International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT2390244

Design and Develop a Secure CPS Flexible Framework to Improve the Cyber Security using a New Security Algorithm

P Salman Raju[1*], P Venkateswara Rao[2], S Sreenivasa Murthy[3]

[1,2]Department of Computer Science and Engineering, Adikavi Nannanaya University, Rajahmundry, India

[3]Department of Systems, Institute of Public Enterprise, Hyderabad-India

ARTICLEINFO

Article History:

Accepted: 01 April 2023
Published: 20 April 2023

Publication Issue
Volume 10, Issue 2
March-April-2023

Page Number
388-402

ABSTRACT

CPS is an active system that transforms a physical system into a computerized system through the use of technology and a set of instructions that govern how the system operates. Because of CPS, even the most basic of equipment can function as a smart device. For the most part, these devices have limited processing capabilities, operate at low power, and have a small amount of storage space. The Internet of Things integrates everyday "things" with the internet. Computer Engineers have been adding sensors and processors to everyday objects since the 90s. However, progress was initially slow because the chips were big and bulky. Low power computer chips called RFID tags were first used to track expensive equipment. As computing devices shrank in size, these chips also became smaller, faster, and smarter over time. Existing security mechanisms works efficiently on high end CPS devices. The performance analysis also shows these algorithms perform well against different attacks. But when constraint-based applications come into the picture it was found that existing mechanism identifies many installation and configuration problems. Even these algorithms if installed in constraint-based application overall performance of the system degrade. To overcome these problems, we proposed a secure CPS flexible framework to improve the cyber security using a new session key security algorithm. So proposed algorithm must focus on constraint-based applications. It must support all the parameters of constraint-based devices. Key generated through algorithm must follows the key management design principles which includes scalability, freshness and accountability.

Keywords: Internet of Things, Smart Home Networks, Network Security, flexible framework, Cyber-attacks, Cyber Physical systems, New Security Technique, Secure session and token-based authentication algorithm

I. INTRODUCTION

Cyber Physical system (CPS) is defined as a new generation of electronics system which works with integration of physical system and computational algorithm. It not only detects the ambient temperature, but it also recognizes human objects and detects human activity. Through the Seventh EU

Framework Programme, the European Union (EU) is making investments more than 100 million euros in numerous connected device projects, that will be actively deployed in areas such as health, intelligent transportation, smart grid, smart cities, and utility services, among others [1]. India is accelerating the development of CPS and has launched a number of CPS-based projects, including smart cities, healthcare system and smart transportation, among others. The government of India has announced the Broad Public Sector Modernization and Smart Cities Plan. The plan lays out short- and long-term development goals and objectives, as well as alternative approaches to achieving the goal. The plan also includes a timeline for completion [2]. Agriculture based mobile application on cloud platform. Through internet data is analysed and processed and revert back with some important suggestions related to crop and land. The suggestions are helpful for farmer for the growth of crop [3].

1.1. Formation of Cyber Physical System

CPS associated with four things. Figure 11. Shows as below.

1. **Physical system:** It has a less dynamic and more static feel to it. Using this system, completing a task takes time [4].
2. **Computation:** Computation monitors and controls a device's basic task or physical process, assisting in the transformation of a basic physical device into an intelligent device.
3. **Communication:** Communication between devices is essential when performing a task with multiple devices. Bluetooth [5], a wireless ad-hoc network that connects various physical equipment, is an example of a communication protocol that is used in a variety of devices such as home automation, healthcare devices, low-powered radio devices, and so on.
4. **Information:** In a critical situation, the device will address problems with the help of information to find a solution [6].

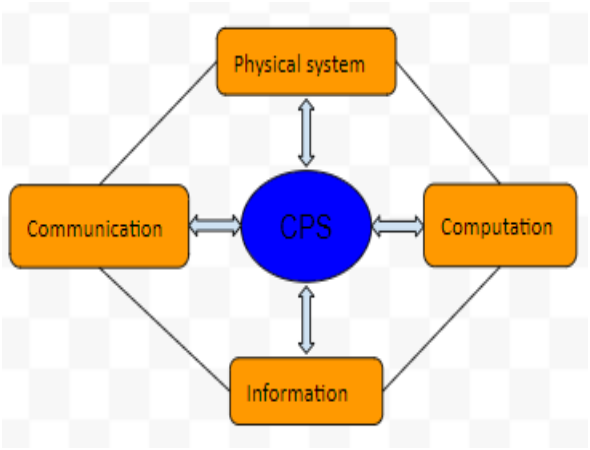

Figure 1.1: Formation of Cyber Physical System

1.2. Overview of Research work

Existing research efforts addresses CPS security related challenges and issues. Many researchers focus on security issues in applications. Some try to find solutions with their proposed security mechanisms. Few of them mentioned below. Some existing solutions implement by designing security framework. In some solutions Communications protocols like CoAP, MQTT used [7]. Some researcher specially develops a solution by focusing on Smart home system [8].

II. BACKGROUND

Cyber physical system was developed for some applications where constraint-based devices are used. When discussing the security of these devices, we want to concentrate on device security as well as network security, which deals with communication between these devices [9].

2.1. Limitations of Cyber Physical system

Existing security mechanisms will be used to provide security. Under these security mechanisms, CPS applications operate safely. However, when constraint-based applications attempt to execute existing security mechanisms, hardware issues arise. There are limitations in processing capabilities, memory issues, and energy backup issues. It is quite difficult to install existing security mechanisms. Even if it is installed, the application's performance suffers. To avoid this, it is preferable to remove existing security mechanisms, which will improve performance [10].

2.2. Impact of Security algorithm on CPS devices

Security mechanism is a preventive measure against attacks. As earlier said, existing security algorithm are better implemented on strong hardware but when constraint-based devices used with these algorithms it degrades the performance also it opens a window for attacker to perform attacks. The very famous attacks like Replay, DoS, Masquerade and Man in the Middle attack [11] easily performed on such type of devices. Data confidentiality and integrity also provided by security algorithm. In days cyber world it is essential that each and every device must be protected from internal and external attacks so as a preventive measures implementation of security algorithm is essential for each and every cyber physical system [12].

2.3. Attacks On Cyber Physical System

The cyber physical system consists of two main important components: the cyber system and the physical system (also known as the cyber network). Figure 2.1. shows two types of attacks that can be carried out on it, namely, cyber-attack and physical attack.

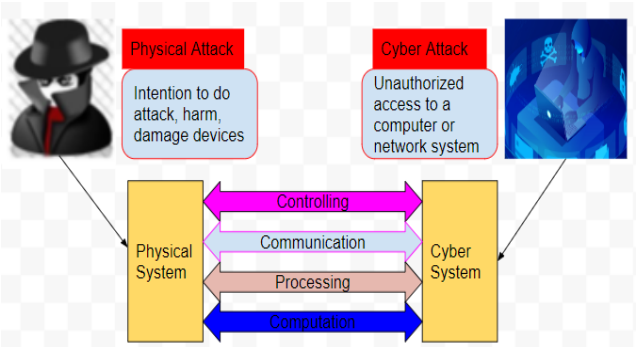

Figure 2.1: Cyber Physical System attacks

Physical Attack: A physical attack on CPS aims to destroy both the physical infrastructure and the control system. Tampering with devices, destroying devices, and physically snooping into a building are all examples of physical attacks. In such environment, an attacker's decrease or increase in temperature causes the sensors processing unit perform malfunction, resulting in damage to the CPS [13].

Cyber-Attack: Cyber-attacks are all too common; they are just like any other attack that occurs on a computer network, smart phone device, or cloud-based network. During a cyber-attack, a cyber attacker sets up an unauthorized network node, which then connects with a legitimate node and loses its identity [11] [14].

Typically, CPS network under attack at the end points, such as server and client nodes. From the technical perspective attacks are classified as Passive and Active attack.

- Passive Attack – It is an interception attack. Interception means gaining unauthorized access to CPS resources. Where it cannot modify it. So general solution to prevent those attack is precautions or prevention instead of correction [12].

- Active Attack -In this attack data will be modified in some manner or create false

impression. Interruption, modification and fabrication are some forms of these attacks [15].

- Masquerade Attack – It is an interruption type of attack where unauthorized entity pretends to be authorized entity.
- Replay attack – In this attack attacker capture the user credentials and other important information and these details can be used or replayed to take privileges of authorized user or to produce unauthorized effect [16].
- Denial of Service (DoS) of attack- In DoS attack authorized user prevents to access services they own. In DoS disruption of entire CPS network either by disabling the network or by overloading it with requests or messages to reduce the system performance or crash the system.

III. LITERATURE REVIEW

Many researchers who have carried out exploration in this field have concentrated more on providing security mechanism to strong hardware-based devices. constraint-based devices not performed well with existing security mechanism. Considering these issues in CPS literature review focuses on existing security mechanisms, security framework, attacks on CPS and machine learning approach.

3.1. Security Mechanism Approach

A. V. Jerald et al. [17] proposed architecture for security for IoT device-based network. Security architecture proposed by authors with the algorithms adding different security levels. The performance analysis of the architecture proposed uses simulated environment for evaluation, and the generated results are also explained in the paper. The performance of the security architecture analysed by using experimental setup. In security architecture, the authenticated user is guaranteed authorised service with more securely encrypted at the appropriate time. Cyberattacks are protected against communication system in the integrated smart services environment. The combination of a secure architecture and a security algorithm with a secure infrastructure provides a more effective solution to security issues.

Qaidjohar Jawadwala et al. [18] mentioned Cyber physical resource constraint devices issues which include a lack of processing power, a lack of storage space, and an absence of a standard security techniques that will not provide safety and security. They served as a critical establishment security mechanism for smart home devices. The algorithm proposed in the paper offers a solution to various cyber-attacks such as replay, IP spoofing, Denial of Service, and eavesdropping. They also use proof of concept to show the feasibility of the proposed mechanism and assess results to demonstrate the performance and effectiveness of the suggested mechanism.

3.2. Security framework or model

Bin Dai et al. A systematic approach is proposed for improving physical layer security (PLS) in Internet of Things (IoT) systems through the use of channel feedback. Overall, the importance of using feedback for IoT devices in physical layer security was highlighted in this study [19].

Fabio Pasqualetti et al. They characterise essential monitoring limitations from both a framework and a graph-theoretic standpoint, and they design both centralised and distributed detection mechanism and identification observes. Future work includes analysing our distributed monitors' convergence, designing distributed identification monitors, and designing monitors resistant to system noise and

unmodeled dynamics.to system noise and unmodeled dynamics [20].

Huang K. et al. mentioned that existing security protocols in industrial Cyber Physical Systems (ICPS) do not have the active decision capability to defend against highly organised cyber-attacks. By modelling the attack-defense interaction in ICPSs, the proposed technique considers both the cyber and physical layers of ICPSs and can start generating the optimal defense plan profile [21].

L. Pietre-Cambacedes et. al. proposed a referential framework model which is called as SEMA, it gives latent differences of security and safety. Where SEMA framework provides information related to their respective meanings explicit and provides inconsistencies and overlaps by considering security and safety [22].

S. Bernardi et. al. proposed a framework called as SURREAL which includes methodology and its tool support. The methodology shows a misuse case specification enriched with UML profile annotations and results in byproduct which is a survivability assessment model (SAM). It also validates the methodology and the framework using a cyber–physical system (CPS) case study, in the automotive field [23].

Akm Jahangir Alam Majumder et al. designed and developed a CPS that analyses the power consumption of a mobile wireless sensor device that included a Raspberry Pi and a smartphone to detect IoT security threats on a group of smart IoT devices, experimental and verification studies were conducted using a variety of test cases, including the device in an idle and active state, and also a distributed denial-of-service (DDoS) attack and a man in the middle (MITM) attack. It is also possible that the system will have various applications, such as smart grid security analytics or a smart house system, among others [24].

3.3. Attacks on CPS

Y. Chen et al. investigated dynamic sensor attacks on cyber-physical systems with high observability. They first find conditions for an attacker to create a dynamically undetectable sensor attack and relate them to system dynamics eigenvector properties. Then they provided an index that indicates the minimum number of sensors required to be attacked to be undetectable. Finally, quantify their findings using the Quadruple Tank Process. Undetectable dynamic sensor attacks against cyber-physical systems are proposed [25].

Byungho Min et al. they adapted a sophisticated malware technique known as feature-distributed malware for the Internet of Things. They develop and test various attacks, such as cyber physical system attacks and advanced cyber-attacks. Using traditional web attack techniques such as cookie stealing, an attacker is able malicious actions such as unlocking the passcode lock installed at the target premises and disabling security alarms. They hope that this study will shed new light on the implications of integrating the home automation with the Internet of Things, paving the way for future more safe and secure smart home environments [26].

3.4. Machine learning Approach

Fatima Hussain et al. mentioned existing solutions are insufficient for encompassing IoT networks. To deal with a variety of security issues, Machine Learning (ML) and Deep Learning (DL) techniques, which are capable of providing embedded intelligence in Internet of Things (IoT) devices and networks, can be used. The author discussed the security and privacy challenges in the Internet of Things, attack vectors, and security requirements, as well as the role of machine learning and deep learning in the Internet of Things. They also talked about various machine learning and deep learning techniques, as well as how they apply to IoT security [27].

Regazzoni, F. et al. raspberry pi-based framework for home security system which uses different sensors including PIR, IR, Piezoelectric sensors and sound sensor. An intrusion can be detected with the help of these sensors which works on motion detection, temperature variation and sound at the location. If deviation in output identifies unauthorized user and system sent alarm to the owner of home system [28].

3.5. Cost- Security and Security-Performance Trade off

Constraint based CPS devices invested more in hardware of the system. Better hardware gives better results. If we add security in it. It will increase the overall cost of CPS application. Use of existing mechanism is a good solution for it. It will reduce the cost on security. But it will arise new issue of performance. Figure 3.1. shows Cost-Security-Performance Trade-off.

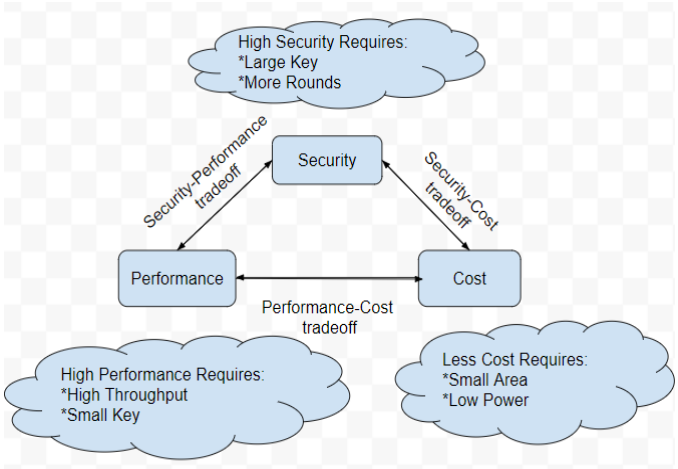

Figure 3.1: Cost-Security-Performance Trade-off

As existing security mechanism required strong hardware to perform well. In major requirement high performing central processing unit is a basic requirement for that with sufficient primary storage. As the purpose of the constraint-based devices are limited to specific task so, it reduces the cost over high performing processing unit and with limited storage. Also, energy backup limit to a specific range as per the requirement of application. Because of these limitations existing security mechanism will not work efficiently. If we try to add this mechanism it will degrade the performance of the system. the trade Off statement mentioned that "If security implemented with existing mechanisms, it will reduce the cost but decrease the performance of the system. If performance of the system decreases it increases the maintenance cost of the system". So, security, performance and cost are corelated with each other.

A new lightweight security solution is the need of the current constraint-based CPS system. which balance in between security-Performance and cost.

IV. REQUIREMENTS AND SYSTEM DESIGN

Proactive and reactive approaches are used in many research activities. The proactive approach efficiently handles attacks because it is a defence against attacks before they occur on the system. While the reactive approach is attempting to find a solution to a previously performed attack. The research employs a two-tiered approach. To achieve the research objectives, the first approach employs a survey-based research methodology. Various challenges associated with CPS-based devices were identified using this approach. It identifies the shortcomings of various existing security mechanisms. It also describes various attacks on the CPS system.

The second approach focuses on algorithm implementation and testing. This method identifies a suitable test bed. The implementation via test bed must demonstrate the algorithm concept. Overall system analysis is included in testing. This demonstrates the algorithm's efficiency. To demonstrate the proof of concept, various attacks must be implemented on the system. The successful defence against such penetration testing attacks demonstrates the algorithm's efficiency. It is also critical to identify the constraints of various CPS

devices. It will determine whether the proposed algorithm performs well on these constraint-based devices.

4.1. Functional Requirements

Functional requirements represent statements of services the system should provide the requirements of the proposed algorithm should be checked with scope and objective of the system. Identified functional requirements are mentioned below

- Identification of characteristic of Security algorithm.
- Architecture of the system defined
- Technology has been defined
- Complexity of the system defined.

Security algorithm identifies different characteristics which includes key elements of security. security, privacy, authentication and authorization. These key elements prove the efficiency of the algorithm.

4.2. Non-Functional Requirements

Non-functional requirements focus on constraints, performance and external interface requirements. Some non-functional requirements are as listed below.

- Usability
- Reliability
- Performance
- Supportability
- Implementation
- Cost

Usability defines effectiveness and efficiency of the system. It defines how system is effective against different cyber-attacks. Usability also shows efficiency of the interface used by the user. Where it can upload and configure cyber security code of algorithm into devices.

CPS's performance and operations are based on five pillars:
Figure 4.1 shows various key properties of cyber-physical systems (CPS).

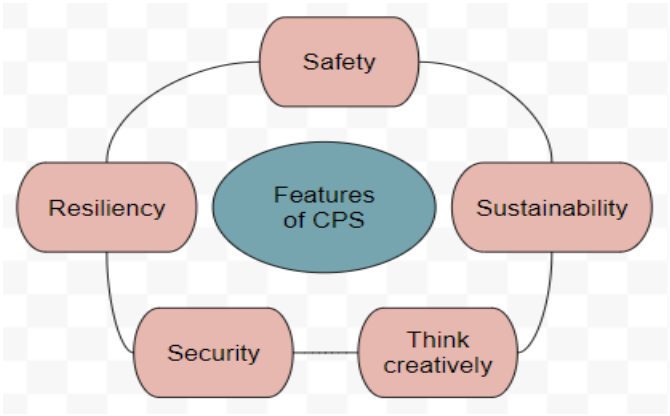

Figure 4.1: Key properties of cyber-physical systems (CPS).

[1] Design thinking: It is an iterative process that identifies strategies and solutions by challenging assumptions.

[2] Safety: hazard prevention and avoidance

[3] Security: assurance of three key properties of security, namely information confidentiality, integrity, and availability (CIA).

[4] Sustainability: ensuring the system's long-term operation,

[5] Resilience: Enabling endpoint and network self-healing.

4.3. Secure CPS Flexible framework

Figure 4.1 shows secure CPS flexible framework.
It is divided into four different layers.

- **Physical Layer:** Bottom layer of the CPS framework is physical layer it is divided into two sub parts

- **Hardware component:** It describes hardware used for the development of security mechanism for cyber physical systems. Microcontroller interface includes Raspberry pi or Arduino. Both the interfaces are small in size but capable to handle heavy tasks. These interfaces act as a Gateway server. While at the client side can choose communication interface depends on environment. Where IEEE 802.11, 802.15 or 802.15.4. can be used. It is totally depending on wireless environment which is used for implementation. Whether it is short range or long range. Depends on physical distance between Gateway controller and client node can choose suitable hardware interface like ESP8266, ESP32, XBEES2C or BLE4.0.
- **Device Driver:** Second sublayer is device driver. It provides device drivers for hardware interfaces which is used for security mechanism. These device drivers are used to activate all hardware which is used to implement security mechanism in cyber physical system. It also works for power management of all the hardware. Handling of Input/Output devices also done in this layer.

• **Communication Layer:** It is a bridge in between Application user, application software and hardware. Which works for the mobility of the application. It provides connection establishment between gateway server and client node. It also used to exchange messages in between the nodes for authentication and authorization purpose.

• **Software framework Layer:** It contain two modules. First module works for development environment for security mechanism. It is used for execution of code building procedure. While second module is used to code development for security mechanism. Secure session and token-based authentication algorithm executed with software framework.

• **Application Layer:** The top most layer is Application layer, which includes applications that used in cyber physical system. Security mechanism is specially developed in a way that where it supports client server environment.

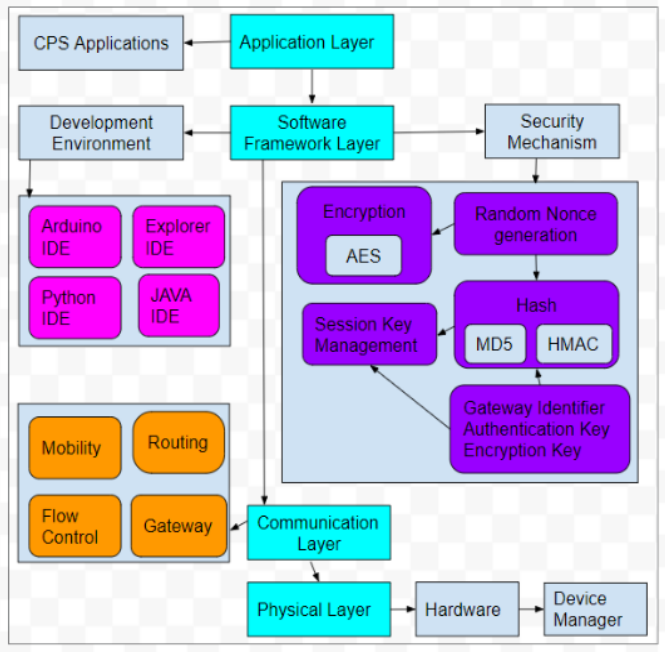

Figure 4.1: Secure CPS flexible framework.

4.4. System Design-Object Oriented Approach

The object-oriented approach is concerned with encapsulating information system structure and behaviour in small modules that combine data and processes. Object Oriented Design (OOD) is ensuring a better quality and production efficiency by making building information modelling more usable.

OO models are used during the analysis phase to act as an intermediary between the problem and the solution. It works well in situations under which systems are regularly designed, adapted, and maintained. It recognises and categorises objects in the specific problem basis of information and behaviour.

The following points mentioned that why object-oriented approach is used in the development of Security algorithm.

- Algorithm based program is organized by having number of classes and objects.
- Message passing is used in between devices.
- Reusability of code implementation
- It is suitable for in house project development
- UML based Class diagram, sequence diagram, state chart diagram, and use cases all contributes in the development of security algorithm.
- Reduction in the code is possible which is used for lightweight code.
- It supports for distributed environment.

V. TEST BED DEPLOYMENT

It demonstrates the Secure session and token-based authentication algorithm's implementation. Smart Home Automation System as a Cyber physical system application to demonstrate the concept.

5.1. Testbed setup for Research Work

To show the proof-of-concept smart home automation system application selected. It is a Cyber physical system application.

Smart Home Systems (SHSs) are made up of a variety of low-capacity devices (sensors and microcontrollers) that are linked together via wireless networks. The network's smart devices (SDs) must communicate in a secure manner. There seems to be a lack of standard security measures that can provide adequate security due to resource constraints such as limited computational power and low space. The disclosed method provides a critical agreement method for smart home systems. The proposed mechanism protects against various security attacks such as replay, masquerade, and eavesdropping.

To monitor and regulate devices in the physical domain, A cyber-physical system is one that combines computation complexity, communication, detecting, sensing and programming interfaces. A cyber-physical system can detect real-world objects, make decisions (such as whether to turn on or off a switch), and perform physical actions (ON or OFF the switch). The current implementation is concerned with systems and methods for preventing cyber-physical system intrusions. The technique enables smart home cyber physical systems to authorize connected devices to gateway devices while keeping interaction privacy and security. Cyber physical components are connected in small chips with network connectivity in smart home applications. As a result, they are vulnerable to network intrusions. The present invention is a system and method for securely communicating and authenticating smart devices in smart home applications while maintaining interaction privacy and security.

5.2. Plan of Test bed Execution

a. Identification – Identification of applicable CPS based application which is suited for implementation of Secure session and token-based authentication algorithm. Choosing and finalising one of them for future implementation.

b. Conceptual model and design – The concepts needed to build the test bed with the specified application are thoroughly studied. The overall design of implementation is done at this stage.

c. Design phase – At this phase, low-level design is done. The user interface is intended to improve visual representation of the implementation. It mentioned application interface which is used to show implementation with proof of concept.

d. Writing the code – At this point, the system's actual implementation begins. Coding for each module which include coding at gateway server and client device which is here smart devices.

e. Assessment (Testing) –All functionalities will be interconnected and then the proof of concept will be demonstrated, it performs cyber-attacks on the system. It will show whether the system defended against attack or attacker break the wall of security. It evaluates the test bed. Performance evaluation also done here. Which shows performance of the system under different circumstances.

5.3. Components Description

The proposed system contains three core components namely gateway server, Wi-Fi network and microcontroller with wireless module.

• **Gateway Server:** The purpose of the gateway server is to interact with smart devices and application interface. In proof-of-the-concept implementation of the system, Raspberry Pi microcontroller is used as a gateway server. The gateway server handles asynchronous requests from the SDs. It also runs a web server for accepting commands from the user and securely communicating instructions to the smart devices.

• **Microcontroller with Wireless Module:** To allow devices to connect to the network and securely communicate with gateway server a microcontroller with wireless module and TCP/IP capability is needed. ESP 8266 microchip is used which is a low-cost Wi Fi module with TCP/IP and microcontroller capabilities. The ESP 8266 microchip contains 32 KiB instruction RAM and 80 KiB user-data RAM. This microchip used in end devices such as fan, led lights etc, to establish connection in between the gateway server (Microcontroller) and end point device.

• **Functionality of a smart device:** To implement the functionality of a smart device, custom-built NodeMCU firmware using Cloud Build Service used and embedded an additional crypto module in the firmware to add capability to perform cryptographic operations. Esptool is used, which is a Python based open-source tool to flash the ESP8266 module with custom-built NodeMCU firmware. LUA script is used to write code for smart device functionality and perform various operations.

• **Wi-Fi Hotspot:** Wireless network or Wi-Fi hotspot is required for gateway server and end devices to communicate with each other. It develops a wireless network in between smart devices and central controller gateway server.

Hardware platform mentioned above required minimum hardware requirement. Which include desktop-based computer or laptop which is used as application programming interface. If it is not available smartphone (mobile) can be used, which has any internet browser installed in it. For portable microprocessor many choices are available, Raspberry pi with A+, OR B+ module is sufficient to store and execute algorithm.

When CPS concept comes, to convert simple physical device into smart device communication interface is required. In market for IoT devices many communicating interfaces are available. Bluetooth, or Wi-Fi module can be used. Here we used ESP 8266 Wi-Fi module.

Access point can be used to develop wireless network. If Smartphone is used as a application interface then it can use Wi-Fi hotspot to create wireless network in between smart devices and gateway server. Physical devices which are used for home automation system which has a ON/OFF functionality.

The application will execute on distributed platform of operating system. To demonstrate the working of application interface currently it is working on any web browser. NodeMCU firmware is used for configuration of Wi-Fi module ESP 8266/ESP32. ESPlorer is an Integrated Development Environment (IDE) used for development of ESP8266 module.

Python is programming language. It is used for software development and web development. Lua is a scripting language that is effective, efficient, small

and light, and embeddable. It supports object-oriented and procedural programming, as well as data-driven programming. LUA script is used to write code for smart device functionality and perform various operations. PHP with HTML is used for handling user interface which performs operations (ON/OFF) on smart devices.

5.4. System Architecture of Secure session and token-based authentication algorithm-based CPS system

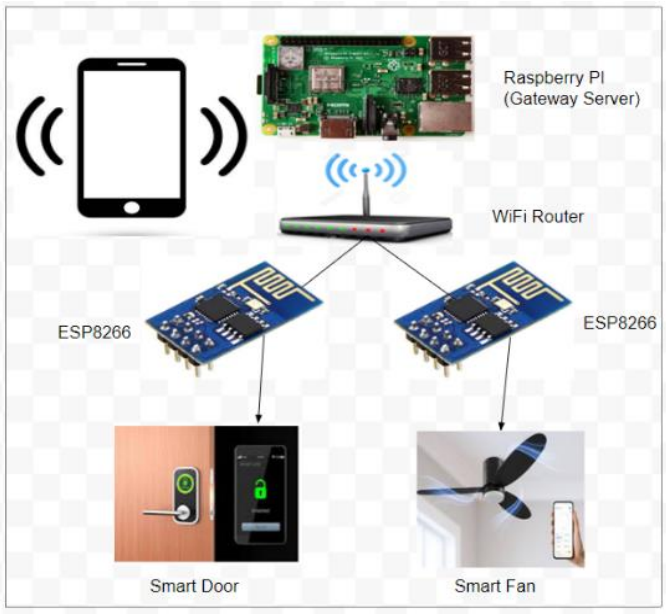

Figure 4.1: Detailed Architecture of Cyber Physical System in Wireless Network

Figure 4.1. shows one smartphone which acts as a user device and handles all smart devices. The smartphone only connected to gateway server. It is not possible to send direct instruction to the end point smart devices through smart phone. Every instruction must pass through gateway server to smart device. Implementation of Secure session and token-based authentication algorithm has two parts which is as follows

1. Secure Authentication code at Gateway server
2. Secure Authentication Code at client side.

Both the code works according to algorithm. It generates and share the keys with which other. Session key exchange in between them. If session key not matched and instructions sent by smartphone to perform ON/OFF operations on smart device. The instruction will not be executed as session key is not matched.

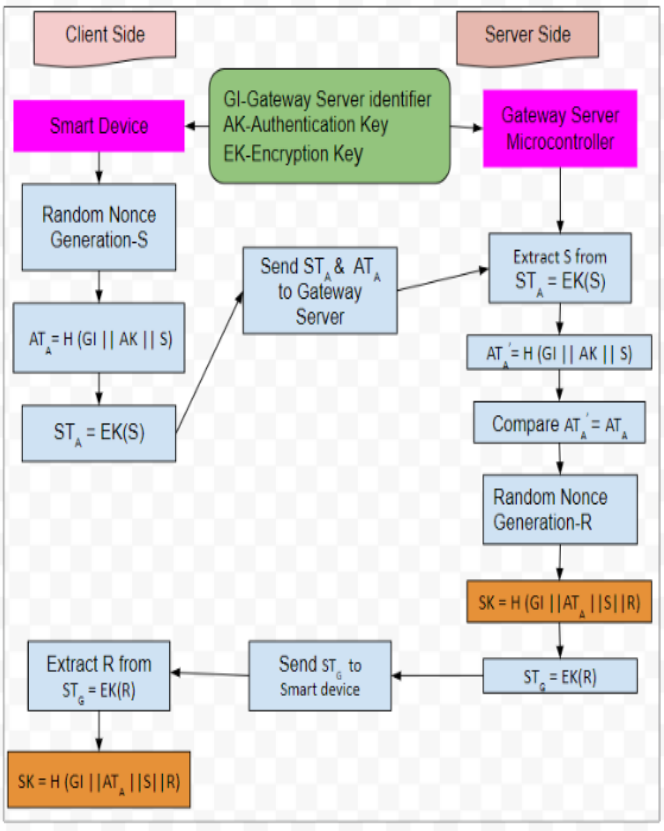

Figure 4.2: Code execution through Secure session and token-based authentication algorithm

As mentioned in figure 4.2. the Secure authentication code at client side generate session and authentication token by using common parameters. It was already discussed and explained detailed in my previously published research paper [29]. It also extracts random nonce from packets which contain session token sent by gateway server. Finally, it generates session key.

5.5. Experimental setup Configuration

Raspberry pi3 B+ Module: Broadcom BCM2837B0, Cortex-A53 (ARMv8) 64-bit SoC @ 1.4GHz 1GB

LPDDR2 SDRAM, 2.4GHz and 5GHz IEEE 802.11.b/g/n wireless LAN, BLE Gigabit Ethernet over USB 2.0 (maximum throughput 300Mbps), Bluetooth 4.2, Extended 40-pin GPIO header, Full-size HDMI, 4 USB 2.0 ports, CSI camera port DSI display port connecting.

ESP8266 Wi-Fi Module: Power input: 4.5V~9V (10VMAX), Communication Interface Voltage(V) 3.3 V, USB-Powered, Transfer rate: 110-460800bps, Support UART / GPIO data communication interface, Flash size: 4MB

As per the algorithm first process is extracting random nonce S value from incoming packet. Which is shown by

dec_val = (dec(str(cred_holder[SD]['EK']),ST)).split(',')

AS per the algorithm next process is generating and comparing Authentication token (ATA)from it.

AT_1=hashcalc(str(cred_holder[SD]['GI'])+str(cred_holder[SD] ['AK'])+str(s_nonce))

Next step is to generate random nonce R. with below mentioned function, it will generate 64-bit random nonce R

r = randomstr()

Session key generation is performed by following code

SK=hashcalc(str(cred_holder[SD]['GI'])+str(AT)+str(s_nonce)+str(r))

It shows the preconfigured parameters stored in the device. Which includes Gateway server identifier, smart device identifier, encryption and authentication key. It shows stored pre generated values of common parameters. It also shows the functions which is used for implementation of Hash function, AES encryption and AES decryption.

It shows generation of random nonce S of 64 bit.

s_nonce = randomstr(8)

It also shows the generation of value of authentication token and session token by using following functions

AT_A = hashcalc(GI_A..AK_A..s_nonce)
ST_A = enc (EK_A,s_nonce)

The function shows generation of session key by using function

function sessionKeyCreate(STR)

The above function extracts the value of random nonce R and generate session key by using following code

SK_A2 = hashcalc(GI_A..AT_A..s_nonce..r)

VI. EVALUATION

6.1. Replay attack test bed

To perform replay attack two wireless environment created,

1.Secure Zone: In secure zone all devices are configured with Secure session and token-based authentication algorithm. Where gateway server and smart device configure with security algorithm.
2. Unsecure zone: In unsecure zone Cyber physical system is developed without any security mechanism.

This attacker node is used to perform attacks on both unsecured node and secured zone. In Secured zone Gateway server is a microcontroller which handles smart devices like fan and Led light. In figure

raspberry pi module is a gateway server. While Fan and Led Light connected with ESP 8266 Wi-Fi module. The proposed algorithm code is stored in raspberry pi and in ESP 8266. The common parameters also stored into these devices. All are interconnected with access point which develops wireless network in between these devices.

Unsecured zone contains attacker node and one unsecured node led light. Through laptop unsecured node perform ON/OFF operations. Here Laptop itself work as a gateway server to work with unsecure smart device. The proposed algorithm is not configured in unsecured zone. In laptop attacker code is also stored which performs attack on unsecured and secured zone. The below steps show implementation of replay attack.

Step by step execution of Attacker Module to perform replay attack

1. Attacker node try to connect Wi-Fi and successfully connected to it. It identifies network address of the network.

2. Now first task for attacker node is to detect live IP addresses of network. To detect live IP address attacker node, install nmap tool.

3. To install nmap tool it uses command

terminal: ~$ sudo apt-get install nmap.

4. Now it tries to fetch all devices IP Addresses by using following command

terminal: ~$sudo nmap –Sp 192.168.43.0/24

here it identifies that network address with class C IP address scheme. So, it will try to find all IP under in it.

VII. CONCLUSION

Security mechanism for cyber physical system mainly focuses on constraint-based devices. with three parameters – Processing capabilities, memory and energy backup. Previous research works have either used existing heavy loaded algorithm or security framework. The security issues, challenges and observations related to CPS system explained by the many researchers. The existing security algorithm works smoothly on CPS system where better hardware support given. But for constraint-based application light weight security mechanism is required which support and will works with minimum hardware capabilities. Secure CPS flexible framework shows that the Secure session and token-based authentication algorithm will work on distributed environment. It is not hardware dependent. The flexible framework showing that security mechanism will work on Distributed CPS architecture. Example- current system works on wireless network. If it changed to Bluetooth network and even if changed to communication network, it will execute system smoothly. Mathematical model of the system shows that execution of algorithm through mathematics where it will detect intrusion who perform cyber-attacks on the system. It also mentioned requirement analysis, which includes the software and hardware requirements for the test bed and implementation of algorithm through programming language. Any secure system tested by performing attacks on that system. Efficiency of Secure session and token-based authentication algorithm proved by performing attacks on that system. The cyber-attack performed on the system which is Replay Attack

II. REFERENCES

[1]. Anonymous (2016). Seventh Framework Programme: Building the Europe of Knowledge. [online] Mobility and Transport - European Commission. Available at: https://ec.europa.eu/transport/themes/research/fp7_en.

[2]. Smartcities.gov.in. (2020). Home page | Smartcities. [online] Available at: https://smartcities.gov.in/.

[3]. Thite, S. and Thakore, D. (2020) 'A Survey on the Internet of Things: Applications, Challenges and Opportunities with India Perspective', Lecture Notes in Electrical Engineering, 601, pp. 1263–1272. doi: 10.1007/978-981-15-1420-3_138.

[4]. Gaddadevara Matt Siddesh (2016). Cyber-physical systems: a computational perspective. Boca Raton, Fl.: Crc Press.

[5]. Connectivity Standards Alliance. (n.d.). IoT Solutions. [online] Available at: https://zigbeealliance.org/solutions/ [Accessed 18 Sep. 2021].

[6]. Balushi, A. (2019). Cyber Security for Cyber Physical Systems. S.L.: Springer.

[7]. Raza, S. et al. (2011) 'Securing communication in 6LoWPAN with compressed IPsec', 2011 International Conference on Distributed Computing in Sensor Systems and Workshops, DCOSS'11. doi: 10.1109/DCOSS.2011.5982177.

[8]. Komninos, N., Philippou, E. and Pitsillides, A. (2014) 'Survey in smart grid and smart home security: Issues, challenges and countermeasures', IEEE Communications Surveys and Tutorials, 16(4), pp. 1933–1954. doi: 10.1109/COMST.2014.2320093.

[9]. Lokesh, M. R. and N, Y. S. K. T. K. (2016) 'Challenges and Current Solutions of Cyber Physical Systems', 18(2), pp. 104–110. doi: 10.9790/0661-1821104110.

[10]. Sabaliauskaite, G. and Mathur, A. P. (2014) 'Countermeasures to enhance cyber-physical system security and safety', Proceedings - IEEE 38th Annual International Computers, Software and Applications Conference Workshops, COMPSACW 2014, pp. 13–18. doi: 10.1109/COMPSACW.2014.6.

[11]. Karmakar, K.K., Varadharajan, V., Nepal, S. and Tupakula, U. (2020). SDN Enabled Secure IoT Architecture. IEEE Internet of Things Journal, pp.1–1.

[12]. Ashibani, Y. and Mahmoud, Qusay H (2017) 'Cyber physical systems security: Analysis, challenges and solutions', Computers & Security, 68, pp. 81–97. doi: 10.1016/j.cose.2017.04.005.

[13]. Chen, Y., Kar, S. and Moura, J. M. F. (2017) 'Dynamic Attack Detection in Cyber-Physical Systems with Side Initial State Information', IEEE Transactions on Automatic Control, 62(9), pp. 4618– 4624. doi:10.1109/TAC.2016.2626267.

[14]. Gamundani, A. M. (2015) 'An Impact Review on Internet of Things Attacks'

[15]. Madnick, S., Nourian, A. and Madnick, S. (2018) 'A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet', 15(1), pp. 2–13. doi: 10.1109/TDSC.2015.2509994.

[16]. Lei, L. et al. (2013) 'A threat to mobile cyber-physical systems: Sensor-based privacy theft attacks on android smartphones', Proceedings - 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2013, pp. 126–133. doi: 10.1109/TrustCom.2013.20.

[17]. Vimal Jerald, A., Albert Rabara, S. and Bai, D. P. (2017) 'Algorithmic Approach to Security Architecture for Integrated IoT Smart Services Environment', Proceedings - 2nd World Congress on Computing and Communication Technologies, WCCCT 2017, pp. 24– 29. doi: 10.1109/WCCCT.2016.16.

[18]. Jawadwala, Q. and Patil, K. (2016) 'Design of a novel lightweight key establishment mechanism for smart home systems', 11th International Conference on Industrial and Information Systems, ICIIS 2016 - Conference Proceedings, 2018-Janua, pp. 469–473. doi: 10.1109/ICIINFS.2016.8262986.

[19]. Dai, B. et al. (2019) 'Enhancing Physical Layer Security in Internet of Things via Feedback: A General Framework', IEEE Internet of Things Journal, PP(c), p. 1. doi: 10.1109/JIOT.2019.2945503.

[20]. Pasqualetti, F., Dorfler, F. and Bullo, F. (2013) 'Attack detection and identification in cyber-

physical systems', IEEE Transactions on Automatic Control, 58(11), pp. 2715–2729. doi: 10.1109/TAC.2013.2266831.

[21].Huang, K. et al. (2020) 'A Game-Theoretic Approach to Cross-Layer Security Decision-Making in Industrial Cyber-Physical Systems', IEEE Transactions on Industrial Electronics, 67(3), pp. 2371–2379. doi: 10.1109/TIE.2019.2907451.

[22].Pietre-Cambacedes, L. and Chaudet, C. (2010) 'The SEMA referential framework: Avoiding ambiguities in the terms "security" and "safety"', International Journal of Critical Infrastructure Protection, 3(2), pp. 55–66. doi: 10.1016/j.ijcip.2010.06.003.

[23].Bernardi, S. et al. (2021) 'Security modelling and formal verification of survivability properties: Application to cyber–physical systems', Journal of Systems and Software, 171(xxxx), p. 110746. doi: 10.1016/j.jss.2020.110746.

[24].Majumder, A. J. A., Veilleux, C. B. and Miller, J. D. (2020) 'A cyber-physical system to detect IoT security threats of a smart home heterogeneous wireless sensor node', IEEE Access, 8, pp. 205989–206002. doi: 10.1109/ACCESS.2020.3037032.

[25].Chen, Y., Kar, S. and Moura, J. M. F. (2015) 'Cyber-physical systems: Dynamic sensor attacks and strong observability', ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings, 2015-Augus (1), pp. 1752–1756. doi: 10.1109/ICASSP.2015.7178271.

[26].Min, B. and Varadharajan, V. (2016) 'Design and Evaluation of Feature Distributed Malware Attacks against the Internet of Things (IoT)', Proceedings of the IEEE International Conference on Engineering of Complex Computer Systems, ICECCS, 2016-Janua, pp. 80–89. doi: 10.1109/ICECCS.2015.19.

[27].Hussain, F. et al. (2020) 'Machine Learning in IoT Security: Current Solutions and Future Challenges', IEEE Communications Surveys and Tutorials, 22(3), pp. 1686–1721. doi: 10.1109/COMST.2020.2986444.

[28].Regazzoni, F. and Polian, I. (2017) 'Securing the Hardware of Cyber-Physical Systems', pp. 194–199.

[29].P Salman Raju, P Venkateswara Rao, S Sreenivasa Murthy. (2023) 'Create a New Session Key Generation Algorithm for Cyber Physical System to Improve Cyber Security', International Journal of Computer Sciences and Engineering, pp.18-25, Feb-2023. Doi: 10.26438/ijcse/v11i2.1825

Cite this article as :

P Salman Raju, P Venkateswara Rao, S Sreenivasa Murthy, "Design and Develop a Secure CPS Flexible Framework to Improve the Cyber Security using a New Security Algorithm", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 2, pp.388-402, March-April-2023. Available at doi : https://doi.org/10.32628/CSEIT2390244
Journal URL : https://ijsrcseit.com/CSEIT2390244