Real-Time Applications of Machine Learning in Cyber-Physical Systems

Balamurugan Easwaran
University of Africa, Toru-Orua, Nigeria

Kamal Kant Hiran
Sir Padampat Singhania University, India

Sangeetha Krishnan
University of Africa, Toru-Orua, Nigeria

Ruchi Doshi
Azteca University, Mexico

A volume in the Advances in Computational Intelligence and Robotics (ACIR) Book Series

IGI Global
PUBLISHER of TIMELY KNOWLEDGE

Published in the United States of America by
IGI Global
Engineering Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Names: Easwaran, Balamurugan, 1975- editor.
Title: Real-time applications of machine learning in cyber physical systems / Balamurugan Easwaran, Kamal Hiran, Sangeetha Krishnan, and Ruchi Doshi, editors.
Description: Hershey, PA : Engineering Science Reference, an imprint of IGI Global, [2022] | Includes bibliographical references and index.
Identifiers: LCCN 2021043068 (print) | LCCN 2021043069 (ebook) | ISBN 9781799893103 (ebook) | ISBN 9781799893080 (h/c)
Subjects: LCSH: Electronic security systems. | Medical informatics. | Agriculture--Decision making--Data processing. | Cooperating objects (Computer systems) | Machine learning--Industrial applications.
Classification: LCC TH9737 (ebook) | LCC TH9737 .H36 2022 (print) | DDC 621.389/28 23/eng/20211--dc27
LC record available at https://lccn.loc.gov/2021043068

This book is published in the IGI Global book series Advances in Computational Intelligence and Robotics (ACIR) (ISSN: 2327-0411; eISSN: 2327-042X)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 4
Differential Privacy Techniques-Based Information Security for Cyber Physical System Applications: An Overview

A. Kanagaraj
Nallamuthu Gounder Mahalingam College, India

S. Sharmila
Nallamuthu Gounder Mahalingam College, India

A. Finny Belwin
Angappa College of Arts and Science, India

A. Linda Sherin
A. M. Jain College, India

Antony Selvadoss Thanamani
Nallamuthu Gounder Mahalingam College, India

ABSTRACT

A cyber physical system (CPS) is a mechanism that monitors and controls entire devices which are connected together. Secured data transmission in CPS systems is a major problem. To provide information security for CPS applications, certain privacy preservation strategies need to be followed. Encryption and anonymization are existing traditional privacy preservation techniques which are not suitable to provide information security for advanced systems called CPS. Differential techniques is an emerging privacy technique where a required amount of noise is added using various mathematical algorithms with data while sharing information between devices in CPSs. The process of adding noise with data is called data perturbation. There

DOI: 10.4018/978-1-7998-9308-0.ch004

are three major data perturbations mechanisms followed to provide information security. They are exponential mechanism, Laplace mechanism, and Gaussian mechanism. This chapter presents a detailed review about applications of CPSs, significance of implementing differential privacy techniques, challenges, and future research directions of CPSs.

INTRODUCTION

The research on Cyber-Physical Systems (CPS) has recently becomes broad impact on society, economics and the environment. Differential privacy is currently emerging as a future of privacy. Differential privacy safeguards statistical or real-time data by introducing a desired level of noise while maintaining a good balance between privacy and accuracy. In differential privacy, the user can select the level of privacy or distinguishability, resulting in the maximum feasible privacy protection for any individual in the dataset. Over the last ten years, improvements in CPSs have attracted a lot of interest. The dual character of CPSs, by which they blend the dynamic properties of embedded computers with those of information and communication technologies, is the primary reason for this enormous interest (ICT).

To protect data privacy, a number of researchers suggested cryptographic methods. Many cryptographic algorithms are computationally costly because of the users need to maintain large number of encryption keys. When public data sharing is required, maintaining privacy also becomes more difficult. Researchers have also proposed anonymization techniques such as k-anonymity to address privacy concerns. However, because the chance of re-identification increases as the amount of attributes in the dataset grows, this anonymization technique does not ensure perfect security against adversaries. Differential privacy is currently gaining traction as a potential future of privacy. Even though security and privacy are the primary difficulties of modern technology, privacy and security issues influence cyber-physical systems. This chapter provides suggestions and solutions for CPS's security issues.

BACKGROUND

CPS refers to a group of interconnected systems that can monitor and manipulate real-world objects and processes. CPS focuses on the interplay of physical, networking, and compute processes. As a result of their integration with IoT, a new CPS element, the Internet of Cyber-Physical Things, has emerged (IoCPT).In this paper, the main characteristics of CPS, as well as the related applications, technology, and standards, are discussed (Jean-Paul A. Yaacoub, 2020). Furthermore, CPS security

vulnerabilities, threats, and attacks are examined, as well as major difficulties and challenges. In addition, existing security methods are given and examined, with their primary weaknesses identified. Finally, based on the lessons learnt throughout this exhaustive examination, various suggestions and recommendations are made. Because of complex cybernetics and the interplay of (independent) CPS domains, the exponential expansion of cyber-physical systems (CPS) has created various security vulnerabilities, particularly in safety-critical applications. (Muhammad Shafique, 2018) presents a concise but thorough overview of current static and adaptive detection and prevention strategies, as well as their inherent shortcomings, such as the inability to detect latent or uncertainty-based runtime security assaults. This study also presents intelligent security methods against many described attacks on different tiers of the CPS stack to meet these problems.

CPS are employed in a variety of industries to provide for process optimization and previously unattainable capabilities (Muhammad Shafique, 2018). The inherent properties of networked digital systems and analogue physical processes influence how security theory is used. As a result, security and privacy are important considerations in the design, development, and operation of CPSs. (Glenn A. Fink, 2018) explain how CPS security and privacy differ from that of pure cyber or physical systems, as well as what may be done to make these systems safer. The purpose is to assist young CPS designers in creating more secure, privacy-enhancing products in the future.CPS are cyber-physical systems that interact in a feedback loop with the help of human intervention, interaction, and utilization. As the foundation for developing and future smart services, these systems will empower the essential infrastructure and have the potential to have a substantial impact on daily life. The rising usage of CPS, on the other hand, introduces new hazards that could have serious ramifications for users. New dangers and cyber-attacks will continue to be exploited, necessitating the development of new strategies to defend CPS.(Yosef Ashibani, 2017) gave an examination of security challenges at various layers of the CPS architecture, risk assessment, and approaches for securing CPS. Finally, the obstacles, prospective study areas, and potential solutions are given and addressed.

A complete study of differential privacy approaches for CPSs is presented in (Muneeb Ul Hassan, 2019). The authors look at how differential privacy is used and implemented in four important CPS applications: energy systems, transportation systems, healthcare and medical systems, and the industrial Internet of things (IIoT). This chapter also discusses unresolved concerns, challenges, and future research directions for CPS differential privacy approaches. This study can be used to help develop new differential privacy strategies that can be used to handle a variety of CPS difficulties and data privacy scenarios. Using the VERIS Community Database, (Steven Walker Roberts, 2020) explores the risk spectrum of a cyber security incident occurring in the cyber-physical-enabled environment. The bulk of known perpetrators

were from the United States and Russia, the majority of victims were from western countries, and geographic origin tended to follow global events, according to the research. Information was the most often targeted asset, with the bulk of attack techniques focusing on privilege misuse. This demonstrates the critical necessity for a significant re-evaluation of cyber security's core ideas.

CYBER PHYSICAL SYSTEM

Cyber physical systems are a new type of time-critical and safety-critical real-time embedded systems that have a strong interaction between computing and communication in order to regulate the vast and complicated global world. The challenges of scientific, social, and technical problems have an impact on the cyber physical system. The following sections discuss about cyber physical systems in detail.

CPS Layers

The architecture of CPS systems is made up of various layers and components that communicate with one another using various communication protocols and technologies. The perception layer, transmission layer, and application layer are the three main layers of the CPS architecture. Sensors, actuators, aggregators, Radio-Frequency Identification (RFID) tags, Global Positioning Systems (GPS), and other devices are all part of the perception layer. In order to monitor, track, and understand the physical world, these gadgets acquire real-time data. Between the perception and application levels, the Transmission Layer exchanges and processes data. Local Area Networks (LANs) and communication protocols are used to transmit and interact data over the Internet. This layer also ensures data routing and transmission over cloud computing platforms, routing devices, switching and internet Gateways, firewalls, and intrusion detection and prevention systems (Jean-Paul A. Yaacoub, 2020).The application layer interprets the data received from the data transmission layer and sends commands to the physical devices, such as sensors and actuators. This is accomplished through the use of complex decision-making algorithms based on aggregated data. Furthermore, before deciding the appropriate automated actions, this layer receives and processes information from the perception layer.

Components

CPS components can be used to detect information or regulate signals. Sensing Components (SC) collect and detect data, and Controlling Components (CC) monitor and control signals, are the two basic categories of CPS components.

Sensors capture and record real-world data using a correlation process known as "calibration" to ensure that the data collected is accurate. Data sensing is critical since judgments will be made based on the analysis of this data. Aggregators are typically found at the transmission layer, where they evaluate sensor input before issuing the appropriate decision.

Data aggregation, in reality, is based on the gathered information on a certain goal, which is gathered and summarized after a statistical analysis. Actuators are positioned at the application layer and are responsible for making information visible to the surrounding environment based on the aggregators' judgments. Because actuators are so reliant on other network nodes, each action taken by the CPS is dependent on a previous data aggregation process. Actuators also process electrical signals in terms of operations (Jean-Paul A. Yaacoub, 2020). Signal Controlling Components are used to control signals and play an important role in signal control, monitoring, and management in order to obtain greater levels of accuracy and protection from intentional attacks or accidents, such as signal jamming, noise, and interference.

Characteristics of CPS

CPS is a self-organizing and reconfiguring control system with a high degree of automation, complexity at many spatial and temporal scales, and closed control loops at all scales. Embedded systems, real-time systems, (wired and wireless) networking, and control theory are all represented by CPS. Because many of the computers engaging directly with the real world perform only a few specialized operations, they do not require the general computational capacity of traditional computers or even mobile systems, and hence have limited resources. The time it takes to perform computations in safety-critical systems is critical in ensuring the system's correctness. Developers can use real-time programming languages to specify timing requirements for their systems, and Real-Time Operating Systems guarantee the time it takes for an application to accept and complete a task. Another feature of CPSs is that they communicate with one another, which is increasingly done using IP-compatible networks. Wireless networks are a common feature of CPS as well. The task at hand is to construct networks on top of low-powered, lossy wireless communications. Control theory aims to use differential equations to characterize a physical process and then develop a controller that meets a set of desired properties such as stability and efficiency.

CPSS Security

In the physical layer, an attacker might intervene directly or destroy the physical objects that are being monitored and controlled, such as sensors and controllers,

resulting in false sensed measurements, incorrect control decisions, and improper actuator movements. In the sensor or actuator layer, an attacker can use brute force attacks to destroy or hack the sensors or actuators in order to collect critical information and modify them. An attacker can use the power distribution mechanisms of sensors and actuators to drain energy for denial-of-service attacks or to activate malicious circuitry with that energy (Yosef Ashibani, 2017).The network layer of CPS has security vulnerabilities connected to communications. Networking attacks are divided into two categories: replay attacks and denial of service attacks. Because control mechanisms are heavily dependent on timeliness, desynchronization is a common security problem in the control layer of CPS. As a result, even a minor desynchronization in the control signals might be regarded disastrous, as wrong judgments can result in CPS failures. The majority of attacks at the information layer steal information through eavesdropping or analyzing traffic data. Manipulation of key information, on the other hand, can be used to carry out various attacks such as jamming, collision, denial of service, and so on.

Applications of CPS

A cyber physical system can be used in a variety of situations. The following sections describes some of the applications of CPSs. Medical gadgets for patient diagnosis, monitoring, and treatment, such as x-ray machines, magnetic resonance imaging (MRI), surgery, and other medical instruments, have all benefited from technological advancements. With limited computational capability, communication complexity, and battery life, health-care-related CPS in the areas of implantable medical devices, body area networks, and wearable devices necessitates privacy, security, and trust. One of the newer fields of CPSs is intelligent transportation systems (ITSs) (D. Li, Q. Yang. 2017).

ITSs are concerned with the development of traffic systems, automobiles, mass transit, and other comparable variables in order to improve efficiency, congestion, sustainability, and safety (M. Gohar, 2018). Cyber-systems, such as communication networks, control automation systems and centres, and Intelligent Electronic Devices, are installed in power grid components (A. V. Kayem 2017). Smart grids are described as next-generation infrastructure capable of handling all of the energy and environmental needs by supplying with reliable, cost-effective, and environmentally friendly electricity.

Unfortunately, despite its importance, smart house cyber security, which is a key part of smart home system research, is understudied. Security issues in smart homes are addressed at both the system and device levels. Smart city applications are intended to manage urban traffic and provide real-time responses to concerns such as energy efficiency, demand-side response, and energy management. The term

"smart city" covers a wide range of topics, including "smart" power, "smart" grid systems, "smart" environment, "smart" transportation, "smart" homes, and "smart" management. (M.-C. Chuang, 2011)

One of the most significant advantages of smart metering is precise bill calculation in a dynamic pricing system (D. Alahakoon, 2016) This pricing strategy necessitates detailed energy consumption data, which, on the other hand, may expose smart meter users' personal information. As a result, researchers face a hurdle in providing differential privacy alongside correct dynamic pricing billing. Many scholars are working on efficient algorithms to overcome this trade-off to the greatest extent possible. Industrial IoT systems have unique needs, including as operation in hostile environments, predictable throughput, maintenance by people other than communication experts, and extremely low downtown. Differential privacy is a new standard for protecting IIoT systems' privacy. Differential privacy defines a detailed attack model, decreases data exposure privacy threats, and ensures data availability at the same time as the query or decision.

CPS THREATS AND ATTACKS

Adversaries are always attempting to breach critical systems in order to gain total or partial access to data. The adversary can recognize the defined list of receivers based on observed traffic in a disclosure attack, which is a traffic pattern analysis attack (Muneeb Ul Hassan, 2019). Adversaries employ this attack approach to identify and compromise a specific receiver's communication. The linking attack is a sort of assault in which external data is coupled with anonymized or protected data in order to derive essential information. To avoid any privacy violations, direct requests regarding any individual are normally banned throughout a query assessment.

A differencing assault is a type of attack like this (Steven Walker-Roberts, 2020). Strong correlation may occur in real-world data, such as shared relationships and family members sharing attributes in various social networking datasets, when using correlation attacks. If an adversary attempts a correlation attack with similar datasets, the existing correlation may result in the revelation of more information than planned. A privacy-preserving system with efficient data handling is necessary to prevent correlation attacks, which decreases the danger of information leaking even in the case of public query evaluation (P. L. Ambassa, 2018).

CPS SECURITY SOLUTIONS AND RECOMMENDATIONS

With the rising use of CPS in many critical domains, security has become a pressing concern, necessitating a thorough risk assessment. With so much reliance on the Internet, the security focus of risk assessment has shifted from computer risk assessment to network risk assessment (enn A. Fink, 2018). The purpose of assessing CPS security is to create a quantifiable risk that can be used to defend future systems. When assessing CPS risk, three factors should be considered: asset identification, threat identification, and vulnerability identification.

Asset identification refers to a resource value that must be preserved, which can be either tangible or immaterial. In truth, the majority of assets are intangible; as a result, assets have a direct value in many daily transactions and services and should be safeguarded. Asset quantification can also be assessed using direct and indirect economic losses and the resulting losses. Threat identification is used to assist in identifying threats that are of high priority concern in the field of CPS, which is a difficult task. Historical data can be utilised to quantify the threat's frequency, whereas sampling records and logs from the Intrusion Detection System (IDS) can be used to determine the risk's frequency, among other things.

DIFFERENTIAL PRIVACY

Differential privacy can save a significant amount of data from both databases and real-time data. The bulk of differential privacy techniques use data disruption. In data perturbation, the amount of noise is determined using differential privacy techniques, then added to the query data to make it secure and unrecognizable to the observer. This disturbance has a direct impact on the data reporting accuracy. The more perturbed data, on the other hand, ensures that privacy is well maintained. As a result, while adopting differential privacy, it's important to strike a balance between accuracy and privacy. Because of this trade-off between privacy and accuracy, implementing differentiated privacy in CPSs is a difficult issue, as many CPSs applications, such as health care and medical systems, require accurate data reporting.

To date, researchers have developed a variety of privacy preservation solutions to combat distinct privacy threats. Because it provides the property of data inaccessibility to unauthorized users, encryption is one of the conventional privacy-preserving techniques employed by the majority of systems to secure data from adversaries and unauthorized users. Because of the sensors' limited computer capacity, encryption can only be used sparingly in current CPSs. The production and distribution of public and private keys in public key cryptography, also known as asymmetric

cryptography, is a computationally expensive job that cannot easily be carried out with small devices with minimal resources.

Furthermore, any weakness can utilize multiple methods, such as a brute-force assault, against the encrypted CPS data. Similarly, encryption schemes in a network of numerous sensors necessitate the interconnection of each node for the production and transmission of private keys in the network. As a result, if one node in a network of n nodes fails, decryption and data gathering from CPSs nodes becomes almost impossible due to the lack of keys in the network. Furthermore, by altering the noise addition parameter in differential privacy, CPSs users can control the level of privacy according to their needs. Three major data perturbation mechanisms are the Laplace mechanism, Gaussian mechanism and Exponential mechanism.

FUTURE RESEARCH DIRECTIONS

Because of the dynamic nature of CPSs, differential privacy implementation in cyber physical systems is now confronting a variety of obstacles. Some of the CPS research challenges are:

- The smart grid is the future of energy systems, because it incorporates capabilities of both; traditional energy systems and modern information and communication technologies. This pricing model necessitates thorough energy use data, which, on the other side, may expose smart metre customers' personal information. As a result, researchers face a hurdle in providing differential privacy alongside correct dynamic pricing billing.
- Small wind turbines and solar panels will be used to power most of these energy sources in smart houses. Some smart homes may sell surplus energy to other purchasers; they can auction this energy, and buyers can purchase it based on their needs. The buyer and seller, on the other hand, usually do not want to reveal their identities to each other during this procedure. As a result, preserving this data is critical for the proper operation of the smart grid's auction mechanism.
- Smart meters are often controlled by programming that determines all of their functions. This firmware is often generated by smart meter vendors, who then update it to improve functionality or fix any bugs that are discovered. When only a subset of smart meters needs to be updated rather than all of them, the utility may require case access control. However, specific security and privacy-based methods are required to protect this firmware file.
- Micro-grid resource restricted designs are the best option for a cost-effective supply and power management solution in remote places. Certain lossy

networks are utilized to communicate across these resource restricted systems in order to reduce operational costs. Due to their unstable nature, these lossy networks are vulnerable to a variety of adversaries and privacy assaults. This invasion of privacy can lead to a variety of crimes, such as energy theft.

- A smart city requires a smart transportation system. Route planning applications frequently incorporate real-time traffic data. If the network is open, any intruder can gain access to the live location monitoring of connected cars by hacking the system of these applications. Differential privacy can give real-time location privacy by disrupting location or identity to protect the privacy of drivers.
- V2V (vehicle-to-vehicle) communication is becoming increasingly prevalent. Certain privacy and security concerns with V2V communication have surfaced in recent years. Differential privacy may be the best approach for maintaining privacy in communication between two vehicles.
- In the healthcare and medical system, the trend of integrating the online and physical worlds has exploded. With the evolution of wireless technologies, the use of body sensors for medical applications is becoming more popular. These sensors keep track of your current data and send them to your doctor or trainer. One solution for this type of application is encryption, however it is computationally difficult. Differential privacy-based real-time data reporting, on the other hand, may be a lightweight solution to this challenge.
- Retirement homes and elderly homes demand special attention because the residents require round-the-clock care and attention. Protecting electronic patient records, which contain all useful information, identification, and medical records of persons residing in that home, is one of the potential applications of differentiated privacy in elderly homes.
- Modern IoT technologies have a significant impact on industry advancements. These malicious adversaries can also control machinery, or can even destroy industrial systems. As a result, key IIoT sectors must be secured initially in order for IoT systems in industry to work smoothly.
- One of the most difficult aspects of differentiated privacy is identifying the exact privacy. Even with mathematical proofs and a rigid privacy model in place, differential privacy falls short of providing an intelligible notion of privacy in the context of massive data. The problem of calculating the optimal composition of differential privacy in big data analytics is yet unsolved. Similarly, ensuring privacy protection while also dealing with the issue of dimensionality as a result of enormous data volumes and computing overhead is a major difficulty for researchers in the field of big data.

- Any machine learning algorithm's main goal is to extract useful information from given data. However, one of the most difficult tasks for future machine learning algorithms is maintaining individual privacy while harvesting data.
- The massive volume of data generated by pervasive connection among smart gadgets paved the way for cloud computing, a reliable and secure storage system. Outsourcing this information to a third party may result in privacy concerns. Information redundancy in big data from various sources, multi-tenancy, and ubiquitous access aspects of cloud computing platforms are all factors that contribute to these privacy concerns. Differential privacy is currently gaining traction as a viable solution to the privacy challenges that cloud computing presents. Researchers have begun work on preserving the privacy of cloud computing data by employing differential privacy.
- A substantial amount of private data is stored in wireless edge computing networks and cannot be supplied directly for data prediction and processing. As a result, before evaluating any query, it is necessary to ensure that critical elements of wireless edge computing are protected. To address this problem, researchers propose differential privacy-based techniques as the best approach.
- Block chain has evolved as an unique distributed technique in recent years that provides for the secure storing of transactions or any other sort of data without the requirement for any predetermined centralized data authority. Its feature of public accessible without a centralized authority made it popular among its users, but it also created certain security and privacy concerns.

CONCLUSION

Cyber Physical Systems (CPSs) have become an essential part of daily life. It is a collaboration of computation, communication and control. CPSs is advanced technology to IOT. CPSs basically integrates huge number of sensors and private data. Adversaries can attack in two ways either passive attack or by using active attack. Here passive attack is privacy oriented attack and active attack is security oriented attack. Encryption and anonymization techniques are existing traditional techniques which is not suitable to provide information security for advanced system called CPSs. Since CPSs is an advanced system, implementation of encryption technique based privacy preservation technique cannot provide more accuracy. This technique is not suitable for small devices which have limited resources. In multiple sensors network, sharing and maintaining public, private keys for connections between every node is difficult task. This leads to data loss. So encryption technique provides computationally complex, more expensive, as well as it reduces system speed. Apart from all it is not suitable for public databases. Anonymization is another privacy

preservation technique which is used to provide data security. Since it is suitable for work with high dimensional data, lot of drawbacks are there. If size of attributes increased there may be a chance of re-identification of information also increases in this technique. While converting anonymized data to non-anonymized and vice versa there may be a chance of losing 100% original data.

One of the most optimal solutions to overcome these privacy hazards is preserving data by noise addition using differential privacy perturbation mechanisms. In this case users can control level of privacy. This data perturbation has the direct effect with data accuracy. Adding more noise provides more security but less accuracy, where as adding less noise provides low security but more accuracy. So, therefore user needs to concentrate both accuracy as well as security. This technique has the capability to preserve huge amount of data on both real-time and databases. The major objective of this technique is not to provide enough information about any individuals in query output. Exponential mechanism, Laplace mechanism and Gaussian mechanism are the three major data perturbation mechanisms which will provide more information security for CPSs. This chapter presented a detailed and up-to-date survey of CPSs applications security threats, attacks, solutions and recommendations. This chapter concluded the survey article by highlighting challenges, open issues, and future research directions in differential privacy techniques for CPSs.

ACKNOWLEDGMENT

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

Alahakoon, D., & Yu, X. (2016). Smart electricity meter data intelligence for future energy systems: A survey. *IEEE Transactions on Industrial Informatics*, *12*(1), 425–436. doi:10.1109/TII.2015.2414355

Ambassa, P. L., Kayem, A. V. D. M., Wolthusen, S. D., & Meinel, C. (2018). Privacy risks in resource constrained smart micro-grids. *IEEE 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, 527-532.

Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security, ELSEVIER*, *68*, 81–97. doi:10.1016/j.cose.2017.04.005

Chuang, M.-C., & Lee, J.-F. (2011). Ppas: A privacy preservation authentication scheme for vehicle-to-infrastructure communication networks. *IEEE International Conference on Consumer Electronics, Communications and Networks (CECNet)*, 1509-1512. 10.1109/CECNET.2011.5768254

Fink, G. A., Edgar, T. W., Rice, T. R., MacDonald, D. G., & Crawford, C. E. (2018). *Overview of Security and Privacy in Cyber-Physical Systems. Overview of Security and Privacy in Cyber-Physical Systems: Foundations*, *Principles and Applications*. doi:10.1002/9781119226079.ch1

Gohar, M., Muhammad, M., & Rahman, A. U. (2018). Smart tss: Defining transportation system behavior using big data analytics in smart cities. *Sustainable Cities and Society*, *41*, 114–119. doi:10.1016/j.scs.2018.05.008

Hassan, Rehmani, & Chen. (2019). Differential Privacy Techniques for Cyber Physical Systems: A Survey. *IEEE Explore*, 1-44.

Kayem, A. V., Meinel, C., & Wolthusen, S. D. (2017). A smart microgrid architecture for resource constrained environments. *IEEE 31st International Conference on Advanced Information Networking and Applications (AINA)*, 857-864.

Li, D., Yang, Q., Yu, W., An, D., Yang, X., & Zhao, W. (2017). A strategy-proof privacy-preserving double auction mechanism for electrical vehicles demand response in microgrids. *IEEE 36th International Performance Computing and Communications Conference (IPCCC)*, 1–8.

Shafique, M., Khalid, F., & Rehman, S. (2018). Intelligent Security Measures for Smart Cyber-Physical Systems. In *21st Euromicro Conference on Digital System Design*. Conference Publishing Services. 10.1109/DSD.2018.00058

Walker-Roberts, S., Hammoudeh, M., Aldabbas, O., Aydin, M., & Dehghantanha, A. (2020). Threats on the horizon: Understanding security threats in the era of cyber-physical systems. *The Journal of Supercomputing, Springer*, *76*(4), 2643–2664. doi:10.100711227-019-03028-9

Yaacoub, J.-P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and Microsystems, ELSEVIER*, *77*, 1–33. doi:10.1016/j.micpro.2020.103201 PMID:32834204