The role of deep learning in cyber security for healthcare organizations

Weerasinghe K.M
IT21831904
3rd year 1st semester
AIA -IE3022
Sri Lanka Institute of Information Technology
IT21831904@my.sliit.lk

Abstract- The rising danger of cyberattacks in healthcare organizations needs extensive cybersecurity measures to protect sensitive patient data and critical infrastructure. Deep learning, a form of artificial intelligence, is establishing itself as a promising technique to strengthen cybersecurity measures in healthcare organizations. The research presented here analyzes the role of deep learning in improving cybersecurity for healthcare, emphasizing on its application in identifying and preventing typical cyber threats such as ransomware, denial of service (DoS) attacks, and phishing attacks. Through a comprehensive analysis of existing literature and current research, the benefits and limitations of deep learning in healthcare cybersecurity are addressed. Deep learning algorithms demonstrate the ability to assess massive volumes of complex information, adapt to evolving threats, and automate security operations, resulting in enhancing response times and scalability. However, challenges like the demand for high-quality data for training, processing power, and susceptibility to adversarial attacks give substantial limitations. The report concludes by pointing out the need for additional studies to address new vulnerabilities and assure the ethical deployment of deep learning in healthcare cybersecurity. Overall, deep learning offers great potential for enhancing cybersecurity in the healthcare area, promoting confidentiality for patients while preserving the integrity of healthcare services.

Index Terms – deep learning, cybersecurity, healthcare, artificial intelligence, cyber threats, convolutional neural networks (CNN), Artificial Neural Network (ANN), Long Short-Term Memory (LSTM)

I. INTRODUCTION

Cybersecurity assists in safeguarding digital assets such as computer systems and network devices against the theft of data, information breaches, and harm to other hardware and software [1]. Due to cybercrimes using digital data, cyber security aids with the majority of issues [2]. One of the most important requirements for every firm, particularly healthcare companies, these days is cyber security.

Deep learning has become a major topic in the cyber security sector due to the growth of the artificial intelligence deep learning and the machine learning are two sub class of the artificial intelligence [2]. The first mentioned sub class or the machine learning class has been long used to identify different threats such as analyzing malwares, intrusion detection systems and phishing attack prevention in the cyber security field [1]. One area of machine learning technique known as "deep learning" is defined by its ability to help computers recognize and categorize a variety of file formats, especially when it comes to detecting potentially harmful files. This procedure involves preparing the computer models by exposing them to defined features that are taken via samples that have harmful characteristics [1]. Even though deep learning has showed lot of potential in detecting cyber-attacks using deep learning methods are limited [3].

The world is getting more and more advanced technologically with each passing day. These days, the healthcare sector is similarly progressing towards technologies. These technological advancements are needed and help with treating patients and accessing data, but it becomes more vulnerable to attacks due to these developments. The Cybercrimes are also rising as a result of these developments [4]. In order to profit financially these cybercriminals are taking advantage of the vulnerabilities in health care organizations to steal patient data, medical data, employees' data, credit card and other banking information [4]. Because of its vital infrastructure and the essential nature of the healthcare services, the healthcare industry is particularly vulnerable to cyberattacks. The organization as a whole is at risk in the event of a major cyber incident, such as a ransomware or malware attack, which might compromise patient care, sustainability of the organization, and continued operations. Healthcare organizations are affected by threats that are internal as well as external threats [4].

Healthcare providers, patients, regulatory agencies, cybersecurity experts, IT staff, insurance companies, and technology suppliers are just a few of the many stakeholders involved in healthcare cybersecurity [4]. In order to guarantee the availability, confidentiality, and integrity of healthcare data, each stakeholder is essential.

II. RESEARCH STATEMENT

This literature review aims to review the existing past literature relevant to the topic and give an overview of what the existing literature and experts are saying about the topic of deep learning of cybersecurity in the healthcare sector an update on the recent research about in the field.

The objective of this study is to investigate,

- Identify the most frequent attacks occurring inside healthcare establishments.
- introduction for the attacks identified.
- Investigate past attacks and assessment.
- Explore the deep learning methods that are currently available or researched to prevent this attacks in the healthcare organization

III. REVIEW OF THE LITRITURE

1) cyber security challenges in the healthcare system

Due to their critical function and handling of extremely personal patient data, health care organizations have become an increasingly popular target [4]. Cybercriminals are now increasingly concentrating on the healthcare industry in an attempt to profit financially and maliciously from its vulnerabilities [4]. The subsequent segment will conduct an in-depth study of the cybersecurity obstacles encountered by healthcare establishments.

The ramifications of a cyberattack in the health industry are far more severe. There is a real chance that a cyberattack in the medical field could result in fatalities [5]. Instances of mental problems have also been reported amongst healthcare cyberattack victims [5]. Even the elevators in healthcare facilities have been exploited by cybercriminals [5].

These obstacles include the confidentiality of healthcare information, such as patient data, frequent cyber security breaches encountered by the industry, and the existing cybersecurity measures implemented in order to prevent them [4].

a. Key challenges in healthcare organizations

Safeguarding the integrity of their systems and protecting patient information through strong cybersecurity safeguards is a challenging endeavor for healthcare organizations. These difficulties arise from a wide range of sources, such as human error, financial limitations, and the constantly changing nature of security risks [6]. The following major issues have been noted:

- Managing of the endpoint devices [6].

Because endpoints may act as entry sites for cyber threats, managing them presents several issues [6]. Due to the wide range of systems and devices connected inside their networks, including IoT devices, specialist medical equipment, remote access points, and standard desktop and laptop computers, the endpoints of healthcare organizations can become quite intricate. Vulnerability is increased and compatibility is compromised when new devices are integrated with dated systems [6]. Instead of considering the complexity of endpoint security, healthcare companies frequently depend on the perimeter defensive techniques [6].

Healthcare organizations may reduce the risks linked to endpoints and improve their overall cybersecurity posture by emphasizing endpoint security and deploying active risk mitigation techniques.

- Human errors

In cybersecurity events involving healthcare institutions, human error continues to be a prevalent issue that presents major challenges to patient privacy and data protection [6]. These occurrences can be considered intentional or accidental [6]. Because healthcare work is very demanding, employees can encounter high levels of stress and excessive workloads, which may make it more difficult for them to remain cautious about security threats [6]. Employees who are overwhelmed by work can mistakenly ignore indicators of email phishing or other harmful activity, which increases the possibility that they can become targets of cyberattacks [6]. The situation is made more severe by the limited usage of human error analysis frameworks and the absence of root cause analysis for security-related incidents [6]. Human behaviors on the system can be called as the weakest link in the system of in organizations [7]. An IBM statement from 2014 said that "over 95% of all security incidents examined comprehend 'human error' as a significant factor." [7] Employee conduct was the root reason for 46% of healthcare-related security incidents in 2017, according to Info guard Cyber Security [7].

Developing an atmosphere of cybersecurity knowledge and responsibility across the organization, strengthening staff comprehension, and setting up strong incident response mechanisms are just a few of the many strategies needed to deal with these challenges [7]. healthcare needs to be cyberaware and aware that even with the strongest cybersecurity protections in place, they could still be targets of

phishing attempts [7]. The idea of IT as an obstacle must change; instead, it should be seen as a mediator and protector. It is important to provide employees with education on cyber awareness and the perils associated with cyberattacks [7].

- Lack of security awareness

Healthcare personnel's lack of knowledge about cyber threats makes them more vulnerable to cyberattacks [6]. More staff training is often required for incident response, showing a need for more awareness and education. Furthermore, healthcare workers are not given enough regulations or incentives to act carefully [6].

- Vulnerable medical systems

The weak cybersecurity capabilities of medical equipment make healthcare systems susceptible to exploitation [6]. Cybersecurity vulnerabilities are increased by our increasing reliance on devices that are connected, and they might be introduced by weak Internet of Things devices [6].

The rapid growth of Internet-connected devices in houses, offices, healthcare organizations, poses a serious risk to cybersecurity, as the Internet of Things (IoT) expands to include these contexts. These electronic devices acquire private information, raising issues with confidentiality and anonymity [7]. IoMT devices are being employed more and more in healthcare organizations for remote patient observation and health-related distress notifications and especially when elderly patients are being cared upon. Patients with diabetes may have their blood sugar levels monitored, their heart rates and blood pressure recorded by smart device [7].

The reach of linked devices is immense, yet the design and manufacture of IoT devices are not subject to many enforced regulations. IoMT devices often contain proprietary operating systems, are constructed from inexpensive, insecure parts, and are linked to applications that upload data to servers [7]. Software upgrades may be hard to find or may not be available at all, which puts the device in an unsafe default configuration.

Medical instruments are better built to adhere to industry-specific rules and specifications, but since many IoMT devices use proprietary software and firmware, it may be challenging to implement security [7]. IoMT devices are susceptible to hacks as they are unable to run external software programs [7].

Because they are wirelessly connected, implanted electronic devices including pacemakers, ICDs, deep brain stimulators, and infusion pumps are also susceptible to hacking [7]. Robots are not very useful in healthcare, but they do produce a lot of data that is categorized as PHI; therefore, it has to be safeguarded. The main concern is that this data will be compromised and used illegally, Mainly for financial benefits [7].

There will be enormous problems in developing and supporting IoMT devices as well as making sure they are properly protected to lessen the risk of an attack as technological advance progresses [7]. Since the introduction of such devices is happening at a rapid rate, rules must be established and implemented in conjunction with manufacturers.

2) Common Cyber-attacks in healthcare systems and prevention using deep learning

Ransomware, distributed denial of service, insider attacks, and phishing email attacks are some of the most dangerous and common cyberattacks against healthcare organizations [3]. The cyberattacks arising within healthcare organizations have been categorized based on several variables, including the attack's design, severity of the attack, vulnerability, legality of the attack, and to some extent [3].

a. Ransomware

Ransomware name is made from the two words of malware and ransom malwares are used to gain access or destroy and damage user machines and these malware main objective is to gain financial advantages [8]. Ransomware is a very dangerous attack that could have severe consequences if happens in any organization. It is a topic that should be talked heavily in information security. There are no guaranteed tools that will help to prevent ransomware attacks from happening [8].

Users are especially susceptible to ransomware given that they often lack security measures necessary for self-defense [8]. Even while businesses utilize firewalls, antivirus programs, and anti-spyware software to protect themselves from such attacks, users lacking sufficient understanding of information security and cyber security may still be vulnerable to an attack if they haven't taken any measures to protect themselves [8]. Locker ransomware and crypto ransomware are the two main categories of ransomwares [8]. The primary ways that ransomware spreads are via phishing emails with malicious links and content, downloading insecure files, accessing compromised websites,

and other techniques [8] [9]. In addition, ransomware is being propagated via online messaging applications and social networking platforms [8].

- **Ransomware attacks on healthcare**

Since 2016, 172 attacks have cost the US healthcare sector more than $157 million. In 2020, the Comparitech analysis found that 74% of attacks involving ransomware affected medical facilities and medical clinics, while 25% targeted IT firms, senior citizen care facilities, dentistry offices, plastic surgery practices, healthcare coverage, public health, and manufacturing companies supplying medical equipment [9]. The demands that were made by the ransomware varied from about $11600 to $14 million.

A ransomware attack that affected the Hollywood Presbyterian Medical Center in Los Angeles in February 2016 forced patients to move to other hospitals and compromised the facility's computer infrastructure for more than a week [9]. All registrations and medical information had to be logged on to paper, and the staff was only able to interact via telephones and fax machines. To get the decryption key and recover the computer systems and administrative capabilities, the center chose to pay. [9].

A ransomware assault against Virtual Care Provider Incorporated occurred on November 17, 2019, preventing over 100 care facilities and nursing homes from accessing critical patient medical records [9]. The corporation declined to pay the attackers' $14 million ransom demand to access the data [9]. Because to several mitigation variables, including recognizing of unusual network activity and the use of different verification procedures for offshore data backups, VCPI was able to prevent the Ryuk ransomware assault from completely devastating the organization [9].

Recorded Future is a technology company that specializes in threat intelligence [9]. Researchers at Recorded Future examined 634 reported hacking and IT incident breach types between January 1, 2016, and September 15, 2019 [9]. Recorded Future discovered 25 ransomware incidents against US healthcare organizations during January and May 2020 [9].

b. Denial of service attack

A denial-of-service attack is a type of cyberattack when a malicious entity aims to prevent an electronic device such as a computer from operating normally, hence rendering it unusable for its intended users [10]. DoS attacks usually work by overloading or flooding a targeted computer with requests till regular traffic cannot be handled, causing additional users to experience a denial of service [10]. This is one of the most common type of attacks that are faced by healthcare and other organizations. DDoS attacks are mainly divided into two types, and they are volumetric attacks and application layer attacks [10].

Healthcare organizations make excellent victims for DDoS attacks due to a mix of vital services, confidential information, dependence on technology, insufficient safety precautions, and compliance with regulations. Strong cybersecurity measures must be put in place by these institutions with the objective of minimizing the likelihood of these kinds of attacks and protecting client information as well as services.

c. Phishing attacks.

The most popular kind of ransomware attack is phishing because it focuses on human error, which is the weakest link in healthcare and other industries [11]. Phishing attacks are a sort of cyberattack in which people are deceived into disclosing confidential information, including usernames and passwords credit card information, or their social security numbers, by means of deceptive messages, emails, or phone calls [12].. These kinds of attacks are becoming an increasing threat to people and organizations all around the globe because they have become more advanced in the past few years. To properly defend against these dangers, it is important to have a thorough grasp of phishing attacks and countermeasures [12].

Phishing attacks pose an imminent danger to people and businesses everywhere, and their significance cannot be understated [12]. Phishing attacks have caused large-scale monetary losses, theft of information, and harm to an organization's image [12]. Phishing attacks may also result in ransomware attacks, identity theft, and other digital crimes [12]. It is essential to acknowledge that phishing attacks are not exclusive to any one sector or size of firm. Phishing attacks may affect anybody who has an internet connection or an email account [12]. To stop and lessen the effect of these assaults, it is crucial to research and comprehend their nature as well as the methods attackers use [12]. Analysis of phishing attempts and their defenses will provide people and businesses with the information and resources they need to defend against these risks and ensure the security of their confidential information [12].

Healthcare personnel are susceptible to phishing attempts because of their line of work [11]. Because of the tremendous

workload, and sometimes they deal with emergency circumstances at work, which adds to their mental stress [11]. Medical staff may also lack awareness and information security training, which might lead to them undermining improved cyber security [11].

3) Introduction to Deep learning models

a. Autoencoder

The deep neural network, also known as an auto-encoder uses unsupervised pattern learning to efficiently process encoded and decoded data [13]. It is capable of distinguishing strong characteristics from raw data [13]. The two main steps of this method are the encoding and decoding process [13]. features an input layer, an output layer, and one or more layers that are hidden. During the encoding phase, the input is condensed into a lower-dimensional feature with a significant interpretation [13].

b. Convolutional neural network

A variant of conventional MLP, convolutional neural networks (CNNs) are primarily employed in computational image processing applications [1]. CNN is used on several data dimensions. The spatial organization present in the data may be captured by them. Convolution ID, pooling ID, and fully linked layer for ID data make up the CNN network [1]. The ideal characteristics from the input matrix are to be captured by the convolution layer [1]. A linear process that moves across the rows of the input matrix is used in convolution. A new feature set known as a feature map will be created by grouping the characteristics that are taken from each filter [1].

c. LSTM and RNN

RNNs are an instance of neural networks with internal state of memory that allows them to process sequential input [14]. One element at a time, they analyze input sequences, changing their hidden state depending on both the previous and current hidden states at each stage [14]. RNNs can capture linkages and correlations between components of a sequence because of their recurring structure [14]. The vanishing gradient problem, on the other hand, prevents conventional RNNs from learning long-range relationships [14]. To successfully capture long-term dependencies in sequential data, LSTM networks provide a gating mechanism that actively maintains and updates information in the memory cell [14].

4) deep learning approaches in cyber security for healthcare

a. Deep learning for detecting ransomware

There have been few studies that have demonstrated the effectiveness of the deep learning techniques in enhancing ransomware detection capabilities. By using these techniques cyber security professionals can better understand, identify, and mitigate the threats posed by ransomware attacks.

- Deep convolutional neural networks [15].

In their research on ransomware detection, Ashraf et al [15]. Explored the effectiveness of deep convolutional neural networks alongside traditional machine learning methods [15]. They used a method called transfer learning method [15]. For the purpose of evaluation, two different [12]datasets static and dynamic were employed. Experiments have shown that DLLs, API calls, and registry alterations are the most important features for ransomware detection [15].

- LSTM (Long short-term memory) [15].

In their research on ransomware detection, Maniath et al [15]. They have proposed a LSTM network as a method. to differentiate between mild and dangerous executables [15]. They assessed that the problem was with the executable's API calls' binary sequence classification [15]. Using a dynamic analysis, the API calls which the program's executable made as it was operating were extracted [15]. 96.67% of accuracy level was able to achieve using this technique [15].

- Autoencoder [15].

In their research on ransomware detection, AbdulsalamYa'u et al [15]. They have proposed a deep learning approach based on behavioral data [15]. This behavioral deep learning encoder was trained to identify between harmless and malicious ransomware [15]. 99.7% of accuracy level was able to achieve using this technique [15].

b. Deep learning for detecting DDoS attacks

Deep learning algorithms' application in the categorization and foreseeing of DDoS attacks is regarded as a complex field of study [10]. Design and development of many deep learning-

based defenses against diverse DDoS attack types across several tiers, as well as behavior analysis of these defenses when used in an environment of distributed computing [10].

- ANN model for DoS detection [10]

The input layer, hidden layer, and output layer are the three primary layers of an ANN model. The hidden layer consists of many layers [10]. Sorting or extracting significant features may help with gradient problems that approach the output layer [10]. A widely used method for comparing how well machine learning algorithms work is cross-validation [10]

- LTSM and RNN for DoS detection [10]

Due to its ability for handling vanishing gradients in Recurrent Neural Networks (RNNs), LSTM networks are particularly beneficial in identifying Distributed Denial of Service (DDoS) attacks [10]. Anomaly-based detection and signature-based detection are two popular methods for identifying active DDoS attacks [10].

- TEHO-DBN Classifier for DoS detection [10]

In their research on DoS detection Velliangiri et al have proposed a new DDoS detection method in a cloud setting employing a deep learning-based classifier [10]. The characteristics that are believed to be input to the classifier were gathered and organized by individuals [10]. The classifier for DDoS attack detection uses a Deep Belief Network (TEHO-DBN) that relies on Taylor-Elephant Herd Optimization [10].

c. Deep learning for detecting phishing attacks

Numerous studies into the use of deep learning to detect and prevent phishing attacks have produced positive outcomes [16]. Traditional machine learning techniques have not performed as well as deep learning techniques [16].

- CNN model for phishing detection. [17]

In CNN model for detecting phishing attacks a series of characters is transformed into 2D graphics, and significant aspects are identified utilizing filtering [17]. After this, a neural layer adds filtering to the image in order to identify patterns of behavior in phishing emails or URLs [17]. A pooling layer keeps important aspects of the image intact while reducing its dimensionality [17]. the fully linked layer assigns if the output is harmful or not [17].

- LSTM model for detecting phishing attacks

LSTM model is paired with the RNN model for effectively detecting phishing attacks. A Deep Learning Multi-Agent Model (RNN) for phishing detection makes use of the LSTM architecture [17]. A character string, like the text of an email or URL, makes up the input data. Established connections in the sequence are captured by an LSTM layer, which also recognizes scattered patterns [17]. A fully linked layer is then applied to the output, mapping characteristics to the final output [17]. Phishing attacks can be effectively recognized using this technique [17].

5) benefits and limitations of deep learning in cyber security for healthcare

An analysis of the benefits and limitations of deep learning in the context of cybersecurity for healthcare is of utmost importance. Healthcare organizations can make well-informed decisions on the implementation of deep learning-based cybersecurity solutions to preserve patient data and defend critical healthcare infrastructure by learning the capabilities and challenges associated with these technologies. Examining the primary advantages and limitations of deep learning in the field of cybersecurity for healthcare, underlining its capacity to adjust to changing cyber environments while addressing concerns about data privacy, complexities, and need for resources.

From the research conducted, the concluded benefits and limitations of deep learning models are as follows:

- **Benefits.**

- Deep learning algorithms possess an ability of analyzing huge quantities of complex data and identifying complex patterns that may serve as more precise signs of cyber dangers compared to traditional methods.

- Deep learning models can gain knowledge and adapt their behavior in response to emerging cyber threats and attack strategies, resulting in increasing their effectiveness in swiftly recognizing emerging dangers.

- The use of deep learning methods enables the automation of various security tasks, in turn reducing the demands on cybersecurity professionals while improving response times.

- Deep learning algorithms can scale well to deal with the increasing amount and intricate nature of healthcare data, making them suited for large-scale cybersecurity operations in healthcare organizations.

- **Limitations.**

- Deep learning models rely mainly on high-quality data sets for training, which may be limited or challenging to acquire in healthcare settings due to privacy issues and data access restrictions.

- Training deep learning models requires significant computational resources, including expensive equipment and large datasets, which may pose issues for resource-constrained healthcare organizations with limited budgets and infrastructure.

- Deep learning algorithms are vulnerable to adversarial attacks, where attackers can modify input data to trick the algorithms and make false projections, providing a security issue in healthcare applications.

- The application of deep learning in cybersecurity creates ethical considerations linked to data privacy, discrimination, and responsibility, requiring healthcare organizations to maneuver complex legal frameworks and assure that they comply with regulations governing data protection.

IV. Future research

The healthcare industry has changed and is growing progressively digitized. Deep learning research has great potential in the domains of healthcare and cyber security. The fields of cyber security and healthcare will be revolutionized by two subtopics of artificial intelligence: deep learning and machine learning. When it comes to providing high-quality services, improving system efficiency, handling administrative tasks, and other duties in the healthcare industry, deep learning and AI will have greater possibilities. Because of the advances and research in deep learning, cyber security will also change to protect and prevent organizations, healthcare, and patient data from cyber-attacks in these and other critical infrastructure fields. To solve the issues and maintain organizations, this field needs further study. It's also critical to monitor any emerging vulnerabilities identified by the implementation of AI and deep learning models to the cyber security and health domains. For a safe and cutting-edge healthcare environment, researchers and business stakeholders must give top priority to addressing cybersecurity issues and guaranteeing the ethical application of AI. [15]

V. Conclusion

This research paper analyzes the role of deep learning in cybersecurity for healthcare organizations. It underlines the challenges faced in securing health information as well as vital infrastructure against cyber-attacks. Deep learning techniques, such as deep convolutional neural networks, LSTM networks, and autoencoders, offer potential solutions for detecting and mitigating cyber-attacks. However, restrictions such as high-quality datasets, computational resources, and vulnerability to adversarial attacks must be addressed. Ethical considerations including data privacy, discrimination, and responsibility must be addressed correctly in order to guarantee ethical application of deep learning in healthcare cybersecurity. Future studies should focus on strengthening deep learning models' capabilities, resolving future weaknesses, and assuring compliance with regulations.

VI. Acknowledgement

I would like to extend my appreciation to the Lecturer in Charge (LIC), Mr. Kanishaka Yapa for their timely selection of the research paper subject and their offering of detailed instructions for its successful completion. The selection of this topic in their assessments helped the examination of important problems in the field of cybersecurity. The clear instructions provided served as a blueprint for conducting the research and ensuring compliance with academic requirements.

VII. References

[1] V. a. K. S. a. P. P. a. S. A. Ravi, "Application of Deep Learning Architectures for Cyber Security," 2019.

[2] M. A. &. M. L. &. J. H. &. S. R. .. 1. Ferrag, "Deep Learning Techniques for Cyber Security Intrusion Detection : A Detailed Analysis," (2019).

[3] B. a. A. S. a. A. C. Kale, "Cyber-Attacks on Digital Infrastructures in HealthCare: The Secured Approach," p. 12, 2022.

[4] Mohd Javaid and Abid Haleem and Ravi Pratap Singh and Rajiv Suman}, "Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends," vol. 1, 2023.

[5] E. Obaitan, "healthcare cyber attacks," 2021.

[6] P. A. A. M. M. E. P. C. L. P. Ying He, "Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review," no. PMCID: PMC8059789PMID: 33764885, 2021 .

[7] A. Cartwright, "The elephant in the room: cybersecurity in healthcare," *Journal of Clinical Monitoring and Computing,* vol. 37, pp. 1-10, 2023.

[8] A. Mohammad, "Ransomware Evolution, Growth and Recommendation for Detection," vol. 14, p. 68, 2020.

[9] A. Al Qartah, "EVOLVING RANSOMWARE ATTACKS ON HEALTHCARE PROVIDERS," 2020.

[10] a. B. s. Gayathri, "Impact of Machine Learning and Deep learning techniques for Denial of service attack detection," 2021.

[11] P. a. F. M. a. Y. B. a. N. P. Yeng, "Investigation into Phishing Risk Behaviour among Healthcare Staff," 2022.

[12] M. a. G. S. Kumar, "A COMPREHENSIVE STUDY OF PHISHING ATTACKS AND THEIR COUNTERMEASURES," 2023.

[13] F. a. A. M. Bachay, "Hybrid Deep Learning Model Based on Autoencoder and CNN for Palmprint Authentication," *International Journal of Intelligent Engineering and Systems,* 2022.

[14] G. Olaoye, "Deep Learning Approaches for Natural Language Processing: Advancements and Challenges," *Machine Learning,* 2024.

[15] L. a. A. M. a. B. A. Moujoud, "A State-of-the-Art Survey on Ransomware Detection using Machine Learning and Deep Learning," 2023.

[16] O. a. B. E. a. K. E. Sahingoz, "EPHIDES: Deep Learning Based Phishing Detection System," *IEEE Access,* 2024.

[17] P. a. R. S. Kaushik, "Deep Learning Multi-Agent Model for Phishing Cyber-attack Detection," *International Journal on Recent and Innovation Trends in Computing and Communication,* vol. 11, 2023.

VIII. Author profile

Kavindu Weerasinghe is a 3rd year undergraduate student in SLIIT information technology specializing in cyber security. I am very motivated to investigate various aspects of cybersecurity and develop practical skills that can be effectively used in real-world scenarios.