Key Establishment Algorithm for Secure Cyber Physical System to Prevent Cyber Attacks

Sandip Thite, DevendraSingh Thakore

Abstract*: Extensive research effort is going on to contribute to the Cyber Physical system (CPS). It will create a physical system capable of computation, communication and sharing information between physical devices. Physical devices become smart devices because of CPS. CPS are engineered systems that are built with sensors, microcontrollers which performs computation, communication, control, process and analysis of physical objects. CPS playing important role in smart cities, home automations and other applications. Due to resource constraints like low processing power and low storage space there is a lack of standard security mechanism which can provide adequate security in CPS. In the research paper, we proposed Key establishment mechanism which prevents CPS from cyber-attacks. The goal of this research paper are six -folds: i) to give a detailed overview of cyber physical system. ii) To study architecture of CPS. iii) To study different attacks on CPS with attack points. iv)Application areas of CPS v) security threats in CPS vi) Key establishment algorithm to prevent cyber-attacks in CPS.

Keywords: Cyber Physical system, Internet of Things, Security threats, Cyber-attack, Physical attack.

I. INTRODUCTION

In recent year there is rapid growth in the development and deployment of cyber physical system. Many physical systems converted into cyber physical system by using computational algorithm. Internet of things is a good example of such type of system. In next few years more than 50% of physical devices which we used in our day to day life will have converted into cyber physical system. For example, door locking system, smart refrigerator, smart oven and washing machine. All these devices interconnected with microcontroller and Wi-Fi module.

Increase in the use of cyber physical system with negligence about security of devices causes open gate for attackers to perform attacks on such type of insecure devices [13]. As per the Kaspersky report attacks on cyber physical system increases significantly in the first half of 2019. As mentioned in the report, 105 million of attacks on CPS coming from 276000 unique IP addresses in the first six months of 2019. In last year, i.e. 2018 in the same duration only 12 million attacks performed on CPS. From this report we can easily conclude that it is very easy to perform attacks on Cyber physical system [6]. The main reason behind this now a days people taking precautions about security of their desktop computers, laptop. At the same time, they protect their smartphones. But they are careless about security of cyber physical system based devices which they used in day today life. Good example is CPS based Car locking system [10]. Many people unaware about threats which can easily break the car locking mechanism by capturing signals. These signals can be used to break security of locking mechanism and used for stolen car.

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author

Sandip S. Thite*, Department of Information Technology, Bharati Vidyapeeth Deemed to be University College of Engineering, Pune, India. Email: Sandip.thite@bharatividyapeeth.edu

DevendraSingh Thakore, Department of Computer Engineering Bharati Vidyapeeth Deemed to be University College of Engineering, Pune, India. Email: dmthakore@bvucoep.edu.in

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

II. BACKGROUND

A. Cyber Physical System

It is a new generation of electronics system. It is an integration of physical systems with the help of computational algorithm. Set of instructions in a computational algorithm performs different activities on a physical system. CPS contain embedded computers, which interact with network to monitor and control different physical processes of the equipment. CPS gives birth to the many automatic equipment's which reduces human effort towards the system. It reduces malfunctioning of the system which causes due to human errors. Smart appliances, smart car these are the examples of CPS. Internet of things is a branch of CPS which drives in all sectors of global economy. Which is used to develop smart home to smart cities. The impact of networking and information technology open a door for CPS in almost every sector which is from mechanical to biotechnology. In previous generations of electronics automated systems are present. But due to the presence of CPS these system becomes more dynamic and result oriented. Good example is home automation system, where automated air conditioners works by sensing the room temperature. But due to CPS it not only sense the room temperature but it identifies human object, it senses the activity perform by human object, it also analyzes the information and set the proper temperature in room. Due to CPS system becomes more dynamic which perform run time decision making activities. CPS already used in different sectors like automobile, mechanical, civil, medical, cargo, marine industry etc. CPS is a dynamic system which convert basic manual system into automated system by using technology and set of instruction on which system works. Basic equipment work as a smart device due to CPS. Basically these devices are low capacity devices which has minimum processing capabilities, low power and minimum storage capacity.

B. Basic Architecture of CPS

A basic architecture of CPS can be categorized into four different stages [14]

1. Physical system – basic device is a part of the physical system. It is more static than dynamic. It works manually. Most important to handle the system we require the involvement of human being who perform a task from physical device. Executing a task through this system is time consuming process. It is an error prone device due to surrounding issues with the device.

2. Computation – to convert normal device to the smart active device we need to add set of instructions into the system. Adding instructions into the system causes it follows and execute all these instructions to become a smart device. Due to computation device becomes self-configuring device and become more and more powerful. Due to computation passive device becomes more and more active. Basic task or physical process of device monitored and controlled by computation which help to convert a basic device into a smart device.

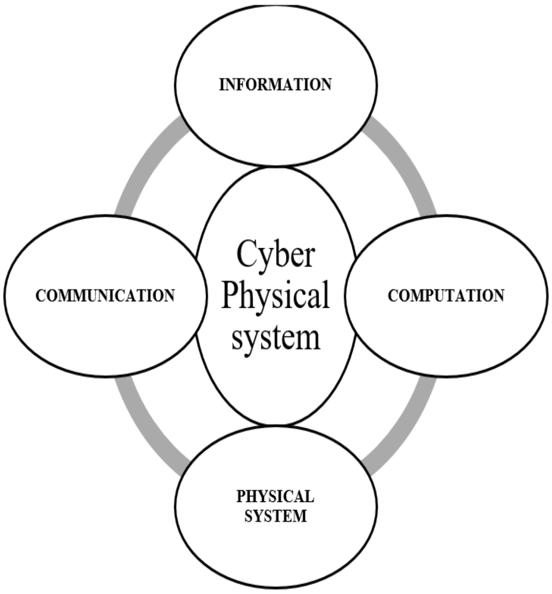

Figure 1: Architecture of Cyber Physical System

3. Communication – To execute a task through different devices communication between devices has more importance. Even to execute a sequence of action in between devices communication is needed. The Cyber physical system follows wired and wireless communication under different protocols and standards. Zigbee is an IEEE 802.15.4 based specification is a good example of communication protocol used in different devices. Such as home automation, low powered radio devices etc. Which works in wireless ad-hoc network to connect different physical devices.

4. Information – Computation execute the task through devices while communication is used in between devices to interact with each other. Generated information through device is used to analyze and sharing purpose in between devices. Information is used to add decision making capability into the device which causes device becomes more and more smart. In critical situation device itself tackle the problems with the help of information to get the solution.

III. ATTACKS ON CYBER PHYSICAL SYSTEM

Cyber physical system consist of two important parts, first is physical system and second is cyber system. Communication, computation and controlling process executed in between cyber and physical system.

Two basic attacks performed on cyber physical system i.e. Physical attack and Cyber-attack [2].

A. Physical attack

physical attack is all about destroying physical infrastructure and control system of CPS. Physical attack includes physical tampering of devices, destruction of physical devices, physical intrusion. In this attack attacker access and modify internal structure of devices. Good example of this attack is unregulated flow of voltage given by attacker to the system damage the physical devices. In destruction of physical devices attacker physically damage the devices by using physical tools so that devices are no useful for assigned task. Sensor based devices damaged with environmental tampering. In some region temperature sensors are deployed to perform specific task. In such environment attacker increase or decreases temperature causes malfunctioning of processing unit of sensor which cause damage in the CPS.

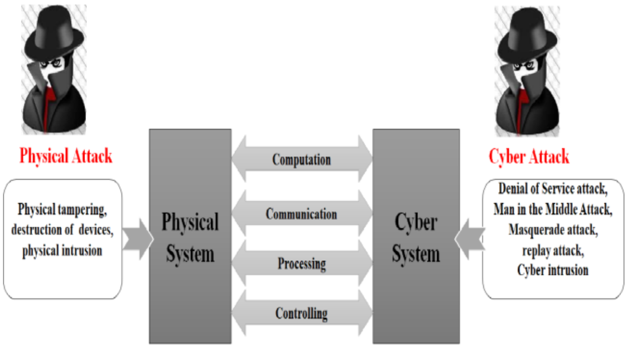
Physical Attack
Physical tampering, destruction of devices, physical intrusion
Physical System
Computation
Communication
Processing
Controlling
Cyber System
Cyber Attack
Denial of Service attack, Man in the Middle Attack, Masquerade attack, replay attack, Cyber intrusion

Figure 2: Attacks on Cyber Physical System

B. Cyber Attack

We are much familiar with cyber-attacks its same like attack which performs on computer network, smart phone devices and cloud based network. Cyber-attacks can have different number of forms through which it can different types of attacks i.e. Denial of Service attack (DoS) [9], Man in the Middle Attack, Masquerade attack, replay attack, Cyber intrusion [11] etc. Cyber attacker creates unauthorized node in network where legitimate node connects with unauthorized node and lost its identity.

IV. ATTACK POINTS IN CPS

Fake Devices – Attacker perform attacks on authorized device and stolen its identification and authorization information with this it adds fake device in cyber physical environment which perform attacks on whole system [12]. Cyber physical system cannot identify fake device due to it is showing identity of authorized device.

Weak Protocol – To establish communication and for data transfer CPS uses predefined communication protocol. Due to weak protocol structure attacker can easily decrypt header and data from protocol which causes easy way to perform attacks on Cyber physical system.

Rouge Access point- Every CPS developed in a way that router or centralized access point handle different smart devices in the network [8]. It is a single gateway to enter into system. Attackers create rouge router or access point by capturing authorized router information. Many smart devices connected with rouge AP assuming that they connected with legitimate node. Through this rouge router attack is possible on CPS.

Spoof User Interaction – User interact with each other with smart devices or wearable devices. Attacker monitor their communication channel and try to spoof their important information.

Spoof manufacturer infrastructure- CPS developed with sensor node, microcontroller, WI-FI modules. In market we found many manufacturing companies who develop such types of product. Attacker use such type of infrastructure which is easily available in market through that it performs attacks on the CPS.

Weak Application Programming Interface (API) – Weak API is another gateway for attacker to perform attacks on the CPS. Attacker try to get pseudo code of system by working on API. With the help of Weak API, it damages the CPS. [14]

Fake Infrastructure Input – Attacker adds fake devices like sensors, microcontroller in CPS environment by acquiring authorized devices information. With this it develops fake infrastructure of CPS. Many users connect to such fake infrastructure and share their important data with system which is easily available to attacker.

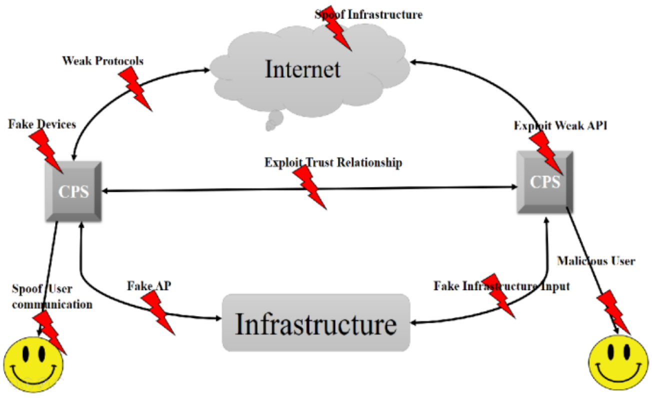

Figure 3: Security threat in Cyber Physical System

V. CPS APPLICATION AREAS WITH SECURITY THREATS

A. Home Automation system

In home automation system existing components replaced by sensor, microcontroller and Wi-Fi modules i.e. ESP 8266 or ESP 32 etc. due to this home automation system connected to cloud environment which causes from anywhere anyplace we can control our home physical equipment's which converts these homes into smart homes [5]. Many physical components in home which works on ON/OFF theory works on instruction to become automated by using microcontroller and Wi-Fi module. Increase in the use of cyber physical components in home which causes energy efficient, automated smart devices.

As the smart devices increased in the home causes extra points of access in the home. These added extra points of access causes more opportunities for attacker in the home. Attack can create rouge access point in home network [4] where all smart devices connected with rouge access point assuming that they are connected with authorized node. Rouge access point performs attack on different smart devices which causes controlling of all home devices or malfunctioning of devices.

B. Healthcare system

Old health care system works with different monitoring tools which work manually causes delay in patient treatment. With the cyber physical system old monitoring equipment replaced by sensor & microcontroller based smart devices which continuously monitoring human body. These devices are capable of collecting data from human body, processing and transmitting data also done by these devices [3]. These are the new technological solutions in healthcare system which is very helpful for doctors in medical line as well as for patients. Patient health continuously monitors through smart devices of Cyber physical system. These devices also connected to internet so doctor can monitor patient from different locations and guide also about treatments. With CPS we can monitor patient from their homes also to save the cost and time.

Wireless body Area network (WBAN) is the best solution for Healthcare system for monitoring health status of patient. Attacker can perform Physical and cyber-attacks on the system which causes malfunctioning of life critical system which damage the health of patient. Attacker can view, access or modify collected medical data which include patient medical reports

C. Smart cities with Cyber Physical system

A smart city is evolving concept which is also called as Digital city, intelligent city and connected city. Smart city is an integrated effort with the help of cyber physical system towards digital world. Rapid growth of urban population due to development of rural areas causes necessity of urban development with high living standard and comfort of the peoples. Implementation of cyber physical systems in cities from home to transportation system, smart mobility to smart government will help smart cities. These thing only possible after increase in the use of cyber physical devices in different applications which built the cities.

In smart city project vulnerabilities can be identified by attackers where he tried to implement physical and cyber-attacks on the system. Such types of attacks have major impact on smart city lives. Smart city project implement with Wireless Sensor Network (WSN). Attacks on WSN causes interruption in the services. Interruption in services may affect the daily activities of citizens. Long term interruption may cause dangerous consequences. Some examples of interruption are traffic signal malfunctioning, water and electricity resource management, CCTV system etc. Other than this privacy infiltration, damage of property, damage of transportation system etc. also possible with attacks.

D. Smart Grid

Smart grid system is a future power grid system which integrates information and communication techniques for efficient and reliable energy services [1]. Implementation of cyber physical system in grid will not only improve the performance but also efficiency of the energy resources. Cyber physical system controls the operations, establish the coordination between different equipment it also provides predictions about life of equipment. Due to cyber physical system analysis of system and performance is easily available. Smart grid works with algorithm which add automation in the system attackers can enter in the system through PLC controller or through Wireless sensor node which attacks on computational algorithm and modify algorithm which causes dangerous impact on grid project. Such as electricity power down in the region.

E. Smart Building

Implementation of cyber physical system in building which causes building equipped with automation system, telecommunications, life safety, facility management system and energy efficient and cost saving equipment [7]. Cyber physical system implemented in building for heating, ventilation and air conditioning system, light control system, fire alarm system, video surveillance system, and access control system. Implementation of Fully integrated cyber physical system in building achieves overall comfort level and energy consumption. Adding smart sensors, smart devices, smart meters, and smart alarming equipment's in building helpful to achieve performance and proper resource utilization.

Smart building is an attractive target for cyber attackers. In such types of building many applications are interconnected with each other for better services. So it is easy for attackers when distributed application interconnects with each other. Such types of system work with well-developed intranet but distributed nature creates open gate for attacker to steal information of different system and deactivate the system. Performing the Man in the middle attack provide easy access to unauthorized peoples in the system. Also Denial of service attacks creates problems in heating, ventilation and air conditioning system. these attacks possible due to negligence about sharing data of systems

F. Personal CPS

Personal CPS includes wearable devices such as smartwatch, toys, tracking tags, medical devices, fitness wearable devices etc. Attacks on these devices causes security and privacy issues. Personal information of users easily available for attacker through these Personal CPS devices.

VI. PROPOSED SYSTEM

The cyber Physical system consists of various low capacity devices (Microcontrollers and sensors) connected through wireless networks. The smart devices in the network must establish communication and functioning with adequate security. But due to resource constraints like low processing power, less energy and lower space there is a lack of standard security mechanism which can provide adequate security.

We proposed a new security algorithm for CPS. We try to develop a lightweight mechanism so it will helpful for low powered and memory based CPS devices. The proposed technique provides a key establishment algorithm for CPS. It provides solutions against various security attacks like man in the middle, replay and eavesdropping.

A. Key establishment Algorithm for CPS

The algorithm works in between cyber physical devices and microcontroller. Where following parameters used in the algorithm

GK- Gateway key
AK – Authentication Key
EK – Encryption Key
R1 , R2 – Random numbers
AT – Authentication token at cyber physical device
ST – Session Token at cyber physical device
AT1 – Authentication token at microcontroller
St1 – Session token at microcontroller
SK – Session Key

Common Parameters used at Cyber physical device and Microcontroller

GK = Gateway key
AK = Authentication key
EK = Encryption Key

Steps at Cyber Physical Device

Step 1: R1 is a random Number generated at cyber Physical device
Step 2: AT = HASH (GK||AK||R1)
Step 3: ST=EK(R1)
Step 4: Send generated value of AT and ST to Microcontroller

Steps at Microcontroller

Step 5: Extract value of R1 from ST=EK(R1)
Step 6: AT1=HASH(GK||AK||R1)
Step 7: Compare AT1=AT
Step 9: If value of AT1=AT is same then execute step no 10 else discard cyber physical device
Step 10: R2 is a random Number generated at microcontroller
Step 11: SK=HASH(GK||AT||R1||R2)
Step 12: ST1=EK(R2)
Step 13: Send ST1 value to smart device

Steps at Cyber Physical Device

Step 14: Extract value of R2 from ST1=EK(R2)
Step 15: SK=HASH(GK||AT||R1||R2)
Step 16: Value of SK at Cyber physical device and Microcontroller is same then Secure channel established between microcontroller and Cyber physical device

In above Key establishment algorithm GK, AK, EK these are the known keys available at microcontroller and cyber physical device. At cyber physical device with the help of random number R1 and hash function Authentication token (AT) and Session token (ST) generated. These values sent to the microcontroller. With the help of common values GK, EK, AK and ST send by the Cyber physical device value of R1 extracted. This value again used by a hash function to generate Authentication token (AT1) at microcontroller. If value of AT1 and AT both are same then partial authentication done at one side. Now at microcontroller Random number R2 and Hash function is used to generate a Session Key and session token(ST1). ST1 value sent to smart device. At Cyber physical device value of R2 is extracted and using hash function Session key(SK) is generated. If the value of SK at microcontroller and at cyber physical device both are same then successful two-way authentication done by using a key establishment algorithm.

B. Experimental Setup

A cyber physical system includes capabilities like sensing the physical world, make decisions (whether the switch is ON or OFF) and perform the actions in the physical world (ON or OFF the switch). Experimental setup to implement key establishment algorithm is shown in figure 4. We used basic equipment's which works on ON and OFF principle of working system. All these basic equipments connects with ESP 8266 WI-FI module. Through this Wi-Fi module all these devices connected to the microcontroller via router or access point.

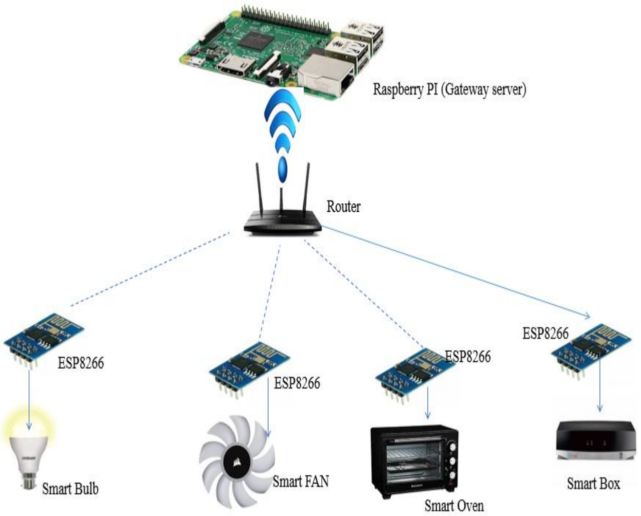

Figure 4: System Architecture of CPS

Devices mentioned as smart bulb, fan, Oven and set top box are becoming cyber physical devices because of ESP 8266 module connectivity. We use the Raspberry Pi B+ module as a microcontroller. Key establishment algorithm was implemented on above experimental setup. Which create a secure communication environment between microcontroller and cyber physical devices.

C. Results

At every communication session between microcontroller and cyber physical device new keys generated, if attacker got authentication or session token by attacking on microcontroller but during new session old key replaced by new one so old keys are not useful for attacker to perform attacks on cyber physical system. We tested this algorithm

D. System Analysis

Computational overhead is most important part for implementation of security algorithm in lightweight devices. Figure 5 shows performance time for advanced encryption standard (AES) and MD5. In figure performance time mentioned in milliseconds. Both these algorithms required less storage space on ROM and for execution on RAM compare to asymmetric algorithm. We used hash function, so we can say that it required very less storage space and low processing power for execution of algorithm. So algorithm mentioned in this paper can be suitable for small, tiny physical devices which works with low processing capabilities, less power and minimum storage.

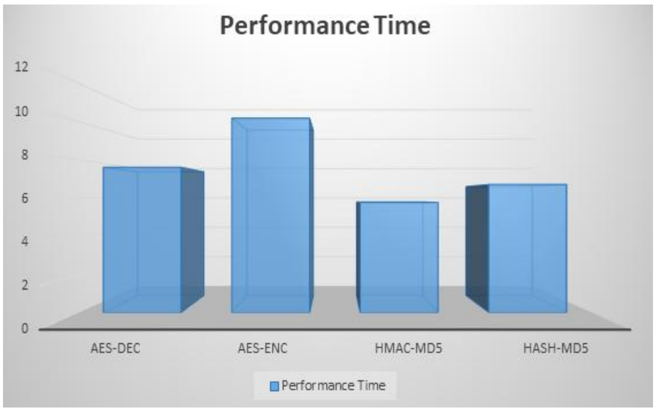

Figure 5: Performance time of different algorithms

VII. CONCLUSION

In this research paper, we gave brief overview of cyber physical system architecture. We also given detailed explanation about different attacks on CPS with attack points. In future Cyber physical system will be implement in every infrastructure. Many manual and offline system replaced by cyber physical system. But due to negligence of security many systems affected by cyber-attacks. Better security mechanism is need of CPS. We proposed Key establishment algorithm which generate new keys at every session of communication between cyber physical devices. Our proposed algorithm easily implemented on lightweight devices which has low processing capabilities, less memory and storage space. Due to new key generation at every session causes difficult for attacker to break security mechanism of cyber physical system. It is first lightweight key establishment algorithm which can be easy to implement on different cyber physical devices without modifying the structure of the system.

REFERENCES

1. Mehmet Hazar Cintuglu , Osama A. Mohammed , Kemal Akkaya , A. Selcuk Uluagac "A Survey on Smart Grid Cyber Physical System Testbeds" in IEEE Communications Surveys & Tutorials, Vol-19, Issue-1, 2017 DOI 10.1109/COMST.2016.2627399.
2. Fardin Abdi, Chien-Ying Chen, Monowar Hasan, Songran Liu, Sibin Mohan "Preserving Physical Safety Under Cyber Attacks" in IEEE Internet of Things Journal , volume: 6 , Issue: 4 , Aug. 2019, DOI: 10.1109/JIOT.2018.2889866

3. Bhujbal Yuvaradni, Darandale Dhanashri, Gunjal Sonali, Tekale Gauri, Sandip Thite "Health Monitoring Services Using Wireless Body Area Network" in Imperial Journal of Interdisciplinary Research (IJIR) VOL- 02, Issue -5, 2016.
4. S. Vanjale, P.B. Mane, S. Thite "Elimination of Rogue access point in Wireless Network", International Journal of Scientific & Engineering Research, Volume 4, Issue 12, December-2013
5. Y. Chen and B. Luo. S2a: Secure smart household appliances. Second ACM Conference on Data and Application Security and Privacy, pages 217–228, 2012.
6. Marilyn Wolf "Safety and Security in Cyber–Physical Systems and Internet-of-Things Systems" in Proceedings of the IEEE *Vol. 106, No. 1, January 2018*
7. Andrea Zanella, Lorenzo Vangelista, "Internet of Things for Smart Cities" in IEEE INTERNET OF THINGS JOURNAL, VOL. 1, NO. 1, Feb. 2014.
8. S. Vanjale, Sandip Thite, "A novel approach for fake access point detection and prevention in wireless network", International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), Vol 4, Issue 1, Feb 2014, 35-42
9. A. Y. Nur and M. E. Tozal, "Defending cyber-physical systems against dos attacks," in 2016 IEEE International Conference on Smart Computing (SMARTCOMP), May 2016, pp. 1–3
10. L. Pan, X. Zheng, H. Chen, T. Luan, H. Bootwala, and L. Batten, "Cyber security attacks to modern vehicular systems," Journal of Information Security and Applications, vol. 36, pp. 90–100, 2017..
11. Y. Chen, S. Kar, and J. M. Moura, "Dynamic attack detection in cyber physical systems with side initial state information," IEEE Transactions on Automatic Control, vol. 62, no. 9, pp. 4618–4624, 2017..
12. A. Ar, S. F. Oktu, and S. B. . Yaln, "Internet-of-things security: Denial of service attacks," in 2015 23nd Signal Processing and Communications Applications Conference (SIU), May 2015, pp. 903–906.
13. J. Wurm, Y. Jin, Y. Liu, S. Hu, K. Heffner, F. Rahman, and M. Tehranipoor, "Introduction to cyber-physical system security: A cross-layer perspective.".
14. Security and Privacy in Cyber Physical Systems, Foundations, principles and Applications, Wiley Publication, 2018

AUTHORS PROFILE

Sandip S. Thite is a PhD scholar in Bharati Vidyapeeth Deemed to be University Pune, Maharashtra, India. He is working as assistant Professor in Information Technology department of Bharati Vidyapeeths college of Engineering for Women Pune. His area of interest includes Computer Network, Internet of Things**.**

Prof. Dr. D. M. Thakore working as a Professor and Head of Computer Engineering department in Bharati Vidyapeeth Deemed to be University College of Engineering, Pune, India. He was awarded his Ph.D in Computer Engineering. He guided many project at under graduation and post-graduation level. He participated several seminars and conferences. His area of interest includes Internet of Things, Big Data, Machine Learning.