

SMART HEALTH AND SECURITY MONITORING CYBER PHYSICAL SYSTEM

KUNDANKUMAR RAMESHWAR SARAF¹ and P. MALATHI²

¹Ph.D. Research Scholar, Department of Electronics and Telecommunication Engineering, D.Y. Patil College of Engineering, Akurdi, Pune, Maharashtra, India. E-mail: kundansaraf@gmail.com

²Head, Department of Electronics and Telecommunication Engineering, D.Y. Patil College of Engineering, Akurdi, Pune, Maharashtra, India.

Abstract

Cyber Physical System (CPS) contains internet based interactive physical and computational components to achieve a higher objective than Internet of Things (IoT) device. This paper shows the construction of smart health and security monitoring CPS using Splunk. Splunk is a software platform to analyse the machine data. Using Splunk platform one can collect the machine data at the Splunk indexer and take appropriate decision by analysing it. Security of CPS is prime important to prevent smart medical system against the cyber-attacks. Splunk platform can also be used for securing the CPS. This paper briefly describes the use of Splunk in smart health and security monitoring system. It also demonstrates the Splunk use to secure CPS. Finally, it compares the Splunk with other machine learning tools that can be used to secure CPS.

1. INTRODUCTION TO CPS

Cyber Physical System (CPS) is integration of physical and computational components interact with each other to achieve certain objective. Examples of CPS are smart grid, driverless car etc. This paper shows the implementation of smart health and security monitoring Cyber Physical System. This system can remotely monitor the health of patient and physician can perfectly diagnose the patient for multiple diseases and suggest appropriate medication. Splunk software platform is used to implement this system. Splunk is a used to search, analyze and visualize the machine data. The sensors connected to the patient body collects the health details of patient in syslog server placed near the patient. Splunk Universal forwarder transfers these details to Splunk Indexer. The CPS admin has created the dashboard to monitor various physical parameters of patient. CPS system can be susceptible to multiple cyber-attacks. The Splunk based system also analyzes the cyber-attacks on each CPS component. This system also generates the alert on detection of any emergency health condition. The alert also be generated on detection of cyber-attack on any component of CPS.

1.1. Need of smart health and security monitoring system

In case of pandemic situation huge number of people needs treatment to save their life. In such situation number of physicians are less as compared to number of patients. This situation also increases the cost of treatment which can be unaffordable by poor citizens. Huge patient crowd at the clinic also increases the number of affected patients. Villagers needs to travel to urban areas for appropriate treatment. To overcome all these issues the smart health and security monitoring system is useful. This system

monitors the health of remotely located patient and trigger the alert in case of emergency health issue. This system also protects itself against the cyber-threats. It triggers the alert in case of occurrence of any cyber threatening activity detection.

1.2. Comparison of Splunk with other log monitoring tools for CPS security

Table 1 below shows the comparison of all existing log monitoring tools for CPS security. As shown in the table IBM QRadar can only monitor the logs of IBM tools. All other tools are compatible with all system components. For log searching and visualization using the ELK tool integration is essential. In Sumo Logic on premise setup is not available. Input and data type can be used by using external plugins for Sumo Logic and ELK tools. Better customer support provided by Splunk only. Better threat intelligence is provided by Splunk and QRadar. Finally, it can be concluded that the Splunk is useful tool for log monitoring and CPS security. Hence this research uses Splunk in Smart Health and Security Monitoring System.

Table 1: Comparison of log monitoring tools for CPS security

Features	Splunk	Sumo Logic	ELK	Arcsight	LogRhythm	QRadar
Compatibility	Compatible with all system components					Compatible with IBM Tools only
Searching	Possible		Possible with integrations only	Possible	Possible	Possible
Analysis	Possible					
Visualization by Dashboard						
SaaS Setup						
On-Premises setup	Possible	Not Possible	Possible			
Plugins and Integration	Possible					
Input any data type	Possible	Possible with plugins only	Possible with plugins only	Possible		
Customer Support	Better	Not proficient	Not proficient	Good		
Documentation and Community	Better	Not available	Available	Good		
Threat Intelligence	Better	Good	Good	Better		

Cost	\$40 per month (Splunk IT Solutions)	\$270/month (Sumo Logic Free)	\$16/month (on Elastic Cloud)	Details not available	\$800/month (QRadar on Cloud Standard)
------	--------------------------------------	-------------------------------	-------------------------------	-----------------------	----------------------------------------

1.3. Block diagram of system

Figure 1 below shows the block diagram of smart health and security monitoring CPS. In this system one bed is placed in every village. This bed is equipped with various health monitoring sensors. These sensors collect the health-related data of patient such as body temperature, weight, SpO2 oxygen level, perfusion index, heart beats per minute, and height. These sensors send this data to the syslog server placed near to bed. This syslog server contains the preinstalled Splunk Heavy Forwarder (HF). This HF parse the data in the form of events.

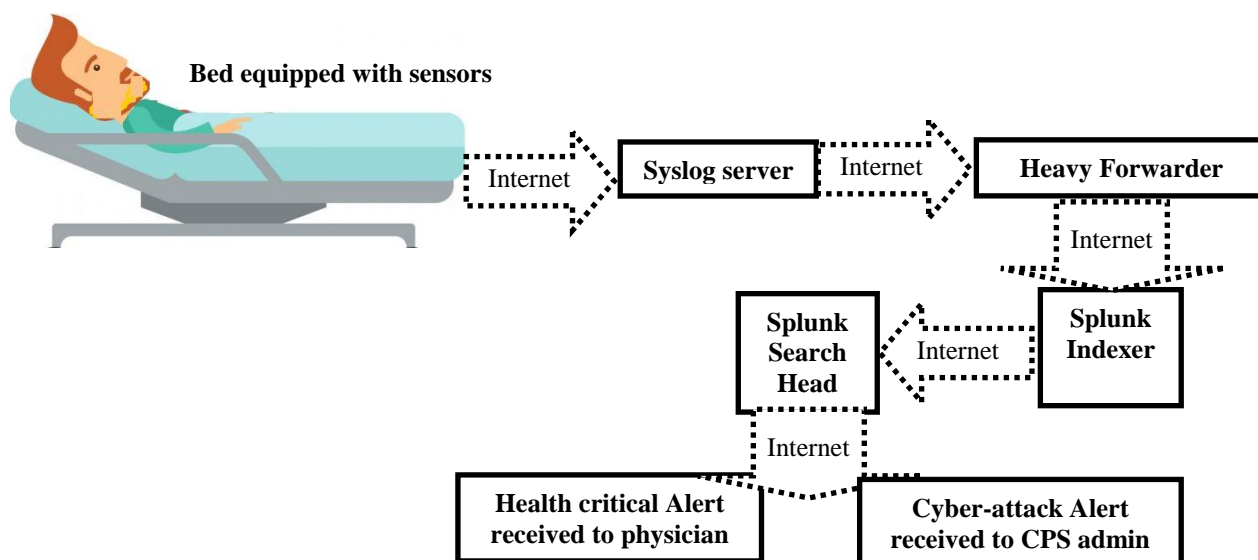


Figure 1 Smart Health and Security Monitoring System (SHSM)

This HF further send this data to remotely be located Splunk Indexer. Splunk Indexer stores the data in the form of indexes. Splunk Search Head (SH) is located at the remote location near to physician as well as near to CPS admin. Physician can monitor the present health status of every patient using health monitoring dashboard. Similarly, CPS admin can monitor the security status of all CPS components using CPS security dashboard. Physician receives the alert on occurrence of any abnormal health condition. CPS admin receives the alert on any cyber threat to CPS. Physician can suggest the medication to the patient relative to avoid further major harm to patient's health. CPS admin can block the attacker's IP address to prevent the major loss to the CPS.

1.4. Flowchart of SHSM system

The flowchart 2 below shows the operation of smart health and security monitoring system. In this system Sensor measures the physical condition of patient. These details

are sent to syslog server which contain the heavy forwarder. This forwarder sends these details to the indexer. Splunk search head used to visualize the indexed data and to create dashboard and alerts. On reception of health issue related alert physician suggest the medication to the patient's relative. On reception of security related alert, CPS admin can follow the appropriate security measure to overcome the cyber-attack.

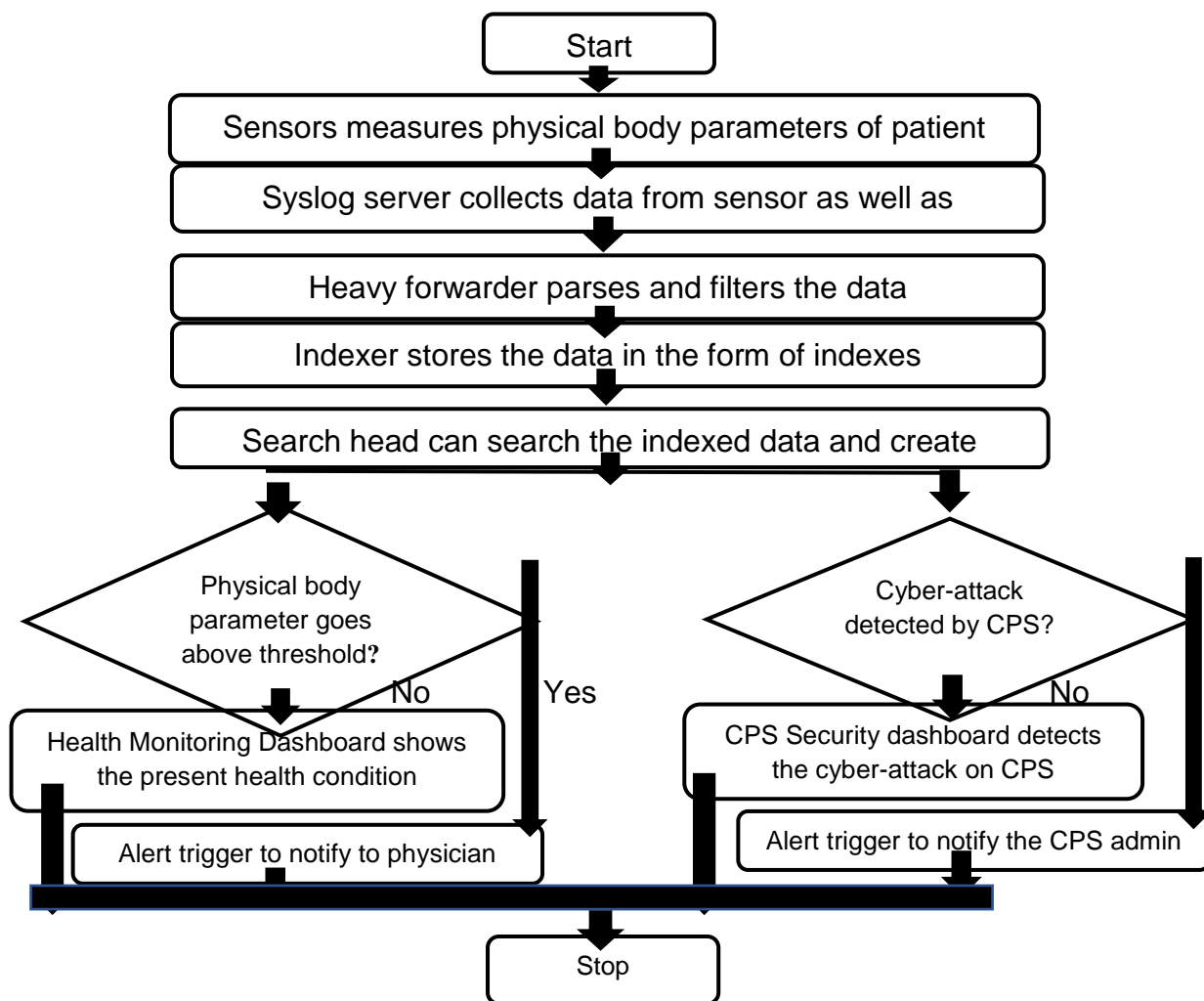


Figure 2 Flowchart of SHSM System

2. Health Monitoring by SHSM system

Below section describes the parameters monitor by SHSM system, dashboard, and alert created for health monitoring.

2.1 Parameters monitor by SHSM System

This system monitors below given 8 body parameters either by using sensors or by other methods. All these parameters are detected by Splunk. Predefined threshold levels of all these parameters are stored in Splunk. Splunk creates the alert on crossing

of any threshold. All 8 body parameters along with the detection method and their threshold level is presented by table 2 below.

Table 2 List of body parameters detected by SHSM system

Sr. No.	Physical Parameter	Sensor or method of detection	Threshold level
1	Body Temperature	Temperature Sensor - Thermistor	More than 98°F
2	Body weight	Load Cell	Not Applicable
3	SpO2 level	Pulse Oximeter	Less than 94%
4	Heart beats per minute (BPM)	Pulse Oximeter	More than 100 BPM or less than 60 BPM
5	Perfusion Index (PI)	Pulse Oximeter	Below 2% or above 20%
6	Height	Scale on wall	Not Applicable
7	Glucose level in blood	Continuous glucose monitoring (CGM)	More than 140 mg/dL
8	Body mass index (BMI)	Body Mass Index = (Body weight in Kilogram) / (Height in meter) ²	Between 18.5 and 24.9

As shown in table 2 above thermistor is used to monitor the body temperature. Load cell is used to measure the body weight. Pulse oximeter measures the SpO2 level, heart beats in minute and perfusion index. Wall scale indication used to measure height and continuous glucose monitoring machine (CGM) measures a glucose level in blood. Body mass index (BMI) is calculated by below given formula,

$$\text{Body Mass Index} = \frac{\text{Body weight in Kg}}{\text{Height in meter}^2}$$

The Splunk triggers an alert in any of the below cases,

Body temperature goes above 98°F and/or SpO2 level goes less than 94% and/or heartbeat rate goes more than 100 BPM or less than 60 BPM and/or perfusion index goes below 2% or above 20% and/or glucose level in blood goes above 140mg/dL and/or body mass index is less than 18.5 or more than 24.9.

2.2 Splunk Alert for abnormal health status of patient

Figure 3 below shows the alert created in SHSM system. Any of the parameter mentioned in table 1 above goes beyond the threshold level, Splunk triggers alert through phone call, SMS, and E-mail. This alert notifies to the physician as well as to the relative of patient.

Save As Alert
✕

Settings

Title

Description

Permissions Private Shared in App

Alert type Scheduled Real-time

Expires hour(s) ▼

Trigger Conditions

Trigger alert when

Throttle ?

Trigger Actions

When triggered

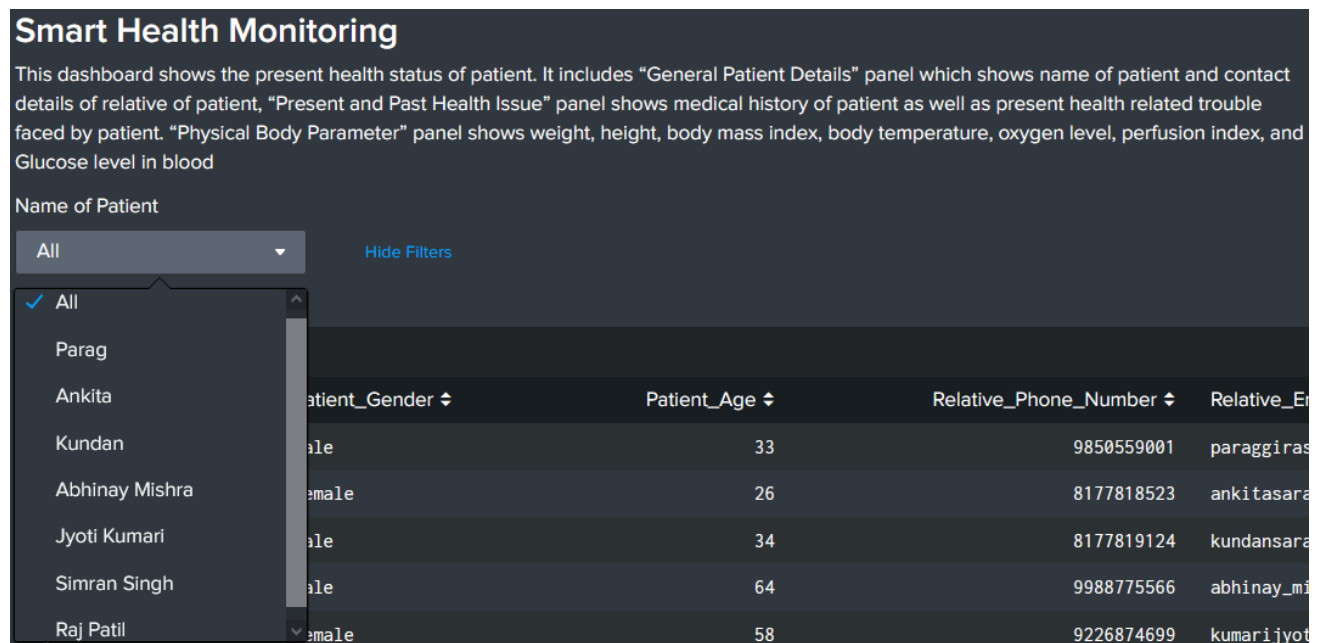
▼	<div style="display: flex; align-items: center;"> Add to Triggered Alerts Remove </div> <div style="margin-top: 5px;"> Severity <input style="width: 100px;" type="text" value="Critical ▼"/> </div>
>	<div style="display: flex; align-items: center;"> Webhook Remove </div>

Figure 3 Alert by SHSM system to notify the critical health condition detection

This alert is configured using third-party website in webhook option. Email ID and phone number of physician as well as patient relative are inserted on this third-party website. Webhook option redirects every Splunk alert to this third-party website which in turn notifies to the physician and patient relative.

2.3 Splunk Dashboards

On occurrence of alert, the physician opens the Splunk console and observe the preconfigured dashboard on Splunk. This dashboard has dropdown menu as shown in the figure 1 below.



The screenshot shows a dashboard titled "Smart Health Monitoring". Below the title is a descriptive paragraph: "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". Below this is a section labeled "Name of Patient" with a dropdown menu currently set to "All". A "Hide Filters" link is visible to the right. The dropdown menu is open, showing a list of patient names: "All" (checked), "Parag", "Ankita", "Kundan", "Abhinay Mishra", "Jyoti Kumari", "Simran Singh", and "Raj Patil". Below the dropdown is a table with columns: "Patient_Gender", "Patient_Age", "Relative_Phone_Number", and "Relative_E". The table contains data for several patients, including Ankita.

Patient_Gender	Patient_Age	Relative_Phone_Number	Relative_E
male	33	9850559001	paraggiras
female	26	8177818523	ankitasara
male	34	8177819124	kundansara
male	64	9988775566	abhinay_mi
female	58	9226874699	kumarijyot

Figure 4 Dropdown menu of Smart Health Monitoring dashboard

In the first situation physician has open the dashboard for the patient's name Ankita. Physician has observed that except body mass index, all other physical parameters of Ankita are normal. Hence no urgency of treatment is essential for Ankita as shown in figure 5 below.

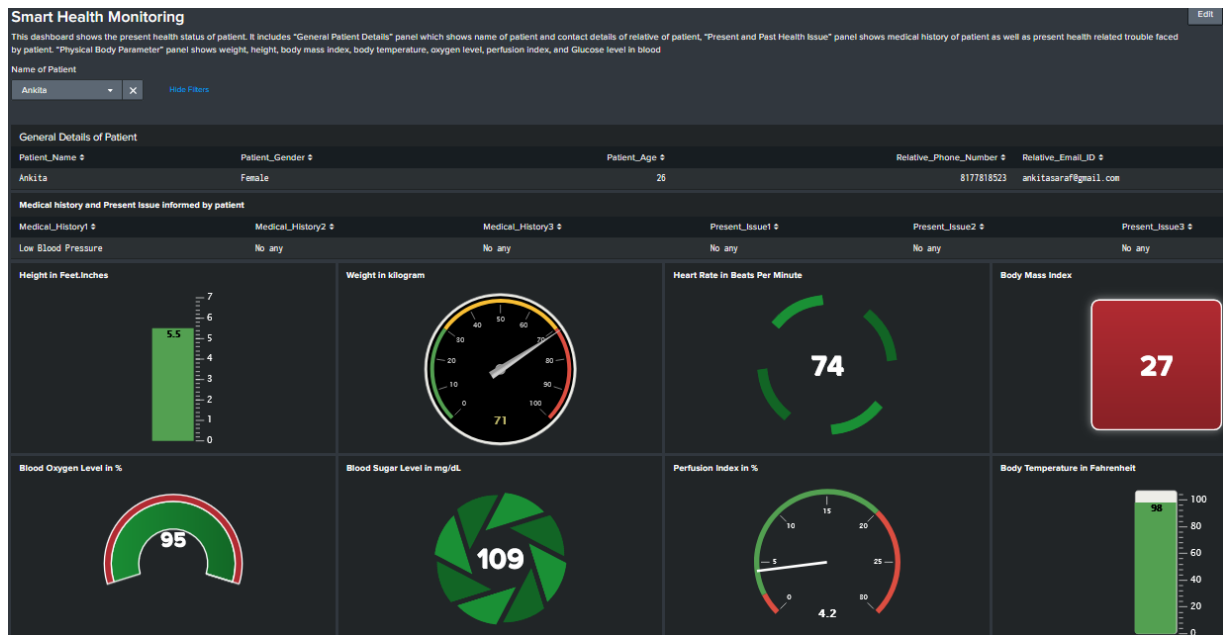


Figure 5 Health details of normal patient in Smart Health Monitoring dashboard

Physician now received an alert for the patient's name Kundan. Physician open the Smart Health Monitoring dashboard and select Kundan from drop down list. As shown in figure 6 it can be concluded that the body oxygen level and body temperature of patient is beyond the threshold limit. Hence emergency medication is essential for this patient. In this case physician will contact the relative of patient and suggest the essential medication to avoid further harm to the health of patient.

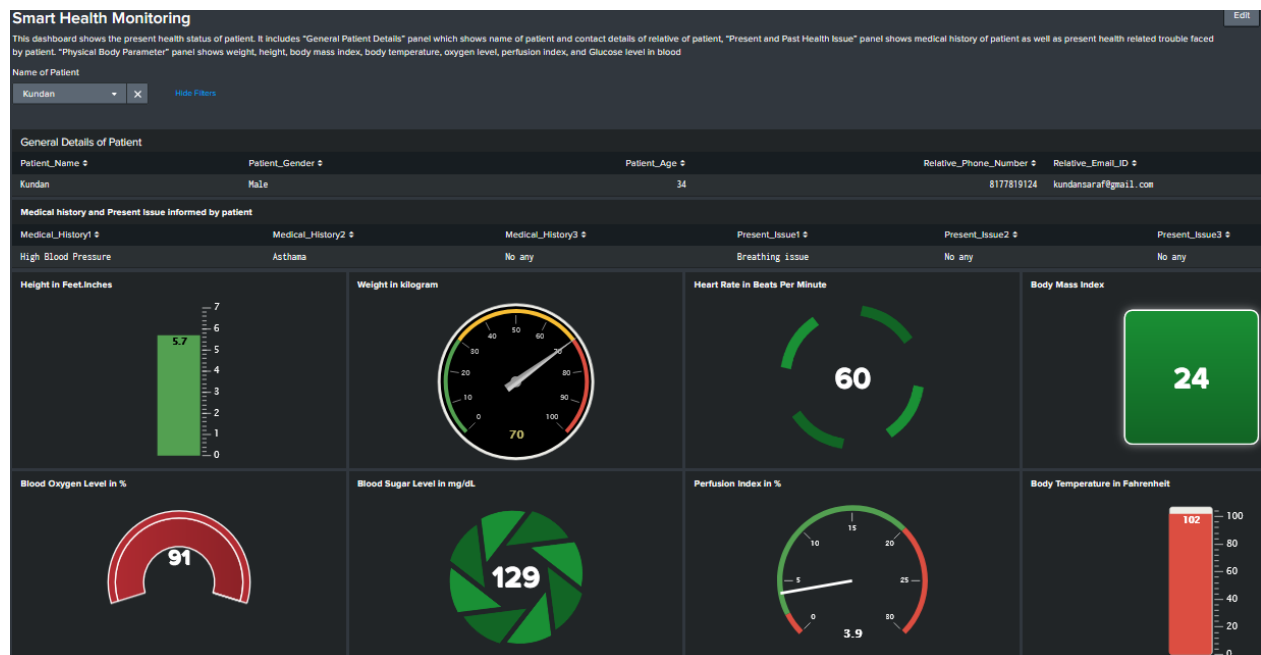


Figure 6 Health details of patient with serious health issue in Smart Health Monitoring dashboard

2.4 Possible attacks on CPS

Figure 7 shows all possible attacks on CPS. On CPS sensor Denial of Service (DoS) attack can happen which can make the sensor inaccessible for the other CPS component. In sensor and data spoofing attack, attacker can spoof the IP address to get the details detected by sensor. Actuator of sensor can miss the deadline of operation by miss of deadline attack. Attacker can perform the authentication failure attack on actuator to prevent the access of legitimate CPS components. Within the communication of CPS component attacker can modify the intermediate packet and perform the Man-In-The-Middle attack. Attacker can also sniff the traffic by eavesdropping attack. Attacker can also block the complete access of any CPS component by resource blocking attack. Attacker can alter the stored data in the Splunk indexer by storage alteration attack. Attacker can show the removed indexer data using data remanence attack. Attacker can also access the confidential information during computation phase at Splunk search head using attack on confidentiality. Attack can insert the computing error by computing error insertion attack. Timing error can also be inserted during the computation using timing error insertion attack.

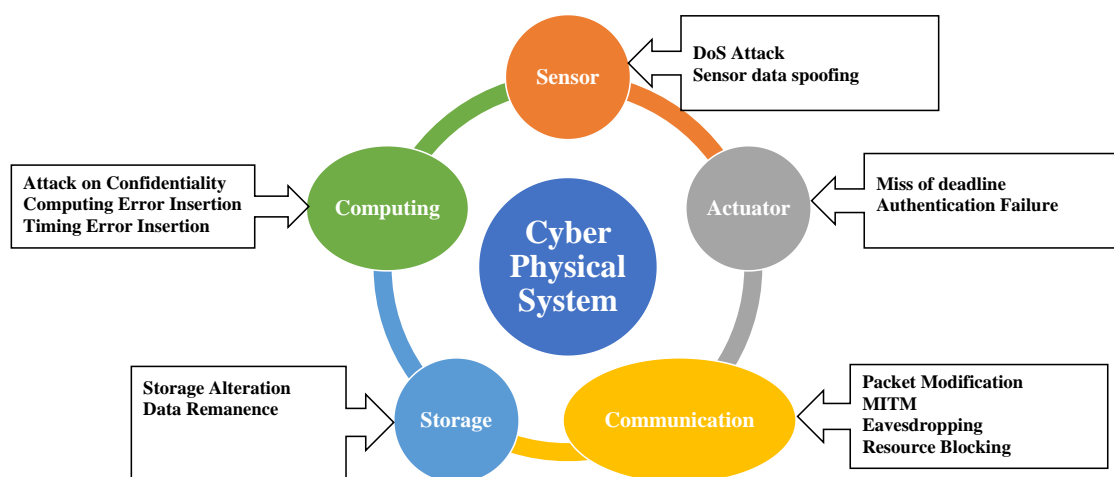


Figure 7 Possible attacks on CPS

2.5 Splunk Alert for cyber-attack on CPS component

This system monitors the DoS attack, Brute Force attack and CPS component IP and port scan detection attack. The figure 8 below shows the alert trigger on occurrence of DoS attack on Splunk Indexer.

Save As Alert



Settings

Title: Denial of Service Attack has detected on Splunk Indexer

Description: This alert indicates that the DoS attack has detected on Splunk Indexer. Urgent action is expected to prevent the further loss of the system.

Permissions: Private | Shared in App

Alert type: Scheduled | Real-time

Expires: 24 | hour(s) ▼

Trigger Conditions

Trigger alert when: Per-Result ▼

Throttle ?

Trigger Actions

+ Add Actions ▼

When triggered: > Add to Triggered Alerts Remove

Figure 8 Alert for Denial-of-Service Attack

In a similar way the Splunk triggers an alert for Brute Force attack and CPS component IP and port scan detection. In case of any attack, the CPS admin will monitor the CPS threat detection dashboard as shown in the figure 8 below to understand the severity and other details of attack.

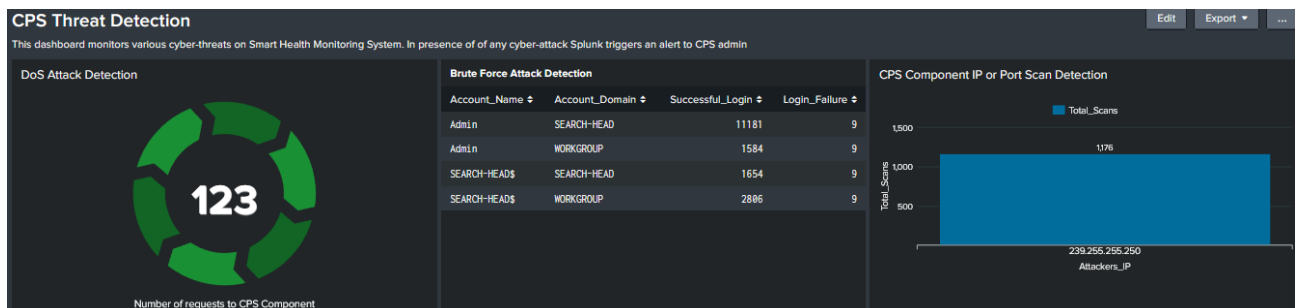


Figure 9 CPS threat detection dashboard to monitor the attack on CPS

Appendix I

List of Abbreviation

°C	Degree Celsius
°F	Degree Fahrenheit
BPM	Beats Per Minute
CPS	Cyber Physical System
DoS	Denial of Service Attack
E&TC	Electronics and Telecommunication Engineering
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
Kg	Kilo Gram
PI	Perfusion Index
SMS	Short Message Service
SpO2	Oxygen Saturation Level

CONCLUSION:

This system monitors the health status of remotely located patient and trigger the alert in case of any emergency. The physician will monitor the preconfigured Smart Health Monitoring dashboard and suggest the medication to the patient relative according to the health status of patient. In a similar way this system triggers an alert in case of network attacks on CPS component like Denial-of-Service attack, Brute Force attack and CPS component and port scan detection. On triggering of these attacks, the CPS admin will monitor the CPS threat detection dashboard and immediately block the attackers IP address by enabling Intrusion Prevention System or at firewall.

REFERENCES

- 1) Anish Hemmady, "Significance of Big Data on Healthcare and Data Security", International Journal of Scientific & Engineering Research, Volume 5, Issue 12, December 2014.
- 2) Press release by Splunk on "Splunk Builds Strong Traction in Healthcare", 2015 https://www.splunk.com/en_us/newsroom/press-releases/2015/splunk-builds-strong-traction-in-healthcare.html
- 3) Press release by Splunk on "Splunk IT Service Intelligence Helps Molina Healthcare Deliver Innovation to Patients", 2017 https://www.splunk.com/en_us/newsroom/press-releases/2017/splunk-it-service-intelligence-helps-molina-healthcare-deliver-innovation-to-patients.html.
- 4) Data insider, "What is the Internet of Medical Things (IoMT)?", 2017 https://www.splunk.com/en_us/data-insider/what-is-the-internet-of-medical-things-iomt.html.

- 5) VenketeshPalanisamyRamkumarThirunavukarasu, "Implications of big data analytics in developing healthcare frameworks – A review", Journal of King Saud University - Computer and Information Sciences, Volume 31, Issue 4, Pages 415-425, October 2019.
- 6) Splunk, "Reintroducing Splunk Dashboards", 2019
https://www.splunk.com/en_us/blog/platform/reintroducing-splunk-dashboards.html.
- 7) Splunk, "Splunk at the Service of Medical Staff", 2021
https://www.splunk.com/en_us/blog/platform/splunk-at-the-service-of-medical-staff.html.
- 8) Angelina Prima Kurniati, Geoff Hall, David Hogg, Owen Johnson, "Process Mining on the Extended Event Log to Analyse the System Usage During Healthcare Processes (Case Study: The GP Tab Usage During Chemotherapy Treatments)", International Conference on Process Mining, ICPM 2020: Process Mining Workshops pp 330-342, 31st March 2021.
- 9) White paper, "Using Healthcare Machine Data for Operational Intelligence", 2012
https://davidhoglund.typepad.com/files/splunk_for_healthcare.pdf
- 10) Medigate Splunk, "Clinical SOC Solution Delivering Complete Visibility and Control Over Medical and IoT Devices", 2021 <https://medigate.pathfactory.com/medigate-and-splunk>
- 11) S Geetha, Uma N Dulhare, Siva S Sivatha Sindhu, "Intrusion detection using NBHoeffding rule based decision tree for wireless sensor networks", Second International Conference on Advances in Electronics, Computers and Communications (ICAIECC), 2018.