Crawler and Spiderin usage in Cyber-Physical Systems Forensics

M. Abedi[1] and Sh. Sedaghat[2]
[1]Jahrom University APA CENTER, Jahrom, Iran
[2]Faculty of Information Technology Engineering Department, Jahrom State University, Jahrom, Iran
clvmoein@gmail.com, shsedaghat@jahromu.ac.ir

Abstract **- As a featured subset of cyber-physical-systems, Mobile cyber-physical-systems can make use of Mobile devices, such as smartphones, which serve as a convenient and economical platform for Mobile applications in all places between humans and the geographic world around it. Today, cyber physical systems are popular in power grids, healthcare devices, transportation networks, industrial processes and infrastructure. Cyber- physical systems (CPS) are used more widely, the security of physical cyber systems in the design, implementation, and research of the system is very important. Various types of attacks in the cyber-physical-system (e.g. Stuxnet worms) cause severe casualties and potentially serious security risks. Over the past few years, researchers have focused on aspects of the security of cyber-physical systems. In this paper, after analysing CPS security objectives and CPS security approaches, we propose a security technique to provide security and improve intrusion detection methods for cyber-physical systems, which is used to improve CPS immunization. Mobile CPS that has expanded the benefits and scope of CPS applications in recent years has become increasingly popular. For example, mobile CPS can be a kind of basic techniques to support the development of transport network systems, thus protecting the privacy and security of users in the dynamic transport environments Improves. In this article, we first recognize the Mobile CPS of the traditional CPS. Then, we recommend a solution using the Crawling and Spidering techniques used in search engines to detect and cope with the influence of information security systems**

KEYWORDS - Cyber-Physical System Security, Intrusion Detection, Information Security, Crawling, Spidering

I. INTRODUCTION

Cyber-Physical System or CPS combining the physical world with cyber-components is a key research field for more than a decade [1]. Traditional CPS1 is effective in many engineering projects such as intelligent power grids, manufacturing systems, aerospace systems and defence systems [2]. Today, with the development of inclusive Mobile devices, Mobile CPS has attracted more attention. Compared to the traditional CPS, which rely on fixed machines or massive sensors and emphasizes the use of cyberparks to dominate the physical world, the Mobile CPS focuses on its mobility, which can be integrated seamlessly and everywhere. Everyday life gets people. Therefore, Mobile CPS can easily be used in each person's life and be deployed in a wider range of physical worlds.

Although some may believe that Mobile CPS is a subset of traditional CPS [3], this is not the case, because they have unique features that offer opportunities in many functional areas that traditional CPS cannot do it. Because Mobile devices are equipped with a variety of sensors, the Mobile CPS benefits from the continued acquisition of information in the physical world. So, compared with traditional CPS, the Mobile CPS can have much more information resources and can analyse physical systems with more data. Additionally, Mobile CPS integrates traditional features of the CPS with the help of technology development, benefiting from their combination.

Therefore, the Mobile CPS is not a subgroup of the traditional CPS but overlapping it. Due to this characteristic, there is a common challenge for the traditional CPS and Mobile CPS, and some examples are shown as a subset between traditional CPS and Mobile CPS in Figure 1. Additionally, due to the fact that the traditional CPS and Mobile CPS share common challenges and some similarities in the architecture of the system, some traditional CPS solutions for Mobile CPS can also be used. However, as shown in Figure1, since Mobile CPSs are more than a subset of the CPS, they have particular challenges, including Mobile device power constraints, unstable Mobile networks, and very dynamic environments.

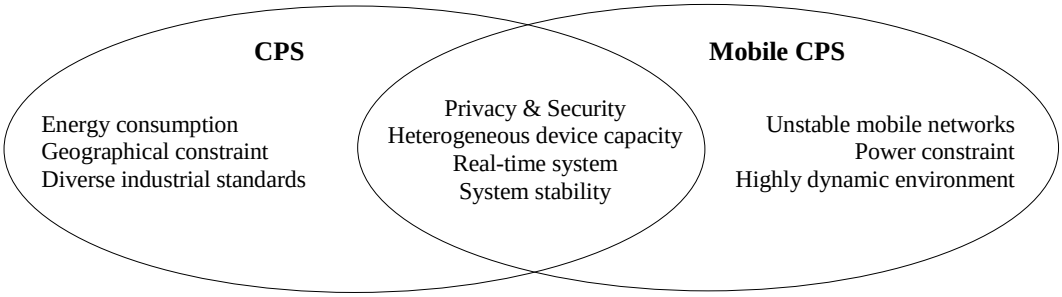

Figure 1: Relation between traditional CPS and Mobile CPS

CPS can be described as intelligent systems that comprise computing components (i.e., hardware and software) and physical components that act seamlessly and closely together to control the changing real-world situation. The prevalence and vulnerability of CPS has left researchers and influencers focused on these systems. In order to ensure the safety of Mobile cyber-physical security systems, there are several security goals to achieve, including six major security objectives: Confidentiality, integrity, availability, robustness, reliability and trustworthiness.

Compared to Internet attacks, it is more difficult to detect and prevent attacks on the CPS goal. To prevent intrusion detection, hackers may apply multiple steps and combine types of attacks to access a traditional or Mobile Cyber-physical system. The continuous integration of cloud technology in all aspects of our daily lives creates business opportunities, operational risks, and research challenges. But as companies continue to provide services and increase access to customers and employees, they continue to expand software access and create new supply chain management chains, the risk of cyber-physical attacking increases. Increasing the level of digital communication between physical devices (such as sensors and thyristors) and cyber-equipment (such as intelligent decision-making systems), CPS (such as power grids) has turned to large ecosystems that require a scalable and flexible infrastructure. Integrating cyber-physical-systems through a cloud computing infrastructure is a Cyber-Physical Cloud or CPC that not only potentially improves the interaction between cyber-physical devices, it also provides the ability to store and analyse large-scale data [4]. News organizations are increasingly highlighting the dangers of integrating this technology. For example, another article cited a cyber-physical attack report that had damaged an explosive furnace in a steel plant in Germany. An excellent example of an attack on a cyber-physical system is the Stuxnet virus that targets Iran's nuclear power plant and reduces the efficiency of systems [5].

In fact, moving from a cyber-physical-network to the cloud can lead to various security issues. There are only a few cyber crime cases known in CPS, but a successful attack could have catastrophic consequences. A recent survey found that the role of digital forensic in managing CPC incidents was not well understood [6]. Although Digital forensic tools and techniques are unlikely to stop an attack in real-time, a forensic approach to design can help provide several methods. For example, this approach can help identify an incident by its source and determine its type, maintain and analyse critical vital data, rebuild parts of the data, and obtain results and speed. Microsoft proposes a "assume breach" approach to cloud security - an innovative design, engineering, and operational approach that predicts an attack has already occurred [7]. Ensuring the environment is like a castle because of the asymmetric nature of cyber space. For example, to protect an information space, Kaspersky should ensure that different security technologies are in place, all systems are installed in time, and so on.

However, an internet attacker should only have one or more vulnerabilities in the network to attack and exploit them.

In a security incident, referral plays an important role in research, such as tracking and identifying the source of the attack. This can be facilitated by a digital pharma. Researchers have highlighted potential issues in digital forensic research in cloud environments, such as the appropriateness of data recording techniques, tools, multiple sources of evidence, and qualification issues.

II. CYBER-PHYSICAL CLOUD SYSTEMS

The continued amalgamation of cloud technology into all aspects of our daily lives creates business opportunities, operational risks, and investigative challenges. But as businesses continue to offer customers and employees increased access, improved software functionality, and new supply chain management opportunities, the risk of cyber-physical attacks on CPCs grows. Increasing digital interconnectivity between devices at the physical (such as sensors and actuators) and cyber (such as intelligent decision systems) levels has transformed CPS (such as the electric power grid) into large ecosystems requiring a scalable and flexible infrastructure.

In reality, moving from an internal cyber-physical network to the cloud can lead to various security issues. There are only a few known cyber-attack incidents on CPS, but a successful attack can have real-world and catastrophic consequences. A recent survey suggested that the role of digital forensics in CPCs incident handling isn't widely understood.

As technology dependency and cloud integration continue to escalate, ensuring CPCs security becomes a critical factor in delivering trustworthy and robust services. The nature of Cyber-physical and cloud computing infrastructures, however, presents inherent challenges to ensuring data confidentiality, integrity, and availability.

A. Risk Management Principles and Practices

It would be unrealistic to expect any organization to have infinite resources to identify and act on all potential threats and risks. Therefore, based on the "assumed breach" approach[7], to achieve CPCs systemic resilience the system developer and forensic expert need to adopt risk management principles and practices to identify and prioritize current and emerging threats (for example, potential vulnerabilities in both cloud computing and CPS and how these vulnerabilities can be exploited), risk areas (including risks arising from unexpected and highly unpredictable causes, also known as the "black swan" problem), and potential evidence source and type (see the forensic readiness principles).

B. Incident-Handling Principles and Practices

Guiding principles and practical strategies can minimize the impact of loss after a security incident and help prevent and mitigate future incidents. As earlier work noted, incident handing and digital forensic practices overlap, and both practices should be integrated into an incident-handling strategy [6]. For example, intrusion detection systems can help determine attack sources. In addition, having a forensic database (for pre-incident collection) would benefit incident responders during a preliminary incident response. In earlier work, Grispos and his colleagues note that organizations have opportunities to strengthen policies, standards, and procedures prior to migrating to cloud environments. Organizations need to investigate these opportunities from a CPCS perspective. Additional work by Grispos and his colleagues in the area of security incident response criteria demonstrate the type of industry practices that need to be identified and verified for CPCS incident handling. However, we need to ensure that activities undertaken during incident handling (for example, evidence collection) don't result in service disruption, and therefore system backup and redundancy must be carefully planned in incident handling.

C. Laws and Regulations

When designing forensic strategies, it's important to consider international and local legal and regulatory requirements, because different national laws and regulations might have different evidence requirements. A law designated for data protection might only be applicable to the country in which the data resides, for example. In some scenarios, cloud providers might be required to comply with a court order and surrender user data without notifying the data owner. Relevant standards and industry best practices should also be considered in the design and development phases. The Payment Card Industry-Data Security Standard (PCI-DSS), for instance, mandates regular monitoring of access to network resources, which would require the system to include an efficient logging capability for compliance purposes as well as the digital evidence source.

D. CPC Hardware and Software Requirements

The interdependencies between hardware and software within a CPCS complicate the identification and collection of evidential data. Potential evidence artefacts would exist across several CPC layers (for example, from field devices to cloud aggregators); thus, providing an embedded forensic agent is a potential

solution to remotely collecting the evidential data. Furthermore, specific communication protocols used in cyber-physical systems, such as ModBUS, to control field devices would require a customized forensic approach as compared to the common network protocol (for example, TCP/IP). Understanding hardware and software requirements are, therefore, critical in supporting the collection of forensically sound evidence.

E. Industry specific requirements

Because of the diversity of cyber-physical components (for example, sensor, controller, and networked systems) and data types (for example, sensor data from in-vehicle systems are quite different from sensor data from power grid systems), we must also consider industry-specific (for example, energy, automotive, and transportation) requirements. Therefore, identifying and collecting evidence data sources requires careful planning. Moreover, each industry has a different security risk profile, which would affect the choice of forensic strategies.

F. Validation and Verification

Once a prototype of the system has been designed and developed, it's important to validate and verify to ensure that the evidence collected is adequate and reliable, and that the forensic processes and functions used are sound (for example, there's no contamination of evidence). As Yinghua Guo and his colleagues discuss, "validation refers to the confirmation by examination and the provision of objective evidence that a tool, technique or procedure functions correctly and as intended" and "verification is the confirmation of a validation with laboratories tools, techniques and procedures." [8].

Ensuring reliable evidence data is an important aspect of producing digital evidence that's admissible in a court of law (that is, forensically sound). We can use Rodney McKemmish's criteria as guidelines to establish forensic soundness [9]:

- *Meaning*. Design digital forensic processes that won't change the data's meaning.
- *Error*. Design digital forensic processes that can avoid undetectable error. If an error is encountered when undertaking forensic processes, it must be identified and explained as evidence.
- *Transparency*. Verify evidence by documenting the chain of custody, including identifying the forensic software and hardware used, detailing the analysis environment, and specifying any problems, errors, and inconsistencies throughout the forensic processes.
- *Experience*. Be sure to task an individual with sufficient and relevant expertise with finding digital evidence.

Assurance refers to the measurement of forensic processes and functions using relevant metrics, such as those involving security incidents, maturity level, and IT performance, and can include incident simulation or testing (for example, penetration testing) as input. The system designer can refine the CPCs based on the validation and verification results before finalizing. As part of the final check, the designer defines a set of actions that constitutes a strategy for incident handling and creates (or updates) digital forensic practices to manage incident occurrence in the product's post release phase.

Any problems resulting from the validation and verification will involve refining the related factors. The completed CPCs should be forensically ready in the aforementioned key areas. To sum up, defining and planning what evidence will be required ensures that better security mechanisms and architecture are in place, and that they can provide the evidence when it's required.

Internet search engines use two crawling and spidering capabilities to get information from web space. On these search engines like Google and Bing, the spider is responsible for loading the pages and the crawler plays the role of commander in the spider. In fact, the crawler decides which pages to load, and ultimately the spider is responsible for loading [10].

III. RELATED RESEARCHS ON CPS SECURITY TECHNIQUES

[11] provides an overview of smart grid operation, associated cyber infrastructure and power system controls that directly influence the quality and quantity of power delivered to the end user. The paper identifies the importance of combining both power application security and supporting infrastructure security into the risk assessment process and provides a methodology for impact evaluation. A smart grid control classification is introduced to clearly identify communication technologies and control messages required to support these control functions.

Table 1 summarizes the most and least studied IDS techniques in the literature grouped by the application type in the order of most to least.

We see that for all applications studied, the most commonly used configurations are behavior-based detection techniques and host-based auditing. Table I indicates that there is little research with regard to automotive applications, knowledge-based detection techniques and network-based auditing.

[12] developing mobile cyber-physical applications in the context of WreckWatch and related projects yielded some lessons, like: Many components of the solutions are highly related, Analysis of properties, such as safety, that span a combination of devices and services is difficult, Factoring social/human properties of systems into system analysis is not well understood, It is hard to integrate mobile Internet devices with conventional sensor networks, Individual mobile devices are prone to unexpected unavailability.

Table 1: Most and Least Studied IDS Techniques, by Citations (some used more than one detection technique)

CPS Application	Detection Technique	Audit Material	Unique CPS Aspects
Smart utility (18)	Behavior (10) Behavior-Specification (6) Knowledge (3)	Host (11) Network (7)	Physical Process Monitoring (8) Closed Control Loops (2) Attack Sophistication (9) Legacy Technology (14)
SCADA (6)	Behavior (5) Behavior-Specification (1) Knowledge (1)	Network (5) Host (1)	Physical Process Monitoring (1) Closed Control Loops (0) Attack Sophistication (1) Legacy Technology (2)
Medical (3)	Behavior (2) Behavior-Specification (1) Knowledge (0)	Host (3) Network (0)	Physical Process Monitoring (1) Closed Control Loops (0) Attack Sophistication (1) Legacy Technology (2)
Aerospace (2)	Behavior (1) Behavior-Specification (1) Knowledge (0)	Host (2) Network (0)	Physical Process Monitoring (1) Closed Control Loops (0) Attack Sophistication (0) Legacy Technology (2)
Automotive (1)	Behavior (1) Behavior-Specification (0) Knowledge (0)	Host (1) Network (0)	Physical Process Monitoring (0) Closed Control Loops (0) Attack Sophistication (1) Legacy Technology (0)

In [13], Researchers developed a mathematical model to analyse survivability of a mobile cyber physical system (MCPS) comprising sensor-carried mobile nodes with voting-based intrusion detection capabilities.

[14] shows that cyber–physical system security demands additional security requirements, such as continuity of power delivery and accuracy of dynamic pricing, introduced by the physical system. Such requirements are usually closely related to the models and states of the system, which are difficult to address by information security alone. Therefore, both information security and system-theory-based security are essential to securing cyber–physical systems.

Vita, a novel mobile CPS for crowdsensing, which leverages the advantages of social computing, service computing, cloud computing, and a number of open source techniques across mobile devices and cloud platform, to provide a systematic approach that supports both application developers and users for mobile crowdsensing applications have been presented in [15].

[16] introduces various research applications which required cyber-physical testbeds to provide representative environments to explore and validate potential solutions.

[17] explores the development of a probability model to analyse the reliability of a cyber physical system (CPS) containing malicious nodes exhibiting a range of attacker behaviours and an intrusion detection and response system (IDRS) for detecting and responding to malicious events at runtime.

The paper [18] gives a comprehensive review on CPS security following the security framework from diverse perspectives.

The forensic-by-design framework presented in [19] provides a starting point for conversations, research and solutions that could be used to address this issue.

[20] Authors have introduced the applications and key challenges and techniques of mobile CPS and distinguished them from the traditional CPS.

IV. A SOLUTION FOR INTRUSION DETECTION IN CYBER-PHYSICAL SYSTEMS

We well explain our method in 3 phases:

Phase 1- We clear how does our solution can be implemented in software and hardware and infrastructure.
Phase 2- We tested the solution for a case by using OPManager software and show the results.
Phase 3- We explain the role of mobile CPS and spidering and crawling techniques in our method.

A. Phase 1

As previously mentioned, the property of Identifying and collecting information around the whole surface web on the search engines is the responsibility of a technique called "spidering", and after identifying web pages, the spider tells the crawler the necessary commands. Our proposed strategy, including the use of this Web space feature in intrusion detection systems, which, of course, requires cyber-physical cloud systems to manage it.
Our proposed strategy includes the following steps:

- **Step 1**: Monitor the critical security and firewall systems throughout the network in the medium-term and long-term time periods (to defining a true network state pattern in traffic, active devices and so on). At this stage, first of all, we should provide an environment that includes samples of our real internal network of organisation components. This environment could be a virtual space or a real- local network in some place. The important issue about the real or virtual network environment is that it must include exact hardware instruments, software applications and cloud technology infrastructures. for virtualization such an environment, we could use different software such as VMware, GNS3, Cisco Packet tracer, etc. and if we want to have a real local network to find out the true state of network and monitor different components of network, like network traffic and users' activities in network, there are useful software such as: OPManager, PRTG, SolarWinds, and etc. Our next action is to monitor all hardware, software and cyber-physical cloud systems infrastructure activities of the cyber-physical and network system before the launch and introduction of the related system and infrastructure, and more critical and more important than previous actions is storing the information has been obtained in a secure and secret database and protect it from stealing or injecting information from the database. It should be noted that this stage is being implemented only by IT security professionals who are fully trusted by the organization, and no internal or external staff are aware of the implementation of this phase.
  In fact, our goal to implementing this step, is to determine and store the normal and ideal functional conditional of our isolated (not connected to the internet) internal organisation's network.

Now and after the implementation of the first step, we determined the normal state of the network and we know the whole information around the internal network when it does not have any malware, spyware and abnormal traffics.

- **Step 2:** Monitor all hardware and software parts and critical security components and systems traffic throughout the network. In the second step, after introducing and launching the system, we examine all of the network traffics and system activities in real-time (Current network status). Some software like OPManager, PRTG, SolarWinds can be useful for monitoring the whole CPS network properties such as bandwidth or memory usage.

- **Step 3**: Match and compare the information obtained in the first step with the data collected in the second stage. In the third step, you can compare the current status and performance of the network with the normal state of the CPS, and if you see the slightest change to the ideal function, check this change, identify the suspect and all the information and potential hazards around the change of the information and report them to the information security specialist.

B. Phase 2

For example; we have monitor memory usage in a practical CPS case by using OPManager and inserted the result in Figure 2. As shown in Figure 2, the amount of memory used in the network and server during the test (yellow lines) is greater than the normal amount of

memory consumption that should be taken in a natural and safe manner according to the pattern (green lines). The blue lines in the form show the maximum amount of memory usage tolerance by the infrastructure on the network. As long as the distance between the blue lines and the yellow lines is lower, the problem with the server and other components and network infrastructure is more likely to occur, and reporting and processing need to be done faster.

Now and after the implementation of our solution in first to phases, we should start phase 3 and detect the abnormal issues through the network and report them to the information security administrator of the organization.

Figure 2: Memory usage in a practical CPS case compared with the normal memory usage

C. Phase 3

Informing the organization's security authorities can be done using the cloud computing, Fog computing and cyber-security tools. In this way, changes made after Real-Time analysis are reported to security administrators via Fog computing technology (which speeds up the operation of cloud computing), and they are also using Mobile cyber-physical devices that always have the ability to set Crawler in a way that disrupts the performance of a malicious or intruder after it is detected and prevents potential attackers from causing damage.

In recent years, the capabilities of Mobile devices have improved dramatically. These features, such as impressive computing resources, multiple radios, sensor modules and high-level programming languages enable Mobile devices to create a Mobile cyber-physical system in our everyday lives. Mobile CPS is the result of the integration of distributed sensors with computing and connectivity all over the internet. It also integrates Mobile CPS, computing, cyber and physical resources, and facilitates the interaction of the digital world with the physical world, and potentially enriches the everyday life of citizens anytime and anywhere. Therefore, the Mobile CPS can be a convenient and affordable platform that facilitates complex and all-round intelligent applications between humans and the physical world around them.

Mobile CPS can be used in various fields including (1) Mobile smart robots and robotic systems, The use of multiple smart sensors, Mobile devices, Intelligent services, Cloud robots, and Improving the efficiency and scalability of complex work processing that is not feasible under the constraints of local resources in different application areas; (2) Intelligent transportation systems, for example, The ability to measure, calculate and communicate with control vehicles in the physical world; To deal with safe challenges (for example, reducing latency in response to traffic accidents), Efficient transportation Fashion and green; for example, Smart city, environmental monitoring, health systems and smart grids, which improves information, comfort, operational Safety and green energy of the human community. Solutions that are defined by software, Distributed systems, Cloud computing, social networking, Security and privacy, Human-centred computing, and other methods and technologies that can be used for moving CPSs are also welcome. The last phase of our proposed solution has two main steps:

- Step 1: Detection any malicious activity on the Network;
  In this step; we need a special spider and crawler to constantly search the different parts of the network and compare current status of network with the normal state.

- Step 2: inform and alarm the information security staff personals and administrators throughout the Mobile CPS to make the network secure.

  If our spider and crawler found detect any differences between current and normal states of network, then is time to use Mobile CPS technology to be useful for inform the intrusion detection to security managers and help to make the network more secure.

V. FUTURE WORKS

Several research fields that facilitate the deployment and securing use of Mobile CPS include:

- Architectural platform for distributed Mobile CPS
- Smart Mobile Robots and Robotic Systems
- Software Solutions for Mobile CPS
- Smart city and smart grid technology
- Man-centric calculations in mobile CPS
- Automobile networks and intelligent transportation systems
- Evaluations and security solutions, privacy, and issues related to the reliability of the Mobile CPS
- Distributed intelligent systems and applications
- Mobile social networks and inclusive apps
- Mobile cloud computing
- Mobile Service-centric and calculations
- Design and optimization of Mobile CPS
- Asymmetric networks in Mobile CPS
- Intelligence processing for Mobile CPS
- Big data analysis on Mobile CPS
- Data mining, machine learning, and sophisticated system design for Mobile CPS
- Scalable monitoring systems with Mobile wireless networks
- Resource Management in Mobile CPS
- Experience to deploy real-world Mobile CPS

VI. CONCLUSION

We first provided some explanations about CPS and named their variants, in terms of the differences and similarities between traditional CPS and Mobile CPS and the security objectives for CPS systems. By pointing out the features of CPS, we conclude that intrusion detection and the prevention of attack on these scalable systems are of great importance in the industry, security systems and even the lives of people every day. Then, using a common technique in internet search engines, such as Spidring and Crowling, have proposed a strategy and idea to detect malicious devices, hacker activities, and manipulate the information network by unauthorized persons. In our proposed approach, the security experts of any organization that needs to protect the information of their organization can remotely attack the attackers and those who intend to sabotage the organization's information space and neutralize their actions. In the end, we also looked at Mobile CPS, and several research areas were proposed to improve the security of the Mobile CPS forensics.

VII. REFERENCES

[1] L. Sha, S. Gopalakrishnan, X. Liu, and Q. Wang, *"Cyber-physical systems: A new frontier"*, in Proc. IEEE Int. Conf. Sensor Netw., Ubiquitous Trustworthy Comput. (SUTC), Jun. 2008, pp. 1–9.

[2] R. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, *"Cyber-physical systems: The next computing revolution"*, in Proc. 47th Design Autom. Conf. ACM, 2010, pp. 731–736.

[3] T. Hanz and M. Guirguis, *"An abstraction layer for controlling heterogeneous Mobile cyber-physical systems"*, in Proc. IEEE Int. Conf. Autom. Sci. Eng. (CASE), Aug. 2013, pp. 117–121.

[4] S. Karnouskos, A.W. Colombo, and T. Bangemann, *"Trends and Challenges for Cloud-Based Industrial Cyber- Physical System"*, *Industrial Cloud-Based Cyber-Physical Systems*, A.W. Colombo et al., eds. Springer Int'l Publishing, 2014, pp. 231–240.

[5] R. Langner, *"Dissecting a Cyberwarfare Weapon"*, *IEEE Security & Privacy*, vol. 9, no. 3, 2011, pp. 49–51.

[6] N.H. Ab Rahman and K.-K.R. Choo, *"A Survey of Information Security Incident Handling in the Cloud"*, *Computer Security*, vol. 49, Mar. 2015, pp. 45–69.

[7] Microsoft, *"Microsoft Enterprise Cloud Red Teaming"*, 2014; http://download.microsoft.com/download/C/1/9/C1990DBA-502F-4C2A-848D-392B93D9B9C3/Microsoft_Enterprise_Cloud_Red_Teaming.pdf.

[8] Y. Guo, J. Slay, and J. Beckett, *"Validation and Verification of Computer Forensic Software Tools—Searching Function"*, *Digital Investigations*, vol. 6, 2009, pp. 12–22.

[9] R. Mckemmish, *"When Is Digital Evidence Forensically Sound?"*, Advances in Digital Forensics IV, I. Ray and S. Shenoi, eds., Springer, 2008, pp. 3–15.

[10] N.H. Ab Rahman, W.B. Glisson, Y. Yang, K.-K.R. Choo, *"Forensic by Design Framework for Cyber-Physical Cloud Systems"*, IEEE Cloud Computing, 2016.

[11] Siddharth Sridhar, Adam Hahn, Manimaran Govindarasu, *"Cyber–Physical System Security for the Electric Power Grid"*, Proceedings of the IEEE, 2012.

[12] Jules White, Siobhan Clarke, Christin Groba, Brian Dougherty, Chris Thompson, Douglas C. Schmidt, *"R&D Challenges and Solutions for Mobile Cyber-Physical*

Applications and Supporting Internet Services", Journal of Internet Services and Applications.

[13] Robert Mitchell, Ing-Ray Chen, *"On Survivability of Mobile Cyber Physical Systems with Intrusion Detection"*, Springer Science and Business Media, 2012.

[14] Yilin Mo, Tiffany Hyun-Jin Kim, Kenneth Brancik, Dona Dickinson, Heejo Lee, Adrian Perrig, and Bruno Sinopoli, *"Cyber–Physical Security of a Smart Grid Infrastructure"*, Proceedings of the IEEE, 2012.

[15] Xiping Hu, Terry H. S. Chu, Henry C. B. Chan, Victor C. M. Leung, *"Vita: A Crowdsensing- Oriented Mobile Cyber-Physical System"*, IEEE Transactions on Emerging topics in Computing, 2013.

[16] Adam Hahn, Aditya Ashok, Siddharth Sridhar, Manimaran Govindarasu, *"Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid"*, IEEE Transactions on smart grid, 2013.

[17] Simrandeep Kaur chana, S. J. Karale, "Analysis of Intrusion Detection Response System (IDRS) In Cyber Physical Systems (Cps) Using Regular Expression (Regexp)", IOSR Journal of Computer Engineering, 2014.