A STUDY OF CURRENT THREATS AND COUNTERMEASURES IN AI AND CYBERSECURITY

J. P. Pramod[1], Bhagavatula Veda Bharati[2] & Kanneboina Vaishnavi Yadav[3]

[1]*Asst Professor, Dept of Physics*

Stanley College of Engineering and Technology for Women

[2&3]*B.Tech Student Dept of Information Technology*
Stanley College of Engineering and Technology for Women

ABSTRACT

The study aims to provide a comprehensive substantiation of applying artificial intelligence tools in the cybersecurity system to automate the protection and timely detection of threats. Traditional means of counteracting cyberattacks are currently unable to withstand the current situation. Therefore, AI-based technologies are seen as an effective solution to the problem. The qualitative synthesis reveals that AI is being utilized in areas such as mental health monitoring, emotional support, and personalized well-being programs, identification of psychosocial risk factors, and training and development. The practical value of research findings lies in the possibility of their use when actualizing the role of AI technologies in the formation of an effective cybersecurity system, given their apparent advantages and possible shortcomings. The pandemic outbreak has replaced the classroom method of teaching with the online execution of teaching practices and simulators. This review contributes to the existing literature by offering a detailed categorization of AI applications in workplace well-being, and it highlights the practical utility of AI in enhancing employee mental health and overall well-being. Rather than the traditional perceptions of robotics crowding out labour jobs, the overall impact on the labour market has exerted a promotional effect. AI technology is positively associated with productivity and employment.

Keywords: *artificial intelligence (AI), cybersecurity, AI technology, well-being, decision-making.*

INTRODUCTION

In the era of technology-driven society, the convergence of artificial intelligence a cyber security is at the forefront of innovative searches. These two significant spheres of influence, acting in synergy, allow for the transformation of the basis of digital security. Many scientific studies by have been devoted to the application of AI technologies and information security issues. Through a multidisciplinary approach, drawing upon expertise from cyber security specialists, AI researchers, ethicists, and policymakers, this study seeks to foster a holistic understanding of the complex interplay between AI and cyber security. By elucidating the theoretical frameworks and offering pragmatic solutions, we endeavor to empower readers to navigate the cyber security challenges of the AI era effectively. They focus mainly on the intersection of cyber security and artificial intelligence. Some modern studies analyze the capabilities of AI tools in the field of information security. Several scholars have highlighted typical threats and risks that accompany the active use of AI systems in cyber defense. However, given the viewpoints of the aforementioned study, it should be noted that in the context of the constant dynamic impact of external and internal factors, there is a lack of research on artificial intelligence in the field of information security as a priority promising component of cyber defense. It should be noted that the results of the scientific research of the aforementioned study do not sufficiently analyze the feasibility of using in the context of automated data protection and rapid threat identification. This enables the formation of a comprehensive concept of cyber security, quick response to new challenges, and the development of a complex of preventive protection against cyber attacks.

LITERATURE REVIEW

Paul Davidsson (2024) The use of Artificial Intelligence (AI) in Internet of Things (IoT) systems has gained significant attention due to its potential to improve efficiency, functionality and decision-making. To further advance research and practical implementation, it is crucial to better understand the specific roles of AI in IoT systems and identify the key application domains. In this article we aim to identify the different roles of AI in IoT systems and the application domains where AI is used most significantly. Eighty-one relevant survey articles were selected after applying the selection criteria and then analyzed to extract the key information. As a result, six general tasks of AI in IoT systems were identified: pattern recognition, decision support, decision-making and acting, prediction, data management and human interaction. Moreover, 15 subtasks were identified, as well as 13 application domains, where healthcare was the most frequent. We conclude that there are several important tasks that AI can perform in IoT systems, improving efficiency, security and functionality across many important application domains.

Rishit Lakhani (2023) In fact, the mushrooming development of IoT has reshaped industries and everyday life in connecting devices, networks, and systems. Accompanying this phenomenal growth are formidable challenges related to cybersecurity. The major reasons why IoT networks are more susceptible to a variety of cyber threats are the limited computational resources of devices, a lack of standardized security protocols, and the large-scale interconnectedness of devices. This paper throws light on some of the major cybersecurity threats to IoT networks, such as device vulnerabilities, network-based attacks, and data breaches. It further pays attention to the root causes of such vulnerability exposures. Further, it discusses an in-depth analysis of some of the existing defense mechanisms involving advanced authentication methods, encryption techniques, and network security measures. The work also probes into some state-of-the-art security technologies like blockchain and artificial intelligence that hold immense promise for securing IoT.

Khaled Alhazmi (2021) The Internet of Things (IoT) has emerged as a technology capable of connecting heterogeneous nodes/objects, such as people, devices, infrastructure, and makes our daily lives simpler, safer, and fruitful. Being part of a large network of heterogeneous devices, these nodes are typically resource-constrained and became the weakest link to the cyber attacker. Classical encryption techniques have been employed to ensure the data security of the IoT network. In addition, node security is still a challenge for network engineers. The rule-based approaches and shallow and deep machine learning algorithms– branches of Artificial Intelligence (AI)– can be employed as countermeasures along with the existing network security protocols. This study presented a comprehensive layer-wise survey on IoT security threats, and the AI-based security models to impede security threats.

Anupam Kumar (2021) A novel strain of Coronavirus, identified as the Severe Acute Respiratory Syndrome-2 (SARS-CoV-2), outbroke in December 2019 causing the novel Corona Virus Disease (COVID-19). Since its emergence, the virus has spread rapidly and has been declared a global pandemic. As of the end of January 2021, there are almost 100 million cases worldwide with over 2 million confirmed deaths. Widespread testing is essential to reduce further spread of the disease, but due to a shortage of testing kits and limited supply, alternative testing methods are being evaluated. Recently researchers have found that chest X-Ray (CXR) images provide salient information about COVID-19. An intelligent system can help the radiologists to detect COVID-19 from these CXR images which can come in handy at remote locations in many developing nations. The selected features were then used to classify the CXR images using a number of classifiers.

Sabrina Jesmin (2020) The stresses and patterns of life are often demanding and require physical and psychological actions to support themselves. An individual responds to mental a stress that is potentially detrimental to health. The mental stress may result hormonal imbalance and noxious stimulus in the body. The 2 (SARS-COV-2) or COVID-19 infection not only stopped people's daily routine, but also created many political, social, financial, psychological and health problems. Mental stress has become common during this pandemic with limited opportunity to reach out health professionals in person. We have proposed artificial intelligence driven cloud based self-stress detection model which takes physiological signals such as Galvanic Skin Response, Heart Rate Variability, Peripheral Capillary Oxygen Saturation to determine the stress level. The sensor are embedded into a wearable device and collects physiological signals and thereby detect stress level of an individual.

History of Artificial Intelligence

The actual birth and origins of artificial intelligence can be difficult to pinpoint but the first examples of the core principles of AI can be traced back to the 1940's. During this decade the writer Isaac Asimov wrote fiction about robots that could emulate human behavior and decision making. Another, more practical example during the same

decade, took place in England, where the English mathematician Alan Turing created The Bombe. This machine, also regarded as the first computer, was able to crack and decipher the German Enigma code during the Second World War. Turing later published an article describing his methods of testing computers and their intelligence that still stands as a springboard for AI as we know it today.

Cybersecurity

In the following section, we will define the word cybersecurity and explain the various traits that characterize it. According to Cybersecurity & Infrastructure Security Agency (CISA), "Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information". In recent years, cybersecurity has become more prioritized in business since users and companies are more aware of the threats concerning their private data. In addition, with specific regulation efforts such as the General Data Protection Regulation (GDPR) in 2016 and the Data Protection Act (DPA) in 2018, there are now clear instructions and consequences to motivate organizations to set up a proper cybersecurity infrastructure and management.

Types of Cybersecurity

As mentioned in the previous chapter, there are various of types of cybersecurity and each of them has its own field of problems to tackle and solve. In this section, we present a couple of them that are most relevant for this thesis. Network security is, in simple terms, the practice of protecting a network from being accessed by unauthorized actors. The main point is to deflect malicious activity in the network and the connections between the devices. The most commonly used network protocol today for transmitting traffic flow is Internet Protocol (IP). The network consists, of course, of many layers and all of the layers are vulnerable to attacks. The two most frequently occurring types of malicious activity on a network are network intrusion and distributed denial of service (DDoS) attacks. Network intrusion can be exploited by introducing unwanted packages to the network whose purpose is to consume resources of the network, interfere with the functions of the resources, and gain information and knowledge about the system that can be used later for more severe attacks.

How Artificial Intelligence Improves Cybersecurity

As we can notice, there is a clear incentive to deploy artificial intelligence solutions in future to fight cyber criminality. In this section, we take a closer look at what the actual benefits of AI methods are and why they are worthwhile. The computational and analytic power of AI tools is faster than human brain power. Compared to current methods, artificial intelligence can achieve a much higher detection speed. In addition to faster identification of threats, unknown attacks can be recognized faster, and proper response methods can be created without a previously implemented method. Human errors are still a big contributor in cybersecurity issues. By implementing AI technology, the number of cases caused humans could be remarkably reduced. This certainly goes for small repetitive tasks that are conducted every day, but artificial intelligence can be exploited in decision making as well. When making decisions, data and software can be tested with AI algorithms and therefore, unnoticed errors and hidden security hazards could be detected early on. The computing power of artificial intelligence may be greater than people's, but creative thinking and innovation are still up to humans. Therefore, AI tools should be implemented in tasks that are routine and repetitive. This frees up more time for security workers to focus on creative thinking and improving the process themselves.

Emerging Threat Landscape: Risks and Vulnerabilities

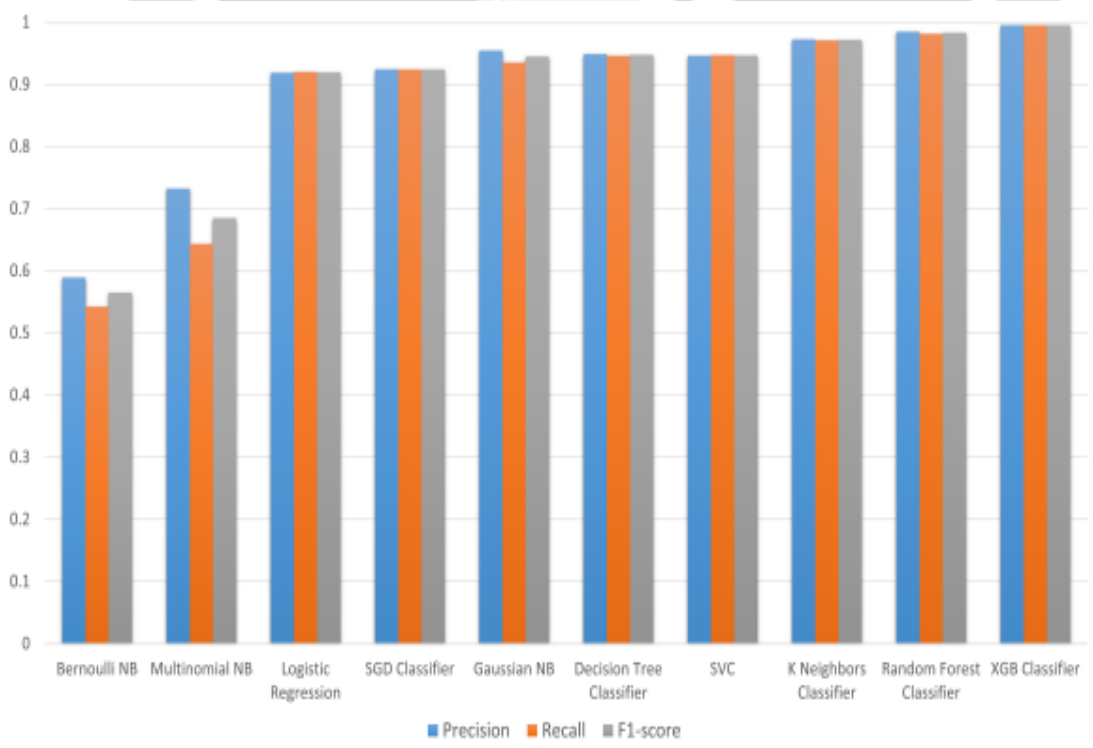
The emergence and proliferation of artificial intelligence (AI) technologies have revolutionized various aspects of our lives, from healthcare to finance, transportation, and beyond. However, with this rapid advancement comes an evolving threat landscape characterized by new risks and vulnerabilities. Understanding and mitigating these threats is essential to safeguarding AI systems and the sensitive data they handle. This essay explores the emerging threat landscape in AI, highlighting key risks and vulnerabilities that organizations and cybersecurity professionals must address. One prominent risk in the emerging threat landscape is the susceptibility of AI systems to adversarial attacks. Adversarial attacks exploit vulnerabilities in AI algorithms by perturbing input data in subtle ways that are imperceptible to humans but can cause the system to make incorrect predictions or classifications. These attacks pose serious implications for AI applications in critical domains such as autonomous vehicles, medical diagnosis, and cybersecurity. For example, in autonomous vehicles, adversarial attacks could manipulate sensor inputs to deceive the vehicle's perception system, leading to potentially catastrophic consequences on the road.

RESEARCH METHODOLOGY

The malicious actors can be a malicious file, i.e. malware or a malicious program in the network intention to compromise the targeted systems and distribute itself to infect others. The machine learning algorithm is trained with different datasets to achieve this objective. We have considered ML technique to address the research questions. According to the dataset, we have considered suitable ML or DL techniques for the detection and classification of cybersecurity threats. We have used four different types of datasets for the classification of a malicious actor. The used dataset includes malware binaries, malware images, intrusions and botnet attack vectors. The datasets are essential to training the machine learning. In the preprocessing steps, we prepare the raw dataset into the understandable format of the ML algorithm. In this process, we clean the dataset, format it a certain way, and organize it directly in any learning algorithm. We design the ML model to train them using the relevant dataset collected in the previous step. The models are used for the classification of malicious actors. We evaluate our model's performance with contemporary state-of-the-art methods. We train our model with real-world benchmark datasets and record their findings. We also did an empirical study of similar methods and compared the results of our proposed model with existing research.

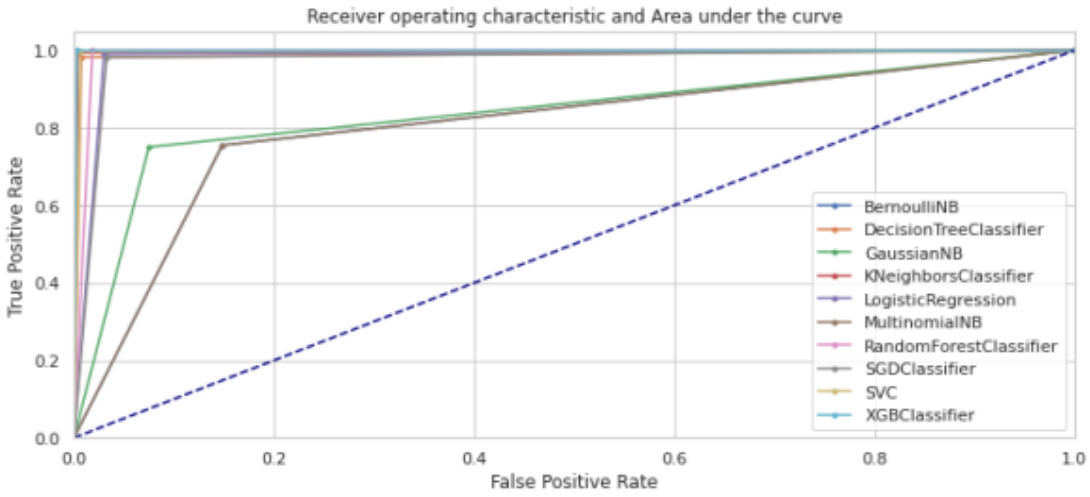
RESULTS AND DISCUSSIONS

The results are compared among all the classifiers. The classification algorithms that we used for the prediction of intrusions are Bernoulli NB, Gaussian NB, Multinomial NB, DTC, k-NC, LR, RFC, SGD Classifier, SVC, and XGB Classifier. The classification models are trained and tested with the paradigm of multi-label classification, and binary-class classification, which is discussed in the subsequence section.



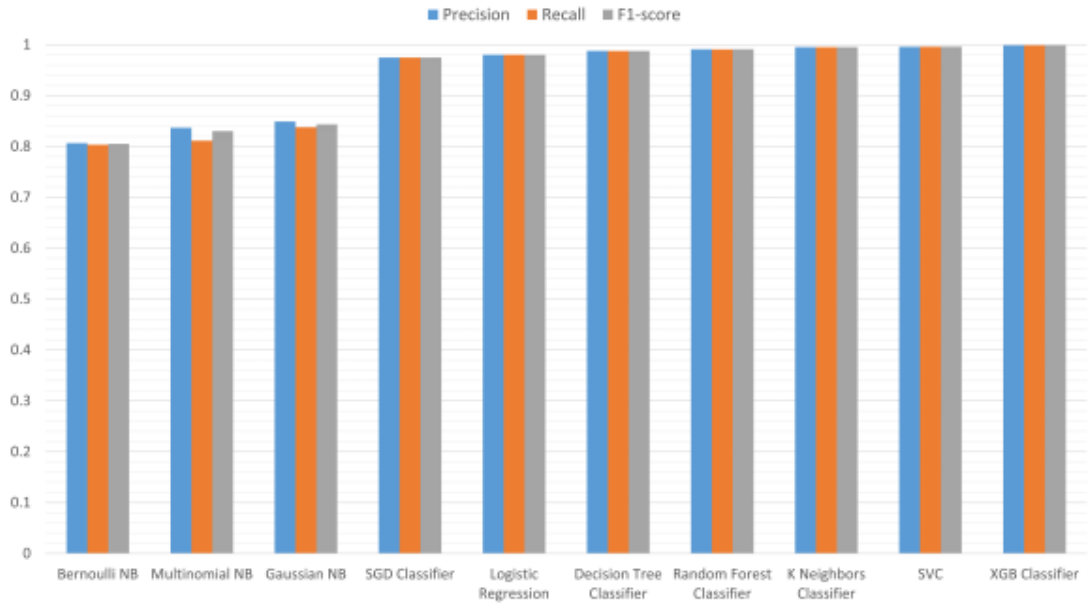
Graph 1: Histogram comparative performance analysis of Multiclass Classifier

It shows the least performing machine learning model and best-performing machine learning model: Bernoulli NB and XGB Classifier. The comparison of precision, recall, and f1-score of the model in the histogram are presented in Graph 1.



Graph 2: Curve Analysis comparative performance analysis of Binary-Class Classifier

The comparative analysis of the performance matrices in terms of precision, recall, f1-score, and accuracy of the proposed models are presented in Graph 3 which clearly shows that the XGBoost classification model has achieved the highest efficacy. It also indicates that Bernoulli NB has least performed among all ten classification models. Furthermore, we have also analyzed the performances of all the classifiers in the ROC curve in Graph 2, which also shows the dominance of XGBoost classifier.



In this section, we have compared our model ML-IDS with the state-of-the-art research available in the literature. Our model's performance shows that the model is efficient and consistent in multiclass as well as binary classification, as mentioned Graph 3. Our model reported 99.511% accuracy in multiclass classification and 99.86% accuracy in binary classification, which is higher than most of the research available.

CONCLUSIONS

One of the main conclusions of this study is that AI can be a powerful tool for monitoring and predicting employees' mental health states. Several studies suggest that AI can identify and monitor mental health risk factors and provide personalized recommendations and feedback to encourage individuals to adopt preventative behaviors. However, it is also essential to consider the potential psychological impacts of AI implementation in workplaces. Additionally, the review only included studies in English, which may have excluded research published in other languages. Moreover, the studies analyzed in this review are primarily cross-sectional and do not provide a comprehensive understanding of the long-term impact of AI on workplace well-being. Developing

ethical frameworks and guidelines will be essential as AI becomes more deeply integrated into workplace environments. Finally, cross-cultural studies are recommended to understand how AI applications in workplace well-being might vary across different cultural contexts. This could help in identifying best practices that are adaptable to a wide range of environments, ensuring that AI-driven solutions are effective globally.

REFERENCES

1. Khaled Alhazmi (2021), "Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey", IEEE Access, issn no: 2169-3536, vol. 99, pages. 1-1.DOI:10.1109/ACCESS. 2021.3089681
2. Anupam Kumar (2021), "COVID-19 Infection Detection from Chest X-Ray Images Using Hybrid Social Group Optimization and Support Vector Classifier", Cognitive Computation, issn no: 1866-9964, vol. 16(4), pages.1-13. DOI:10.1007/s12559-021-09848-3
3. Rishit Lakhani (2023), "Cybersecurity Threats in Internet of Things (IoT) Networks: Vulnerabilities and Defense Mechanisms", International Journal Of Engineering And Computer Science, issn no: 2347-2693, vol.12(11), pages.25965-25980. DOI:10.18535/ijecs/v12i11.4779
4. Paul Davidsson (2024), "Exploring the Role of Artificial Intelligence in Internet of Things Systems: A Systematic Mapping Study", Sensors, issn no: 1424-8220, vol.24(20), pages.6511. DOI:10.3390/s24206511
5. Sabrina Jesmin (2020), "Towards Artificial Intelligence Driven Stress monitoring for mental wellbeing tracking During COVID-19", 2020 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT), issn no: 1875-9289, pages. 845-851. doi: 10.1109/WIIAT50758.2020.00130.
6. Dinesh Visva Gunasekeran (2020), "Digital Health Solutions for Mental Health Disorders During COVID-19", Front Psychiatry, issn no: 1664-0640, vol. 11, doi: 10.3389/fpsyt.2020.582007
7. Vanita; Nair (2021), "Artificial Intelligence and technology in COVID Era A narrative review",Journal of Anaesthesiology Clinical Pharmacology, issn no: 2231-2730, vol. 37(1), pages. 28-34.DOI: 10.4103/joacp.JOACP_558_20\
8. Wenrui Li (2023), "Assessing the role of artificial intelligence in the mental healthcare of teachers and students", Soft Computing, issn no: 1433-7479,https://doi.org/10.1007/s00500-023-08072-5
9. Isabel Saz-Gil (2024), "The Role of Artificial Intelligence in Improving Workplace Well-Being: A Systematic Review", Businesses, issn no: 2673-7116, vol. 4(3), pages. 389-410.https://doi.org/10.3390/businesses4030024
10. Chih-Hai Yang (2022), "How Artificial Intelligence Technology Affects Productivity and Employment: Firm-level Evidence from Taiwan", Research Policy, issn no: 0048-7333, Vol. 51, issue. 6,https://doi.org/10.1016/j.respol. 2022.104536