International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT

ELSEVIER
SSRN

IJIEMR Transactions, online available on 26th Dec 2022. Link :http://www.ijiemr.org/downloads.php?vol=Volume-11&issue=Issue12

10.48047/IJIEMR/V11/ISSUE 12/228

TITLE: A STDY OF CYBER PHYSICAL SYSTEM FOR IMPLEMENT SECURITY MECHANISM

Volume 11, ISSUE 12, Pages: 1740-1749

Paper Authors **MATTIGUNTA CHIRANJEEVEI, DR. RAJEEV YADAV**

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

A STDY OF CYBER PHYSICAL SYSTEM FOR IMPLEMENT SECURITY MECHANISM

MATTIGUNTA CHIRANJEEVEI, DR. RAJEEV YADAV

DESIGNATION- RESEARCH SCHOLAR MONAD UNIVERSITY HAPUR U.P
DESIGNATION- (PROFESSOR) MONAD UNIVERSITY HAPUR U.P

ABSTRACT

A lightweight approach for authenticating cyber-physical objects is one of the expected outcomes. Trustworthy, private, and data-protecting security algorithm for cyber-physical systems that doesn't compromise on flexibility or independence of operation. An advanced middleware component for the Raspberry platform to facilitate communication between CPS-based devices and services, ensuring dynamism and scalability. Secure IoT evaluation framework that may be used in a variety of contexts and is focused on the end user. The suggested technique will allow the two CPS devices to authenticate each other. The proposed technique should have low computational costs and excellent effectiveness. To protect wireless transmissions, it creates random session keys. It provides protection for the system against a wide variety of cyber threats. The current constraint-based CPS system requires a new lightweight security solution.

KEYWORDS: CPS devices, middleware component, data-protecting, security algorithm, cyber-physical systems

INTRODUCTION

CPS was made possible by the pervasive influence of the internet and telecommunications on industries as diverse as manufacturing and the hard sciences. Electrical gadgets from earlier generations often had automatic mechanisms. However, with CPS in place, these mechanisms are now responsive and outcome-focused. It also links up to the web, so it can be used to stay in touch with gadgets anywhere and at any time. Take, for example, a smart home system in which the air conditioners function automatically based on the ambient temperature. It can not only sense the temperature of its surroundings, but also identify human-made items and track human movement. After processing the information, it sets the thermostat to a pleasant temperature. Because of this, the system becomes more adaptive and can make decisions on the go.

"Intelligent and transparent interactivity between things, the physical environment, and people in order to effortlessly transfer data and deliver new applications to users" is how the CPS is described. A few trillion dollars in revenue will be created across a wide range of sectors due to the rapid expansion in the use of connected devices in India, including automotive, utilities, grid computing, smart cities, healthcare, and transportation. CPS has been identified by many nations as a vital engineering and technology for their future economic growth. The European Union (EU) is investing over 100 million euros in numerous connected device projects through the Seventh EU Framework Programme. These devices will be actively deployed in a variety of settings, including healthcare, intelligent transportation, the grid, cities, and utilities. Smart cities, a revamped healthcare system, and advanced transportation are just a few of the CPS-based initiatives India has launched recently. The Indian government has unveiled the Smart Cities and Comprehensive Public Sector Modernization Program. The plan details both immediate and far-off targets for growth, as well as potential avenues for getting there. A schedule for implementation is also included in the plan.

CURRENT TRENDS IN CYBER PHYSICAL SYSTEM

CPS is useful in a wide variety of contexts because of its features. Features such as location and information sensing, information exchange, sensing and monitoring of the physical environment, remote control and handling, self-organizing capabilities, etc.

As many major nations embark on IoT-based projects to better people's lives and enhance their quality of life, the global market is ripe with possibilities for CPS. The demand for CPS programs has grown as a result of civil society's progress toward modernity. These days, CPS can be found in a wide variety of applications, from smart home systems and healthcare to electric vehicles and government infrastructure. 2015 marks the beginning of the smart cities project in India. Smart cities are gaining popularity in many parts of the world. Several nations have already launched smart city initiatives. There will be over twenty "smart cities" in India. The Internet of Things (IoT) market is predicted to be worth several trillion dollars by 2020 (Smartcities.gov.in, 2020) due to rising demand for IoT applications including "Smart Governance," "Smart Healthcare," "Smart Homes," "Smart Mobility," and "Smart Environment." Concerns over security (including privacy, authenticity, and access control) and a lack of interoperability across the many technologies currently employed in cities and urban developments are two of the most urgent technical difficulties relating to the deployment of CPS initiatives in future smart cities.

1. Cyber Physical System for Next Generation network

The acronym NGN refers to the next generation of networks in the field of communications and computer networking. Voice, audio, video, and data are just some of the many services that may be transmitted via this method. NGN uses a layered design that is shared throughout wired and wireless networks. Packer-based network layers are always used for communication. Wired and wireless networks are used in CPS infrastructure. It works with any type of 5G network. A SHS that allows for the usage of audio and video services in the home. Where next-generation networks include CPS-based smart home systems.

2. Cyber Physical System based Application

Intelligent house setup It's a widely used program all across the globe. With the help of IT, comms, and electronics, more and more houses are being upgraded to "smart" status. Smart home system (SHS) use and innovation are continuously on the rise. It consists of a network of interconnected smart appliances that can be remotely managed and monitored. In terms of storage space, computing power, and battery life, smart devices are among the worst offenders. Signals or instructions will be sent to carry out the specified action. It improves safety and comfort while decreasing operational costs. A plethora of new companies are working on Smart home software. The market is hot, and there is a lot to learn about it. A high-tech dwelling is a significant lifeline for the elderly. The freedom it grants them is crucial. Different types of smart devices are used in this scenario, such as sensors, actuators, smart lights, smart fans, etc.

3. Aspects of the Cyber Physical System that present an opportunity

It is possible to devote a lot of resources to studying the Cyber Physical System and investing heavily in its commercialization. As a result of the proliferation of "Smart Cities" and "Smart Homes," an enormous network of billions of interconnected "Things" will be established. CPS applications bridge the gap between the real and the digital by integrating disparate technologies and data sources. It will rely heavily on a wide range of connected device apps, services, business software components, and objects that will be employed in novel ways in the future to accomplish its aims.

4. Existing CPS Protocols

The Cyber Physical System can't function without universally accepted protocols. Researchers in both the private sector and the academic world are trying to perfect CPS-based protocols. There are already many protocols available for secure communication amongst CPS devices. For low-powered CPS gadgets, CoAP and MQTT are the best bets for communication protocols.

Protocols like CoAP and MQTT are open standards. They find usage in limited contexts. Communication tools are a part of it. Both are fully operational and make use of the Internet Protocol. Multiple options for implementation are made available. Reference: (Zahed et al., 2019) Datagram Transport Layer Security (DTLS) is another protocol that is compatible with CoAP. for which the transport layer is responsible. It uses the 6LoWPAN standard in conjunction with a header compression method to cut down on power consumption. 6LoWPAN makes it possible to send IPv6 data over a wireless network. By adhering to its standards, DTLS lessens the amount of data transmitted.

5. Weak Protocols

Records that are insecure due of insecure protocols IOActive's Lucas Lundgren conducted a global web scan of unsecured MQTT endpoints in 2016 and 2017 and found an obvious implementation flaw affecting tens of thousands of nodes. (www.trendmicro.com) The lack of safe setups and the danger of misconfigurations in MQTT-enabled home devices was also highlighted in a smart-home-centric MQTT study published by Avast (blog.avast.com, n.d.). They choose to look into the same issue and incorporate CoAP into their analysis. They were shocked to learn that hundreds of thousands of MQTT and CoAP hosts are accessible via publicly-accessible IP addresses. This gives the bad guys access to millions of sensitive files. Vulnerable endpoints can be found in almost any country thanks to the open nature of the protocols and publicly searchable deployments.

CPS Applications with Security issues

Many CPS-based applications raise serious security concerns, as revealed by key research topics. Various networks, standalone desktop computers, internet services, and cloud security can all take advantage of the many existing security methods. These preexisting systems perform admirably across multiple environments. The following example demonstrates security vulnerabilities in CPS system application domains. Researchers are inspired to improve the security of CPS Applications by these issues.

A. A system of Home Automation

Sensor, microcontroller, and Wi-Fi modules like the ESP 8266 and ESP 32 are integrated into preexisting home automation systems, transforming them into "smart" devices that allow us to remotely monitor and manage our homes' physical infrastructure. A microcontroller plus a WiFi module can be used to automate a wide variety of ON/OFF-controlled home appliances and fixtures. A rise in the use of cyber-physical systems at home, leading to more automated, energy-saving gadgets.

The more connected gadgets there are in a home, the more entry points there are to hack into. These supplementary entryways provide burglars with more options to gain access to the dwelling. A malicious actor can plant a fake access point in a home network, fooling any smart devices it is used with into thinking they are using a legitimate connection. Attacks launched from a rouge access point can compromise the security of your smart home or cause individual devices to stop working.

B. Medical care system

Patient treatment times are longer in the traditional healthcare system because of the reliance on manual monitoring equipment. As part of the cyber physical system, smart gadgets based on sensors and microcontrollers are used to keep tabs on a person around the clock. These gadgets can not only analyze and send data, but also collect data from the human body. Both doctors and patients can benefit greatly from these cutting-edge technical advancements in the healthcare system. In a Cyber physical system, the patient's health is constantly tracked by high-tech gadgets. Doctors may check in on their patients from wherever they happen to be using these internet-connected devices. Using CPS, patients can be monitored remotely, cutting down on hospital visits and associated costs.

The most effective method for tracking a patient's health in a hospital or clinic is a wireless body area network (WBAN). Attackers can use both physical and digital means to disrupt the system, putting the patient's life in peril. The compromised medical records, including those of patients, are accessible to the hacker.

C. Smart Cities Using a Cyber-Physical System

Various terms, including "digital city," "intelligent city," and "connected city," describe this emerging concept of "smart city." A smart city is a community that has made concerted efforts to transition to a digital lifestyle by utilizing cyber physical technologies. Growing cities need to be built with people's comfort and good living standards in mind because of the influx of people from the countryside. Cyber physical systems, which include everything from the household to public transportation, smart mobility, and smart government, all contribute to the success of smart cities. This is only achievable with a greater incorporation of cyber-physical devices into urban planning and development.

He sought to implement both physical and cyber-attacks on smart city initiatives, revealing the vulnerabilities that can be exploited by attackers. The lives of individuals in smart cities are profoundly affected by these kinds of attacks. Putting Together a "Smart City"

Utilizing a WSN, or Wireless Sensor Network. When the WSN is attacked, it disrupts services for everyone.

Citizens' regular routines could be disrupted if essential services go down. Disruption that lasts for a long time might have terrible results. Disruptions in the form of broken traffic signals, faulty water and power distribution systems, malfunctioning closed-circuit television, etc. Attacks can lead to a variety of issues, including privacy breaches, property destruction, and disruptions in transportation.

D. Intelligent Grid

A future power grid system that utilizes information and communication technology to reliably and efficiently supply energy is called an intelligent grid system. The performance and efficiency of energy resources can both be increased through the integration of a cyber physical system into a grid. The cyber physical system manages the operations, ensures that all the pieces of machinery work together, and estimates how long they will last. Cyber-physical systems make it easy to analyze both system and performance.

Algorithms are used in intelligent grids to further automate the infrastructure. A PLC controller or wireless sensor node provides an entry point for attackers to compromise the system and launch a computational algorithm attack, which could have severe consequences for the grid project. There could be a power outage, for instance.

E. Intelligent Construction

Building automation, communications, life safety, a facility management system, and energy-efficient, cost-cutting equipment are all components of a building's cyber physical system. A building's HVAC, lighting, fire alarm, video surveillance, and access control systems can all be managed by a central computer via a cyber physical system. A building's comfort and energy efficiency can both be improved by installing a cyber-physical system. In order to maximize productivity and efficiency within the structure, smart sensors, smart gadgets, smart meters, and smart alarming equipment must be implemented.

Cybercriminals find smart buildings to be an alluring target. Better services may be provided to tenants of these buildings thanks to the integration of numerous applications. Therefore, when distributed applications interact with one another, attackers have an easier time. These systems make advantage of an advanced intranet, but their decentralized architecture makes them vulnerable to data theft and compromise. Through a Man in the Middle attack, hackers can easily obtain access to the system. The HVAC system is particularly vulnerable to Distributed Denial of Service assaults. Lack of information sharing makes these kinds of attacks conceivable.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

F. Individual CPS

Smartwatches, toys, tracking tags, medical equipment, fitness wearables, and so on are all examples of personal CPS devices. Markets, warehouses, restaurants, and highways are all possible destinations for these gadgets to exchange data with. There are security and privacy issues associated with attacks on these devices. The data stored on these Personal CPS devices is easily accessible to attackers.

CONCLUSION

While there is little doubt that CPS has the potential to greatly enhance services in everyday life, its adoption has been impeded by many security concerns. CPS architecture and application development must incorporate security features to prevent national-level disasters or data breaches. Seventy percent or more of the data in a CPS application can be compromised in some way. This is cause for concern and highlights the need for further investigation into security procedures tailored specifically for CPS equipment. The most common security flaws were related to data privacy issues, insufficient authentication techniques, weak authorization mechanisms, a lack of end-to-end security measures, exposed user interfaces, and a lack of security rules. Due to their restricted functionality, these gadgets feature weak hardware. Some of the most crucial parts of these gadgets are the processor, storage, and backup battery. The safety of such an app would be compromised. It has so little processing power, storage space, and energy backup that we couldn't even try to install and configure modern security methods in it. There is a lot of effort being put into finding solutions that are both lightweight and secure for constraint-based devices.

REFERENCES

Friedberg, I. *et al.* (2017) ‘STPA-SafeSec: Safety and security analysis for cyber-physical systems’, *Journal of Information Security and Applications*, 34, pp. 183–196. doi: 10.1016/j.jisa.2016.05.008.

Frustaci, M. *et al.* (2018) ‘Evaluating critical security issues of the IoT world: Present and future challenges’, *IEEE Internet of Things Journal*, 5(4), pp. 2483–2495. doi: 10.1109/JIOT.2017.2767291.

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

Granjal, J., Monteiro, E. and Silva, J. S. (2015) 'Security for the Internet of Things : A Survey of Existing Protocols and Open Research Issues', 17(3), pp. 1294–1312.

Guillet, S., Bouchard, B. and Bouzouane, A. (2013) 'Correct by construction security approach to design fault tolerant smart homes for disabled people', *Procedia Computer Science*, 21, pp. 257–264. doi: 10.1016/j.procs.2013.09.034.

Hammi, M. T. *et al.* (2014) 'A Lightweight IoT Security Protocol', pp. 1–8.

Hou, I. *et al.* (2012) 'Challenges of Cyberphysical systems', pp. 1–30.

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

Humayed, A. *et al.* (2017) 'Cyber-Physical Systems Security - A Survey', *IEEE Internet of Things Journal*, 4(6), pp. 1802–1831. doi: 10.1109/JIOT.2017.2703172.

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.

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.

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

Kim, B., Yoon, S., Kang, Y. and Choi, D. (2020). Secure IoT Device Authentication Scheme using Key Hiding Technology. 2020 International Conference on Information and Communication Technology Convergence (ICTC).

Kim, K. D. and Kumar, P. R. (2013) 'An overview and some challenges in cyber-physical systems', *Journal of the Indian Institute of Science*, pp. 341–352.

Kim, N. Y. *et al.* (2018) 'A survey on Cyber Physical System security for IoT: Issues, challenges, threats, solutions', *Journal of Information Processing Systems*, 14(6), pp. 1361–1384. doi: 10.3745/JIPS.03.0105.

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.