International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

# Splunk-Based Threat Intelligence of Cyber-Physical System: A Case Study with Smart Healthcare

**Kundankumar Rameshwar Saraf[1], P. Malathi[2]**

**Submitted**: 11/11/2022 **Accepted**: 14/02/2023

**Abstract***:* Cyber-Physical Systems (CPS) have been proven for many industrial applications like health monitoring, driverless cars, etc. CPS uses computer-based algorithms to monitor and control the IT infrastructure. CPS establishes a cyber-world connection with the physical world. This connection increases the risk of cyber-attacks. Risk assessment methods of traditional IT systems are not enough to assess the risk of CPS. Proper risk assessment and cyber Security of CPS are essential to overcome cyber threats at the very primary stage of their occurrence. This study has taken an effort to synthesize a secure and smart healthcare CPS system using Distributed Parallel Processing of Map Reduce (DPPMR) algorithm. This system monitors the health of remotely located patients as well as detects cyber-attacks on CPS in a short time to safeguard the sensor-based autonomous health monitoring system. This system sends cyber-attack notifications to CPS admin and emergency health condition notifications to the physician through a phone call, message, and email. This system has tested against specified cyber-attacks and monitors the health of 700+ patients for 50 days. This study has concluded that the detection time for cyber-attack and emergency health conditions is 60 seconds and the notification time is less than 90 seconds. Major cyber-attacks such as Zero-Day attack, Eavesdropping attack, Denial-of-Service attack, Brute Force attack, and Replay attack are considered in this study. Finally, a comparative analysis of developed security system with existing systems proved that security measures used by the developed system are more specific, accurate, and concentrated for CPS protection.

***Keywords:*** *Cyber-attack, Cyber-Physical System (CPS), Cyber Security, Denial-of-Service attacks, Eavesdropping attacks, Replay attacks, smart healthcare CPS, Zero-day attack*

## 1. Introduction

CPSs can monitor and manage the physical world objects using their storage, communication, and computing power (Abioye, 2021). CPS is the integration of physical, biological, and engineering systems used in applications such as smart medical devices, intelligent automotive systems, energy-optimal buildings, zero-fatality highways, etc (Kozak, 2019). CPS has a vast impact on the economy, and environment. Its focus area of study are academia, medical applications, industry, and governments (Griffor, 2017). CPS can help in providing technological improvement and also improves the living standard of a human being through customized smart healthcare (Haque, 2014), emergency alert system (Gelenbe, 2012), transportation management (Xiong, 2015), smart manufacturing system (Lee, 2015; Khalid, 2018), national security and defense (Clark, 2017), secure energy supply system (Clark, 2022).

Current studies focus on the performance, stability, efficiency, and robustness of CPS (Ying, 2019; Goyal, 2022). Researchers have overlooked the CPS security issues (Ananda, 2019). Security breaches in CPS lead to a catastrophic impact on industry and businesses. Unattended vulnerabilities in CPS mark them an easy target for cybercriminals (Lezzi, 2018). Cyber-attacks affect major features of CPS such as real-time response, predictability, high availability, and reliability (Brewer, 2012; Mahoney, 2017; Lu, 2018). An increase in the internet-based automation of the physical system increases the risk of cyber-attack like exploitation attacks (Lezzi, 2018; Horowitz, 2012). In the future, CPS will work in a wide operating range, which makes it more complicated, and hence leads to the possibility of more cyber-attacks such as side-channel attacks (Griffor, 2017). Static risk assessment methods provide only a rough estimate of risk for a given period on CPS; they fail to provide accurate risk estimation at a specific time (Wenbo, 2015). The effectiveness of risk assessment can be improved by using dynamic risk assessment methods, which quickly identify the risk in an ever-changing environment. They have a proactive approach to assessing the newer risk and predicting the safety measures to avoid future risks. This study has implemented the dynamic risk assessment method to predict the risk of the smart healthcare system. This study mainly focuses on majorly affecting cyber-attacks such as Zero-Day attack, Eavesdropping attack, Denial-of-Service attack, Brute Force attack and Replay attack.

[1] *Department of Electronics and Telecommunication Engineering, D. Y. Patil College of Engineering, Pune, Maharashtra, India*
*ORCID ID : 0000-0002-9085-0660*
[2] *Department of Electronics and Telecommunication Engineering, D. Y. Patil College of Engineering, Pune, Maharashtra, India*
*ORCID ID : 0000-0003-3345-540X*
** Corresponding Author Email: kundansaraf@email.com*

Enormous Cyber-attacks on a CPS reduce its efficiency and widespread use. Instantaneous detection of cyber-attack protects the CPS and improves its credibility. This paper uses Distributed Parallel Processing of Map Reduce (DPPMR) algorithm to gather and process the data. Splunk 9.0.2 used to collect the CPS logs. To prove the effectiveness of the used method a smart healthcare CPS system is developed. This system monitors the health of remotely located patients. The Syslog server stores the patient data in the form of logs. Splunk monitors the logs generated by the Syslog server. Splunk search commands are used to create dashboards and alerts. The dashboards show the present health condition, as well as the status of the cyber-attack on the CPS. The physician receives notification for any emergency health issue of the patient. The CPS admin receives notification for any cyber-attack on CPS. This system has built-in risk assessment technology to detect various cyber-attack at their preliminary stage. Monitor the logs to detect the cyber-attacks on CPS and alerts created to notify any security risk instantaneously. This paper also presented a comparative analysis of similar CPS cyber-threat detection and protection systems. The conclusion of this study shows that the developed system detects cyber-attack at an instantaneous speed with improved accuracy.

## 2. Related Work

Live threat identification for cloud-based systems is performed by using Splunk (Ananthapadmanabhan, 2022). It uses threat modeling and threat intelligence to identify the cyber-attack on the cloud. Splunk machine learning toolkit detects DNS malicious behavior such as spam, phishing, malware, and botnet (Cersosimo, 2022). Splunk Enterprise 6.4.2 detects cyber-attacks and suspicious user activities (Zhao, 2022). A proactive threat-hunting model and digital footprints using Splunk in Security Operation Center (SOC) detect network anomalies (Prakash, 20220. Splunk Enterprise Security software detects CPS cyber-attacks (Saraf, 2020). Splunk performs predictive analysis of CPS cyber-attacks (Saraf, 2022). A combination of lightweight cryptographic algorithms and Splunk secures a contactless tachometer-based brushless DC motor (Saraf, 2021).

**Zero-day attack –** Internal or external attackers discover the vulnerabilities in the operating system (O.S.), in-built or externally installed software. The attacker exploits these vulnerabilities to gain unauthorized access to CPS (Guo, 2022). This is a zero-day attack and this attack was overlooked by all the above researchers. This paper shows the method to detect the vulnerabilities in O.S. as well as software in CPS. The CPS admin confiscates these vulnerabilities to protect the CPS against zero-day attacks. As shown in figure 1 below the 'Infected CPS Servers' panel detects the number of servers infected with vulnerability in the last 24 hours. The 'Malware Signatures' panel shows the number of malware signatures detected on CPS servers in the last 24 hours.

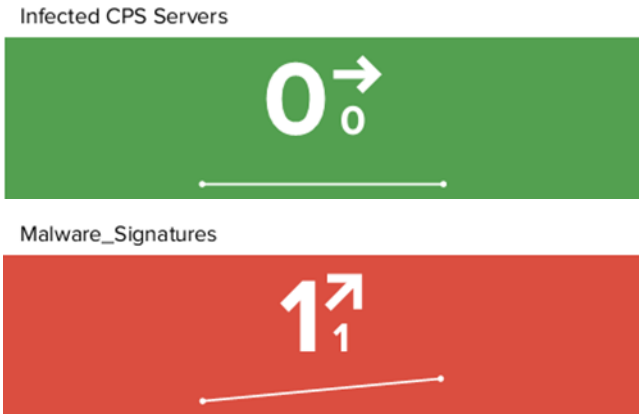
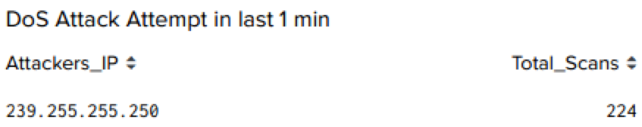


**Fig. 1.** Zero-Day Attack Detection

**Eavesdropping attack –** CPS contains interconnected servers and sensors. Communication between these devices should be protected against intrusion attacks. The unprotected CPS communication can be intercepted, modified, and deleted by the attacker leading to an eavesdropping attack. All above researchers use Splunk 7.2 and below for their study. These Splunk versions have weak encryption capabilities as compared to higher Splunk versions (Xu, 2022). These versions can be susceptible to eavesdropping and man-in-the-middle attacks. This paper uses Splunk 9.0.2 to implement the CPS. This version has improvised the security of communication using Transport Layer Security (TLS) with a valid TLS certificate. In this new version of Splunk, any machine cannot establish a direct inbound connection with the management port of the Splunk universal forwarder. A configuration change in the forwarder is mandatory before every new inbound connection (Splunk, 2022). Because of this new security measure of Splunk 9.0.2 (Splunk, 2022), an attacker can't establish a direct connection with the Splunk universal forwarder which protects the CPS against eavesdropping attacks.

**Denial-of-Service (DoS) attack –** The communication between various CPS devices is dependent on the internet. The attacker can send forged data packets to any CPS server and overwhelm its normal operation. This server denies the service to a legitimate CPS device (Chen, 2022). This increases congestion and hence delays in CPS communication. Sometimes it may completely block communication. This study monitors traffic on every CPS device using Splunk. If any known or unknown CPS device or server sends a high number of packets, the system immediately notifies to CPS admin by an alert. CPS admin monitors and blocks any illegitimate traffic to the CPS. Figure 2 below shows the total number of scanning of CPS servers within 1 minute. DoS attack alert notifies the CPS admin if any user scans any CPS server more than 1000 times in a 1-minute duration.

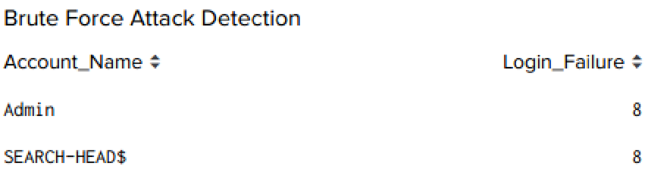


DoS Attack Attempt in last 1 min

| Attackers_IP ⇕ | Total_Scans ⇕ |
|---|---|
| 239.255.255.250 | 224 |

**Fig. 2.** DoS Attack Detection

**Brute-force attack –** Any unauthenticated login attempt to any CPS component using the trial and error method is called a Brute-force attack (Saraf, 2022). Most researchers have ignored this attack. But this study has concentrated to find every unsuccessful login attempt along with brute force attack attempt. Figure 3 below shows the detection of a Brute Force attack attempt. This system sends an alert to the CPS admin if any user made a failed login attempt more than 7 times in the last 24 hours duration. It shows the number of failed login attempts in the below dashboard panel.



Brute Force Attack Detection

| Account_Name ⇕ | Login_Failure ⇕ |
|---|---|
| Admin | 8 |
| SEARCH-HEAD$ | 8 |

**Fig. 3.** Brute Force Attack Detection

**Replay attack –** The attacker takes control of the transmitted data by CPS and deceptively delays it or resends it to the authenticated receiver or victim (Naha, 2022). The inbound and outbound traffic of Splunk 9.0.2 uses TLS and the universal forwarder has a message authentication code (MAC) and a new cipher suite to protect the traffic. Hence, it reduces the chances of a replay attack.

## 3. Mathematical Modelling of CPS Attack

Cyber-attack on CPS depends on various factors such as a set of the attacker, target, victim, channel, layers, severity, and type. This is explained in detail by derivation given below,

Let us assume that 'AT' denotes the set of attackers while 'VC' denotes the set of victims, the set of systems affected by the attack is 'ST'. The set of cyber-attacks is denoted using CYAT. A victim can be a single person or an organization. Attacks done by people are represented by 'P' and attacks done by the organization are presented as 'O'

$$\boldsymbol{VC} \triangleq \{\boldsymbol{P} \cup \boldsymbol{O}\} \tag{1}$$

Every system has many processes running in these systems. 'Pr' denotes this set of processes. This network has multiple routers and bridges, switches, hubs and firewalls, and other network components. All these components are considered as 'C'. Multiple programs are running on every system. These programs handle the data and these systems transmit these data to other systems. The set of data is denoted by 'DT'. According to the proposed model, every attack is generated from attacker 'AT'. Every attack has either a single target or a set of targets. The target of these cyber-attacks can be data, processes, systems, or a network. All these targets denoted by 'TR' as below,

$$\boldsymbol{TR} \triangleq \{\boldsymbol{DT} \cup \boldsymbol{P} \cup \boldsymbol{ST} \cup \boldsymbol{C}\} \tag{2}$$

By using a target, every attacker tries to victimize the person or organization i.e. 'VC'.

$$\boldsymbol{at} \Vdash \boldsymbol{tr} \eqcirc \boldsymbol{VC} \tag{3}$$

Where,

$$\boldsymbol{at} \in \boldsymbol{AT}, \boldsymbol{tr} \subseteq \boldsymbol{TR}, \boldsymbol{vc} \in \boldsymbol{VC}$$

The notation $\Vdash$ shows the direction of the attack. The notation $\eqcirc$ used to point out the respective victim. Channel needed to launch every cyber-attack. Visual, network, and hybrid channels are considered in this study. Using a visual channel the attacker can visually inspect the victim or system, collect the sensitive data and launch the attack by accessing the system physically. Using a network channel, the attacker establishes a connection with the remotely located victim's system and uses the internet to launch the attack. Using a hybrid channel, the attacker collects the victim's data physically and uses the network or internet to launch the attack remotely. The visual channel is indicated by 'VCH', 'NCH' used to indicate the network channel, and 'HCH' used to indicate the hybrid channel. Set of the channels is denoted by 'CH' as given below,

$$\boldsymbol{CH} \triangleq \{\boldsymbol{VCH} \cup \boldsymbol{NCH} \cup \boldsymbol{HCH}\} \tag{4}$$

To communicate with other systems, every computing system has a conceptual model of layers. This study uses TCP/IP protocol. According to TCP/IP protocol, the four layers network interface layer denotes it as an 'NL', the Internet layer denotes it as an 'IL', the transport layer denotes a 'TL', and the application layer denote an 'AL'. For a successful attack to happen, every cyber-attack usually targets a particular layer. Some of the attacks are targeting to multiple layers. After combining these four layers, the set of layers is denoted by 'SL' as follows,

$$\boldsymbol{SL} \triangleq \{\boldsymbol{NL} \cup \boldsymbol{IL} \cup \boldsymbol{TL} \cup \boldsymbol{AL}\} \tag{5}$$

Every attack has a probability of being successful. This probability is denoted as 'Pattack'. The probability of an attack shows its severity. Based on the attack probability the attack has high medium and low severity. Here consider a function 'SV' to denote the severity of the attack.

$$\boldsymbol{SV} : \boldsymbol{ATTACK} \rightarrow \{\boldsymbol{low},\ \boldsymbol{medium},\ \boldsymbol{high}\} \tag{6}$$

To simplify the attack severity in the form of the threshold of probability of attack, use ‘HT’ as a high probability threshold and ‘LT’ as a low probability threshold.

$$SV(ATTACK) = \begin{cases} severe,\ if\ P_{attack} > HT \\ medium, if\ LT < P_{attack} < HT \\ low,\ if\ P_{attack} < LT \end{cases}$$

(7)

There are two types of attacks active and passive. Denote active attack as ‘ACT’ and passive attack as ‘PAT’. By using an active attack, the attacker can insect any bug in a victim’s system or communication, which will disturb its normal way of working. By using a passive attack, the attacker can only eavesdrop on the functioning of the victim’s system or communication but he cannot disturb or modify its normal working behavior. So, the type of attack can be shown in the form of an equation as follows,

$$\boldsymbol{TYPE} \triangleq \{\boldsymbol{ACT}\ \cup \boldsymbol{PAT}\}$$

(8)

Finally, the relation of cyber-attack with various factors is given below,

$$\boldsymbol{attack} \triangleq \{\boldsymbol{at}\ \Vdash \boldsymbol{tr}\ \eqcirc \boldsymbol{vc}, \boldsymbol{ch}, \boldsymbol{sl}, \boldsymbol{sv}, \boldsymbol{type}\}$$

(9)

Where, $attack\ \in ATTACK$ = cyber-attack

$at\ \in AT$ = set of the attacker – refer to equation (3)

$tr\ \in TR$ = set of targets – refer to equation (2)

$vc\ \in VC$ = set of victims – refer to equation (1)

$ch\ \in CH$ = set of channels – refer to equation (4)

$sl\ \in SL$ = set of layers – refer to equation (5)

$sv\ \in SV$ = Severity of attack – refer to equation (6)

$type\ \in TYPE$ = Type of attack – refer to equation (8)

## 4. Need for a Smart Healthcare System

The worldwide pandemic resulting due to Covid-19 had shaken the whole healthcare domain, as the present infra crippled badly to service the patients, especially in highly populated countries like India. As per the Inequality Report 2021 (India, 2021), India had 0.5 beds per 1000 people, whereas as per WHO standards (Govt, 2021), a minimum of 3 beds per 1000 is required. Also, as the same report, India has a ratio of 0.86 doctors per 1000 population, which must be 1:1000 as per WHO. This calls for urgent infrastructure development which must be easy to establish and cost-effective. To create technological support to assist the existing healthcare infrastructure, researchers are exploring the alternate path to hospitalization by developing the architecture for remote patient monitoring and physician alarm system, which can release pressure on hospital infra by creating virtual patient beds at a remote location like a patient’s home. In addition to that online patient monitoring and alarm, reduces the use of human attendants.

Healthcare Cyber-physical system (CPS) creates an eco-system of virtualization, by adapting physical devices with internet-based virtualization systems to form an investigative structure that reacts perceptively to vigorous circumstances. As per the National Institute of Standards and Technology (NIST, USA), “CPS comprises interacting digital, analog, physical, and human components engineered for function through integrated physics and logic” (Griffor, 2017). Three diverse working zones establish the CPS ecosystem, i.e. computation, networking, and physical device or processes (Tyagi, 2021). The CPS architectures must capture a variety of physical information, reliable data analysis, event detection, and security.

## 5. CPS in Smart Healthcare System

In the healthcare environment, there is a large-scale integration of intelligent devices and monitors that are keeping track of patients’ essential parameters, trigger advanced alarms, maintain basic infrastructure data, and pharmaceutical data are used to create analysis reports as per the requirement. This technology is also referred to as Medical 4.0 (Haleem, 2022). This architecture comprises Medical cyber-physical systems (MCPS). These methods are gaining importance in hospital culture to realize an incessant superior healthcare setup. These monitoring systems are mostly integrated with online servers or connected to the internet to access medical data processing tools which enable seamless documentation and file transfer, smooth medical report generation, and also help in medication by predictive analysis to trace any growing health anomaly that enables early treatment or also supports effective patient treatment (Chen, 2021). In the advanced stage, smart medical devices are supporting life support mechanisms by integrating control units to maintain patients’ different physiological aspects. The adaption of high-level computing applications in Healthcare applications is driven by the need for intelligent decision-making based on patient data (Dash, 2019). In this scenario, the cloud-computing tech imbibes the spine of CPS systems to provide powers like scalability for data gathering, storage, and processing. The surveillance level in a controlled healthcare environment is highly intense as the decision and control operation of the machines go a long way in creating a survival situation for the patient. Combining both the assisted and controlled aspects of healthcare transforms the healthcare system into a complex, large and safety-critical cyber-physical system with numerous advantages along with challenges (Shah, 2016). Here, in the study, a generalized healthcare-based CPS is considered, as portrayed in figure 4. It is modeled with one bed, integrated with compute infra for data logging like a

Syslog server. The bed is implanted with an ensemble set of sensors and monitors, which records and retains track of the physical conditions of the patient. Essential monitors considered here include a Heartbeat sensor, a Perfusion Index sensor, a SpO2 sensor on the hands, a Temperature sensor at the arms, and a Weight sensor on the bed.

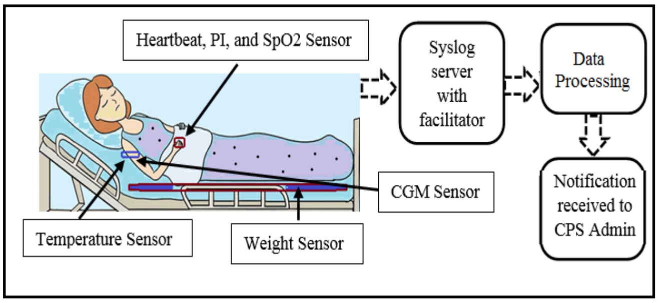

Heartbeat, PI, and SpO2 Sensor
Syslog server with facilitator
Data Processing
CGM Sensor
Notification received to CPS Admin
Temperature Sensor
Weight Sensor

**Fig. 4.** A generalized Healthcare CPS environment

These devices generate proliferates physical data and send it for logging by a Syslog server. Concerning the complexity of the system that can be designed, there are two levels of healthcare CPS levels as detailed in table 1 (Verma, 2022).

## 6. Healthcare CPS reliability

Reliability is a significant stat for CPS and becomes highly imperative while dealing healthcare industry. Figure 2 displays the dependability of healthcare CPS on hardware units like health sensors, actuators, and trustworthiness on software schemes for figuring out patient's well-being, and consistency of communiqué unit of networks for the transfer of patient data. The instigation of CPS necessitates resource optimization and autonomy for effectual, and dependable facilities (Caesar, 2019).

The self-governing ML schemes must recognize the failure of CPS constituents and actuate remedial procedures to handle it (Leung, 2020). Self-adaptive constituent of CPS learns from historical data and decides concerning present data inputs. Smart technologies like nurse robots can auto-order to any drastic dynamic situation to contemplate service quality challenges (Christoforou, 2020). Refer to Table 1 to get the crux of two important complexity levels of creating a CPS-based Healthcare infrastructure.

**Table 1.** Levels of CPS in the Healthcare system

| **Healthcare CPS Level** | **Characteristics** | **Data Types used** | **Monitoring and Control** |
|---|---|---|---|
| Unit Level | Sensors and monitors need to work fine | Analysis system deals with assorted data | Regular monitoring |
| Integrated Level | The whole infra including sensors, monitors in hospitals, ambulances, and remote units along with connectivity among them must work fine | Audio-video data, behavior data along with vital statistics are used for analysis | Monitoring, control, alarm system, notification, reminder system |

## 7. Methodologies for Distributed Processing of Data

The orthodox tactics for healthcare information administration have attained partial triumph due to their incompetent capacity of supervising enormous quantities of complex data from the healthcare CPS with characters of high volume, high velocity, and high variety that asks for big-data analytics. With the adoption of cloud resources, the capacity of data digestion has rapidly increased. Data analytics standards need to be altered to handle an inflow of information, complemented by the need for equally rapid output (Galetsi, 2020; Fang, 2016). The Healthcare CPS system is a continuous patient monitoring and analysis system that deals with a large database with new data getting added continuously. The analysis system must be rapid enough to accelerate the rapidity of data processing to provide meaningful output. The data flow schematic is depicted in figure 4. Big data for CPS necessitates a proper synchronization of data warehouses that are framed on non-relational database methodologies like Presto, Hydra, Hadoop, Map-Reduce, and others. Compute resources powered by any CPS provides the necessary platform for data warehousing (Padhy, 2013; Sahoo, 2016; Kuo, 2019). Orthodox methods cannot sustain in a big-data CPS environment as real-time analytics is mandatory for effective use in healthcare setup. Big data in CPS needs instantaneous data-stream processing and control and also mandates batch processing for modeling and machine learning (Xian, 2021)

In the core of this application study, Distributed data analysis by the MapReduce model is utilized. Hadoop MapReduce is a software framework for the effortless inscription of methods that can handle enormous data in parallel on thousands of nodes of service hardware in a dependable manner. The Data bundle is dispersed crosswise through several computations and storages. The datasets accrued in the server are in Hadoop Distributed File System (HDFS) configuration. It achieves a "Map" function concurrently on individual storages, by appropriation to trace appropriate pieces. Consequently, a "Reduce" function is implemented on the outcome of the preceding action to amass exclusively patched outcomes at all server-end units. The conclusion of the request is returned in HDFS format only (Hadoop, 2022).

### 7.1. Implementation of data management using Splunk

In our execution, the functioning unit has transactions with a flood of sensor data, laterally with numerous security logs, request logs, database logs, transaction logs, network logs, performance data, disk data, memory-associated statistics, and supplementary significant indicators. To empower a laidback and plausible interface, the study application practices a utility entitled InfoSec App for Splunk, applicable through the Splunk platform, which is essentially a log monitoring tool (Infosec, 2022). Admin can formulate console, warnings, and other awareness objects. It allows examination, investigation, and visualization of data resonating through graphs. It also allows on-premises and cloud setup. InfoSec app distributes solutions to confront cyber threats and security circumstances, with topographies of continuous monitoring and security investigations. Its inspection sphere can be prolonged using Security Essentials app that stretches access to superfluous security confronting tools (MLApp, 2022).

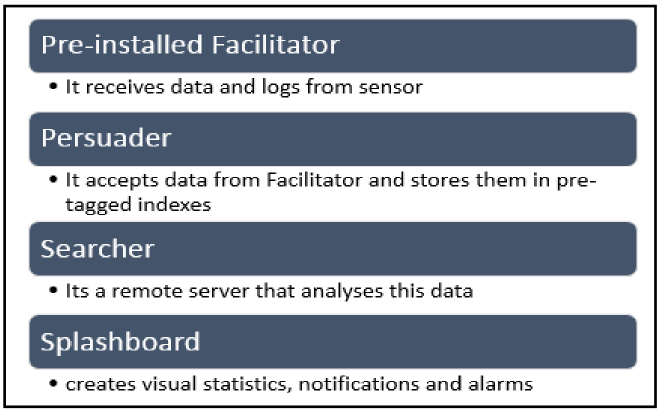

Pre-installed Facilitator
• It receives data and logs from sensor
Persuader
• It accepts data from Facilitator and stores them in pre-tagged indexes
Searcher
• Its a remote server that analyses this data
Splashboard
• creates visual statistics, notifications and alarms

**Fig. 5.** Data flow through the system

To craft an appropriate data passage, as presented in figure 5, the detected information streams into the Facilitator, which is mounted on each Syslog server, after that these are channeled to the following phase, Persuader, which amasses these logs and categorically store them with pre-defined indexes. Here, the system user or admin can customize innumerable probing algorithms to refine the data for the appropriate outcome. Handlers can implement tools to generate announcements to advise on security issues to CPS admin. Also, on the health front, notifications to report to the physician concerning any abrupt health concern of the patient. Splashboards are designed for illustration purposes regarding threat status for CPS components related to cyber threats and patient health statistics.

### 7.2. Data and log Management by DPPMR algorithm

This study explains Distributed Parallel Processing of the MapReduce (DPPMR) algorithm as shown in figure 6 below. At the initial stage of this process, all types of logs are collected at a common Syslog server. Splunk universal forwarder (or facilitator) installed on the Syslog server transfers this data to the Splunk indexer (or persuader). In the mapping phase, Splunk indexer stores this data into various pre-identified indexes. This data is warehoused in an indexed form such as app data index, external index, and performance index. A Splunk search head (or searcher) server utilizes modeled query run to explore the data, with a prefixed time interval. This query is intended on grabbing cyber-attack signatures by monitoring the logs. This query also grabs various health parameters of a patient. If the query hits any signature, it produces a notification to report the user. In addition, on each alarm, the user will pursue the itemized logs and will take recommended action of either blocking the malicious IP address or implementing a firewall, or suggesting appropriate treatment to the patient's relative.

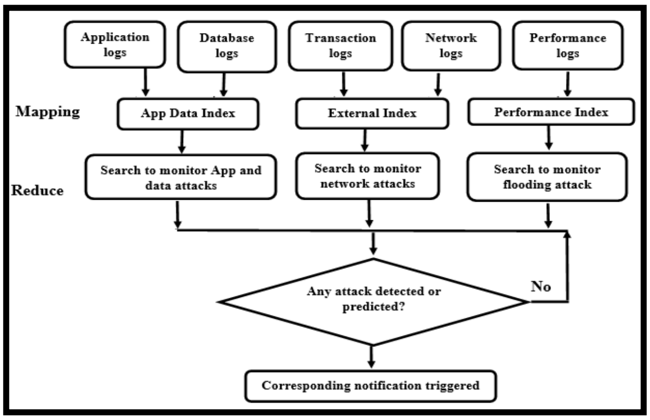

Application logs
Database logs
Transaction logs
Network logs
Performance logs
Mapping
App Data Index
External Index
Performance Index
Reduce
Search to monitor App and data attacks
Search to monitor network attacks
Search to monitor flooding attack
Any attack detected or predicted?
No
Corresponding notification triggered

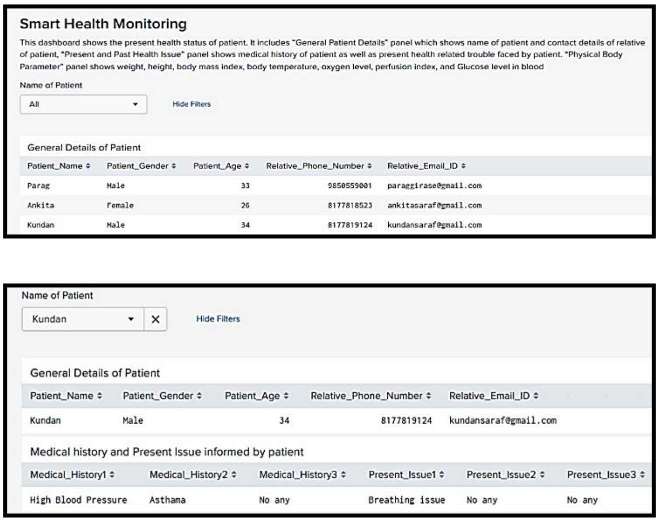
**Fig. 6.** DPPMR Data handling process

## 8. Output Visualization and Results

In this segment, the dialogue is emphasized around the actual case study where the application under confab is in procedure to retain a trail of inbound data from CPS attached to the patient's environment in a healthcare scenario. As deliberated in the preceding segment, Security associated warnings to inform admin concerning the cyber-attack detection on CPS and a patient health alert to advise the physician concerning some perceived emergency health issue. The admin is expected to take relevant action based on the Cyber security dashboard (or splashboard) depicting the status of cyber-attack severity upsetting the CPS. The physician can view the dashboard to understand the unfavorable status of the affected patient.

### 8.1. Health monitoring dashboard in the smart medical system

In this study three, remotely placed patients are considered a part of the CPS environment. The data received is used to populate the dashboard. The stats show the various parameters recorded at the patient level. As shown in figure 7, this dashboard framed in Splunk has data from 3 patients. This dashboard has nine panels. The General Details of Patient panel includes the name, gender, age, phone number, and email id of the patient, and the relative's phone number and mail-id. 'Medical History and Present Issue informed by Patient' panel includes the history of the patient's health and present health issues faced by the patient. As shown below patient's name is 'Kundan', age 34 years, and have high blood pressure and asthma issue. Presently this patient is facing breathing issues as per data available with Smart Health Monitoring CPS.



Smart Health Monitoring

This dashboard shows the present health status of patient. It includes "General Patient Details" panel which shows name of patient and contact details of relative of patient, "Present and Past Health Issue" panel shows medical history of patient as well as present health related trouble faced by patient. "Physical Body Parameter" panel shows weight, height, body mass index, body temperature, oxygen level, perfusion index, and Glucose level in blood

Name of Patient: All

General Details of Patient

| Patient_Name | Patient_Gender | Patient_Age | Relative_Phone_Number | Relative_Email_ID |
|---|---|---|---|---|
| Parag | Male | 33 | 9850559001 | paraggirase@gmail.com |
| Ankita | Female | 26 | 8177818523 | ankitasaraf@gmail.com |
| Kundan | Male | 34 | 8177819124 | kundansaraf@gmail.com |

Name of Patient: Kundan

General Details of Patient

| Patient_Name | Patient_Gender | Patient_Age | Relative_Phone_Number | Relative_Email_ID |
|---|---|---|---|---|
| Kundan | Male | 34 | 8177819124 | kundansaraf@gmail.com |

Medical history and Present Issue informed by patient

| Medical_History1 | Medical_History2 | Medical_History3 | Present_Issue1 | Present_Issue2 | Present_Issue3 |
|---|---|---|---|---|---|
| High Blood Pressure | Asthama | No any | Breathing issue | No any | No any |

**Fig. 7.** Dashboard to show general details, medical history, and present health issues

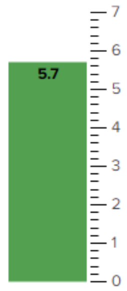
The dashboard shown below in figure 8 shows the height, weight, and body-mass index calculation of the patient. Based on the data, the patient is tagged as Underweight, Normal weight, Overweight, and Obesity category, e.g. Underweight (BMI <= 18.5, Normal (BMI = 18.5 to 24.9), Overweight (BMI >24.9).

$$\boldsymbol{BMI = \frac{Weight\ in\ Kg}{(Height\ in\ Meter)^2}}$$

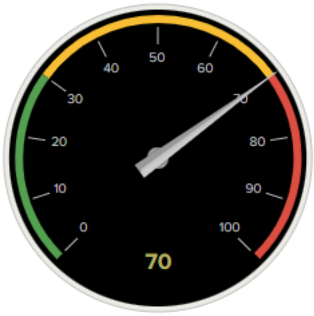
Figure 8 indicates the heart rate per minute and oxygen level of patients. Based on pulse rate, the patient is tagged as Normal or abnormal e.g. pulse rate of 62 to 98 indicates a normal pulse rate. The oximeter is used to measure the heart rate, blood oxygen level, and perfusion index of the patient. SpO2 level for normal middle-aged adults is 94% to 100%. SpO2 level beyond this indicates an abnormal health condition. Less than 3% perfusion index (PI) indicates extremely weak pulse strength and above 20% PI indicates extremely strong pulse strength. Normally PI should be above 3% and below 15% to indicate a normal health condition.

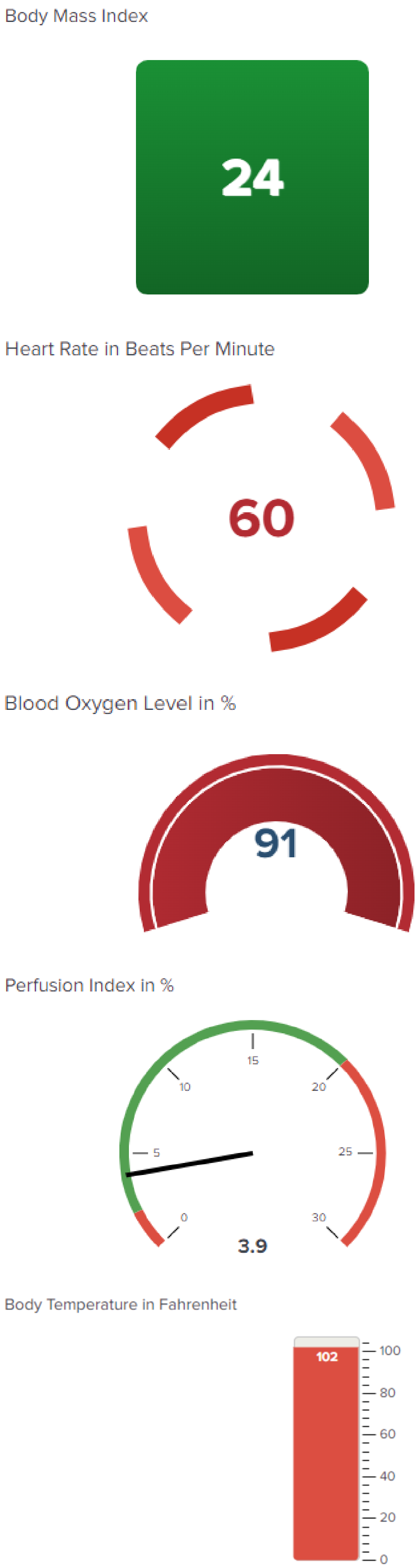
Figure 8 shows the temperature and blood sugar level of a patient. A TMP36 temperature sensor is used to measure the body temperature of the patient. For normal people, the body temperature is 97°F to 99°F. The temperature is beyond this limit showing abnormal body condition. The Continuous Glucose Monitoring (CGM) sensor measures the glucose level in the patient's blood in mg/dL. The patient is tagged pre-diabetic or diabetic depending on the calculations. So, as it can be seen that the heartbeat, SpO2 oxygen level, and body temperature of a patient named 'Kundan' are beyond the normal threshold level, the physician is reported for immediate action to normalize the condition. The green color of the panels in figure 8 shows that the parameter is under the threshold and no alert triggered for it. The red color of the panel shows that the parameter is outside of the decided threshold and an alert is triggered for it.

Height in Feet.Inches



Weight in kilogram





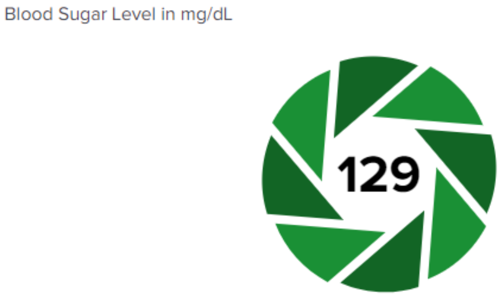
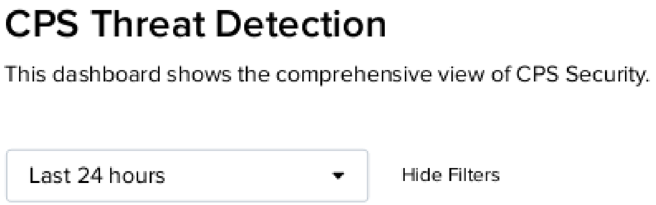


**Fig. 8**. Patient body parameters

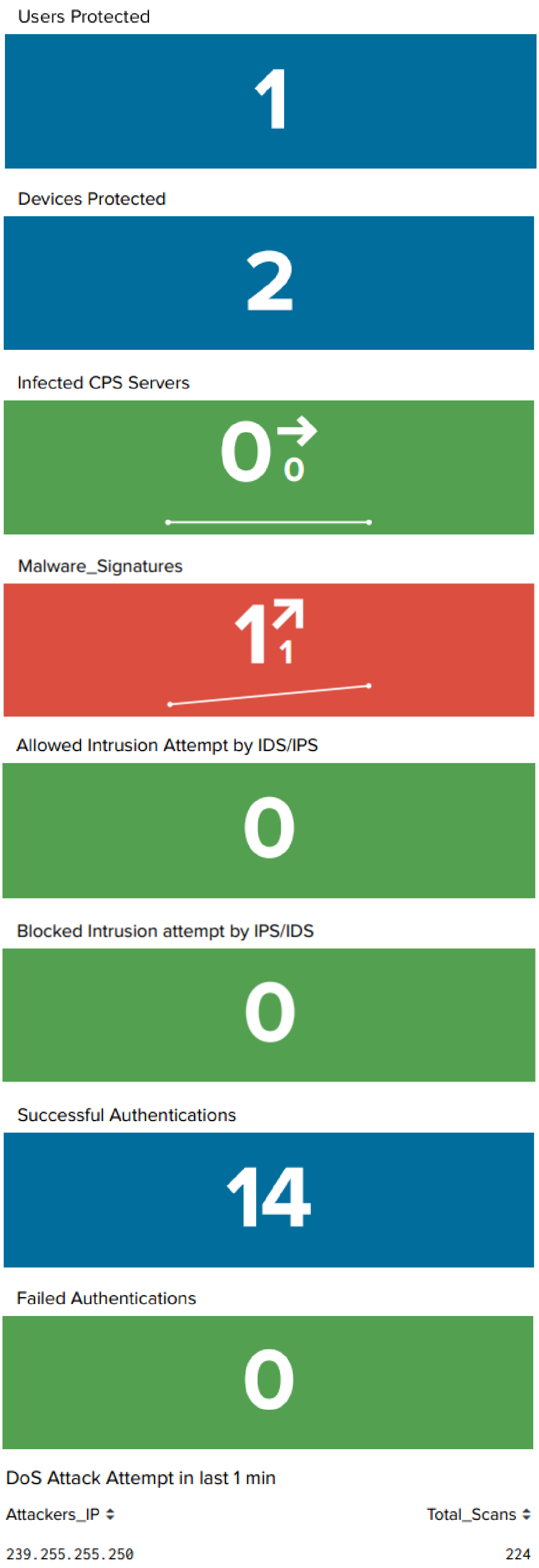
### 8.2. Security Monitoring Dashboard in Smart Medical CPS

In our study, the module is similarly applied for keeping the trajectory of even the slightest cyber-threat signature as medical data is deemed private to the patient and such data must not be exposed to anyone. The objective is the effective screening of malware attacks or spam signatures on CPS and displays analytics on the dashboard, as shown in figure 9. It has a time range picker to select the appropriate time to see the CPS details, presently set to view the CPS condition in the last 24 hrs. The 'Users Protected' shows the total number of users protected against cyber-attack. The 'Devices Protected' panel shows the total number of devices protected against cyber-attack. The 'Infected CPS Servers' panel shows the total number of vulnerable CPS servers. The 'Malware Signatures' panel shows the number of malware signatures found on the CPS servers. The 'Allowed Intrusion Attempt by IDS/IPS' panel shows the total number of undetected intrusions by the Intrusion Detection System (IDS) or by the Intrusion Prevention System (IPS). The 'Blocked Intrusion Attempt by IPS/IDS' panel shows the total number of detected intrusions by the IDS and IPS. The 'Successful Authentication' panel shows the total number of successful login attempts to CPS servers. The 'Failed Authentication' panel shows the total number of unsuccessful login attempts to CPS servers. The 'DoS Attack Attempt in last 1 min' panel shows the CPS which has received more than 100 scanning by the same IP address in the last 1 minute. The 'Brute Force Attack Detection' panel shows more than 7 failed login attempts to the various CPS servers in the last 24 hours. The blue color of the panel in figure 9 indicates that the parameter is informative only and no alert created for it. The green color of the panel indicates the parameter under the threshold and no alert has triggered. The red color of the panel indicates that the parameter is beyond the expected threshold and an alert has triggered for the same.



CPS Threat Detection

This dashboard shows the comprehensive view of CPS Security.



Users Protected

1

Devices Protected

2

Infected CPS Servers

0 → 0

Malware_Signatures

1 ↗ 1

Allowed Intrusion Attempt by IDS/IPS

0

Blocked Intrusion attempt by IPS/IDS

0

Successful Authentications

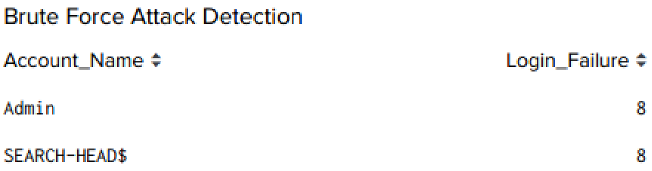
14

Failed Authentications

0

DoS Attack Attempt in last 1 min

| Attackers_IP ⇕ | Total_Scans ⇕ |
|---|---|
| 239.255.255.250 | 224 |



Brute Force Attack Detection

| Account_Name ⇕ | Login_Failure ⇕ |
|---|---|
| Admin | 8 |
| SEARCH-HEAD$ | 8 |

**Fig. 9**. CPS Threat Detection Dashboard

To test the effectiveness of the system, it is important to test its working during the scenario of attack. As shown in figure 10 below, using various tools like Goldeneye and Low Orbit Ion Cannon (LOIC), the attack scenario has been created for a Distributed Denial of Service (DDoS) Attack on various servers of CPS such as Forwarder, Indexer, and Search Head. The dashboard turns red and notifies the DoS attack attempt to the CPS admin by an alert.

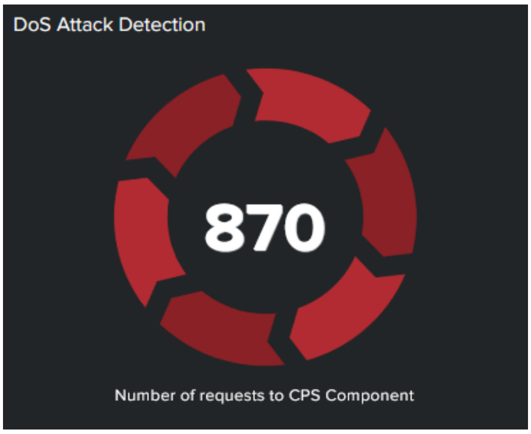
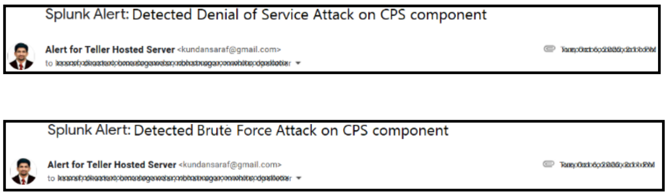


**Fig. 10.** Security Dashboard indicating an attack

Figure 11 below shows the e-mail notifications in case of a DoS attack and a Brute Force Attack respectively. On receiving these notifications, the CPS admin can immediately monitor the infrastructure and block the vulnerability to avoid major damage to the affected CPS component.



Splunk Alert: Detected Denial of Service Attack on CPS component

**Alert for Teller Hosted Server** <kundansaraf@gmail.com> [redacted]
to [redacted]

Splunk Alert: Detected Brute Force Attack on CPS component

**Alert for Teller Hosted Server** <kundansaraf@gmail.com> [redacted]
to [redacted]

**Fig. 11.** Email notifications during attack detection

## 9. Comparative Analysis of Existing CPS

Table 2 shows the comparative analysis of Splunk-based CPS security research with the proposed method.

**Table 2:** Comparative analysis of Splunk-based CPS security research

| *Parameters* | *Our method* | *[21]* | *[22]* | *[23]* | *[24]* | *[25]* |
|---|---|---|---|---|---|---|
| *Splunk Version* | *9.0.2* | *Uses an older Splunk Version* | | | | |
| *Zero-day attack detection* | ✓ | *X* | *X* | *X* | *X* | *X* |
| *Eavesdropping attack detection* | ✓ | *X* | *X* | *X* | *X* | *X* |
| *DoS attack detection* | ✓ | *X* | ✓ | *X* | ✓ | ✓ |
| *Brute Force attack detection* | ✓ | *X* | ✓ | *X* | *X* | ✓ |
| *Replay attack detection* | ✓ | *X* | *X* | *X* | *X* | *X* |
| *Malware Threat detection* | ✓ | ✓ | ✓ | *X* | *X* | *X* |

Table 2 above concludes that the proposed study can detect all major cyber-attacks on CPS. The figure 12 below shows scatter plot for CPS Threat detection.

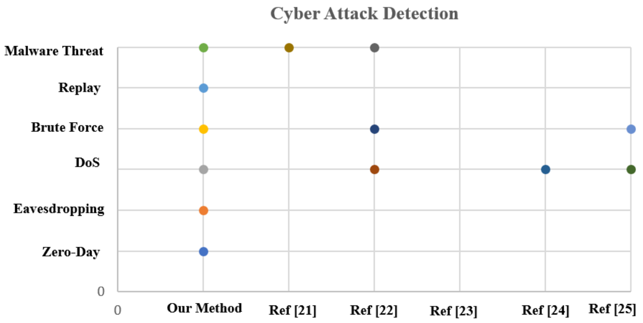


**Fig. 12**. Scatter plot for CPS Threat Detection

Table 2 and figure 12 proves that, our method detects more cyber-threats as compared to other methods in the graph.

This system has tested against all decided cyber-attacks and monitors the health of 700+ patients for 50 days. To test the system, the simultaneous injection of DoS, replay and brute force attacks are performed. The alert has triggered within 80 to 90 seconds of attack injection into the system. Also, the CPS threat detection dashboard takes less than 40 seconds to display the cyber-attacks. This system has detected patients with severe health issue within 60 seconds after the data ingestion into the system. Immediately the alert has triggered to the physician and to the CPS admin in the form of SMS, email, and phone call within 90 seconds. This study has concluded that the detection time for cyber-attack and emergency health conditions is 60 seconds and the notification time is less than 90 seconds.

## 10. Conclusion

This study has implemented a CPS security solution to detect major cyber threats such as zero-day, eavesdropping, DoS, brute-force, and replay attacks. To prove the CPS protection against decided cyber threats a smart health monitoring CPS has implemented for real-time patient monitoring. Splunk App for Infosec is used to create a dashboard panel in this study. The data-driven system is well-defined and uses DPPMR algorithm to gather and process the data. This method provides a parallel way to analyze distributed data for both cyber-threat and medical analysis purposes. To keep the study interactive, various dashboards are created in the application to publish the health status of patients and the cyber security status of healthcare CPS. Along with this, provision is available to notify the admin with security alerts and physicians with medical emergency alerts, making the application suitable for a real-time case in the essential healthcare sector. Experimental results show that the detection time of cyber-attack and serious health issues is less than 60 seconds. The notification is sent to the CPS admin and physician within 90 seconds of the emergency. A comparative analysis of the presented study with the existing method is performed. It can be concluded that the proposed method in this study is more secure and stable. This digital revolution, where patients' statistics will be automatically poised together and analyzed by machine learning (ML) expertise for healthier apprehensions and appropriate diagnosis, substitutes doctor-centric handling practices with a patient-centric environment.

### Acknowledgment

The study was completed with positive output with continuous guidance and support from the Principal and other members of D.Y. Patil College of Engineering, Akurdi, Pune

### Author contributions

Both authors have equally contributed to prepare this manuscript.

### Conflicts of interest

The authors declare no conflicts of interest.

## References

[1] Abioye, Temitope Elizabeth, Oluwasefunmi Tale Arogundade, Sanjay Misra, Kayode Adesemowo, and Robertas Damaševičius (2021) 'Cloud-Based Business Process Security Risk Management: A

Systematic Review, Taxonomy, and Future Directions, Computers 10, no. 12:160.

[2] Kozák, S., Ruzicky` , E., Kozáková, A., Stefano vic, J., Kozák, V. (2019) 'ICT for Advaned Manufacturing', In Proceedings of the 21st International Conference on Enterprise Information Systems (ICEIS 2019), pages 682-688 ISBN: 978-989-758-372-8.

[3] Griffor, Edward R., Christopher Greer, David A. Wollman, and Martin J. Burns (2017) 'Framework for cyber-physical systems: Volume 1, overview', NIST Special Publication 1500-201.

[4] Haque, Shah Ahsanul, Syed Mahfuzul Aziz, and Mustafizur Rahman (2014) 'Review of cyber-physical system in healthcare', International Journal of Distributed Sensor Networks 10, no. 4 (2014): 217415.

[5] Gelenbe, Erol, Gokce Gorbil, and Fang-Jing Wu (2012) 'Emergency cyber-physical-human systems', In 2012 21st International Conference on Computer Communications and Networks (ICCCN), pp. 1-7. IEEE.

[6] Xiong, Gang, Fenghua Zhu, Xiwei Liu, Xisong Dong, Wuling Huang, Songhang Chen, and Kai Zhao (2015) 'Cyber-physical-social system in intelligent transportation', IEEE/CAA Journal of Automatica Sinica 2, no. 3: 320-333.

[7] Lee, Jay, Behrad Bagheri, and Hung-An Kao (2015) 'A cyber-physical systems architecture for industry 4.0-based manufacturing systems', Manufacturing letters 3: 18-23.

[8] Khalid, Azfar, Pierre Kirisci, Zeashan Hameed Khan, Zied Ghrairi, Klaus-Dieter Thoben, and Jürgen Pannek (2018) 'Security framework for industrial collaborative robotic cyber-physical systems', Computers in Industry 97: 132-145.

[9] Clark, Robert M., and Simon Hakim (2017) 'Protecting critical infrastructure at the state, provincial, and local level: issues in cyber-physical security', In Cyber-Physical Security, pp. 1-17. Springer, Cham.

[10] Kumar, Rajesh, Bhavesh Narra, Rohan Kela, and Siddhant Singh (2022) 'AFMT: Maintaining the safety-security of industrial control systems' Computers in Industry 136: 103584.

[11] Ying, Zijian, Qianmu Li, Shunmei Meng, Zhen Ni, and Zhe Sun (2019) 'A Survey of Information Intelligent System Security Risk Assessment Models, Standards and Methods', In Cloud Computing, Smart Grid and Innovative Frontiers in Telecommunications, pp. 603-611. Springer, Cham.

[12] Goyal, Manish (2022) 'Behavioral validation in Cyber-physical systems: Safety violations and beyond', A dissertation submitted to the faculty of the University of North Carolina at Chapel Hill in partial fulfillment of Doctor of Philosophy in the Department of Computer Science.

[13] Ananda, Tulasi K., T. Sukumara, D. Sasikala, and Ramakanth Kumar (2019) 'Robustness Evaluation of Cyber-Physical Systems through Network Protocol Fuzzing' In 2019 International Conference on Advances in Computing and Communication Engineering (ICACCE), pp. 1-6. IEEE.

[14] Lezzi, Marianna, Mariangela Lazoi, and Angelo Corallo (2018) 'Cybersecurity for Industry 4.0 in the current literature: A reference framework' Computers in Industry 103: 97-110.

[15] Brewer, Tanya L. (2012) 'Proceedings of the Cybersecurity in Cyber-Physical Workshop, April 23–24, 2012.

[16] Mahoney, Thomas C., and Jim Davis (2017) 'Cybersecurity for Manufacturers: Securing the Digitized and Connected Factory', CYBERSECURITY FOR MANUFACTURERS.

[17] Lu, Yang, and Li Da Xu (2018) 'Internet of Things (IoT) cybersecurity research: A review of current research topics', IEEE Internet of Things Journal 6, no. 2: 2103-2115.

[18] Lezzi, Marianna, Mariangela Lazoi, and Angelo Corallo (2018) 'Cybersecurity for Industry 4.0 in the current literature: A reference framework' Computers in Industry 103: 97-110.

[19] Horowitz, B.M. and Pierce, K. (2012) 'System Aware Cyber Security Application of Dynamic System Models and State Estimation Technology to the Cyber Security of Physical Systems', Objectives for System Aware Cyber Security Research. In NIST (Ed.).Cybersecurity in Cyber-Physical Systems Workshop (96–97). NISTIR 7916. 10.6028/NIST .IR.79 16.

[20] Wenbo Wu, Rui Kang, Zi Li (2015) 'Risk Assessment Method for Cyber Security of Cyber Physical Systems', The First International Conference on Reliability Systems Engineering, 978-1-4673-8557-2/15/$31.00, IEEE.

[21] Ananthapadmanabhan, A., and Krishnashree Achuthan (2022) 'Threat Modeling and Threat Intelligence System for Cloud using Splunk', In 2022 10th International Symposium on Digital Forensics and Security (ISDFS), pp. 1-6. IEEE.

[22] Cersosimo, Michelle, and Adrian Lara (2022) 'Detecting Malicious Domains using the Splunk Machine Learning Toolkit', In NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium, pp. 1-6. IEEE.

[23] Zhao, Liguo, Derong Zhu, Wasswa Shafik, S. Mojtaba Matinkhah, Zubair Ahmad, Lule Sharif, and Alisa Craig (2022) 'Artificial intelligence analysis in cyber domain: A review', International Journal of Distributed Sensor Networks 18, no. 4: 15501329221084882.

[24] Prakash, G., M. Ganeshan, A. Shenbagavalli, M. Satheesh Kumar, K. Srujan Raju, and K. Suthendran (2022) 'A Proactive Threat Hunting Model to Detect Concealed Anomaly in the Network' In Smart Intelligent Computing and Applications, Volume 2, pp. 553-565. Springer, Singapore.

[25] Saraf, K.R. and Malathi, P. (2020) 'Cyber Physical System Security by Splunk' i-Manager's Journal on Communication Engineering and Systems, 9(2), p.41.

[26] Saraf, Kundankumar Rameshwar, and P. Malathi. (2022) 'Intelligent Learning Analytics in the Healthcare Sector Using Machine Learning and IoT', In Machine Learning, Deep Learning, Big Data, and Internet of Things for Healthcare, pp. 37-53. Chapman and Hall/CRC.

[27] Saraf, Kundan Kumar Rameshwar, P. Malathi, and Kailash Shaw (2021) 'Security Enhancement of Contactless Tachometer-Based Cyber-Physical System', In Machine Learning Approaches for Urban Computing, pp. 165-187. Springer, Singapore.

[28] Guo, Yang (2022) 'A review of machine learning-based zero-day attack detection: Challenges and future directions', Computer Communications.

[29] Xu, Xiaoyu, Hao Hu, Yuling Liu, Jinglei Tan, Hongqi Zhang, and Haotian Song (2022) 'Moving target defense of routing randomization with deep reinforcement learning against eavesdropping attack' Digital Communications and Networks.

[30] Splunk documentation 9.0.2 (2022), https://docs.splunk.com/Documentation/Splunk/9.0.2/Security/ConfigureS2Sonnewcipher

[31] Splunk documentation 9.0.2 (2022), https://docs.splunk.com/Documentation/Splunk/9.0.2/Security/Updates

[32] Chen, Xia, Jianyu Zhou, Mengxuan Shi, Yin Chen, and Jinyu Wen (2022) 'Distributed resilient control against denial of service attacks in DC microgrids with constant power load', Renewable and Sustainable Energy Reviews 153: 111792.

[33] Naha, Arunava, Andre MH Teixeira, Anders Ahlen, and Subhrakanti Dey (2022) 'Sequential detection of replay attacks', IEEE Transactions on Automatic Control.

[34] India, Oxfam (2021) 'Inequality Report 2021: India's Unequal Healthcare Story" Available at: https://www.oxfamindia.org/knowledgehub/workingpaper/inequality-report-2021-indias-unequal-healthcare-story

[35] (2021) 'Govt aims to achieve WHO doctor-patient ratio of 1:1000 by 2024' https://www.livemint.com/news/india/govt-aims-to-achieve-who-doctor-patient-ratio-of-1-1000-by-2024-11635432454203.html

[36] Tyagi, Amit Kumar, and N. Sreenath (2021) 'Cyber-Physical Systems: Analyses, challenges, and possible solutions' Internet of Things and Cyber-Physical Systems: 22-33.

[37] Haleem, Abid, Mohd Javaid, Ravi Pratap Singh, and Rajiv Suman (2022) 'Medical 4.0 technologies for healthcare: Features, capabilities, and applications' Internet of Things and Cyber-Physical Systems.

[38] Chen, Fulong, Yuqing Tang, Canlin Wang, Jing Huang, Cheng Huang, Dong Xie, Taochun Wang, and Chuanxin Zhao (2021) 'Medical cyber-physical systems: A solution to smart health and the state of the art', IEEE Transactions on Computational Social Systems.

[39] Dash, Sabyasachi, Sushil Kumar Shakyawar, Mohit Sharma, and Sandeep Kaushik (2019) 'Big data in healthcare: management, analysis, and future prospects' Journal of Big Data 6, no. 1: 1-25.

[40] Shah, Tejal, Ali Yavari, Karan Mitra, Saguna Saguna, Prem Prakash Jayaraman, Fethi Rabhi, and Rajiv Ranjan (2016) 'Remote health care cyber-physical system: quality of service (QoS) challenges and opportunities', IET Cyber-Physical Systems: Theory & Applications 1, no. 1: 40-48.

[41] Verma, Rupali. (2022) 'Smart city healthcare cyber-physical system: characteristics, technologies, and challenges." Wireless personal communications 122, no. 2 (2022): 1413-1433.

[42] Caesar, Birte, Florian Grigoleit, and Stephan Unverdorben (2019) '(Self-) adaptiveness for manufacturing systems: challenges and approaches', SICS Software-Intensive Cyber-Physical Systems 34, no. 4: 191-200.

[43] Leung, Carson K., Daryl LX Fung, Saad B. Mushtaq, Owen T. Leduchowski, Robert Luc Bouchard, Hui Jin, Alfredo Cuzzocrea, and Christine Y. Zhang (2020)

‘Data science for healthcare predictive analytics’, In Proceedings of the 24th Symposium on International Database Engineering & Applications, pp. 1-10.

[44] Christoforou, Eftychios G., Sotiris Avgousti, Nacim Ramdani, Cyril Novales, and Andreas S. Panayides (2020) ‘The upcoming role for nursing and assistive robotics: Opportunities and challenges ahead’, Frontiers in Digital Health 2: 585656.

[45] Galetsi, Panagiota, Korina Katsaliaki, and Sameer Kumar (2020) ‘Big data analytics in health sector: Theoretical framework, techniques and prospects’, International Journal of Information Management 50: 206-216.

[46] Fang, Ruogu, Samira Pouyanfar, Yimin Yang, Shu-Ching Chen, and S. S. Iyengar (2016) ‘Computational health informatics in the big data age: a survey’, ACM Computing Surveys (CSUR) 49, no. 1: 1-36.

[47] Padhy, Rabi Prasad (2013) ‘Big data processing with Hadoop-MapReduce in cloud systems’, International Journal of Cloud Computing and Services Science 2, no. 1: 16.

[48] Sahoo, Prasan Kumar, Suvendu Kumar Mohapatra, and Shih-Lin Wu (2016) ‘Analyzing healthcare big data with prediction for future health condition’ IEEE Access 4: 9786-9799.

[49] Kuo, Alex, Dillon Chrimes, Pinle Qin, and Hamid Zamani (2019) ‘A Hadoop/MapReduce Based Platform for Supporting Health Big Data Analytics’, In ITCH, pp. 229-235.

[50] Xian, Lam Ying, and Muhammad Ehsan Rana (2021) ‘Application of Cloud Computing for the Development of Big Data’ In 2021 International Conference on Data Analytics for Business and Industry (ICDABI), pp. 70-75. IEEE.

[51] Tutorial -https://hadoop.apache.org/docs/r1.2.1/mapred_tutorial.html

[52] Tutorial-https://docs.splunk.com/Documentation/InfoSec/1.7.0/User/Overview

[53] Tutorial-https://docs.splunk.com/Documentation/MLApp/5.3.1/User/AboutML