Review Paper on Cyber Security threats and mitigations in Healthcare Sector with emphasis on Software Defined Networking

Rukshana M.A.F
IT21026416
3rd year 1st semester
Computer System Engineering Department (Cybersecurity)
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

***Abstract*— Healthcare institutions are using technology in increasing numbers to enhance patient care and operational effectiveness, but this development additionally places them at risk from cybersecurity threats. The sensitive nature of patient data and the importance of healthcare services render the healthcare sector a top target for hackers [1]. A potential technology for enhancing network administration and security in healthcare companies is software defined networking (SDN) [2]. This review paper discusses the cyber security risks that the healthcare industry encounters and the function of SDN in reducing such risks. The paper start by giving a general overview of the healthcare industry adopted to digital word. Next look at the typical cyber security attacks that healthcare dealt in past. The paper leads to, talks about general solutions proposals for better and secure healthcare, and emphasizing the important and effective solution using Software defined Networking (SDN). Finally, the paper underlines healthcare need, organization prioritizing cybersecurity and implementing SDN as a pro-active strategy for controlling cyber threats.**

Index Terms – Cybersecurity, healthcare, SDN, threats, , risks, mitigations, security.

I. INTRODUCTION

Humanity is now residing in the information age [3]. As a consequence of scientific theory and technical development, traditional medicine, which has biotechnology at its heart, has progressively begun to digitalize and informationize [3]. The development of smart healthcare has also incorporated a new generation of information technology [3]. healthcare sector is now widely referred to as "smart healthcare" or "digital healthcare" [3]. Smart healthcare is more than just a simple technological innovation; it is a multidimensional, all-encompassing enhancement. Changes in the design of medical information technology (from clinical to regional medical informatization), the medical model (from diseasecentered to patient-centered care), and medical management (from generic to personalised) cybersecurity challenges, solutions, solution proposals, SDN important in solving the healthcare threats and areas that still need to be improved in management, shifts in the concepts of illness prevention and treatment (from a focus on curing diseases to a focus on preventive healthcare), and are examples of how this change is reflected in the field of medicine [3]. Healthcare cybersecurity threats are currently becoming increasingly prevalent due to the frequency and severity of incidents related to the industry [4]. Cybersecurity is the process of preventing any unauthorized access to computer systems, networks, and programs. To circumvent cyber defenses, cyberattacks have evolved [4].

Due to technological improvements and scientific theory in technology, attackers start to exploit technology weaknesses [5]. Selected publications describing cybersecurity solutions used in the health industry were reviewed. [5].

A cutting-edge approach to developing, deploying, and administering networks, software-defined network (SDN) separates network control and forwarding procedures for a better user experience [2]. Regarding network flexibility and controllability, this network segmentation has many benefits [2]. On the other hand, it makes it possible to combine the advantages of cloud computing and system virtualization, and on the other, it makes it possible to construct a centralised intelligence that makes it possible to create a clear sight over the network for the purposes of straightforward network administration and maintenance as well as improved

network control and reactivity [2]. SDN architecture can support the fulfillment of healthcare related threats and attacks [2]. It has been shown that SDN frameworks are capable of identifying and resisting a variety of networkbased threats. More crucially, as it is explored in Section II of proposed solutions, they are also capable of coordinating the gateway devices to assure authentication [6].

II. RESEARCH OBJECTIVE

In the current global setting, the health sector has been impacted by the most significant and prominent attack and threat vectors, which are outlined in this review study. Furthermore, the paper aims to provide latest solutions for the cyber attacks and threats using SDN and other solutions.

III. LITERATURE REVIEW

Healthcare digitalization alters how patients interact with medical experts, allows for fast decision-making regarding outcomes and treatments, and facilitates the sharing of medical data [7]. Aside from improving patient outcomes, lowering costs, and minimising human error, the main goals of healthcare innovation are to maximise the work of medical professionals and medical software systems [7]. This is accomplished through integrated online and mobile experiences [7]. The digital technology usage in healthcare brought with it several difficulties, the most serious of which was cybersecurityrelated threats. Cyber risks are incredibly extremely expensive [9].

Individuals have the fundamental right to data privacy and data protection [9]. Information acquired by healthcare institutions frequently includes individuals' personal information as well as medical data, and the possibility that a data breach might compromise all of that data, undermining the broader goal of digitalization in healthcare [7].

A. RECENT CYBERSECURITY ATTACK INCIDENTS IN HEALTH INDUSTRY

Several cyberattacks have targeted the healthcare industry in recent years. Among these, the most important cyberattacks are [4]:

UVM Health Network Cyberattack The University of Vermont (UVM) Healthcare system was shut down on October 28, 2020, as a result of a breach being found [10]. The hospital was losing almost $1.5 million each day, which consisted of both expenditures related to the attack and income lost as a result of postponed services [10]. For roughly 40 days the healthcare system, including electronic health records (HER) [10]. Because they were all connected to the same network, over 5000 computers were infected [10]. Approximately 300 employees were unable to work in November due to this outage [10]. By the time everything is said and done, the event is anticipated to cost more than $63 million, according to Stephen Leffler, MD, President and COO of UVM Medical Centre [11].

The NHSD and Ryuk ransomware attacks

On October 26, 2020, six hospital systems suffered from DDoS attack [4]. The hospital suffered a $300,000 loss in order to repair the damage caused by the DDoS strikes [4]. According to The New York Times, the hackers are reputed to seek a ransom payment equal to 10% of the business's yearly income [4]. The federal government mandates that hospital networks and healthcare organisations beef up their security defences, make sure that all software updates are installed, back up their data, and continuously keep an eye on system access [4]. As a payload, Ryuk has been launched from banking [4]. A Hermes 2.1 ransomware clone named Ryuk first surfaced in August 2018 [4]. The demand for ransom payments, which may be quite profitable, is one of the major reasons attackers target healthcare facilities [4]. One of the targets of the ransomware assault in May 2017 was the National Health Services (NHS) of the UK [4]. 16 healthcare establishments' computers were among the almost 200,000 compromised by the

WannaCry attack [4]. The attack caused the shutdown of various crucial medical equipment, which caused thousands of patients to suffer [4].

Nebraska medicine in the Omaha attack

The health centre Nebraska Medicine initially reported the outage in September 2020, and it anticipates that its computer network will continue to be down. [4]. The hostile incident interfered with Nebraska Medicine's IT infrastructure, forcing several patients' appointments to be cancelled or rescheduled [4]. Because Nebraska Medicine powers their EHRs the breach also had an effect on numerous other Regional Health Services' EHRs and computer systems [4]. Furthermore, a security incident at Blackbaud, a firm that keeps donor information for organizations including health systems, exposed patient information from February to May 2020 for more than 46 hospitals and health institutions [4].

DDoS attack on Children's Hospital in Boston When a network is overloaded, it begins to deny availability to its recipients, which is known as distributed denial of service (DDoS) [5]. A DDoS Computer-Mediated Communication assault might occasionally happen accidentally [5]. However, the majority of the time,

cybercriminals design DDoS attacks to access vital data, such as an

organization's financial information [5]. One of the biggest targets for hackers is the healthcare sector [5]. One of the most notable DDoS attacks in 2014 targeted Children's Hospital [5]. The hospital system was targeted when dealing with the situation of a 14-year-old girl's parental withdrawal, is another cyber awareness program. Since the September 2019 debut, almost 340 organizations have downloaded the documents [5].

Montpellier University Hospital data breach Since they are a common type of hack, data breaches in the healthcare sector have been widespread for decades [4]. Nearly all attackers use phishing emails and deceptive websites to trick the user [4]. The attacker obtains access to the account and the network system when the victim clicks on the dubious web link in their email [4]. The Montpellier University Medical Center's healthcare provider learned that a third party had accessed one of the employees' email accounts in March 2019 [4]. The employee of the medical centre accidentally clicked on a dangerous link in the phishing email [4]. The attacker thereafter got access to both his or her account and the hospital network [4]. This data leak affected around 600 PCs. The healthcare provider discovered that the hacked account held private patient data, including name, date of birth, social security number, and insurance information [4].

Insider Threats

In addition to external cybersecurity concerns, healthcare providers must sometimes deal with internal dangers [4]. These internal business risks are brought on by either human mistake or a violation of an employment contract [4]. There are three types of internal assaults, according to several case studies: employee or contractor carelessness or ignorance; criminal or malevolent insider; and credential thief (imposter risk) [4].

B. MITIGATIONS

According to the research paper published by American Nurse Today, aims to inform medical professionals of the value of cybersecurity and the precautions they can take to secure both themselves and the patients from online dangers [11][12]. An important part of preventing and reducing these hazards is played by healthcare providers [11][12]. Healthcare organisations have cybersecurity programmes in place to increase security awareness levels [5]. Examples of contemporary solutions include training programmes and initiatives to raise awareness of cybersecurity [5]. As part of a cybersecurity programme, the IT department sends phoney phishing emails to its employees, and those who
are unable to
are given more instruction in order to recognise them [5]. More than 100 NHS boards in the UK have since the WannaCry incident successfully completed cybersecurity training that has been approved by the Government Communications Headquarters [5].

C. PROPOSED SOLUTIONS FOR A SECURE HEALTHCARE SECTOR

Use endpoint device management software.

- Use perimeter-based defence (firewalls, antivirus) to stave against cyberattacks [5].
- Limit the technologies and gadgets used by medical personnel to ensure compliance during pandemics, including security regulations like the HIPAA (Health Insurance Portability and Accountability Act) [5].
- Adapt the NIST-based approach to managing IoT control medical device security [5].

Protect the remove work environment.

- Use two-factor authentication [5].
- Use a chaotic map-based authenticated security mechanism for distant points of care [5].
- Remote access monitoring, such as the NHS attack surface reduction rules, should be used [5].
- To enable secure access, use a perimeter security system such as NHS (National Health Service) Secure Boundary [5].
- The healthcare must implement data protection procedures to secure system access and transmission [5].

Maintain business continuity.

- Utilise a tool for self-evaluation, such as the NHS Data Security and Protection Toolkit [5].
- Promote a strong culture of cyber vigilance and embrace cybersecurity [5].
- Data backups, firewalls, and intrusion detection and prevention systems can all help to ensure company continuity [5].
- Use a systematic risk assessment to determine the impact on health care company operations.
- Take into account healthcare cybersecurity insurance [5].

Use technical controls.

- To segregate network traffic, use network segmentation [5].
- Encryption, authentication, and authorization detection has been shown for SCADA systems, specifically smart grid [6].

This IDS detects anomalies using an SVM classifier using packet arrival time, inter-packet leaving time and packet size [6]. In general, SDN's flexibility and network-wide perspective make it an effective tool for implementing security controls [6].

- Backups and ransomware can provide greater security than is possible with username/password on a small number of devices. The NHS is running a campaign called Keep IT Confidential are examples of generic technical controls [5].
- Use homomorphic encryption to maintain robust security and privacy while allowing for the analysis of encrypted material, including private medical data [5].
- Increase interoperability in healthcare by using blockchain [5].
- Integrate cryptographic security into network systems for patient data storage and data exchange [5].

Legislation and policies

- Medical cyber-physical system concerns can be mitigated via laws and regulations [5].
- Security rules and regulations layouts is customized [5].
- Manufacturers need to pay greater attention to security during the medical device design process, or regulations need to be changed [5].
- Decision-makers might need to change policies that permit for the application of new technical advancements in health care [5]. The United States Congress approved the 21st Century Cures Act to support patient autonomy over their own health information and to safeguard cybersecurity and privacy [5].

Assistance includes incident reporting and information about online threats.

- NHS Digital prepared a high-severity alert procedure manual and two high-severity CareCERT alerts (BlueKeep and DejaBlue) to make event reporting and sharing easier. [5].
- Use an evidence-based method for incident reporting and exchange, such as the general security template [5].
- To combat cyberthreats with pandemic themes, create a worldwide workforce to simplify threat reporting and sharing [5].

D. SOFTWARE DEFINED NETWORK (SDN) IN HEALTHCARE SECTOR

Firewalls, load balancers, and intrusion detection systems may all benefit from SDN, and other applications [6]. Not only may SDN be used to set specific packets to be dropped by switches based on their headers (usually, Source IP, Source Port, Destination IP, Destination Port, and Protocol), but as explained by Ganjali, SDN-based firewalls may also impose parental controls, gather netflow records, and spot network scans [6]. SDN-based network intrusion used to ensure network authentication [6]. The most straightforward option install a common authentication service on the controller itself, such Kerberos [6]. Running a service for authentication, on the other hand, would probably put the controller under stress [6]. Instead, it is suggested that the controller set switches such that only requests that have successfully completed stateful authentication are sent to the target device. [6]. Attacks using fingerprints can be prevented by rearranging switches with packets [6]. Postponing or repeating packets would interfere with secret channels, like message time, for instance [6] (It could even be able to create some phoney traffic to trick an adversary) [6]. Applications for SDN can do in-depth network traffic analysis, such as machine learning [6].

I. SDN-BASED PROPOSED SOLUTIONS

a. STHM stands for Secured and Trusted Healthcare Monitoring (using Blockchain and SDN).

Today, it's increasingly inescapable that link among the various components and rapid data delivery are two of the biggest issues facing healthcare systems [13]. SDN integration might be seen as a desirable option in this scenario to give network flexibility and efficiency [13]. It allows devices to connect to one another and provides several network services such as Access control, system discovery, network and traffic management, and authentication. The authors (WBAN) study the scalability and network control of connected devices for Ambient Assisted Living (AAL) and Wireless Body Area Network (WBAN) [13]. They recommended that the SDN controller monitors traffic flows and guarantees that traffic rules are successfully exchanged among devices used in networks for better routing and mobility management [13]. Highlighted the number of controllers, which is a major influencer of any SDN and WBAN

combination in the healthcare industry [13]. The authors proposed a mathematical framework based on the

using a convex optimisation technique while considering the quantity of SDN-enabled switches (SDESW), latency, and the number of controllers to estimate the ideal for an SDWBAN, the number of controllers architecture [13]. The mean of simulation results also confirmed their mathematical proposal [13]. In earlier work, they investigated the primary problems about security and privacy for the Healthcare Monitoring System (HMS) [13]. To ensure dependable patient care, they created an integrated security monitoring system. while minimizing health-related concerns [13]. Offered a roadmap for SDN-based telemedicine with enhanced QoS. They recommended SDN adoption to give enough bandwidth, and to support real-time medical information exchanges [13].

b. Framework for SDN-based Security Enforcement in Smart Healthcare Data Sharing Systems.

System Model

A smart healthcare mechanism for distributing data is a massive fusion system that integrates humans, hosts, IoT devices, and cloud services [14]. In this section, they offer a group formal system model in order to formalize such a system [14]. Humans are defined as service consumers and providers, hosts as virtual machines, things as things, and services as services (SM) [14].

Security Enforcement framework based on SDN. They provide an SDN-based security enforcement framework for intelligent healthcare data sharing systems based on the aforementioned system paradigm. [14].

Figure 1 depicts the proposed framework [14]. In their design, cach patient in the data sharing system has a unique virtual computer, the provider of the services, or that run on a virtual computer [14]. Every doctor or Internet of Things gadget is a service consumer (SC), or the person who utilises virtual machine services [14]. The patient has control over which services are provided in her or his virtual computer are freed to consult with whatever doctor or item [14]. Physicians can only access patient personal data housed in virtual machines using the service interfaces listed [14]. The framework can be divided into two primary layers: SDN-based and virtual machine (VM) layer maintains patient's personal data as well as a variety of services such as online data exploration, data updating, data downloading, and so on [14]. The goal of establishing a virtual machine layer is to address the issues posed by insider assaults [14]. A virtual machine is a closed system, the patient could access the data kept on the virtual machine, while others (like the storage provider) cannot. This manner, we may prevent hostile insiders from

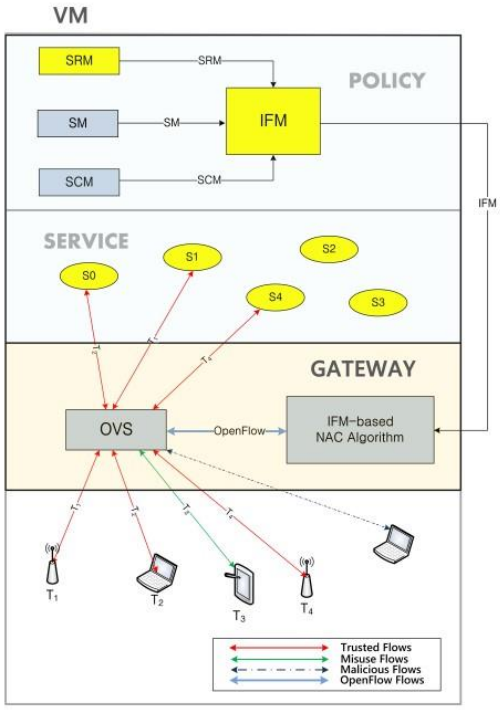

Figure 1: The framework that has been proposed. The yellow components reflect the service provider's services or models, whereas the The system models or system components are represented by deep blue components..

illegally obtaining patients' confidential data [14]. The virtual machine layer is further subdivided the policy layer and the application layer and service layer [14]. Service releasing policies (SRM) are created on the policy layer by service providers to strictly regulate which services can be accessed by which service consumers or which things in the system. Following that, the system will automatically convert a relevant information flow model (IFM) is created using SRM and associated system models like the service model (SM), service consumer model (SCM), or thing model (TM). IFM is a recognised model with underlying network information that can assist the gateway in determining which IoT device is authorised or not, such as the MAC address of the object or the IP address of the virtual machine illegal [14]. The patient is not required to understand since system models, not patients, create and maintain all system models, they are the only sources of underlying network information [14].

The goal of implementing an SDN-based gateway is to address the issues posed by identity theft attempts [14].

Within the framework, each patient's personal virtual computer is shielded by an SDN gateway [14]. The gateway has a firewall feature that can identify clients trying to access the patient's virtual PC based on their MAC addresses [14].

Because per service consumer the framework can successfully authenticate resource-constrained IoT devices and prevent malicious users who have stolen the identities (private keys) of legitimate customers from accessing the patient's virtual machine in the system because each patient can only have a single MAC address in the system and MAC addresses are challenging to forge [14].
The In specifically, the SDN-based gateway layer may be further divided into an OpenFlow virtual switch (OVS) and an SDN controller [14]. Starting off, OVS will identify any accesses to the patient's virtual machine as suspicious flows and send them to the controller for investigation [14]. An Integrated into the controller will be an IFM-based virtual machine access control algorithm compare the incoming flow's header fields to the IFM rules for information flow [14]. The controller will update the flow table in OVS and transfer the flow to the patient's virtual machine if the flow is sent from those authorised items [14]. The controller will toss the incoming flow if the matching is unsuccessful. since it was transmitted by abusing or malicious users or IoT devices [14]. In this approach, the architecture ensures that only approved IoT devices in the system has unrestricted access to the patient's virtual machine. devices cannot [14].

c. Healthcare architecture wireless body area network routing method based on SDN.

The utilising wireless body area networks (WBANs) improvement of intrusion detection and prevention systems utilizing SDN is one area that needs additional study [15]. A wide variety of dangers, including as insider threats, malware attacks, and other cyber threats, should be able to be detected and prevented by these systems [15]. Additionally, since medical devices are particularly susceptible to cyberattacks, research is required to examine the efficiency of SDN in securing these devices [15].

Architecture proposal

Figure 2 depicts the suggested architecture [15]. A WBAN user is defined as someone who has sensor nodes and a HUB [15]. All sensor nodes communicate with the HUB by sending data linked [15]. The form of interaction is known as intraWBAN communication [15]. Furthermore, each WBAN user has access to other WBAN users' communications [15]. The type of communication is known as interWBAN communication [15]. Which is the controller has been introduced in relation to the SDN-based design method, in charge of controlling and managing the interWBAN connection [15].

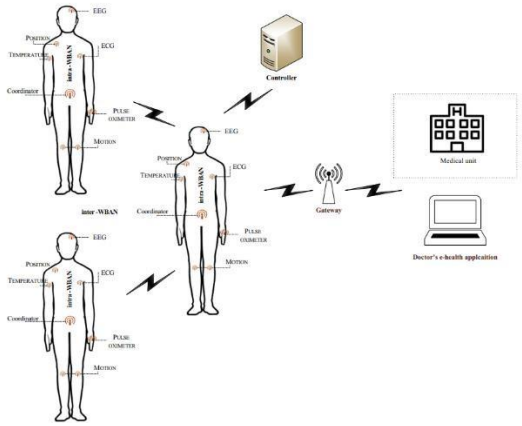

Figure 2: Proposed architecture [15].

Healthcare applications has made it possible to continually and in real time keep an eye on both medical professionals and patient status using wearable wireless sensor nodes [15]. WBANs' diverse and complicated network structure, on the other hand, has several drawbacks in terms of administration and control [15]. A promising technology that specifies a new network design and administration strategy is the software defined network (SDN) approach [15]. The SDN technique is used in this article to construct WBANs have more adaptable and dynamic network designs [15]. For this, a novel energy-aware routing algorithm and a WBAN architecture based on the SDN approach are proposed for healthcare design [15].

IV. FUTURE RESEARCH

There is an abundance of study on software-defined networking (SDN) in cybersecurity risks and mitigations in healthcare industry [16]. To handle the changing threat landscape and the new technologies in the healthcare industry, more research is still needed [16]. The detection and prevention of healthcare network vulnerabilities that might be used by hackers is crucial field of research [17]. This study should concentrate on figuring out the underlying reasons for these vulnerabilities and coming up with solutions [17]. Research is also required to determine how emerging technologies like cloud computing, artificial intelligence, and the Internet of Things, may affect hospital cybersecurity [18][19]. This study should look at the dangers posed by these

technologies and devise suitable security safeguards to reduce those dangers [18][19]. Research on the human issues related to cybersecurity is also necessary [20]. Patients, managers, and healthcare practitioners all have important
responsibilities to
play in keeping healthcare networks secure [20]. In order to increase their cybersecurity knowledge and practices, training programs should be developed that are successful in addressing the elements that affect their behaviors and decision-making processes [20].

V. CONCLUSION

The paper has emphasized the cybersecurity risks that the healthcare industry encounters, as well as the role that Software Defined Networking (SDN) plays in reducing such risks. To safeguard patient safety and secure patient data, healthcare companies must understand the significance of cybersecurity and put the necessary security measures in place. SDN is a promising technology that can improve network security by offering segmentation, centralized network administration, and better traffic monitoring.

SDN implementation must be done carefully to prevent adding additional vulnerabilities, though. For SDN to be effective, healthcare companies must deploy and manage it with the help of qualified experts.
Additionally, it is critical for healthcare organizations to keep aware of the most recent cybersecurity trends and threats and to take preventative action to address them.

Future research can concentrate on investigating the potential of cutting-edge technologies like machine learning and artificial intelligence to enhance healthcare cybersecurity. Research can also examine the possible effects of new laws and other policy changes on healthcare cybersecurity.

To effectively minimize cybersecurity risks, healthcare institutions must prioritize cybersecurity and work with industry specialists, researchers, and legislators. The capacity of the healthcare industry to protect patient information and guarantee patient safety in the face of growing cybersecurity threats is essential to its sustained expansion and success.

VI. ACKNOWLEDEMENT

The lecturer in charge of the Applied Information Assurance module (IE3022), Mr. Kanishka Yapa, has my deepest gratitude, respect, and appreciation for giving me this significant opportunity to do research on a relevant, pertinent issue. I appreciate you sharing your experience in this area greatly. The advice and assistance offered were beneficial.
This acknowledgement and appreciation also goes to the module instructors for providing hands-on experience with this domain during the lab sessions.

VII. REFERENCES

[1] B.Kotkova, “Cyber security in the healthcare sector – Current threats,” SGEM, vol.22, no. 2.1, pp.11-18, 2022.

[2] K. Benzekki, A. El Fergougui and A. Elbelrhiti Elalaoui, "Software-defined networking (SDN): A survey," Security and Communication Networks, vol. 9, no. 18, pp. 5803-5833, Dec. 2016.

[3] S. Tian, W. Yang, J.M. Le Grange, P. Wang, W. Huang, and Z. Ye, "Smart healthcare: making medical care more intelligent," Global Health Journal, vol. 3, no. 3, pp. 62-65, 2019. ISSN: 2414-6447. https://doi.org/10.1016/j.glohj.2019.07.001.

[4] A. K. M. Jahangir Alam Majumder and C. B. Veilleux, ‘Smart Health and Cybersecurity in the Era of Artificial Intelligence’, Computer-Mediated Communication. IntechOpen, Jan. 07, 2022. doi: 10.5772/intechopen.97196.

[5] He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. Journal of Medical Internet Research, 23(4), e21747. https://www.jmir.org/2021/4/e21747 . DOI: 10.2196/21747.

[6] S. Gupta, H. B. Acharya, and M. Kwon, "On Securing Healthcare with Software-Defined Networks," in IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Apr. 2019, doi: 10.1109/infcomw.2019.8845215.

[7] M. Paul, L. Maglaras, M.A. Ferrag and I. Almomani, "Digitization of healthcare sector: A study on privacy and security concerns," ICT Express, vol. 4, no. 2, pp. 81-86, 2023, ISSN 2405-9595, https://doi.org/10.1016/j.icte.2023.02.007.

[8] C. S. Kruse, B. Frederick, T. Jacobson, and D. K. Monticone, "Cybersecurity in healthcare: A systematic review of modern threats and trends," Technology and Health Care, vol. 25, no. 1, pp. 1-10, Jan. 2017.

[9] M. Ventura and C.M. Coeli, "Beyond privacy: The right to health information, personal data protection, and governance," Cadernos de Saude Publica, vol. 34, 2018.

[10] UVM Health Network, "Statement from UVM Health Network on Cyberattack," UVM Health Network Newsroom, Sep. 28, 2020. [Online]. Available: https://www.uvmhealth.org/news/uvmhn/statement-uvm-health-networkcyberattack. [Accessed: Apr. 30, 2023].

[11] Radware, "Boston Children's Hospital Case Study," Radware, 2018. [Online]. Available: https://www.radware.com/getattachment/Security/ERT-CaseStudies/771/Radware_Boston_Childrens_Hospital_Case_Study.pdf.aspx/?lang=en-US . [Accessed: Apr. 30, 2023].

[12] M. Jordan, "Cybersecurity awareness," American Nurse Today, vol. 15, no. 2, p. 5, 2020.

[13] E. Barka, S. Dahmane, C. A. Kerrache, M. Khayat and F. Sallabi, "STHM: A Secured and Trusted Healthcare Monitoring Architecture Using SDN and Blockchain," Electronics, vol. 10, no. 15, p. 1787, Aug. 2021, doi: 10.3390/electronics10151787.

[14] Y. Meng, Z. Huang, G. Shen, and C. Ke, "SDN-based security enforcement framework for data sharing systems of smart healthcare," IEEE Transactions on Network and Service Management, vol. 17, no. 1, pp. 308-318, Mar. 2019. [15] M. Cicioglu and A. Calhan, "SDN-based wireless body area network routing algorithm for healthcare architecture," Etri Journal, vol. 41, no. 4, pp. 452-464, Aug. 2019

[16] W. Li, Y. Wang, W. Meng, J. Li, and C. Su, "BlockCSDN: Towards Blockchain-Based Collaborative Intrusion Detection in Software Defined Networking," IEICE Transactions on Information and Systems, vol. E105-D, no. 2, pp. 272-279, 2022, doi: 10.1587/transinf.2021BCP0013.

[17] M. Rahman and H. Jahankhani, "Security vulnerabilities in existing security mechanisms for IoMT and potential solutions for mitigating cyber-

attacks," in Information Security Technologies for Controlling Pandemics, 2021, pp. 307334.

[18] S. Saif, S. Biswas, and S. Chattopadhyay, "Intelligent, secure big health data management using deep learning and blockchain technology: an overview," in Deep Learning Techniques for Biomedical and Health Informatics, pp. 187-209, 2020.

[19] P. Singh and N. Singh, "Blockchain with IoT and AI: A review of agriculture and healthcare," International Journal of Applied Evolutionary Computation (IJAEC), vol. 11, no. 4, pp. 13-27, 2020.

[20] R. F. McCloud, C. A. Okechukwu, G. Sorensen and K. Viswanath, "Beyond access: barriers to internet health information seeking among the urban poor," Journal.

VIII. AUTHOR PROFILE

Rukshana Alikhan (Rukshana M.A.F) is a 3rd year 1st semester cybersecurity undergraduate, pursuing a bachelor's degree Information Technology, specialization in Cybersecurity in Sri Lanka Institute of Information Technology (SLIIT).