Public Health Care Cybersecurity Challenges and Solutions for Cyber-Attacks on Critical Health Infrastructure

Manish Nandy [1], Ahilya Dubey[2]

[1]*Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India*
[2]*Research Scholar, Department of CS & IT, Kalinga University, Raipur, India*

KEYWORDS

Health care data, attacks, protocols, Artificial intelligence

ABSTRACT

The opportunities for public health care and safety are especially high, and the healthcare industry is particularly susceptible to cybersecurity threats. Cybercriminals find healthcare facilities appealing due to their size, reliance on technology, handling of sensitive data, and susceptibility to certain disruptions. The Internet of Things, or IoT, has gained a lot of traction in recent years due to its many benefits, which include reduced costs, time savings, enhanced user comfort, and effective use of electricity. The most crucial component of the cyber-physical system is the low-capacity sensor node. These components are diverse in nature and can function as hosts or clients on the internet by connecting via a wireless network. The well-known security features found in desktop computers are inoperable on these systems because of resource constraints such low processor power, low storage capacity, and low energy backup. The suggested study uses SNMP in conjunction with an ANN classifier and secure data transmission to detect cybersecurity attacks on healthcare data and medical devices. The vulnerabilities in the security of IoT-centric systems give rise to privacy concerns that impact the use of smart environment applications.

1. Introduction

Data are currently dispersed as forms, reports, statistics, and other items. They serve as inputs for several categories of approaches. Due to the current technological boom, numerous strategies have been developed, and research is ongoing to find solutions for the problems that arise in every industry [1]. Technology has evolved into a highly useful tool for locating flaws in a certain industry and for quickly and efficiently fixing problems. This rapidly advancing technology is particularly significant in the field of health care [3]. When it comes to producing the outcome in a real-time scenario, this has greatly helped. Despite this, a great deal of research and studies have been carried out in a variety of sectors [13]. The medical field, in particular, has expanded the use of technology for official data access and result estimation that can be presented globally [2]. Cybercrime quickly adjusts to changes in the global environment. Malware hackers discovered widespread vulnerabilities during the start of the COVID-19 pandemic's escalation and modified their assaults to take advantage of these flaws [15] [4]. The rest of the paper is organized as follows: Section 2 provides the classification scheme for the survey; Section 3 provides an overview of proposed architecture. Section 4 provides a summary and comparison of the results of the various papers discussed in this taxonomy. Finally, Section 5 concludes the paper.

Related Works

Security is a key worry in a lot of CPS-based applications, according to important research questions [16]. Numerous security procedures are currently in place to safeguard different types of networks, desktop PCs that stand alone, internet services, and cloud security. The current systems function effectively across several platforms [19]. Security threats in CPS system application areas are displayed in the aforementioned application [8]. Various security problems impede the introduction of CPS, despite its huge potential to improve services in daily life. Security methods need to be implemented into CPS design and application development to prevent data breaches or disasters on a national scale [6]. In a CPS application, about 70% of the items are open to different kinds of attacks.

Current research endeavours tackle challenges and issues linked to CPS security [7]. A lot of researchers concentrate on application security problems [5]. Some attempt to solve the problem by suggesting security measures [10]. A select few are listed below. A security framework is used in the implementation of several current solutions [17]. Certain solutions use MQTT and other communications protocols, such as CoAP [21]. A particular solution is developed by a researcher that focuses on smart home systems [9]. Limited support for security mechanisms for devices based on constraints has been noted in several articles [11]. A small number of academics suggested using a lightweight session key generation process in home smart devices with limited resources [18] [14]. The SNMP-ANN may be appropriate for use by CPS devices that are diverse and resource-constrained [12]. It was necessary to design a lightweight security mechanism for heterogeneous and resource-constrained CPS devices that would need the least amount of memory and energy [20].

2. Methodology

The Simple Network Management Protocol (SNMP) provides a standard method for data sharing between nodes and components in a network for the purposes of network maintenance and monitoring. Any networked system that has to be monitored is launched by a Network Management Service, which is a component of SNMP. As the agent, the "snmpd" process on each network element collects network statistics from that node at many layers and for various protocols, such as TCP, UDP, ICMP, FTP, and HTTP. Data gathered by the "snmpd" procedure is stored in a collection of things known as the "Management Information Base" (MIB). The MIBs are nothing more than a group of objects stacked in a manner reminiscent of a tree. The leaves of the trees are the variables that hold the actual values of the network parameters; objects make up the roots. Of the thousands of MIBs available, TCP, UDP, ICMP, and IP are the four unique MIB groups from which 22 variables are chosen.

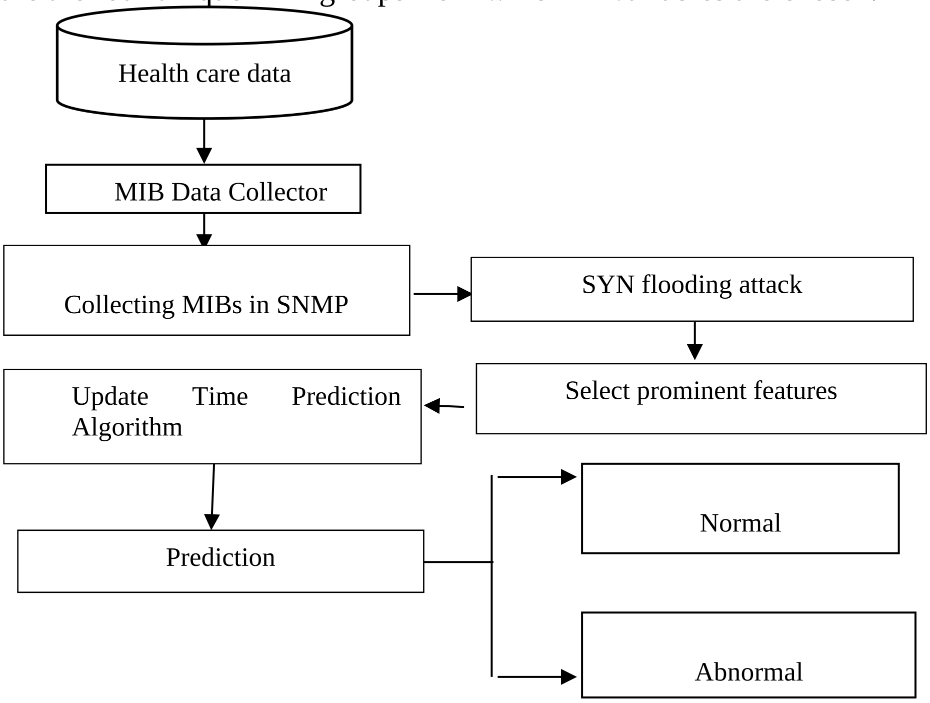

Figure 1: Framework of Proposed Method

ANN The real-time SNMP-MIB data, which is utilised to create the data's classifier, has seven properties. A first-level ANN classifier is constructed to discriminate between the Normal and Attack classes using the real-time data. The second level ANN classifier generates eight classes of network, transport, and application layer attacks in addition to a normal class. The final step of the proposed model focuses on classifying attacks. Once the attacks are identified, the phase of classification assigns a classification of either attack or normal. These classification methods enable the model to discriminate between the Normal and Attack classes.

3. Results and discussion

In order to finish the validation method, TCP specific SNMP MIBs are monitored by running the experimental SNMP setup in a controlled environment in accordance with the study. Four PCs were set up: one as the L2 switch, one as the attacker, one as the typical user, and one as the SNMP manager. An SNMP agent is deployed on both the attacker's and the average user's computers in order to collect statistics. A test bed is configured to mimic both standard traffic requests and the TCP-SYN attack. Any Web servers on the victim PC, like Apache or XAMPP server, will process requests. The simulated outcomes of the recommended method are presented in this section.

Table 1: ANN Testing Results for real time data

Types of attack	**Accuracy (%)**	**Processing time (sec)**	**Memory Utilization (%)**
Normal	97	576.38	75.21
Attack	98.5	193.39	45.25

The tabular summary of the testing outcomes for the ANN-based attack classification is provided in Tables 1.

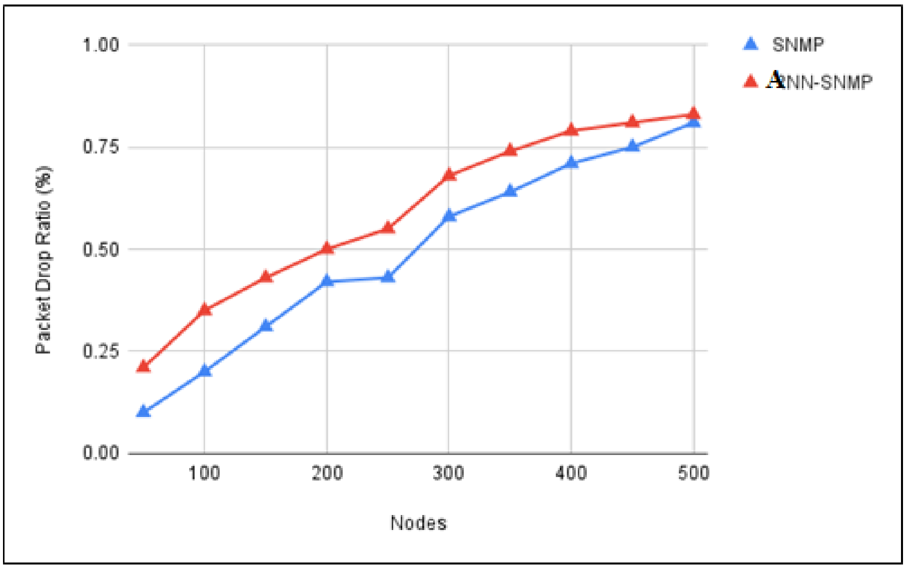

Figure 2: Packet Drop Ratio

Figure 2 and 3 displays sample MIB variable values under both normal and assault settings. When there is an attack, the variable's value is significantly higher than it is under regular circumstances.

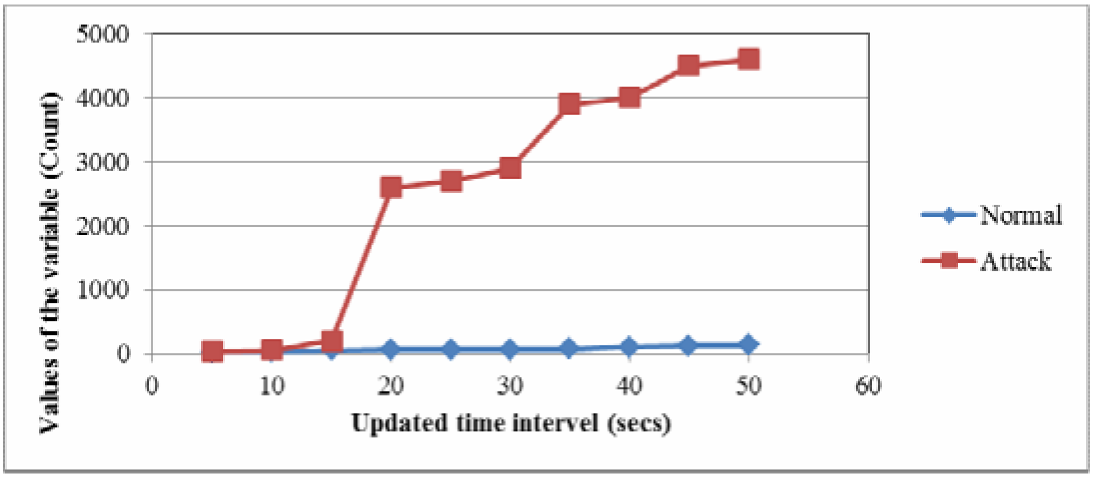

Figure 3: Change of MIB variable during increasing time intervals

The prediction of the network and the assault scenario is highly dependent on the data arrival rate. The assault can be lessened by using the routing protocol with the artificial intelligence model and accounting for the data arrival rate in the network system and to the cluster zone. Future modifications to the artificial intelligence model will depend on the objective and extent of a particular application. In this instance, costs are down while network efficiency rises.

4. Conclusion and future scope

Devices that are based on constraints are the primary focus of cyber-physical systems security mechanisms. The current security algorithm functions flawlessly on the CPS system, which has superior hardware support. However, a light-weight security mechanism that supports and operates with the least amount of hardware capabilities is needed for constraint-based applications. The goal of this research project is to provide a security mechanism that can be used with the current constraint-based CPS application. The research project creates the SNMP security algorithm. This study examined algorithm implementation and security concerns for devices with constraints. The results of the experiment demonstrate that the method requires very little system time to execute, allowing the system to use its lower computing power. The algorithm-based programme is given very little storage capacity.

Reference

[1] Wan, Yichen, Youyang Qu, Wei Ni, Yong Xiang, Longxiang Gao, and Ekram Hossain. "Data and Model Poisoning Backdoor Attacks on Wireless Federated Learning, and the Defense Mechanisms: A Comprehensive Survey." *IEEE Communications Surveys & Tutorials* (2024).

[2] Jebur, Tuka Kareem. "Securing Wireless Sensor Networks, Types of Attacks, and Detection/Prevention Techniques, An Educational Perspective." *ASEAN Journal of Science and Engineering Education* 4, no. 1 (2024): 43-50.

[3] Yashir Ahamed, M., Lalthlamuanpuii, R., Chetia, B., Lallawmawmi, & Lalngaizuali. (2023). Usage of Medical Library Resources: A Study in the Regional Institute of Medical Sciences, Imphal. Indian Journal of Information Sources and Services, 13(2), 1–6.

[4] Moundounga, Anselme Russel Affane, and Hassan Satori. "Stochastic Machine Learning Based Attacks Detection System in Wireless Sensor Networks." *Journal of Network and Systems Management* 32, no. 1 (2024): 17.

[5] Kodric, Z., Vrhovec, S., & Jelovcan, L. (2021). Securing edge-enabled smart healthcare systems with blockchain: A systematic literature review. Journal of Internet Services and Information Security, 11(4), 19-32.

[6] Rajasoundaran, S., SVN Santhosh Kumar, M. Selvi, K. Thangaramya, and Kannan Arputharaj. "Secure and optimized intrusion detection scheme using LSTM-MAC principles for underwater wireless sensor networks." *Wireless Networks* 30, no. 1 (2024): 209-231.

[7] Allen, Ashley, Alexios Mylonas, Stilianos Vidalis, and Dimitris Gritzalis. "Smart homes under siege: Assessing the robustness of physical security against wireless network attacks." *Computers & Security* 139 (2024): 103687.

[8] Malathi, K., Shruthi, S.N., Madhumitha, N., Sreelakshmi, S., Sathya, U., & Sangeetha, P.M. (2024). Medical Data Integration and Interoperability through Remote Monitoring of Healthcare Devices. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 15(2), 60-72. https://doi.org/10.58346/JOWUA.2024.I2.005

[9] Gebremariam, Gebrekiros Gebreyesus, J. Panda, and S. Indu. "Localization and detection of multiple attacks in wireless sensor networks using artificial neural network." *Wireless Communications and Mobile Computing* 2023 (2023).

[10] Marangunic, C., Cid, F., Rivera, A., & Uribe, J. (2022). Machine Learning Dependent Arithmetic Module Realization for High-Speed Computing. Journal of VLSI Circuits and Systems, 4(1), 42-51.

[11] Embarak, Ossama H., and Raed Abu Zitar. "Securing Wireless Sensor Networks Against DoS attacks in Industrial 4.0." *Journal of Intelligent Systems & Internet of Things* 8, no. 1 (2023).

[12] Tengshe, Richa, and Eisha Akanksha. "Security in LP-WAN Technologies: Challenges and Solutions." In *2023 IEEE 8th International Conference for Convergence in Technology (I2CT)*, pp. 1-4. IEEE, 2023.

[13] Jelena, T., & Srđan, K. (2023). Smart Mining: Joint Model for Parametrization of Coal Excavation Process Based on Artificial Neural Networks. Archives for Technical Sciences, 2(29), 11-22.

[14] Donkol, Ahmed Abd El-Baset, Ali G. Hafez, Aziza I. Hussein, and M. Mourad Mabrook. "Optimization of intrusion detection using likely point PSO and enhanced LSTM-RNN hybrid technique in communication networks." *IEEE Access* 11 (2023): 9469-9482.

[15] Bhatti, David Samuel, Shahzad Saleem, Zulfiqar Ali, Tae-Jin Park, Beomkyu Suh, Ali Kamran, William J. Buchanan, and Ki-Il Kim. "Design and Evaluation of Memory Efficient Data Structure Scheme for Energy Drainage Attacks in Wireless Sensor Networks." *IEEE Access* 12 (2024): 41499-41516.

[16] Saleh, Hadeel M., Hend Marouane, and Ahmed Fakhfakh. "Stochastic Gradient Descent Intrusions Detection for Wireless Sensor Network Attack Detection System Using Machine Learning." *IEEE Access* (2024).

[17] Saritha G., et.al VLSI based 1-d ict processor for image coding, Middle - East Journal of Scientific Research, V-20, I-12, PP:2620-2625, 2014.

[18] Kumar, Yogendra, and Vijay Kumar. "A Systematic Review on Intrusion Detection System in Wireless Networks: Variants, Attacks, and Applications." *Wireless Personal Communications* (2023): 1-58.

[19] Xiao, L., Wei, W., Yang, W., Shen, Y. and Wu, X. (2017), ‘A protocol-free detection against cloud oriented reflection dos attacks’, Soft Computing 21(13), 3713–3721.

[20] Bobir, A.O., Askariy, M., Otabek, Y.Y., Nodir, R.K., Rakhima, A., Zukhra, Z.Y., Sherzod, A.A. (2024). Utilizing Deep Learning and the Internet of Things to Monitor the Health of Aquatic Ecosystems to Conserve Biodiversity. Natural and Engineering Sciences, 9(1), 72-83.

[21] Malik, Ayasha, Bharat Bhushan, Surbhi Bhatia Khan, Rekha Kashyap, Rajasekhar Chaganti, and Nitin Rakesh. "Security Attacks and Vulnerability Analysis in Mobile Wireless Networking." In *5G and Beyond*, pp. 81-110. Singapore: Springer Nature Singapore, 2023.