International Journal of Multidisciplinary Research And Studies

Available online at https://ijmras.com/

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND STUDIES
ISSN: 2640 7272
Volume:04; Issue:05 (2021)

Page no.- 1212

INFRASTRUCTURE FROM CYBER AND PHYSICAL THREATS

Durgesh Kumar Thakur

M.Phil., Roll No. :140414; Session: 2014-15

University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur

E-mail-: er.djthakur@gmail.com.

ABSTRACT

Cyber-physical systems, often known as CPS for short, are intelligent systems that consist of constructed networks of both physical and computational components that interact with one another. Being resilient is one of the primary criteria for a CPS, so make sure yours is (NIS, 2017). The next version of the CPS has to be resistant to correlated threats, which are attacks in which more than one attacker operates on an entity. Correlated risks arise in situations in which simple perimeter safeguards are insufficient.

KEYWORDS: Cyber, Physical, Threats, Correlate, Computational Components,

INTRODUCTION

Cyber-physical systems, often known as CPS for short, are intelligent systems that consist of constructed networks of both physical and computational components that interact with one another. Being resilient is one of the primary criteria for a CPS, so make sure yours is (NIS, 2017). The next version of the CPS has to be resistant to correlated threats, which are attacks in which more than one attacker operates on an entity. Correlated risks arise in situations in which simple perimeter safeguards are insufficient. As a result, computer-based control

Upendra Kumar *, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: er.djthakur@gmail.com.*

systems (CPSs) need to be seen in a new perspective, one in which numerous components exist and occasionally overlap, each of which contains entities that communicate with one another. Figure 1. depicts the fundamental design of a smart electric grid, which is comprised of several interconnected components (FitzPatrick and Wollman, 2010). In such designs, in addition to the delivery of the commodity (in this case, power), transmission must interact
with distribution, markets, service providers, operations, and increasingly customers through the flow of information and computation. Classical models are not very good at capturing this; within the context of an electric power system, a subset of domains may be grouped into two fundamental sorts of entities, which are control centers and business network activities. The energy management and Supervisory control and data acquisition (SCADA) systems within the control centers control and read data from remote terminal units (RTUs), which in turn control and read data from sensors and actuators. Additionally, the control centre is required to communicate with other control centers, which may or may not be part of the same organization. By placing the control system at a higher security level, the classical hierarchical model of Biba (Bishop, 2003) forces the arrangement of security partitions into just two (McMillin and Roth, 2017) seen in a modern electric utility. This means that the business enterprise of a utility cannot write up into the control system, which in turn prevents a potential virus that has compromised the business enterprise from impacting the control system as well.

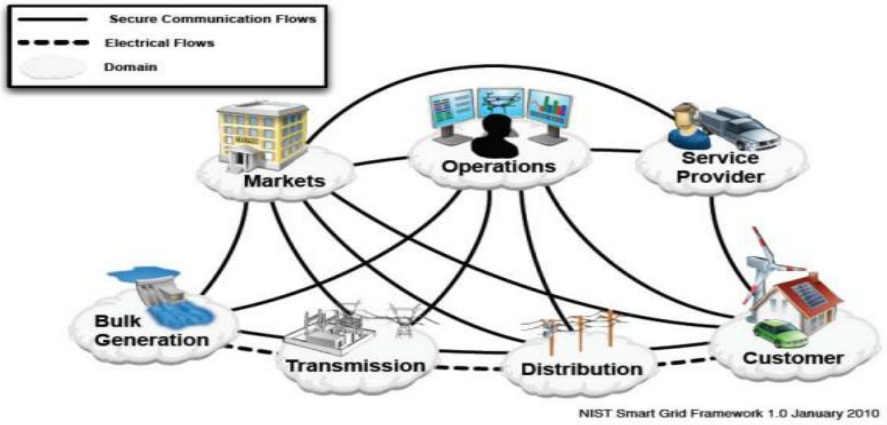

Figure 1. Electric Distribution System Architecture

as may be seen in Figure 1. Unfortunately, it does not prevent assaults that originate from cyber or physical components that are contained inside the security domain, and perimeter defenses cannot safeguard these components since doing so would interrupt the usual flow of information within the power grid. In this paper, we investigate the widespread safety problems

Upendra Kumar *, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: er.djthakur@gmail.com.*

associated with an electric grid by implementing a testbed with a Design-centric approach (DeC) and a Data-centric approach. Both of these methodologies were utilized (DaC). The DeC method tackles the problem of vulnerabilities within a multi-domain setting by employing manually constructed invariants and models based on multiple security domains nondeducibility (MSDND) and logic based on belief, information transfer, and trust (BIT) (Liau, 2003; Liau, 2005). Automating invariant creation is accomplished by the application of the machine learning technique known as linear regression (Lin, 1997) using the DaC methodology. After that, the invariants that were produced by the two different methodologies are compared and contrasted in terms of how well they can detect flaws and assaults within the system.

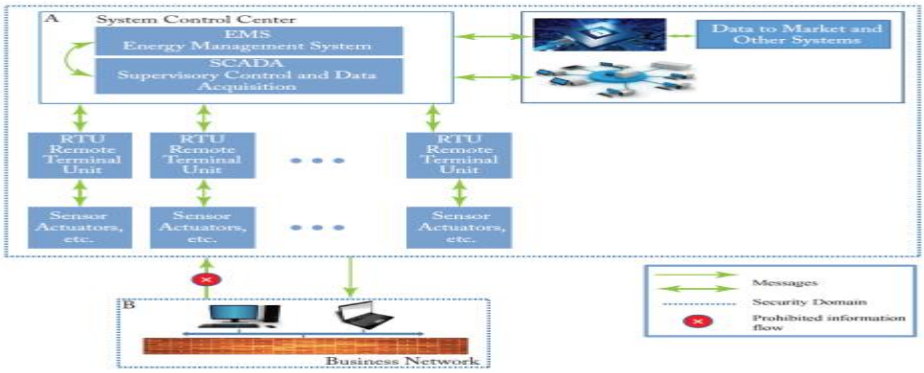

Figure 1. Biba Model of an Electric Power System

Quality Of Service (Qos)

SDN allows finer-grained communication network flow statistics for real-time monitoring and QoS management methods, both of which are beneficial for enhancing the effectiveness and dependability of microgrid energy services. Because the whole communication network is visible globally, it is possible to immediately calculate an optimum routing path that meets QoS standards and then directly programme the network devices to carry out the modification. This is made possible by the availability of the entire network. Despite the fact that there will be many positive effects, we shouldn't lose sight of the fact that there will also be many difficulties. These difficulties will arise from (1) the integration with the electric power infrastructure and the microgrid monitoring and control systems, and (2) the additional security difficulties that will be brought about by the SDN. For instance, malicious packet delay (e.g., rerouting of a data flow to a high-latency link) or selective packet drop (leading to packet re-transfers) may appear completely legitimate at the communication network layer, but they can be used by hackers to cause disruptions in data transmissions.

Upendra Kumar *, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: er.djthakur@gmail.com.*

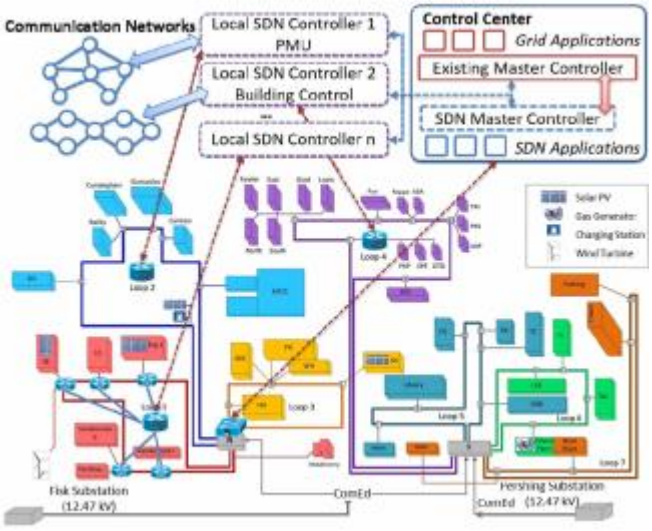

Figure 2 Design of SDN-enabled IIT Campus Microgrid.

potentially lead to synchronization difficulties, control deterioration, and even microgrid destabilization Unanticipated problems with SDN controllers can potentially cause serious interruptions to the microgrid's power sources. Our microgrid SDN controller and application development can benefit from current developments in SDN security research, which largely concentrate on security enforcement frameworks. This will allow us to address the problems that have been identified. In Section VII, we go over a variety of different frameworks. In order to protect against the risk of having a single point of failure, it is critical to investigate the use of distributed controllers. This matter was illuminated by recent developments in the distributed SDN application platform, which included a variety of high-level abstractions that were device- and network-centric. In addition, in comparison to information technology systems, microgrid control systems feature more straightforward network dynamics. These network dynamics include relatively static topologies, pre-defined communication patterns, a restricted number of protocols, and a consistent user population. As a result, designing cyber-security applications such as intrusion detection, network verification, and self-healing management is far simpler than designing typical IT networks with the specifics covered in Section IV.

Sdn-Enabled Campus Microgrid Design

As a successful conclusion of the "Perfect Power Initiative" project financed by the United

Upendra Kumar *, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: er.djthakur@gmail.com.*

States Department of Energy, we transformed the main campus of the Illinois Institute of Technology in Chicago into an island able microgrid. The power distribution system of the IIT microgrid is highly reliable and contains seven separate loops. A centralized microgrid master controller (MMC) is responsible for optimizing the cost of operating a microgrid while also ensuring voltage and frequency stability throughout the microgrid as a whole. Using the SCADA system, MMC is responsible for coordinating the functioning of the onsite generating, storage, and building loads. Continuous monitoring, aggregation, and communication with MMC take place regarding the conditions of DERs as well as other components of the distribution system. MMC is able to interact with a wide variety of field equipment by utilising a number of different communication protocols (e.g., Modbus, BACnet, DNP3). In addition to this, MMC analyses the real-time measurements and improves the energy management throughout the whole microgrid. The software-defined networking (SDN) technology provides improved intelligence and tight coordination between all of the legacy and new devices (such as SCADA devices, sensors, actuators, and other subcontrollers) that share the same communication infrastructure. For this reason, a logically centralised SDN controller is necessary in order to monitor and operate the communication network in real time. Only then can the performance be optimised, and cyber security and resilience will be supported. At the moment, the microgrid control centre that runs MMC functions as an information hub at the microgrid application layer. Because of this, it offers the perfect position from which to deploy the SDN controller. In point of fact, the MMC and the SCADA controller both play distinct roles in the control and administration of the microgrid, and as a result, they may be combined to form a more robust MMC. For example, the existing MMC is responsible for coordinating the operation of on-site generation, storage, and building loads through the use of the SCADA system.

On the other hand, the SDN controller is accountable for configuring and managing the communication network that serves as the system's fulcrum. The design of the SDN-enabled IIT microgrid is depicted in Figure 4, which shows that a hierarchical SDN control technique is used for the communication network. SDN controllers are utilised in the construction of the interlinking layer that exists between the communication network and the microgrid applications. Within the control centre, the SDN master controller has been included into the MMC that was already there. The Master SDN controller is in charge of coordinating and supervising the activities of the various local SDN controllers, each of which is intended to concentrate on a particular subset of communication applications (such as PMU, building

Upendra Kumar *, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: er.djthakur@gmail.com.*

control, and so on) for the purpose of providing fine-grain monitoring and control. This control structure lessens the burden on performance while simultaneously increasing the communication network's resistance to both cyberattacks and mistakes made by humans. The control of the SDN is logically centralised, which makes it an appropriate site for locating security solutions. It also promotes additional novel applications to secure microgrid communications, such as context-aware intrusion detection, self-healing network management, and global network verification, amongst many others. In the following part, we will concentrate on three applications that we are investigating in order to improve the robustness and safety of the IIT microgrid.

CYBER-PHYSICAL TESTBED FOR MICROGRID OPERATIONS

When applied to microgrids, emerging communication networking technologies such as SDN require a testing platform that is both scalable and reliable. This is necessary in order to assist the transition from the conceptual stage of in-house research to the stage of actual production. DSSnet is a cyber-physical microgrid testbed that we have built. It combines modelling of electrical power distribution systems with SDN emulation, and its purpose is to facilitate high-fidelity research of SDN-based applications and the implications those applications have on microgrids Within the scope of this project, we add a communication network operating system to DSSnet in order to increase its functionality.

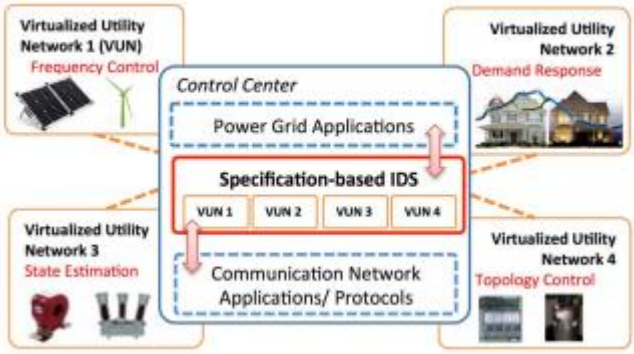

Figure 3 A Specification-based Intrusion Detection System based on Virtualized Utility Networks.

Upendra Kumar *, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: er.djthakur@gmail.com.*

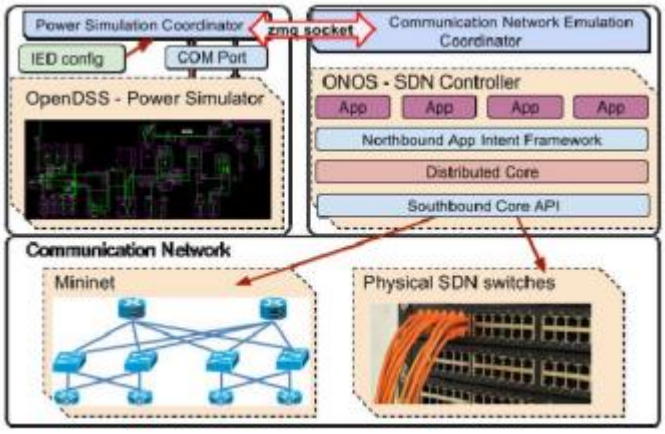

Figure 4 DSSnet: A Cyber-physical Microgrid Testing Platform with Power Distribution System

Simulation (OpenDSS) and virtual-machine-based SDN Emulation (Mininet and ONOS) to simplify the process of management and deployment inside an environment containing a microgrid. The following is a list of the most important components that make up DSSnet:

1. a container-based software defined networking (SDN) simulator known as Mininet, which enables the running of actual SDN software and communication network applications
2. an electrical power distribution system simulator known as OpenDSS, which makes it possible to conduct research on power flow
3. a one-of-a-kind virtual time system that is based on the Linux kernel and is used for synchronisation between the two subsystems. This considerably improves the temporal fidelity difficulties that are present in standard co-simulation or hardware-in-the-loop testbeds.
4. two coordinators for interfacing with the cyber-side modules and the physical-side modules as well as the virtual time system; and
5. a new feature of the distributed SDN control environment, ONOS, that provides high-level abstractions and APIs for microgrid control applications to manage, monitor, and programme the emulated communication network.

Through the use cases shown in this study, we demonstrate that the inclusion of ONOS into DSSnet makes it possible to implement an SDN-controlled microgrid. Extending the testbed to include physical SDN hardware switches in order to enable high functional fidelity research and assessment is a task that is currently under progress. We have utilisedDSSnet to analyse several different microgrid applications. In the following part, a case study of a self-healing

Upendra Kumar *, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: er.djthakur@gmail.com.*

application will be shown to highlight how the adoption of SDN may improve the microgrid's resilience and security.

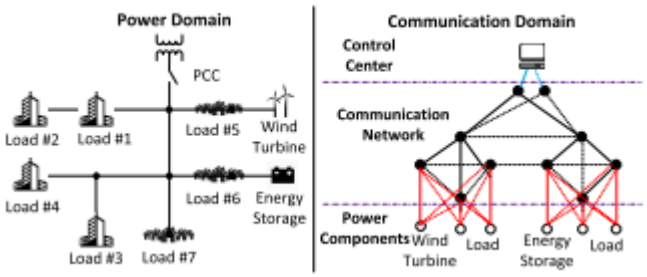

Figure 5Self-healing Micro grid Application Test Scenario

RESEARCH METHODOLOGY

No deducibility (ND)(Sutherland,1986)

The no deducibility method modifies the information flow that occurs between the various system components. The functionality of the system is typically used as the basis for the creation of partitions within the system. High and low are terms that are typically used to describe the system partitions, and they are kept apart from one another. If the information in one partition is not deductible at the other partition, then the two partitions are secure with each other as far as no deductibility is concerned. Absolute and straightforward descriptions of the divisions may be found in the ND model. If the divisions overlap, as they do in the case of essential infrastructure such as industrial control systems, then the ND model does not provide the necessary properties to accurately depict the flow of information. In order to solve this problem, MSDND created a model that provides a greater degree of control over the information that is sent.

Multiple security domain no deducibility

MSDND does not just divide the system into high and low, but rather it divides it into domains that can either overlap with one another, be completely separate from one another, or be totally contained within other domains. These two security domains are said to be MSDND secure with each other if, when seen from one security domain, we do not possess a valuation function that enables us to identify the state of the other security domain. The MSDND model may be characterized in a more technical sense as follows: "There exists some universe with a pair of states where one must be true and the other must be false (exclusive OR), but an entity I has no valuation function for those states." Simply put, I have no way of knowing which state is

Upendra Kumar *, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: er.djthakur@gmail.com.*

real and which one is fake in the security domain SDi. (HowserandMcMillin,2013).

$$\text{MSDND(ES)}: \exists w \in W \vdash [(s_x \vee s_y)] \wedge \sim(s_x \wedge s_y) \wedge [w \models (\nexists V_x^i(w) \wedge \nexists V_y^i(w))]$$

Anequivalentformulais,

$$\text{MSDND(ES)}: \exists\, w \in W \vdash [(s_x \oplus s_y)] \wedge [w \models (\nexists V_x^i(w) \wedge \nexists V_y^i(w))]$$

An MSDND secure information channel is beneficial to the system in terms of its ability to maintain secrecy. On the other hand, an MSDND secure information path is detrimental to the system in terms of its ability to maintain integrity (Dunaka and McMillin, 2017). For instance, when a thief breaks into a house, the owner need to be aware that there has been an incursion (integrity). On the other hand, a thief who approaches a house from the street shouldn't be able to tell whether or not the owner is already inside the house (confidentiality).
MSDND analysis aids in the identification of information routes that are susceptible to integrity attacks and gives ideas for the creation of invariants, both of which can contribute to the enhancement of the robustness of a CPS

DATA ANALYSIS

4.1.1 MSDND Analysis

In MSDND analysis, the information flow pathways of various essential information pieces in the system are studied in the proofs by utilising BIT logic. This is done so that any potential vulnerabilities may be found and eliminated. From the point of origin to the final destination, which is the control system, a mathematical analysis of each individual piece of information is carried out. This occurs while the information is passing through a variety of security domains. A valuation function that can help detect an attack is created by identifying the point at which the information can get damaged and then generating invariants to use in the creation of the function. As can be seen in Section, the testbed has a total of five distinct categories of essential information. Associated with each of these categories of critical information is a specific information flow. Figures 4.1, 4.2, 4.3, and 4.4 illustrate the security domains that are associated with each of the information pathways, respectively. In the subsequent proofs, invariants are utilised to circumvent the MSDND security that is imposed on an integrity attack.

Upendra Kumar *, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: er.djthakur@gmail.com.*

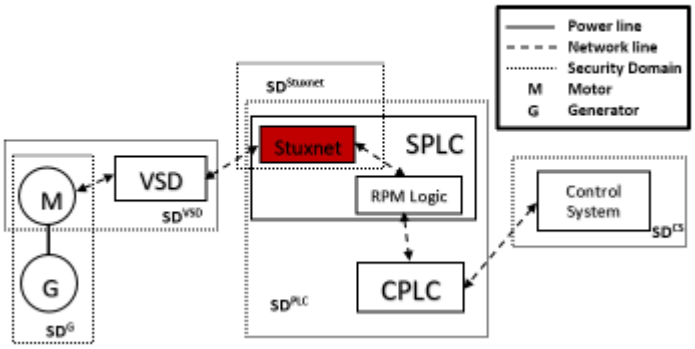

Figure 7. Security domains of 'RPM' in formation path

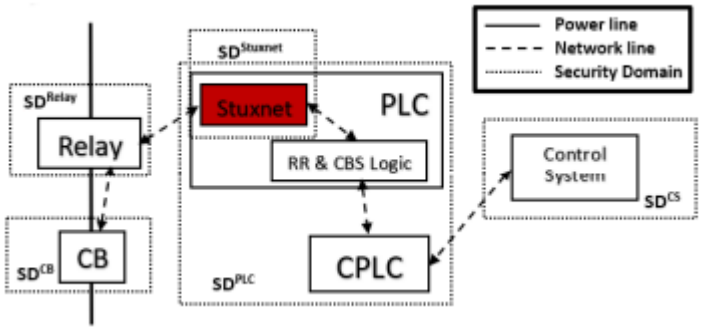

Figure 8. Security domains of 'RR and CBS' in formation path

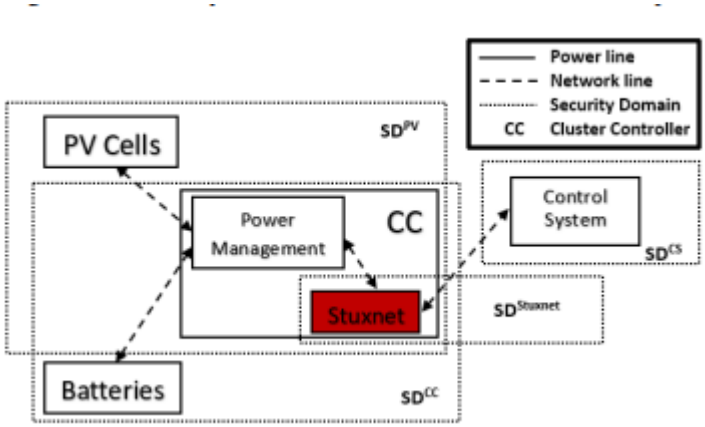

Figure 9.Security domains of 'CD' in formation path

CONCLUSION

Through the use of MSDND analysis, vulnerable information pathways were discovered in the EPIC testbed. Using the physics of the system, over seventy-three invariants were manually

Upendra Kumar *, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: er.djthakur@gmail.com.*

generated. On the live system, we have several of these invariants that have been implemented. Attacks using a man in the middle technique were carried out, and in every instance, the attackers were discovered and the MSDND safe path was compromised, which is beneficial for the system. Additionally, several invariants were executed on the data obtained from EPIC, which assisted in locating the source of the issue inside the logger of the EPIC system. Over one hundred and fifty-two numeric variables were examined with linear regression in the SCADA system of the EPIC testbed, and one hundred and ninety-nine invariants were obtained as a result. Scripts were written in order to automate the process of generating scripts that would be used to implement the invariants that were developed. After that, the invariants were divided into nine different kinds based on the electrical equations that had been created, and the effectiveness of each type was evaluated for a variety of deviation percentages ranging from 1% to 6%, which is the range that the EPIC system permits for deviations.

Reference

1. Kim, Y. and W.-H. Kang, Network reliability analysis of complex systems using a non-simulation-based method. Reliability Engineering & System Safety, 2013. 110: p. 80-88.

2. http://www.nerc.com/pa/CI/ESISAC/Documents/EISAC_SANS_U kraine_DUC_18Mar2016.pdf) (last visited 02-2020)

3. Niu, Y., et al., Smart Construction Objects. Journal of Computing in Civil Engineering, 2016. 30(4): p. 04015070.

4. Shah, J. and B. Mishra, Customized IoT Enabled Wireless Sensing and Monitoring Platform for Smart Buildings. Procedia Technology, 2016. 23: p. 256-263.

5. Sun, E., X. Zhang, and Z. Li, The internet of things (IOT) and cloud computing (CC) based tailings dam monitoring and prealarm system in mines. Safety Science, 2012. 50(4): p. 811-815.

6. Magalhaes, R.P., et al., Speed prediction in large and dynamic traffic sensor networks. Information Systems, 2019.

7. Mishra, B., et al., Drone-surveillance for search and rescue in natural disaster.

Upendra Kumar *, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: er.djthakur@gmail.com.*

Computer Communications, 2020. 156: p. 1-10.

8. Hou, L. and N.W. Bergmann, Novel Industrial Wireless Sensor Networks for Machine Condition Monitoring and Fault Diagnosis. IEEE Transactions on Instrumentation and Measurement, 2012. 61(10): p. 2787-2798.

9. Chae, M.J., et al., Development of a wireless sensor network system for suspension bridge health monitoring. Automation in Construction, 2012. 21: p. 237-252.

Upendra Kumar *, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: er.djthakur@gmail.com.*