A Review on SCADA for Healthcare Systems

Ebenezer Agbozo
Department of Big Data Analytics and Methods of Videoanalysis
Ural Federal University
Ekaterinburg, Russia
eagbozo@urfu.ru

Karla Elena Peláez Cruz
Department of Big Data Analytics and Methods of Videoanalysis
Ural Federal University
Ekaterinburg, Russia
karlaelenapelaezcruz@gmail.com

Adanen Kuakan Arno
Department of Big Data Analytics and Methods of Videoanalysis
Ural Federal University
Ekaterinburg, Russia
arnaudkouakan@gmail.com

Mutahar Mohammed Abdulmalek Mohammed
Department of Big Data Analytics and Methods of Videoanalysis
Ural Federal University
Ekaterinburg, Russia
mohammedmutaher3@gmail.com

***Abstract*—Healthcare systems continue to experience an increased level of technological innovation due to the desire to provide quality services for patients and improve decision-making by healthcare providers. Technologies such as artificial intelligence (AI), digital twins, big data, and blockchain are some of these novel solutions being implemented. This study explores the state of research of one of such innovations in healthcare which is known as Supervisory Control and Data Acquisition (SCADA) systems. Though SCADA systems are widely known in the manufacturing and production spheres, they have experienced a gradual level of adoption in healthcare organizational systems. The study adopts a computational literature review method to extract knowledge from literature using prominent sources and explores the implementation of SCADA systems in healthcare. Our study revealed that SCADA systems research particularly with respect to their deployments in healthcare mainly focused on cyber security. The study presents a snapshot of research on SCADA systems in healthcare and provides research trajectories to guide future research.**

Keywords— Healthcare, SCADA, Cyber Security, Cyber-physical systems, Artificial Intelligence

I. Introduction

The healthcare industry continually experiences huge transformations which have been influenced by the enormous advancements in technology. This has been fuelled by the desire to provide high quality services for patients, increase operational efficiency, and improve decision-making of health experts. In recent times, technologies such as artificial intelligence (AI), machine learning (ML), blockchain and big data have been instruments in the modern technological revolution within various aspects of healthcare; starting from diagnostics to out-patient management. One of such technological innovations that has the ability and potential to transform healthcare operations is Supervisory Control and Data Acquisition (SCADA) systems.

SCADA systems have been developed and implemented in industrial applications primarily for the purpose of manufacturing and production. SCADA systems provide real-time monitoring, control and automation for various functions and processes. In addition, on a minimal level, the healthcare sector is one of such places SCADA systems are deployed in conjunction with medical devices in hospitals as well as healthcare information systems.

The study adopts a computational literature review method to extract knowledge from literature from prominent scientific sources that highlight the implementation of SCADA systems in healthcare. The study presents a snapshot of research on SCADA systems in healthcare and provides research trajectories to guide future research.

II. Digital Transformation in Healthcare

Presently, advancements in technology and science with respect to many domains within the healthcare industry have experienced massive improvement; including that which is related to digital technologies. These advancements seek to develop new therapies and provide best practices for providing better health management procedures; such as improvements in patient care, operational efficiency, and overall healthcare outcomes. These encompass digital transformation which refers to the changes in digital technology used to benefit society [1].

Like any other sector of society, the health industry produces large volumes of data on a regular basis consisting of personal medical records, radiology and fluoroscopy images, clinical trials, surveys, demographic data, human genomes and genetic sequences, etc. [2]. This data for the longest time has been used when the symptoms of a medical condition are evident and can no longer be avoided, but with the use of big data analytics and machine learning, proactive actions can be taken by the decision-maker to help support their medical care. These proactive decision support aid is as a result of descriptive, diagnostic, predictive and prescriptive analytics used for optimization of current processes such scheduling surgeries semi-automatically and offering efficient care and/or cure alternatives to the medical staff [3].

Due to the volume of data generated by patients' medical history, machine learning techniques possess enormous potential in the healthcare field. Common health informatics algorithms and techniques include: K-Nearest Neighbor Algorithm, Support Vector Machines (SVM), K-Means Clustering Techniques and Artificial Neural Networks [2].

During the 2020 COVID-19 pandemic, several studies were performed to study the risk factors on different populations. To identify epidemiological patterns of outbreak

prevalence, K-Means-LSTM was used to forecast the COVID-19 outbreak for the state of Louisiana in the USA. This study suggested K-Means-LSTM as a useful tool for modeling the outbreak based on the results reported given the complex nature of the COVID-19 outbreak and its parish-to-parish behavioral variation [4].

Augmented Reality (AR) and Virtual reality (VR) are another healthcare innovation that are making steps in changing the lives of patients and healthcare professionals alike. Some rehabilitation centers have adopted VR to help patients recovering from stroke or other neurological conditions in order to retrain their brains and learn new skills [5]. The technologies offer individuals an immersive experiences that help them overcome various mental health problems and such rehabilitation therefore helps patients overcome their phobias and improve their quality of life.

Medical technologies also play a crucial role in the treatment and cure of various conditions and diseases: e.g., minimally invasive surgical techniques that can relieve caregivers and minimize patient discomfort (i.e. fewer complications and faster recovery). Examples include robotic surgery or endoscopy, complications and faster recovery), such as robotic surgery or endoscopy. Imaging-guided radiotherapy, nanomedicine, active wound management, "smart" implants (e.g. pacemakers with remote monitoring) and self-catheterization are other examples [6, 7]. Some technological innovations have considerably improved diagnostic possibilities, enabling doctors to make more accurate and faster diagnoses: for example, artificial intelligence-assisted medical imaging, point-of-care testing (POCT) carried out close to the patient, artificial intelligence and machine learning in in vitro diagnostics to assist pathologists in their work, etc.

Innovation certainly facilitates and accelerates the changes needed to achieve (better) quality, targeted care, but an important point is that not all technologies that modify the care process have a purely clinical impact for the patient. Some have a societal added value (e.g., faster return to work after a minimally invasive procedure), while others have an organizational added value (e.g., less travel by or to caregivers and more efficient use of care staff in the case of remote monitoring, better use of equipment thanks to faster radiation in the case of radiotherapy, etc.). Although these results are extremely valuable, innovative technologies are not always fully appreciated and accepted for different reasons. One of them is its organizational added value, which is more difficult to measure, and therefore understand its results.

One of such novel transformations is SCADA systems. These systems have revolutionized the production and manufacturing sector. The health sector has also had its fair share of technological improvement, as such this study aims to explore the state of research on SCADA systems in healthcare from a review perspective. The implementation and the use of SCADA systems in healthcare is in its elementary years, as a result of that this is indeed required to address the challenges and the benefits related to the integration of SCADA systems in the healthcare. Our study discusses the following questions:

1. What are the current use cases of SCADA systems in healthcare?

2. What are the benefits of SCADA systems in the healthcare?

3. What are the obstacles in cybersecurity that face these systems in healthcare and the future aspects need to be explored to improve the use of SCADA systems in healthcare?

The main goal of this study is to offer an in-depth examination of the role SCADA systems play in the healthcare sector, highlighting both the advantages and challenges associated with their implementation, especially concerning cybersecurity. Through a review of existing literature, this study explores the state of current research and potential directions for future research. The subsequent sections of the paper are organized as follows: section 3 highlights a brief overview of SCADA systems and the challenges of the system; section 4 presents the data and method for the study followed by the findings in section 5; finally section 6 concludes on the study.

III. A Brief Overview of SCADA Systems

In the world of industrial automation, the optimization of SCADA systems has become an essential aspect for increasing efficiency. Within these industrial systems, managers and workers play pivotal roles in overseeing and executing tasks, respectively and the use of additional technology is aimed at increasing the uptime and the work effectiveness. Thus, the data coming from the sensors gathered by the SCADA system plays the main role in the decision of the managers and workers.

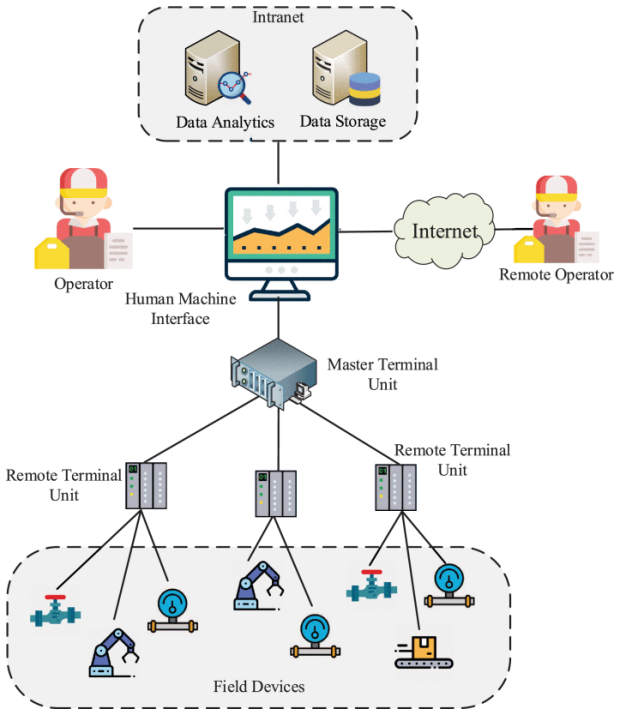

Fig. 1. Architecture of SCADA Systems in Healthcare [8]

Fig. 1 illustrates a SCADA systems consist of: (a) Operator(s) – that oversee the monitoring of entire system (on-premises/remote); (b) Master Terminal Unit (MTU) – collates data from remote terminals and transfers control signals; (c) Human-Machine Interface (HMI) – for managing interactions between the operator and the SCADA system; (d) RTU – handle data and command exchange with the MTU as well as communicates signals with field devices; (e) Intranet – the local network for connecting systems and devices; (f) Field

devices – refer to the systems/devices that perform activities in the organization [8]. SCADA systems are known to be the backbone of numerous critical infrastructures such as water supply systems, oil pipelines, transportation and electricity and play a role in monitoring data fed from transmitters, pumps and valves [9]. With respect to applications, SCADA has been applied in wind turbines for fault detection coupled with machine learning algorithms (forecasting and anomaly detection) [10, 11]. In water treatment plants (WTP), SCADA has been used in intake monitoring for improving plant efficiency and effective energy management [12]. Within the energy sector, SCADA systems are used to monitor as well as control electricity flow through a power grid [13].

Just as local servers and critical infrastructure, SCADA interfaced with internet and network infrastructure is in danger of threats and attacks to the cyber-physical system's performance [14, 15]. As summarized by research, SCADA systems face threats which may include: (a) physical security - due to their geographical location; (b) operating system (OS) vulnerability - updates and patches which may interrupt the system's efficiency; (c) authentication vulnerabilities; (d) legacy systems; (e) wireless network vulnerabilities; (f) leaked critical data and credentials [16, 17]. In addition, researchers have explored the challenges, and security issues of these systems [8, 18]. These studies highlighted challenges such as man-in-the-middle attacks, Masquerade, Eavesdrops, Trojan horse, doorknob rattling, Cinderella, Fragmentation, and denial-of-service (DOS) attacks [19]. Thus, research on SCADA has also focused on safeguarding SCADA systems. A study focused on using honeypots and recommended the implementation of strong security measures, regular software updates, as well as secure remote access [20]. Another study highlighted that due to the increased levels of cyber-attacks, intrusion detection systems (IDS) which can be host-based or network-based, can be deployed in SCADA systems [13].

In recent years a significant number of cyberattacks on the SCADA systems related to healthcare have been reported and it's noticed that it is in continuous growth. The cyberattacks and the attackers mostly targeted SCADA systems gaining unauthorized access and potentially compromising sensitive healthcare process. The attackers use high level tools and sophisticated ways to take advantage from the weaknesses of SCADA systems. This study highlights some of the recent incidents that affected the healthcare sector.

The SamSam Ransomware Attack on Atlanta in early 2018 paralyzed municipal services in a major U.S. city without a single shot being fired, exemplifying the concept of a "Silent Battle". Healthcare organizations in Indiana, Virginia, New York, and Buffalo, were also hit. While other ransomware attacks have affected broader scales, the SamSam attacks, which brings the issue of cybersecurity on the table again [21]. Another example for this cyberattacks is "Wannacry Ransomware attack 2017", Wanncy Ransomware attack it consider to be one of the largest attacks that were ever carried out in the history of cyberattacks. It grabbed the world by storm. According to eScan antivirus reports, India was one of the worst affected by cyber-attack [22]. Such attacks halted hospital facilities and infected large corporations and consumers in over 150 countries [23]. The WannaCry ransomware attack affected more than 300,000 Windows computers across more than 150 countries. The malware's dropper contained two key parts: one that exploited the "EternalBlue" vulnerability in Windows' Server Message Block (SMB) protocol to spread, and another that served as the WannaCry ransomware component, encrypting data on infected systems [23].

IV. Data and Method

To answer the research questions posed above, this research adopted the computational literature review approach. In conducting the study, the research adopted the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to support the process of collating the data (which in this case was from Web of Science database) for analyzing the literature for the study. The PRISMA framework was adopted for the study so as to support the selection of valid research that align with the study's goal(s) [24]. After the dataset was obtained, the study uses computational algorithms for knowledge extracting from literature through computational literature review (CLR). CLR though in its early days has been commended due to the fact that it contributes immensely to the literature review process [25]. The search query was: ("Supervisory Control and Data Acquisition" OR "SCADA" AND "Healthcare"). The inclusion criteria: all articles written in English, and conference articles and journal articles. On the other hand, the exclusion criteria exempted all non-English articles. The resultant articles were used to conduct the computational review which would provide a snapshot of research with regards to SCADA systems in healthcare.

V. Results

A total of 16 articles (10 journal papers and 6 conference articles) were obtained from the Web of Science database and the research publication years span 2013 to 2023 (with a research growth rate of 14.87%); from 15 sources; 52 authors (with approximately 3.31 co-authors per document and 18.75% international collaboration). With respect to research output, majority of studies on SCADA and healthcare are associated with IEEE conference proceedings (International Conference on Global Security, Safety and Sustainability (ICGS3); IOT, Electronics and Mechatronics Conference (IEMTRONICS); and IEEE International Conference on Systems, Man, and Cybernetics), and journals such as MDPI's Applied Sciences; International Journal of Critical Infrastructures; International Journal of Information Security; Cluster Computing; Communications in Computer and Information Science; Forensic Science International-Digital Investigation; and Expert Systems with Applications. These scientific sources, though not many due to the intersection of domains being in its early days, serve as relevant and necessary for the growth of the themes.

Fig. 2 highlights the annual research production of SCADA systems in healthcare which spans a decade (2013 to 2023) and has experienced an undulating trajectory. In present times it is evident that research after 2021 has experienced a minimal rise which can be associated to the increased discussions surrounding themes that complement SCADA within healthcare such as artificial intelligence, and cyber security.

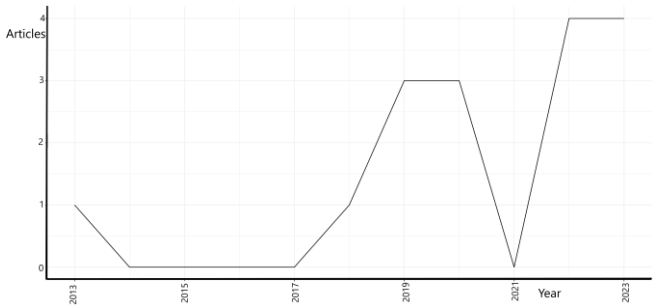

Fig. 2. SCADA Systems in Healthcare – Yearly Scientific Output (Source: Authors)

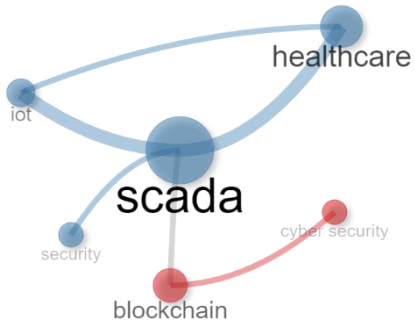

Fig. 3. SCADA Systems in Healthcare – Co-Occurrence Network (Source: Authors)

With respect to applications of SCADA systems in healthcare, research has identified their applicability in the monitoring and management of medical equipment, diagnostic facilities, healthcare systems, and laboratories, as well as collecting and analyzing real-time data of patients [26]. Another study highlighted the use of SCADA systems within IoT healthcare ecosystems and medical centers as relevant within the modern era of ubiquitous medical service provisioning and as a result of potential cyber security threats introduced machine learning techniques (K-Nearest Neighbors, Support Vector Machines, and Decision Trees) for the classification of cyber-attacks [27]. A study indicated that clinical or medical center workflow (within the context of operating rooms) can be improved by interoperability between heterogeneous medical devices and clinical information systems through the integration of automation via SCADA systems. According to the study, bottlenecks and instability challenges with respect to hospital networks can be mitigated through monitoring [28]. In another SCADA use case, researchers demonstrated remote real-time patient supervision through web-based infrastructure and non-invasive devices [29]. Research also highlighted the use of SCADA systems for the purpose of securing medical infrastructure [30]. With respect to medical cleanrooms, researchers designed an IOT-based approach in conjunction with SCADA for minimizing human intervention, identifying system anomalies and improving the supply of clean air [31]. Another study developed an intelligent monitoring system (based on causal reasoning) for real-time electrocardiogram (ECG) monitoring (anomaly detection) of patients which alerts the SCADA system for preventative measures to be taken by healthcare professionals [32]. Similarly, another study implemented a cloud-based SCADA system and a remote nerve stimulator for cardiac patients through bio-signals received from ECG embedded in wearable devices [33]. For another study, the application of SCADA is observed in the operating room, a safety critical environment, where medical devices are interconnected via network and must be monitored in real-time to prevent unwanted scenarios such as network failure, hard disk failure, or application crashes [34].

Fig. 3 highlights the salient themes in a co-occurrence network. These themes are currently at the core of SCADA in healthcare research. Fig. 4 provides a snapshot of the present and future state of research regarding SCADA in healthcare in the form of a thematic map. The thematic map classifies the state and possible trajectory of research summarized into four (4) quadrants to guide future research, policy makers and experts [35]. The quadrants are as follows: (A) Niche themes: topics located in the top-left quadrant are known to be highly specialized and central to the research domain; (B) Motor themes: located at the top-right quadrant, these topics are highly-developed and very relevant structuring themes of a research domain; (C) Emerging/declining themes: topics in the bottom-left quadrant have a low level of development and degree of relevance; (D) Basic themes: these topics are important but are still under development.

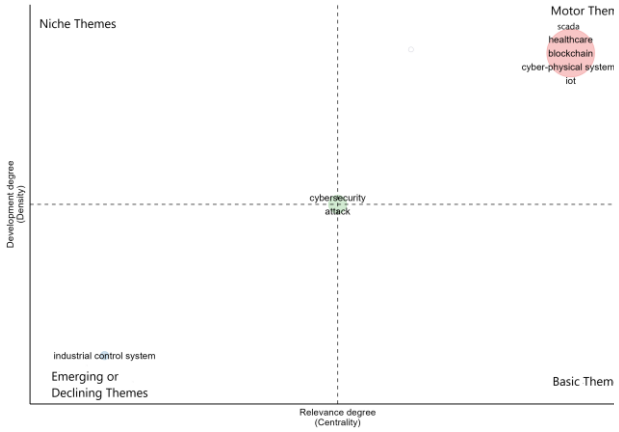

Fig. 4. SCADA Systems in Healthcare – Thematic Map (Source: Authors)

From the four (4) quadrants in Fig. 4, only two (2) clusters fall within the emerging/declining themes and motor themes quadrants, as well as one cluster that is central. The central cluster consists of two keywords namely, “cybersecurity” and attack. This is indicative of the fact that presently each study on SCADA systems in healthcare, whatever the focus, ensures to cover the essential topic to SCADA systems which is security. This is evident in the study that advocated for a framework for modelling cyber threats [36]. Another study identified the tendency of ransomware threats on SCADA systems to stall productivity and disrupt critical structure [37]. In the motor themes quadrant, terms like SCADA, healthcare, cyber-physical systems, blockchain, and internet of things (IOT). Blockchain technology and IOT devices in SCADA systems for healthcare infrastructure are evident in research that leverages hardware security primitives and distributed ledger for authentication of trusted devices to safeguard the entire system [38]. With respect to emerging/declining themes, the term Industrial Control System (ICS) stands out. With respect to ICS and SCADA, research continuous to focus on integrating efficient machine learning algorithms, and preventing cybersecurity threats to such systems [39–42]. In summary, the core focus of SCADA research is presently

focused on developing blockchain technology, digital twins, implementing formidable cybersecurity solutions, and applying AI algorithms to improve decision-making.

VI. Conclusion

This article conducted a review on research regarding the state and applications of SCADA systems in healthcare. SCADA systems have been an instrumental paradigm within the industrial setting for monitoring processes within the entire system. This study observed that all technological innovations integrated within SCADA systems are aimed at improving decision support with intelligent algorithms and play a major role in ensuring security of the system to prevent threats and unauthorized access. One limitation of the study is the scope of data (i.e. Web of Science) used for the study. As such, future research will focus on expanding the data sources to other researching indexing resources. In addition, future research should expand the query search to non-English articles, as well as build upon leveraging novel technological innovations to expand the integration of big data, AI, and machine learning into SCADA for improved healthcare decision-making.

References

[1] A. I. Stoumpos, F. Kitsios, and M. A. Talias, "Digital Transformation in Healthcare: Technology Acceptance and Its Applications," International journal of environmental research and public health, vol. 20, no. 4, p. 3407, 2023.

[2] N. Berros, F. El Mendili, Y. Filaly, and Y. El Bouzekri El Idrissi, "Enhancing digital health services with big data analytics," Big data and cognitive computing, vol. 7, no. 2, p. 64, 2023.

[3] J. Lopes, G. Vieira, R. Veloso, S. Ferreira, M. Salazar, and M. F. Santos, "Optimization of surgery scheduling problems based on prescriptive analytics," in Proceedings of the 12th International Conference on Data Science, Technology and Applications, DATA, 2023, pp. 474–479.

[4] S. R. Vadyala, S. N. Betgeri, E. A. Sherer, and A. Amritphale, "Prediction of the number of COVID-19 confirmed cases based on K-means-LSTM," Array, vol. 11, p. 100085, 2021.

[5] W. Powell, A. Rizzo, P. Sharkey, and J. Merrick, "Innovations and challenges in the use of virtual reality technologies for rehabilitation," Journal of Alternative Medicine Research, vol. 10, no. 1, 2018

[6] R. Ascione, The future of health: How digital technology will make care accessible, sustainable, and human. John Wiley & Sons, 2021.

[7] A. Awad et al., "Connected healthcare: Improving patient care using digital health technologies," Advanced Drug Delivery Reviews, vol. 178, p. 113958, 2021.

[8] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A survey on SCADA systems: secure protocols, incidents, threats and tactics," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1942–1976, 2020.

[9] M. Alanazi, A. Mahmood, and M. J. M. Chowdhury, " SCADA vulnerabilities and attacks: A review of the state - of - the - art and open issues," Computers & Security, vol. 125, p. 103028, Feb. 2023, doi: 10.1016/j.cose.2022.103028.

[10] P. W. Khan, C. Y. Yeun, and Y. C. Byun, "Fault detection of wind turbines using SCADA data and genetic algorithm-based ensemble learning," Engineering Failure Analysis, vol. 148, p. 107209, 2023.

[11] S. Sun, W. Hu, Y. Liu, T. Wang, and F. Chu, "Matching contrastive learning: An effective and intelligent method for wind turbine fault diagnosis with imbalanced SCADA data," Expert Systems with Applications, vol. 223, p. 119891, 2023.

[12] C. Rohmingtluanga, S. Datta, N. Sinha, and T. S. Ustun, "SCADA based intake monitoring for improving energy management plan: Case study," Energy Reports, vol. 9, pp. 402–410, 2023.

[13] A. Balla, M. H. Habaebi, E. A. A. Elsheikh, M. R. Islam, and F. M. Suliman, "The Effect of Dataset Imbalance on the Performance of SCADA Intrusion Detection Systems," Sensors, vol. 23, no. 2, Art. no. 2, Jan. 2023, doi: 10.3390/s23020758.

[14] B. Kesler, "The vulnerability of nuclear facilities to cyber attack; strategic insights: Spring 2010," Strategic Insights, Spring 2011, 201.

[15] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," in 2011 International conference on internet of things and 4th international conference on cyber, physical and social computing, IEEE, 2011, pp. 380–388.

[16] Y. Perwej, S. Q. Abbas, J. P. Dixit, N. Akhtar, and A. K. Jaiswal, "A systematic literature review on the cyber security," International Journal of scientific research and management, vol. 9, no. 12, pp. 669–710, 2021.

[17] G. Yadav and K. Paul, "Architecture and security of SCADA systems: A review," International Journal of Critical Infrastructure Protection, vol. 34, p. 100433, Sep. 2021, doi: 10.1016/j.ijcip.2021.100433.

[18] J. Gao, J. Liu, B. Rajan, R. Nori, B. Fu, Y. Xiao, W. Liang, and P. Chen, "SCADA communication and security issues: SCADA communication and security issues," Security Comm. Networks, vol. 7, no. 1, pp. 175–194, Jan. 2014, doi: 10.1002/sec.698.

[19] S. Ghosh and S. Sampalli, "A Survey of Security in SCADA Networks: Current Issues and Future Challenges," IEEE Access, vol. 7, pp. 135812–135831, 2019, doi: 10.1109/ACCESS.2019.2926441.

[20] M. Mesbah, M. S. Elsayed, A. D. Jurcut, and M. Azer, "Analysis of ICS and SCADA Systems Attacks Using Honeypots," Future Internet, vol. 15, no. 7, Art. no. 7, Jul. 2023, doi: 10.3390/fi15070241.

[21] K. Kraszewski, "SamSam and the Silent Battle of Atlanta," in 2019 11th International Conference on Cyber Conflict (CyCon), May 2019, pp. 1–16. doi: 10.23919/CYCON.2019.8757090.

[22] S. Mohurle and M. Patil, "A brief study of wannacry threat: Ransomware attack 2017," International journal of advanced research in computer science, vol. 8, no. 5, pp. 1938–1940, 2017.

[23] Q. Chen and R. A. Bridges, "Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware," in 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA), Dec. 2017, pp. 454–460. doi: 10.1109/ICMLA.2017.0-119.

[24] B. Hutton et al., "The quality of reporting methods and results in network meta-analyses: an overview of reviews and suggestions for improvement," PloS one, vol. 9, no. 3, p. e92508, 2014.

[25] V. A. Principe et al., “A computational literature review of football performance analysis through probabilistic topic modeling,” Artificial Intelligence Review, vol. 55, no. 2, pp. 1351–1371, 2022.
[26] V. Pabalkar and R. Verma, “SCADA in Healthcare,” in ICT Infrastructure and Computing, M. Tuba, S. Akashe, and A. Joshi, Eds., Singapore: Springer Nature, 2023, pp. 91–102. doi: 10.1007/978-981-99-4932-8_10.
[27] T. Öztürk, Z. Turgut, G. Akgün, and C. Köse, “Machine learning-based intrusion detection for SCADA systems in healthcare,” Netw Model Anal Health Inform Bioinforma, vol. 11, no. 1, p. 47, Nov. 2022, doi: 10.1007/s13721-022-00390-2.
[28] R. S. Tolentino, “Efficient SCADA Module for Improving Medical Information Monitoring and Reliable Medical Service in Hospital Networks,” 보안공학연구논문지, vol. 7, no. 4, pp. 311–318, 2010.
[29] J. K. Pollard, M. E. Fry, S. Rohman, C. Santarelli, A. Theodorou, and N. Mohoboob, “Wireless and Web-based medical monitoring in the home,” Medical Informatics and the Internet in Medicine, vol. 27, no. 3, pp. 219–227, Jan. 2002, doi: 10.1080/1463923021000014130.
[30] V. Kanchana, S. Nath, and M. K. Singh, “A study of internet of things oriented smart medical systems,” Materials Today: Proceedings, vol. 51, pp. 961–964, 2022.
[31] B. Amangeldy, N. Tasmurzayev, M. Mansurova, B. Imanbek, and T. Sarsembayeva, “Design and Development of IoT Based Medical Cleanroom,” in Advances in Computational Collective Intelligence, N. T. Nguyen, J. Botzheim, L. Gulyás, M. Nunez, J. Treur, G. Vossen, and A. Kozierkiewicz, Eds., Cham: Springer Nature Switzerland, 2023, pp. 459–469. doi: 10.1007/978-3-031-41774-0_36.
[32] U. Qidwai, J. Chaudhry, S. Jabbar, H. M. A. Zeeshan, N. Janjua, and S. Khalid, “Using casual reasoning for anomaly detection among ECG live data streams in ubiquitous healthcare monitoring systems,” J Ambient Intell Human Comput, vol. 10, no. 10, pp. 4085–4097, Oct. 2019, doi: 10.1007/s12652-018-1091-x.
[33] N. Rajasingam, S. Padmanaban, C. Ramkumar, and D. Ganeshkumar, “Design and Implementation of Remote Nerve Stimulator for Cardiac Patients,” in 2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA), IEEE, 2023, pp. 975–978. Accessed: May 10, 2024.
[34] S. Bohn, M. Leßnau, and O. Burgert, “Digital Operating Room,” Int J CARS, vol. 4, no. 1, pp. 145–149, Jun. 2009, doi: 10.1007/s11548-009-0329-7.
[35] M. Andrade, S. Sharman, L. Y. Xiao, and P. W. Newall, “Safer gambling and consumer protection failings among 40 frequently visited cryptocurrency-based online gambling operators.,” Psychology of Addictive Behaviors, vol. 37, no. 3, p. 545, 2023.
[36] T. M. Balogun, H. Bahsi, O. F. Keskin, and U. Tatar, “A comparative framework for cyber threat modelling: case of healthcare and industrial control systems,” IJCIS, vol. 19, no. 5, pp. 405–431, 2023, doi: 10.1504/IJCIS.2023.133282.
[37] U. J. Butt, M. Abbod, A. Lors, H. Jahankhani, A. Jamal, and A. Kumar, “Ransomware Threat and its Impact on SCADA,” in 2019 IEEE 12th international conference on global security, safety and sustainability (ICGS3), IEEE, 2019, pp. 205–212.
[38] A. O. Gomez Rivera, D. K. Tosh, and U. Ghosh, “Resilient sensor authentication in SCADA by integrating physical unclonable function and blockchain,” Cluster Computing, pp. 1–15, 2022.
[39] A. Alzahrani and T. H. Aldhyani, “Design of Efficient Based Artificial Intelligence Approaches for Sustainable of Cyber Security in Smart Industrial Control System,” Sustainability, vol. 15, no. 10, p. 8076, 2023.
[40] A. M. Y. Koay, R. K. L. Ko, H. Hettema, and K. Radke, “Machine learning in industrial control system (ICS) security: current landscape, opportunities and challenges,” J Intell Inf Syst, vol. 60, no. 2, pp. 377–405, Apr. 2023, doi: 10.1007/s10844-022-00753-1.
[41] B. Babu, T. Ijyas, P. Muneer, and J. Varghese, “Security issues in SCADA based industrial control systems,” in 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), IEEE, 2017, pp. 47–51.
[42] M. Nankya, R. Chataut, and R. Akl, “Securing Industrial Control Systems: Components, Cyber Threats, and Machine Learning-Driven Defense Strategies,” Sensors, vol. 23, no. 21, p. 8840, 2023.