495	0.823095	0.9045
	F1-Score	0.98882	0.88792	0.8085	0.98882	0.98882	0.95855	0.98882	0.98049	0.8844	0.77385
DCNN	**P**	0.936352	0.936352	0.693	0.98882	0.936352	0.836461	0.98882	0.9744	0.93264	0.6633
	RC	0.99891	0.99891	0.945	0.997901	0.99891	0.89801	0.997901	0.990495	0.99495	0.9045
	F1-Score	0.976712	0.976712	0.798	0.96864	0.976712	0.904064	0.96864	0.968484	0.97284	0.7638
Diffie-Hallman	**P**	0.927271	0.826371	0.6615	0.99891	0.927271	0.826371	0.99891	0.96495	0.823095	0.63315
	RC	0.97873	0.88792	0.903	0.97873	0.97873	0.87783	0.97873	0.970485	0.8844	0.8643
	F1-Score	0.98882	0.897001	0.7665	0.97873	0.98882	0.88792	0.97873	0.98049	0.893445	0.73365
Naïve Bayes	**P**	0.89801	0.997901	0.798	0.99891	0.89801	0.89801	0.99891	0.9345	0.993945	0.7638
	RC	0.936352	0.98882	0.924	0.92828	0.936352	0.936352	0.92828	0.9744	0.9849	0.8844
	F1-Score	0.97873	0.99891	0.8085	0.97873	0.97873	0.97873	0.97873	0.970485	0.99495	0.77385
Proposed	**P**	0.99891	0.95855	0.8295	0.96864	0.99891	0.97873	0.96864	0.990495	0.95475	0.79395
	RC	0.98882	0.89801	0.9345	0.94846	0.98882	0.99891	0.94846	0.98049	0.89445	0.89445
	F1-Score	0.999919	0.99891	0.924	0.99891	0.999919	0.927271	0.99891	0.991496	0.99495	0.8844

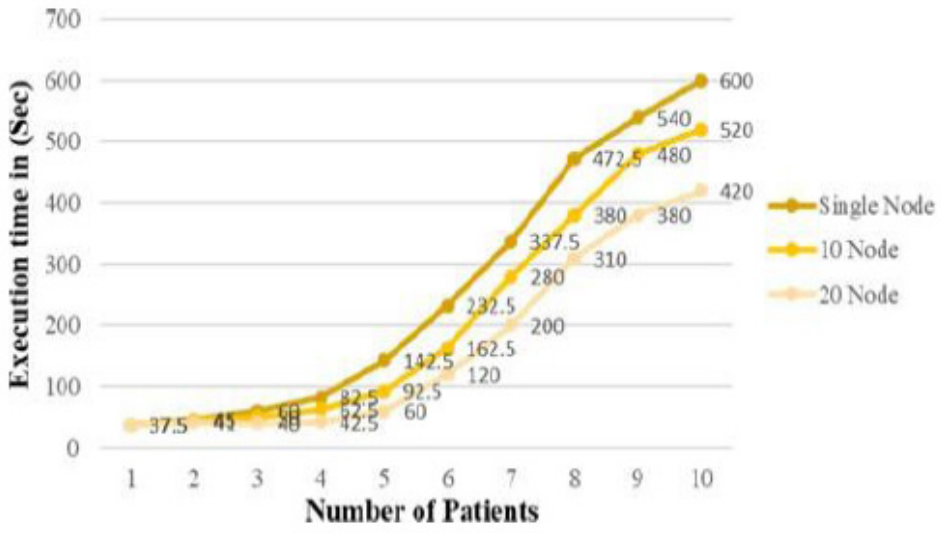

Fig. (4). Local analysis for varying edge-IoT devices for proposed model.

Retailers, Table **11** is for Wholesalers & Raw Material Manufacturers, Table **12** is for Investors, Table **13** is for Drug Manufacturers, and lastly, Table **14** is for PBM & Governance. Algorithm 1 will collect sample data from all 10 stakeholders, and in the loop, Algorithm 2 will run multiple times to detect the attack and will update the stakeholder's state in Q-Table. Tables **5**-**14** display the results achieved with the suggested approach for the same metrics. The suggested model works well in predicting various assaults. Different types of attacks include: Social engineering attacks, Cryptography attacks, Control Hijacking attacks, Computer network attacks, Phishing attacks, Malware attacks, Password attacks, DDoS Attack, Identity-Based Attacks, and DoS Attacks. All stakeholders will be identified for these attacks. So we have 10 tables as a result for each stakeholder by running different algorithms for attack detection.\color{black} The suggested approach achieves high accuracy rates of 93.98% for precision, 94.42% for recall, and 96.67% for F1-Score for diverse assaults, including Social engineering attacks, Cryptography attacks, Control Hijacking attacks, Computer network attacks, Phishing attacks, Malware attacks, Password attacks, DDoS Attack, Identity Based Attacks, DoS Attacks. Compared to current strategies, our suggested model outperforms all others and achieves a high detection/accuracy rate for 16-class classification. Fig. (**4**) illustrates the local analysis performance of the proposed model on several edge IoT devices with varied patient counts. Using the EOT framework, we utilized an Intel i7-3200 CPU with three cores and a virtual machine with 32GB RAM and 3.2GHz for local and global processing. Increasing data size results in a linear speedup for the suggested model. The distributed technique significantly reduces performance overhead by

reducing global and local processing steps based on the number of virtual machines. Different Edge IoT devices are used to determine the time difference between single, 8, and 16 devices for a specific number of patients. Fig. (**5**) illustrates the performance study of a simulated dataset across several edge IoT devices. Fig. (**6**) depicts a study of accuracy for synthetic datasets with varying numbers of data points. Distributed analysis requires a shorter execution time than centralized analysis. The accuracy varies according to the size of the data set. Furthermore, VMs with a range of 1% to 20% may be impacted. In the end, we did a comparative analysis of all algorithms for all stakeholders and found that the proposed algorithm best determines the precision, recall, and F1 score, which is shown in Fig. (**7**).

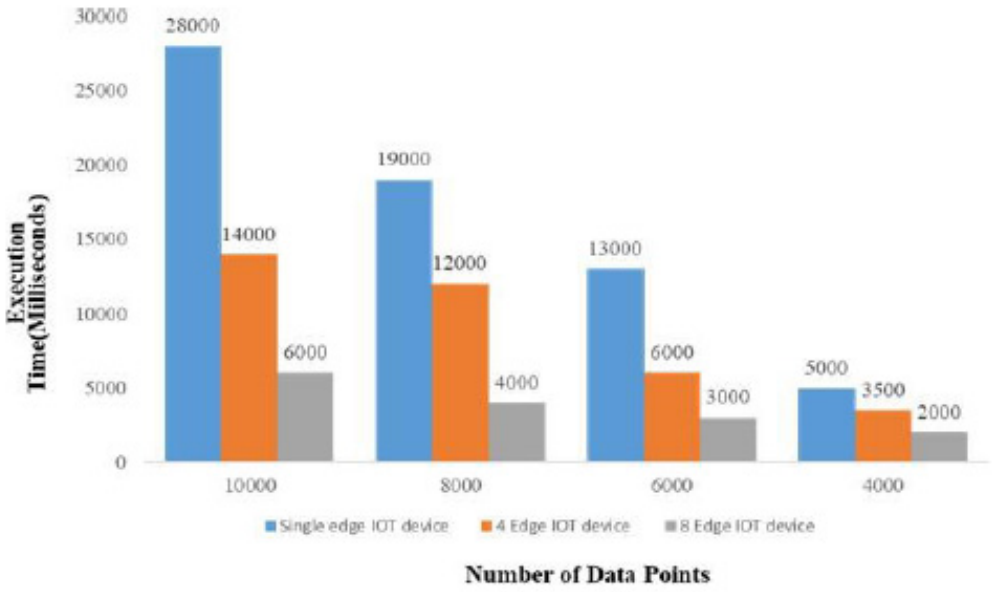

Fig. (5). Data analysis performance for local analysis on varying edge-IoT devices.

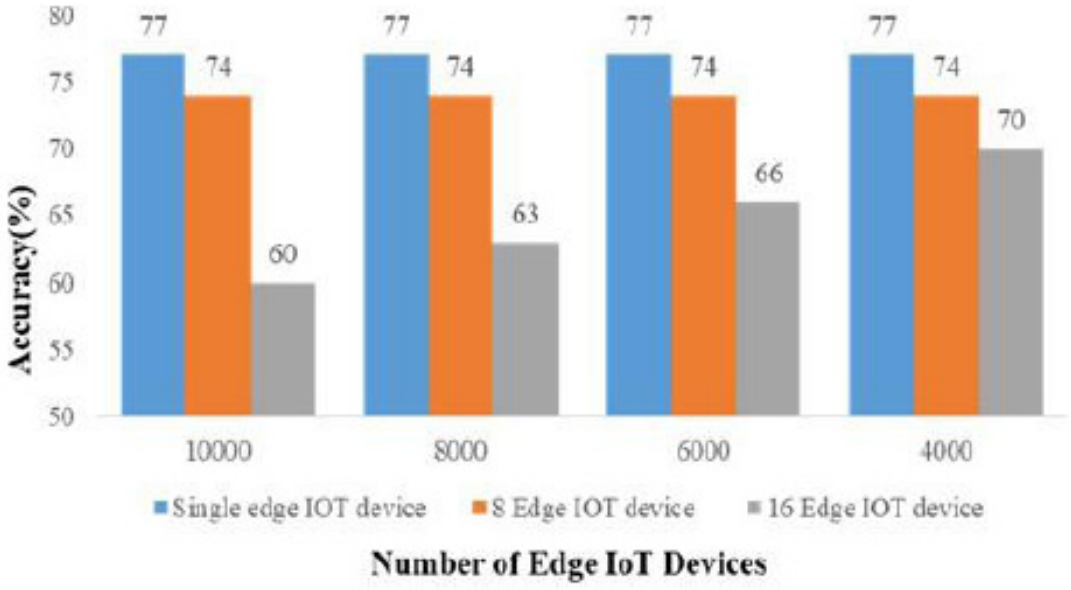

Fig. (6). Accuracy analysis for synthetic dataset.

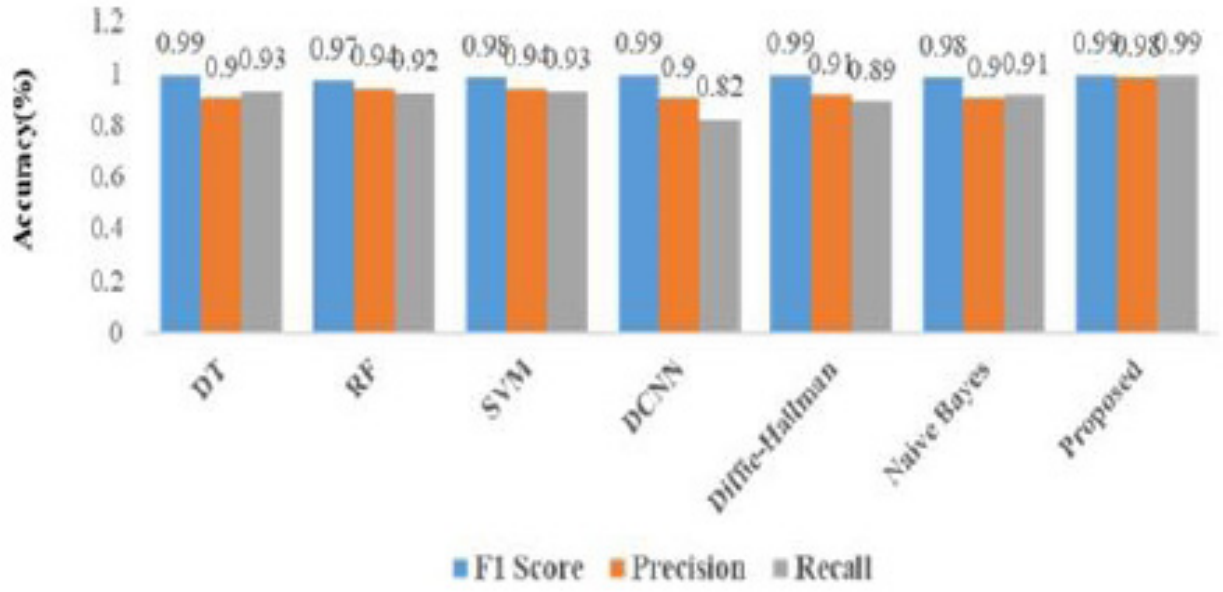

Fig. (7). Comparative analysis among algorithms.

CONCLUSION & FUTURE SCOPE

This paper proposes an Edge of Things (EoT)-based centralized Multi-Source Transfer Learning system to analyze cybersecurity attacks in pharmaceutical care services. This model focuses on assessing machine learning-based intrusion detection systems in a centralized mode. We utilized principal component analysis to extract 16 major features from three datasets and analyzed accuracy, precision, recall, and F1-score for the suggested model. The simulation results of the proposed study are compared to existing machine-learning approaches. The suggested model outperforms existing models, achieving more than 95% accuracy in detecting diverse attacks. In the future, we aim to investigate multi-class classification performance using additional datasets and feature selection strategies. The key constraint of this proposed work is the impact of training settings on model performance. Furthermore, the spread of Edge IoT devices is limited, and other distributions cannot be obtained owing to time constraints. The execution duration of our model grows with more patient data. However, we would prefer to use this effort to address the constraint as a future concern.

AUTHORS' CONTRIBUTION

It is hereby acknowledged that all authors have accepted responsibility for the manuscript's content and consented to its submission. They have meticulously reviewed all results and unanimously approved the final version of the manuscript.

ETHICS APPROVAL AND CONSENT TO PARTICIPATE

Not applicable.

HUMAN AND ANIMAL RIGHTS

Not applicable.

CONSENT FOR PUBLICATION

Not applicable.

STANDARDS OF REPORTING

STROBE guidelines were followed.

AVAILABILITY OF DATA AND MATERIALS

The data and supportive information are available within the article.

FUNDING

None.

CONFLICT OF INTEREST

The authors declare no conflict of interest, financial or otherwise.

ACKNOWLEDGEMENTS

Declared none.

REFERENCES

[1] Huang Z. Analysis of iot-based smart home applications. 2021 IEEE International Conference on Computer Science, Artificial Intelli- gence and Electronic Engineering (CSAIEE). SC, USA, 20-22 August 2021, pp. 218-221

[2] Devliyal S, Goyal HR, Sharma S. Security techniques in cyber physical system for pharmaceutical care services. 2023 IEEE International Conference on Contemporary Computing and Communications. 2023, vol. 1, pp. 1-6 http://dx.doi.org/10.1109/InC457730.2023.10263156

[3] Tabaa M, Monteiro F, Bensag H, Dandache A. Green Industrial Internet of Things from a smart industry perspectives. Energy Rep 2020; 6: 430-46. http://dx.doi.org/10.1016/j.egyr.2020.09.022

[4] Brincat AA, Pacifici F, Martinaglia S, Mazzola F. The internet of things for intelligent transportation systems in real smart cities scenarios. 2019 IEEE 5th World Forum on Internet of Things (WF-IoT). Limerick, Ireland, 15-18 April 2019, pp. 128-132 http://dx.doi.org/10.1109/WF-IoT.2019.8767247

[5] Alluhaidan A S, Alluhaidan M S, Basheer S. Internet of Things based intelligent transportation of food products during COVID. Wirel Pers Commun 2022; 127(Suppl 1): 27. http://dx.doi.org/10.1007/s11277-021-08777-6 PMID: 34456512

[6] Harb H, Mansour A, Nasser A, Cruz EM, de la Torre Diez I. A sensor-based data analytics for patient monitoring in connected healthcare applications. IEEE Sens J 2021; 21(2): 974-84. http://dx.doi.org/10.1109/JSEN.2020.2977352

[7] Ray PP, Dash D, Salah K, Kumar N. Blockchain for iot-based healthcare: Background, consensus, platforms, and use cases. IEEE Syst J 2021; 15(1): 85-94. http://dx.doi.org/10.1109/JSYST.2020.2963840

[8] Khan F, Alturki R, Rahman MA, Mastorakis S, Razzak I, Shah ST. Trustworthy and reliable deep-learning-based cyberattack detection in industrial iot. IEEE Trans Industr Inform 2023; 19(1): 1030-8. http://dx.doi.org/10.1109/TII.2022.3190352 PMID: 37469712

[9] Ghubaish A, Salman T, Zolanvari M, Unal D, Al-Ali A, Jain R. Recent advances in the internet-of-medical-things (iomt) systems security. IEEE Internet Things J 2021; 8(11): 8707-18. http://dx.doi.org/10.1109/JIOT.2020.3045653

[10] Nandy S, Adhikari M, Khan MA, Menon VG, Verma S. An intrusion detection mechanism for secured iomt framework based on swarm-neural network. IEEE J Biomed Health Inform 2022; 26(5): 1969-76. http://dx.doi.org/10.1109/JBHI.2021.3101686 PMID: 34357873

[11] Rasool RU, Ahmad HF, Rafique W, Qayyum A, Qadir J. Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ML. J Netw Comput Appl 2022; 201: 103332. http://dx.doi.org/10.1016/j.jnca.2022.103332

[12] Newaz AI, Sikder AK, Rahman MA, Uluagac AS. A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. ACM Trans Comput Healthc 2021; 2(3): 1-44. http://dx.doi.org/10.1145/3453176

[13] Li Y, Liu Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Rep 2021; 7: 8176-86. http://dx.doi.org/10.1016/j.egyr.2021.08.126

[14] Stoneburner G, Goguen A, Feringa A. Risk management guide for information technology systems. Nist special publication 2002; 800(30): 800-30. http://dx.doi.org/10.6028/NIST.SP.800-30

[15] Devliyal S, Goyal HR, Sharma S. Cyber attack detection techniques in cyber physical system for pharmaceutical care services. 2023 Third International Conference on Secure Cyber Computing and Communication (ICSCCC). Jalandhar, India, 26-28 May 2023, pp. 281-286 http://dx.doi.org/10.1109/ICSCCC58608.2023.10176986

[16] Wu Y, Guo H, Chakraborty C, Khosravi MR, Berretti S, Wan S. Edge computing driven low-light image dynamic enhancement for object detection. IEEE Trans Netw Sci Eng 2023; 10(5): 3086-98. http://dx.doi.org/10.1109/TNSE.2022.3151502

[17] Zhou X, Liang W, Wang KI-K, Yang LT. Deep correla- tion mining based on hierarchical hybrid networks for heterogeneous big data recommendations. IEEE Trans Comput Soc Syst 2021; 8(1): 171-8. http://dx.doi.org/10.1109/TCSS.2020.2987846

[18] Alcaraz C, Zeadally S. Critical infrastructure protection: Requirements and challenges for the 21st century. Int J Crit Infrastruct Prot 2015; 8: 53-66. http://dx.doi.org/10.1016/j.ijcip.2014.12.002

[19] Vijayan R, Mareeswari V, Sridhar K. Healthcare data security in multi-cloud infrastructure using heuristic algorithms. Role of Artificial Intelligence, Telehealth, and Telemedicine in Medical Virology. Springer 2025; pp. 253-67.

[20] Nasayreh A, Khalid HM, Alkhateeb HK, Al-Manaseer J, Ismail A, Gharaibeh H. Automated detection of cyber attacks in healthcare systems: A novel scheme with advanced feature extraction and classification. Comput Secur 2025; 150: 104288. http://dx.doi.org/10.1016/j.cose.2024.104288

[21] Algarni AM, Thayananthan V. Digital health: The cybersecurity for ai-based healthcare communication. IEEE Access 2025; 13: 5858-70. http://dx.doi.org/10.1109/ACCESS.2025.3526666

[22] Janjua F, Masood A, Abbas H, Rashid I. Handling insider threat through supervised machine learning techniques. Procedia Comput Sci 2020; 177: 64-71. http://dx.doi.org/10.1016/j.procs.2020.10.012

[23] Lakhan A, Mohammed MA, Nedoma J, Martinek R, Tiwari P, Kumar N. Blockchain-enabled cybersecurity efficient IIOHT cyber-physical system for medical applications. IEEE Trans Netw Sci Eng 2023; 10(5): 2466-79. http://dx.doi.org/10.1109/TNSE.2022.3213651

[24] Czekster RM, Webber T, Furstenau LB, Marcon C. Dynamic risk assessment approach for analysing cyber security events in medical iot networks. IoT 2025; 29: 101437.

[25] Manimurugan S, Al-Mutairi S, Aborokbah M M, Chilamkurti N, Ganesan S, Patan R. Effective attack detection in internet of medical things smart environment using a deep belief neural network. IEEE Access 2020; 8: 77396-404. http://dx.doi.org/10.1109/ACCESS.2020.2986013

[26] Syed M, Syed S, Sexton K, *et al*. Application of machine learning in intensive care unit (ICU) settings using MIMIC dataset: Systematic review. Informatics 2021; 8(1): 16. http://dx.doi.org/10.3390/informatics8010016 PMID: 33981592

[27] Kumar PM, Kavin BP, Jagathpally A, Shahwar T. Transforming the cybersecurity space of healthcare iot devices using deep learning. 2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC). Houston, TX, USA, 05-07 February 2025, pp. 1-6

[28] Thapliyal S, Wazid M, Singh DP, Das AK, Shetty S, Alqahtani A. Design of robust blockchain-envisioned authenticated key management mechanism for smart healthcare applications. IEEE Access 2023; 11: 93032-47. http://dx.doi.org/10.1109/ACCESS.2023.3310264

[29] Ganin AA, Quach P, Panwar M, *et al*. Multicriteria decision framework for cybersecurity risk assessment and management. Risk Anal 2020; 40(1): 183-99. http://dx.doi.org/10.1111/risa.12891 PMID: 28873246

[30] Thapliyal S, Wazid M, Singh DP. Blockchain-enabled intelligent internet of things system for secured healthcare applications. Ubiquitous and Transparent Security. CRC Press 2024; pp. 86-103. http://dx.doi.org/10.1201/9781003362685-5

[31] Tantawy A, Abdelwahed S, Erradi A, Shaban K. Model-based risk assessment for cyber physical systems security. Comput Secur 2020; 96: 101864. http://dx.doi.org/10.1016/j.cose.2020.101864