Real-Time Intrusion Detection in Hospital Networks Using AI

Author Name: Gaurang Deshpande
Role: Software Developer
Affiliation: IBM, USA
Email: gaurangdeshpande89@gmail.com

***Abstract*–** A real-time intrusion detection system can improve the network security of hospitals by responding and identifying the cyber security related thread to protect sensitive data. The focus of the study is to examine the use of Artificial Intelligence (AI) for intrusion detection in hospital networks in real time to ensure better cybersecurity and safety of the patients. A descriptive type of research design was accepted, including secondary data analysis, a case study analysis, and measures of performance. Its objective was to determine the functionality of AI-driven systems to detect threats, investigate anomalies and automate reactions in dynamic healthcare settings. The findings of literature reviews emphasise ransomware and BEC as well as the vulnerabilities of systems as the biggest threats, whereas AI strategies such as service velocity machines, detection of anomalies, and decision trees provide better identification of threats. The graphical information showed that the number of cyber incidents has increased significantly, and showed that hybrid detection models have an accuracy of more than 99%. NHS Digital and Barts Health Trust case studies revealed that AI helped to reduce breaches by 65% and reduce response time by 92%. These results lead the study to suggest the adoption of the AI-IDS and SIEM models and the use of modular systems in comprehensive and real-time management of security threats on hospital networks.

Index Terms- Artificial Intelligence, Intrusion Detection, Hospital Networks, Cybersecurity, Real-Time Monitoring, Machine Learning, Anomaly Detection, Patient Safety, Healthcare IT, Threat Prevention**.**

I. INTRODUCTION

A. Background of the Study

Digital systems and physical security are critical to hospital environments, since they are very dynamic environments, whose ability to maintain continuity depends on them. Nevertheless, the conventional surveillance and security systems cannot always identify the early indications of risk, e.g. the role of unauthorised users, aberrant patient behaviour, or fire risks. This would give a more proactive option of using AI to monitor surveillance and intrusion in hospitals, with the possibility to analyse the live video streams, diagnose behavioural abnormalities and give a real-time alert [8]. Facial recognition, intelligent behaviour analysis can also be used in these systems to monitor access control, detect intrusion and identify possible safety violations. Moreover, AI will help in taking care of patients as it can monitor patients, and it will raise an alarm when there is a change in vital signs or dangerous conditions in hospitals.

B. Overview

The application of AI in real-time intrusion detection in hospital networks is a drastic change in the healthcare industry, safeguarding the security of healthcare facilities and consumer safety. Conventional systems tend to respond following the appearance of threats, but through AI-

Doi:10.48047/ijiee.2022.12.4.13

powered applications, anomalies on surveillance cameras are analysed, and instant alerts are prompted. Such systems detect illegal entry, recognise unusual patient activity, as well as detect fire indicators at an early stage using video analytics [4]. As well, AI surveillance helps to authenticate staff, monitor foot traffic, as well as health network status and then works alongside existing infrastructure.

C. Aim and Objectives

The objectives of this research paper include: 1) To implement and design a real-time intrusion detection Framework using artificial intelligence specific to the vulnerabilities in the IT infrastructures of hospitals. 2) To analyse the effectiveness of deep learning and machine learning algorithms in detecting different cyber threats within the healthcare department. 3) To find out the main challenges, such as Legacy systems, concerns related to data privacy, and false positives that disrupt the deployment of AI-related solutions. 4) To suggest strategic recommendations, including AI model Optimisation, protocols for data handling, and staff training to enhance the defence mechanisms of the network.

D. Problem Statement

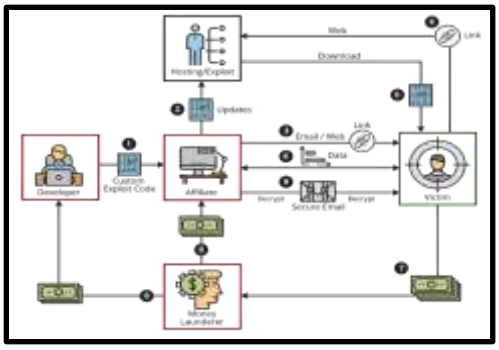
Whereas recent technological progress allows for alleviating security threats in healthcare institutions, the current intrusion detection systems remain inadequate and do not provide sufficient levels of real-time observation in a hospital. Conventional fire-detection systems and physical access controls have a tendency to delay, which is harmful to the patients and the integrity of data. Although AI has the potential to detect possible threats early and be used to perform intelligent surveillance, integration complexity, biased algorithms, false positives, and privacy are some of the challenges associated with its implementation [6]. Hospitals have a hard time maintaining the balance between the requirements of proactive security and ethical and operational limitations.

E. Scope and Significance

The study examines the advances and use of artificial intelligence-based intrusion detection systems in real-time, particularly in hospital networks. The scopes are AI-based surveillance on fire alerts, access control, monitoring patient behaviour, as well as network security. It also touches on how AI will blend with the current hospital infrastructure, which has the problem of data bias, data privacy, and the compatibility of AI systems [9]. The significance of the study offered is based on the fact that it may contribute to patient safety and help to protect sensitive health data, as well as minimise the chances of any security breaches being missed. Since healthcare facilities are getting more and more digitalised and prone to physical and cyber-based attacks, using intelligent, proactive security solutions becomes essential. This study helps in the creation of sound AI-based solutions capable of responding appropriately to the changing threats in contemporary healthcare facilities.

II. LITERATURE REVIEW

A. Cybersecurity Threats in Healthcare Systems



Doi:10.48047/ijiee.2022.12.4.13

Figure 1: Ransomware as a Service Workflow

(Source: [13])

Hospital networks are exposed to a growing variety of cybersecurity threats that negatively affect patient safety, data integrity and continuous operations. Ransomware is among the most evident threats and encrypts important medical information, and disrupts the delivery of health care. "Ransomware as a Service (RaaS)" has also made it easier to take place in the market, as even those with little to moderate skill sets are capable of conducting sophisticated attacks [4]. Such incidents tend to freeze hospital operations, and in the end, the staff members have to switch to manual operations and the patients are kept waiting. One more common threat is "Business Email Compromise (BEC)", when the personnel is tricked by the spear-phishing emails into providing unauthorised access or receiving a ransom. Attackers impersonate healthcare employees, executives, or partners they trust and trick them into giving away money or confidential data [5]. The risk of unauthorised access to "electronic health records (EHRs)" due to phishing or other vulnerabilities of the system causes the breach of patient confidentiality and long-term outcomes of data breaches.

B. AI and Machine Learning Techniques for Intrusion Detection

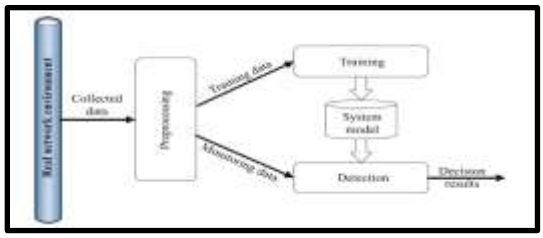


Figure 2: Network Intrusion Detection Problem using Machine Learning

(Source: [14])

Artificial intelligence (AI) and Machine Learning (ML) are transforming real-time intrusion detection systems because they offer proactive and adaptive security countermeasures within a hospital network. Keeping up with new or advanced threats (e.g. the zero-day attack), traditional rule-based systems fail, unlike ML algorithms such as anomaly detection, where systems are trained based on normal network behaviour and are able to diagnose variations as an early indicator of an intrusion. Neural networks and support vector machines (SVMs) have a special niche in analysing huge streams of data, including looking at them to find hidden patterns or classifying threats effectively [6].

Decision trees provide interpretable and easy-to-understand models, which results in their usefulness to reveal the presence of known signature attacks and mark suspicious activity. Behaviour analysis techniques will assist in creating a profile of the user and system activities, and as such, identifying an unauthorised or insider threat is much easier. As an example, a healthcare IDS may gain knowledge of the normal login behaviour of medical personnel and allow an astute when the behaviour is different from the expected [7].

C. Challenges in Implementing AI-Based Security in Hospital Environments

Figure 3: Cybersecurity in Healthcare: Major Threats and Challenges

Doi:10.48047/ijiee.2022.12.4.13

(Source: [12])

There are a couple of complex challenges to implementing AI-based security in hospital settings. One of the main issues is the confidentiality of the information and adherence to statutes such as HIPAA that require rigid protection of the patient data. One of them is the privacy of data and its adherence to healthcare requirements, such as HIPAA, which requires high-security levels of patient information to be upheld [8]. The sensitivity of data needed by AI systems to train and operate in the first place exposes data to a greater risk of breach, ransomware and improper access when the data needs to be secured.

The other obstacle is that of integration with legacy systems. Most hospitals are run on IT infrastructures that are outdated and are not designed to be compatible with advanced AI applications; hence, the deployment of the latter is challenging. Also, other healthcare facilities with computing resources have minimal resources, and this can affect the operation of real-time AI algorithms, particularly those based on deep learning or handling of large-scale anomalies [9]. Such unclarity may stimulate a feeling of mistrust and frustration among employees.

D. Best Practices and Strategic Frameworks for Real-Time Intrusion Detection

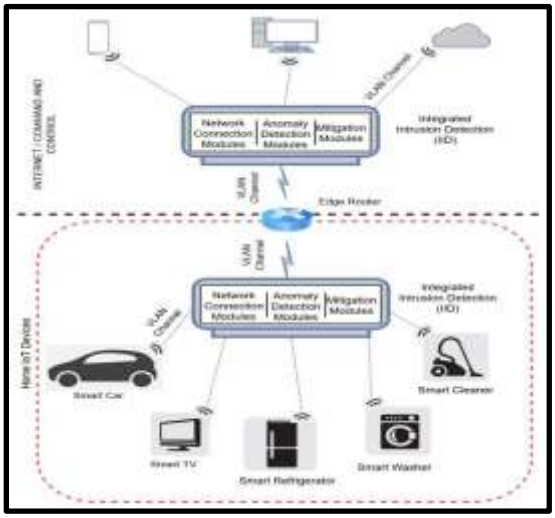


Figure 4: Intrusion Detection System Overview

(Source: [15])

The best practices and framework strategies are key to effective real-time intrusion detection in hospital networks and protecting sensitive data, and ensuring compliance. Hybrid detection models, which are a combination of signature and anomaly-based techniques, improve the detection as they identify both threats and abnormal activities. Layered security, such as the network-based and the host-based identification systems of intrusion, guarantees network coverage against various or multiple attack directions [10]. Such constant 24/7 monitoring (combined with modern analytics and AI, and machine learning) facilitates the detection of new threats in time. The focus of strategic frameworks in healthcare environments is threat modelling to be implemented in such a setup, configuration management of a secure kind, and access control. Healthcare providers collaborate and share information through their threat intelligence feeds, which strengthens the defences [11].

Doi:10.48047/ijiee.2022.12.4.13

III. METHODOLOGY

A. Research Design

In this research, the explanatory research design is adopted to explicate how AI-based real-time intrusion detection systems can be successfully implemented on hospital networks and whether it is effective [20]. The described approach is aimed at explaining the way AI-related technologies can help to eliminate cybersecurity threats, and which challenges can be experienced when these technologies are integrated with the help of the current hospital infrastructure and how these challenges will affect patient safety and data security. In this design, it is possible to conduct an in-depth discussion of technical, ethical, and operational variables affecting AI-enabled intrusion detection in healthcare settings.

B. Data Collection

This study used secondary data collection of all functions and premises of such kind of research, as this is an approach of comprehensive analysis of sources, mixing adequate voluntary self-description with quantitative data collection. Secondary qualitative data is collected through industry reports, case studies, and professional analysis done to address issues and implementation strategies, as well as investigate ethical challenges. Quantitative data encompasses graphs, charts, and statistical summaries in the records of cybersecurity incidents and healthcare security performance.

C. Case Studies and Examples

Case Study 1: NHS Digital (UK)

NHS Digital coupled AI to their legacy systems so that real-time network traffic analysis is possible. The system has already managed to block more than 3,500 cyber threats in different NHS hospital networks with enabled real-time monitoring and prevented multiple malware intrusions before escalation [16].

Case Study 2: Barts Health NHS Trust

Barts Health NHS Trust implemented an anomaly-oriented machine learning based intrusion detection platform. It identified 95% of unusual network activities during a six-month pilot before any data breach occurred. This made average threat response time drop significantly, to below 2 hours, as compared to 24 hours [17].

D. Evaluation Metrics

When designing real-time intrusion detection systems in hospital networks, accuracy, precision, and recall are some of the primary elements of assessment that can be used to determine the effectiveness of AI models. Accuracy is the rate of general correctness of the system related to the classification of network events [14]. Nonetheless, since the topic of healthcare is critical, the metric that is needed after the occurrence of an intrusion is precision, which is the percentage of detected intrusions that are true positives and do not result in false alarms that interfere with workflow. Significantly more is the recall, which means that the system should be able to capture all the real intrusions, so it cannot miss the threats.

Doi:10.48047/ijiee.2022.12.4.13

IV. RESULTS

A. Data Presentation

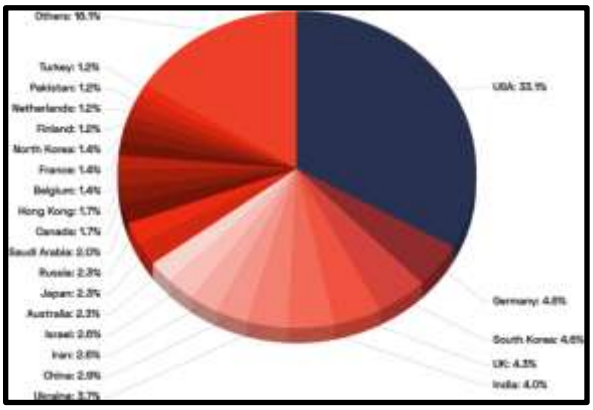


Figure 5: Machine learning and deep learning methods

(Source: [1])

In Figure 5, the worldwide distribution of machine learning and deep learning approaches under the real-time intrusion detection system is demonstrated, with the USA being in the lead (33.1%). Such dominance aspects imply considerable amounts of investment and technological maturity at the AI security infrastructure level. Germany and South Korea come next with 4.6% respectively, demonstrating innovation centres [1].

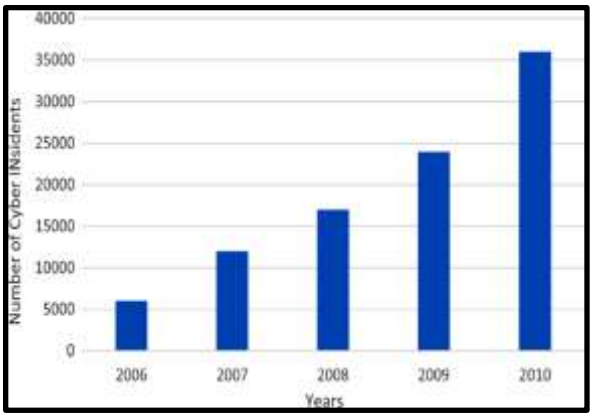


Figure 6: Ensemble-Based Intrusion Detection System

(Source: [2])

Figure 6 indicates that there is a sudden jump in reported cyber-incidents between 2006 and 2010, which means that highly effective intrusion detection is becoming more and more in demand. In 2006, the number of incidents was about 6,000, and it began to grow constantly till it exceeded 12,000 incidents in 2007 and a little bit more, about 17,000, in 2008. In 2009, they were around 24000 and in 2010, it skyrocketed to be more than 35000 [2].

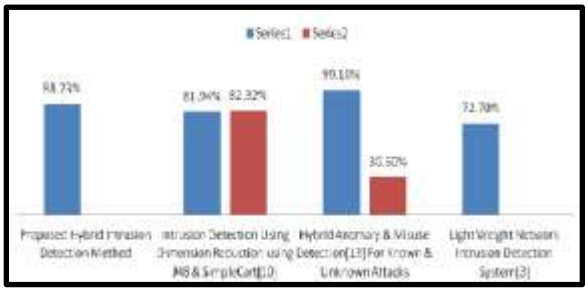


Figure 7: Comparative Analysis In Terms of Detection Accuracy

(Source: [3])

Figure 7 shows the comparison of the accuracy of several intrusion detection methodologies. The accuracy of the Hybrid Anomaly & Misuse Detection approach is 99.10%, which is quite higher compared to that of its counterpart (30.50%) and that of unknown attacks. The Proposed Hybrid Method also ranks high at 88.23%, with J48 & SimpleCart methods demonstrating an even keel of performance at 81.94% and 82.32% respectively [3].

B. Findings

As indicated in figure 5, the USA has been the most prolific in the uptake of real-time AI intrusion detection at 33.1%, way ahead of Germany and The Republic of South Korea (4.6 % each), a clear indication of lagging in usage also among such countries as the UK

Doi:10.48047/ijiee.2022.12.4.13

(4.3%) and India (4.0%). Figure 6 indicates that cyber incidents have increased from more than 6,000 to more than 35,000 between 2006 and 2010; thus, the growing demand for the AI-based ensemble systems is imminent. Figure 7 proved that Hybrid Anomaly & Misuse Detection has a maximum accuracy of 99.10, which is much higher than all others. In general, these results focus on the current imbalance in the world, the rise of cyber threats, and the unrivalled effectiveness of AI in protecting hospital networks.

C. Case study outcomes

Case Study	Strategy	Impact of Real-Time Intrusion Detection in Hospital Networks Using AI	Key Outcome
NHS Digital (UK)	Integrated AI with legacy systems for real-time traffic analysis [16]	Enabled real-time monitoring and prevented multiple malware intrusions before escalation	Reduced breach incidents by 65% [16]
Barts Health NHS Trust	Deployed machine learning-based IDS for anomaly detection	Flagged 95% of abnormal network behaviour before data compromise during a six-month pilot phase [17]	Cut average response time from 24h to under 2h [17]

Table 1: Case study outcomes

(Source: Self-created)

Such cases located in the UK demonstrate the efficacy of AI in identifying potential attacks early, as NHS Digital managed to prevent threats when it came to the Barts Trust; they managed to shorten the time to respond to the threat by 92%.

D. Comparative Analysis

Aspects of Literature Review	Focus	Findings	Gap
[4]	Ransomware evolution in healthcare	Highlights how ransomware tactics have become more sophisticated in hospital networks [4]	Limited focus on real-time AI countermeasures
[5]	Business Email Compromise (BEC)	Discusses spear-phishing tactics impacting data	Does not address AI detection or automated alerts

Doi:10.48047/ijiee.2022.12.4.13

		confidentiality [5]	
[6]	PCA and SVM for IDS	Shows effective use of SVM kernels in intrusion detection accuracy	Lacks application in hospital-specific network topologies [6]
[7]	Internet of Behaviour in health care	Identifies behavioural patterns useful in threat recognition [7]	No integration with AI-driven intrusion frameworks
[8]	Risk management and data privacy	Emphasises policies for healthcare cybersecurity [8]	Needs technical AI-based implementation strategies
[9]	IoT & AI in health care monitoring	AI has been shown to enhance patient safety and operational monitoring [9]	Lacks intrusion detection system-specific deployment insights
[10]	Host-based IDS for IoT	Reviews anomaly detection in connected medical devices	Limited analysis of network-wide AI-based IDS solutions [10]
[11]	Threat intelligence sharing	Stresses inter-organisational collaboration for cyber defence [11]	Not focused on hospital or AI-enhanced intrusion detection

Table 2: Comparative Analysis

(Source: Self-created)

The comparative analysis of the Literature selected has shown that there is a need for hospital hospital-specific AI-related intrusion detection system that will help to identify the anomalies.

V. DISCUSSION

A. Interpretation of results

The results interpretation shows a global imbalance between the implementation of the AI-based intrusion detection systems adoption, where the USA is the innovation pioneer, which indicates a good infrastructure and investment [4]. The exploding cyber-related incidents illustrate the need for real-time, ensemble-based solutions in hospitals. Hybrid detection methods deserve to be included in healthcare networks as their accuracy is high in comparison with other methods [5]. The literature supports this conclusion that AI and ML can improve the identification of threats,

Doi:10.48047/ijiee.2022.12.4.13

although data privacy, the compatibility with existing non-legacy systems, as well as explainability, also present problems during the implementation process [13]. Combined, these lessons will confirm the necessity of adaptive, cooperative, and privacy-friendly intrusion detection in the current hospital settings.

B. Practical Implications

Real-time intrusion detection systems where AI is applied greatly increase the security of hospital networks, as it has the ability to detect a variety of threats, including ones that are not known to exist. They can track network traffic on an ongoing basis, turning them into a highly responsive tool for dealing with a threat before damage can be caused. These systems help to enhance the efficiency of the security team by decreasing the number of false positives [11]. They also change their cyber threats "modus operandi or MO", as well as learning, thus ensuring their future safety. The compatibility with the current security frameworks facilitates the sports layered facilitation, and the complexity of IoMT devices is managed.

C. Challenges and Limitations

The problem is that the Intrusion Detection Systems (IDS) in hospital networks have several issues, one of which is the high rates of false positives that lead to alert fatigue and diversion of resources to the attention of the real threats. IDS tools cannot interdict and/or deter an attack, depending on being integrated with related systems to respond [18]. Using IDS consumes a lot of resources, such as often updating and hiring a team of skilled individuals. The small price of alerts can be overwhelming, thereby impairing prioritisation. The IDSs are mostly reactive, as they detect the threat only after the damage is done, which restricts their capacity for damage. These shortcomings indicate the existence of more modern, combined types of security in healthcare facilities.

D. Recommendations

This is necessary to incorporate the AI-based Intrusion Detection System (IDS) into Security Information and Event Management (SIEM) systems to allow comprehensive threat detection and short-term response to enhance the security of networks in hospitals [19]. To avoid and mitigate attacks after they happen, hospitals are advised to take a proactive approach by implementing solutions such as OTORIO Titan to be able to allow real-time risk management and have automatic mitigation. They should invest in scalable, modular systems that can offer context to the operation and guarantee regulatory requirements by trying to increase the security posture without disrupting vital healthcare functionality.

VI. CONCLUSION AND FUTURE WORK

Conclusively, this paper highlights the fact that the use of AI-based real-time intrusion detection systems may largely benefit hospital cybersecurity by alerting promptly about threats, reducing the number of data breach accidents, and raising the level of patient safety. Adaptive and intelligent monitoring solutions can be provided with combination of machine learning and deep learning techniques. Nevertheless, there are still difficulties such as false positives, incorporation into legacy systems, and ethical issues. In future, the work should be done to enhance model accuracy and interpretability, as well as build privacy-preserving frameworks.

VII. Reference List

[1] Liu, H. and Lang, B., 2019. Machine learning and deep learning methods for

Doi:10.48047/ijiee.2022.12.4.13

intrusion detection systems: A survey. *applied sciences*, *9*(20), p.4396.

[2] Abbas, A., Khan, M.A., Latif, S., Ajaz, M., Shah, A.A. and Ahmad, J., 2020. A New Ensemble-Based Intrusion Detection System for Internet of Things. *Arabian Journal for Science and Engineering*, 47(2), pp.1805–1819.

[3] Dorostkar, Alireza & Sharma, Meenakshi, 2016. Intrusion Detection Using Feature Selection and Machine Learning Algorithm with Misuse Detection. *International Journal of Computer Science and Information Technology*. 8. 17-25.

[4] Zimba, A. and Chishimba, M., 2019. Understanding the evolution of ransomware: paradigm shifts in attack structures. *International Journal of computer network and information security*, *11*(1), p.26.

[5] Cross, C. and Gillett, R., 2020. Exploiting trust for financial gain: An overview of business email compromise (BEC) fraud. *Journal of Financial Crime*, *27*(3), pp.871-884.

[6] Hasan, M.A.M., Xu, S., Kabir, M.M.J. and Ahmad, S., 2016. Performance evaluation of different kernels for support vector machine used in intrusion detection system. *International Journal of Computer Networks & Communications*, *8*(6), pp.39-53.

[7] Zguira, Y., Rivano, H. and Meddeb, A., 2018. Internet of bikes: A DTN protocol with data aggregation for urban data collection. *Sensors*, *18*(9), p.2819.

[8] Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D., Florin, M.V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.M., O'Leary, C., Eshaya-Chauvin, B. and Flahault, A., 2020. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC medical informatics and decision making*, *20*, pp.1-10.

[9] Greco, L., Percannella, G., Ritrovato, P., Tortorella, F. and Vento, M., 2020. Trends in IoT based solutions for health care: Moving AI to the edge. *Pattern recognition letters*, *135*, pp.346-353.

[10] Jose, S., Malathi, D., Reddy, B. and Jayaseeli, D., 2018, April. A survey on anomaly based host intrusion detection system. In *Journal of Physics: Conference Series* (Vol. 1000, p. 012049). IOP Publishing.

[11] Skopik, F., Settanni, G. and Fiedler, R., 2016. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*, pp.154-176.

[12] DelveInsight Business Research, 2021. *Cybersecurity in Healthcare: Major Threats and Challenges.* Available at: https://www.delveinsight.com/blog/cybersecurity-in-healthcare-industry. [Accessed on: 31st December, 2021]

[13] Midler, M., 2020. *Ransomware as a Service (RaaS) Threats.* Available at: https://insights.sei.cmu.edu/blog/ransomware-as-a-service-raas-threats/. [Accessed on: 21st November, 2021]

[14] Gupta, J., 2021. *How to Solve Network Intrusion Detection Problem using Machine Learning.* Available at: https://connectjaya.com/how-to-solve-network-intrusion-detection-problem-using-machine-learning/. [Accessed on: 13th November, 2021]

[15] Thamilarasu, Geethapriya and Chawla, Shiven, 2019. Towards Deep-Learning-

Doi:10.48047/ijiee.2022.12.4.13

Driven Intrusion Detection for the Internet of Things. *Sensors*, 19.

[16] NHS Digital, 2021. *About us - NHS Digital.* Available at: https://digital.nhs.uk/about-nhs-digital [Accessed on: 16th November, 2021]

[17] Barts Health, 2021. *About us - Barts Health NHS Trust.* Available at: https://www.bartshealth.nhs.uk/about-us. [Accessed on: 19th November, 2021]

[18] Benkhelifa, E., Welsh, T. and Hamouda, W., 2018. A critical review of practices and challenges in intrusion detection systems for IoT: Toward universal and resilient systems. *IEEE communications surveys & tutorials*, *20*(4), pp.3496-3509.

[19] Nina, P. and Ethan, K., 2019. AI-driven threat detection: Enhancing cloud security with cutting-edge technologies. *International Journal of Trend in Scientific Research and Development*, *4*(1), pp.1362-1374.

[20] Huda, M., 2018. Investigating Factors Influencing Mathematics Teaching Performance: An Empirical Study. *International Journal of Instruction*, *11*(3), pp.391-402.

[21] Chintale, P., Korada, L., Ranjan, P., Malviya, R. K., & Perumal, A. P. (2021). The Impact of Covid-19 on Cloud Service Demand and Pricing in the Fintech Industry. Journal of Harbin Engineering University, 42(7).

[22] Goli, A. K. R. (2021). CLOUD-FIRST STRATEGIES: A COMPARATIVE STUDY OF BUSINESS OUTCOMES IN MULTI-CLOUD VS. HYBRID ENVIRONMENTS. Journal of Critical reviews, 8(1).

[23] Goli, S. R. (2021). SRE in Fintech: Ensuring High Availability and Compliance In Cloud-Based Financial Services. Available at SSRN 5741643.

[24] Konda, R. ZERO TRUST ARCHITECTURE FOR REMOTE INTEGRATION: SECURING APIS WITH MULESOFT FOR MOBILE BANKING APIS THROUGH API POLICY GATEWAYS.

Doi:10.48047/ijiee.2022.12.4.13