IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 7, July 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207147 |

Protecting Industrial Healthcare Systems: An Integrated SDN and RL Approach

Deepika M[1], Seema Nagaraj [2]

Student, Department of Master of Computer Applications, Bangalore Institute of Technology, Bengaluru, Karnataka, India[1]

Assistant Professor, Department of Master of Computer Applications, Bangalore Institute of Technology, Bengaluru, Karnataka, India[2]

ABSTRACT: With the advent of IoMT, the healthcare industry is entering a new tech age with numerous benefits such as virtual care, continuous monitoring and widespread supervision. However, this progress also brings significant cybersecurity and confidentiality challenges. This paper focuses on the application of IEC 60 870-5-104 standards, commonly used in corporate medical environments. We investigate the intrusion based on this norm and assess their severity using an analytical threat model that incorporates Attack Défense Tree and Common Vulnerability Scoring System v3.1. Subsequently, we propose an intrusion detection and prevention system (IDPS) specifically designed to counter IEC 60 870-5-104 threats. This IDPS leverages both software-defined networking (SDN) and neural networks (ML) technologies. Furthermore, we utilize Transmission Control Protocol /Internet Protocol network traffic to identify IEC 60 870-5-104 hacks and analyse payload flow statistics and metrics related to the norm.

KEYWORDS: Cyber-attacks, Protocol, Medical assistance, Healthcare.

I. INTRODUCTION

The Internet of Medical Things (IOMT) is rapidly revolutionizing the medical sector, providing valuable benefits such as remote surveillance, faster diagnosis, preventive care, and health education. Especially in the context of the current COVID-19 pandemic and potential future pandemics, this transformation and the complete digitalization of hospital cyber-physical infrastructure have become more crucial than ever before. However, despite the advantages, this advancement brings forth significant personal and cybersecurity concerns due to the immense value of medical data and the vulnerabilities present. Healthcare applications collect a vast amount of personally identifiable information, making the medical services sector one of the most sensitive critical infrastructures regarding information security. The recent WannaCry ransomware outbreak in May of this year, which severely impacted the health systems in England and Wales, serves as a typical example of digital safety challenges hospitals face.

II. RELATED WORK

The existence of trustworthy intrusion detection and prevention techniques is thus essential in light of the previous observations. The IEC 60 870-5-104 protocol, which is commonly used by workplace medical organisations, is the subject of the current paper [1]. IEC 60 870-5-104 has serious security weaknesses given that it lacks sufficient systems for registration and permission. Therefore, it enables suspected online criminals to carry out a variety of intrusions such Attack of Unapproved access and denial of customer service. Sophisticated assault on ISO 60 870-5-104 has the potential to have catastrophic effects on the health care industry. It is also significant that various other CIs employ IEC 60 870-5-104.

The problems with safety in the healthcare sector have been studied in a number of articles. Several varieties are detailed in They et al., in particulars, explore the weaknesses of the smart medical devices and provide appropriate defensive measures in [2]. The cybersecurity and privacy issues posed by electronic healthcare services in web-based environments are discussed by Chenthara et al. in. Comparable to this, Wolker-Roberts et al. talk about pertinent defences over internal dangers within healthcare CIs.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

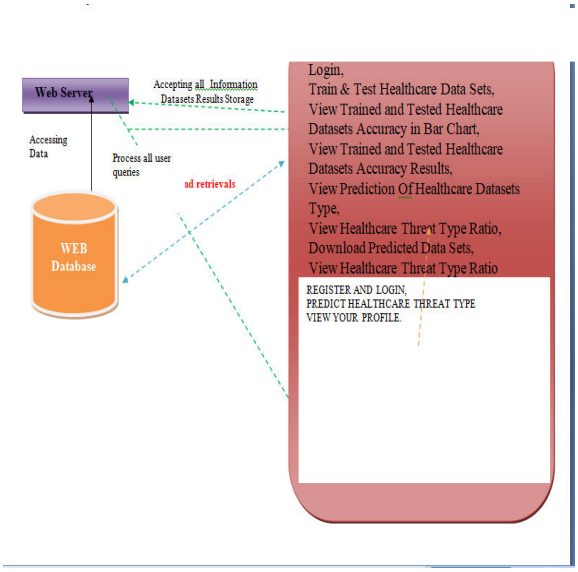
| DOI:10.15680/IJIRSET.2023.1207147 |

III. METHODOLOGY

The proposed IEC 60 870-5-104 threat modelling integrates ADT or CVSS, which identify the potential vectors of attack and associated risks. An ADT is made up of two antagonism nodes, and namely eight offensive elements and 32 protecting elements. The assault nodes outline the objective and possible course steps that an internet criminal might take in order to jeopardise the intended target it's stability. The defensive tubes represent the protections an opponent can employ to counter or lessen an attack from hackers. Each node can have one or more offspring who belong to the same kind (for example, an assault node or a protecting tree), signifying the division into more precise subobjectives and operations. A node in the hierarchy is considered a nonrefined node, and then as denotes a fundamental action, if it has no refine Kids of an identical type). Additionally, a node may have off-type offspring, suggesting a measure to counteract. The proposed system implemented 1Performances for abatement and discovery are sufficient processes on facts.

The notification and response module (NRM) for datasets prediction was built by the idea that was put forward.

IV. EXPERIMENTAL RESULTS



The researchers of [5] undertake an abstract threat analysis of the businesses that comply with IEC 60 870-5-104. Two kinds of cyberattacks are identified according to an investigation using coloured Petri nets (CPNs): 1) Physical assaults; and 2) online assaults. The inaugural group includes any actions taken by someone who has direct physical access to the target system. On one hand, intrusions are those that take use of IEC 60 870-5-104 flaws. According to the authors, the second group especially contains the following four kinds:

1) unauthorized access;
2) man-in-the-middle (MITM);
3) DoS;
4) traffic analysis

The recommended IDS utilizes specialized state-of-the-art computers, which, in turn, can employ a detection level generator. The experimental results corroborate the effectiveness of the suggested IDS.

The results of this assessment indicate that J48 performs at its peak. To identify intrusions linked to IEC 60 870-5-104, Yang et al. [4] develop signature and specification rules that are Ats responsive. The distinction from sign norms and spec rules is that one of them classifies malevolent motifs, whilst the latter class categorizes typical behaviour. The comparable investigators provide an intrusion detection system (IDS) based on specifications that may identify IEC 60 870-5-104 irregularities in [7].

V. CONCLUSION

The insecure legacy healthcare systems and the development of the Internet of Things (IoMT) create opportunities for attacks, necessitating digitalization in the healthcare sector. We focused on the frequently used IEC 60 870-5-104

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207147 |

standard in the article. Firstly, we designed a quantitative threat model to assess potential cyberattack severity based on IEC 60 870-5-104 directives. Next, we proposed an IDPS system combining ML or SDN to detect and prevent IEC 6180-5-104 breaches. The IDPS uses a CART algorithm to analyze payload flow statistics and TCP/IP communication characteristics. On the other hand, SDN-based abatement resolves MAB risk using the TS technique. The results showed the effectiveness of the suggested IDPS. Our long-term goals are to upgrade the monitoring service to recognize multistep intrusions related to IEC 60 870-5-104 and other protocols in the medical sector, like Modbus, MQTT, and EtherCAT, using ML-based association rules techniques.

REFERENCES

[1] T. Yaqoob, H. Abbas, and M. Atiquzzaman, "Security vulnerabilities, attacks, countermeasures, and regulations of networkedmedical devices—A review," *IEEE Commun. Surv. Tut.*, vol. 21, no. 4, pp. 3723–3768, Oct./Dec. 2019.
[2] M.Conti, D. Donadel, and F. Turrin, "A survey on industrial control system testbeds and datasets for security research," 2021, *arXiv:2102.05631*.
[3] E. Hodo, S. Grebeniuk, H. Ruotsalainen, and P. Tavolato, "Anomaly detection for simulated IEC-60870-5-104 traffic," in *Proc. 12th Int. Conf. Availability, Rel. Secur.*, 2017, pp. 1–7.
[4] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, B. Pranggono, and H. Wang, "Intrusion detection system for IEC 60870-5-104 based SCADA networks," in *Proc. IEEE Power Energy Soc. Gen.Meeting*, 2013, pp. 1–5.
[5] P.Radoglou-Grammatikis, P. Sarigiannidis, I. Giannoulakis,E.Kafetzakis, andE. Panaousis, "Attacking IEC-60870-5-104SCADAsystems," in *Proc.*
IEEE World Congr. Serv. (SERVICES), 2019, pp. 41–46.
[6] P. R. Grammatikis, P. Sarigiannidis, A. Sarigiannidis, D. Margounakis, A. Tsiakalos, and G. Efstathopoulos, "An anomaly detection mechanism for IEC 60870-5-104," in *Proc. 9th Int. Conf. Modern Circuits Syst. Technol.*, 2020, pp. 1–4.
[7] Y. Yang, K. McLaughlin, S. Sezer, Y. Yuan, and W. Huang, "Stateful intrusion detection for IEC 60870-5-104 SCADA security," in *Proc. IEEE PES Gen. Meeting Conf. Expo.*, 2014, pp. 1–5.
[8] P. Radoglou-Grammatikis *et al.*, "Spear SIEM: A security information and event management system for the smart grid," *Comput. Netw.*, vol. 193, 2021, Art. no. 108008.
[9] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, "Security and privacy-preserving challenges of e-health solutions in cloud computing," *IEEE Access*, vol. 7, pp. 74361–74382, 2019.
[10] S. Walker-Roberts, M. Hammoudeh, and A. Dehghantanha, "A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure," *IEEE Access*, vol. 6, pp. 25167–25177, 2018.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details