IJCSMS (International Journal of Computer Science & Management Studies)
Volume 48, Issue 03 and Publishing Date: 10th June, 2026
An Indexed, Referred and Peer Reviewed Journal with ISSN (Online): 2231-5268
www.ijcsms.com

AI in Cyber Security & System Solutions

Bulkesh Sinhmar[1], Dr Bijender Bansal[2], Dr Vinit Kumar Lohan[3] and Dr Deepak Goyal[4]

[1]M. Tech. Student, Department of CSE, Vaish College of Engineering, Rohtak (India)
[2]Professor, Department of CSE, Vaish College of Engineering, Rohtak (India)
[3]Associate Professor, Department of CSE, Vaish College of Engineering, Rohtak (India)
[4]Principal, Vaish College of Engineering, Rohtak (India)

Abstract

The groundwork for event detection in football match analysis using audio. It describes the structure, annotated event categories and preparation of synchronized audio data for the Soccer Action Compilation (SADC) dataset. The chapter outlines the major steps in the pre-processing such as segmentation, noise reduction and feature extraction of match-sounds using Mel-Frequency Cepstral Coefficients (MFCCs), which are important for the temporal and spectral properties. The design and implementation of the audio event detection model are explained and the key event detection such as goal, goal attempt, penalty and yellow card is explained with the use of deep learning architectures. Training configurations, parameter selection and evaluation strategies are discussed to make sure that the models are reliable and reproducible. Results of the model are presented using quantitative measures and confusion matrices, and are followed by a discussion on important results, strengths and limitations that were observed. In general, this chapter provides the methodological and analytical framework for the subsequent visual and multimodal event detection in football videos, while showing the effectiveness of using audio cues in understanding the dynamics of a game and summarising the key moments.

Keywords: *Multimodal Deep Learning, Skeletal Motion Analysis, Cross-Cultural Dance Recognition and Cultural Heritage Informatics and Explainable AI (XAI).*

Introduction

Phishing is one of the most common and all-encompassing types of cyber-attack. Phishing attacks are everywhere, from personal computers to businesses to organizations. Phishing emails can often be identified and eliminated with traditional rules-based filtering (such as blacklisting) or traditional phishing detection based approaches. Innovating the approaches related to identified recognized threats may be limited versus simply identified threats through known evaluative threats and completely miss potential known phishing threats based on new techniques. AI based phishing techniques will use analytical algorithms to evaluate emails as well as identify potential phishing acts, recognize emerging patterns and correlations that the algorithms model is training on and take into account when the data entered into the model.

AI based techniques will identify your user behavior as you relate that to how you are utilizing your emails to possibly create new phishing acts. For example, if engage with a confirmed phishing email, if you interact with your potential data, or click links in a SUSPECT phishing email, engage in their data the AI will observe your engagement or request and determine the engagement as questionable, and provided alerts to other security professionals to use your behavioral activities when evaluating potential phishing acts. Most security log analysis relies on rule based systems and has the underlying concept according to behaviors related to upon immediacy, therefore is a common initial approach focused on the immediacy of understanding security events, thus still does not recognize new or emerging threats as a consequence of this lack of accompanied acknowledgement of theory underpinning behavior. AI systems focused on security log analysis, processes large amounts of data that are security logs, and applies learning algorithms to rank the results.

AI systems can also recognize behaviors and understand trends or anomalies or behavioral trends or anomalies that may be associated to indicative of security breaches that may be associated to an appropriate threat profile or potentially nothing at all (not recognizing a threat). These functions can allow organizations the opportunity to . This means organizations can begin to process and get advantage of methods for security log analysis typically with known behaviour information recognized against margins and

the matter of organization uses the "big data" framework characterized by all security logs are very vast quantity of data. AI systems can also recognize and observe user behavior in many systems and applications to identify user behavior that is out of the ordinary or unusual to detect possible indicators of threat possibilities, such as unauthorized access or data transfer patterns. Through security log analysis, organizations may be able to manage or even implement functions to prevent a potential data breach or security event objective with in "speedy outcomes."AI enabled as a function of security log analysis, organizations may help to supported objective to identify matters and remediate issues quickly that may have been previously unable to remediate.

Data privacy is a major concern when implementing AI, ML, and DL in cybersecurity, these technologies often require access to amounts of data to function effectively, raises concerns about data is collected, stored, and used. The use of AI in cybersecurity necessitates a balance data-driven insights and the protection of individual privacy, a challenge that is exacerbated by stringent data protection regulations. The potential for AI systems to misuse or mishandle sensitive information is another significant risk. AI models trained with personally identifiable information open up the models to further unintended leaking of personally identifiable information, because the model is replicating itself and receiving the training data when working in a model inversion attack. Moreover, also with the data from multiple sources if you mixed in that someone could also create another barrier for organizations to share it to, as it would heighten their target if the data was leaked at some point in the chain. Sometimes it can be very complicated to keep up-to-date with the data protection compliance and service at pace at the same time that AI is relying on the cybersecurity processes you are already capsulated with other organizations for data sharing. Most if the AI based models that are created to operate the security models are created in datasets or training data that are created due to data sharing between organizations and or sectors. In short, what is the data integrity is creating huge value, the value is far greater, it needs massive support in ache in this virtual world that we have become, which in a way is communicating without a policy, and in most cases privately sensitive proprietary data. In addition to this, even datasets that are being used as deemed to anonymous, majority are described as anonymized at source if datasets are pooled together with publicly logged approved external datasets run the risk of reverse-identity there goes third-third who could identify an individual in third dataset in their data analysis. We can probably hundred, thousands of opportunities around AI and security implications can think created to keep safe, but how are securing, share so many different dimensions it becomes more and more facile the safety of our processing and privacy become increasingly import.

Adversarial AI and Security Vulnerabilities

The rise of adversarial AI presents a challenge to the implementation of AI, ML, and DL in security. Adversarial attacks involve the manipulation of inputs to AI models in ways that cause the model to make incorrect predictions. These attacks can be subtle, making them difficult to detect, and can severely undermine the effectiveness of AI-driven security systems.

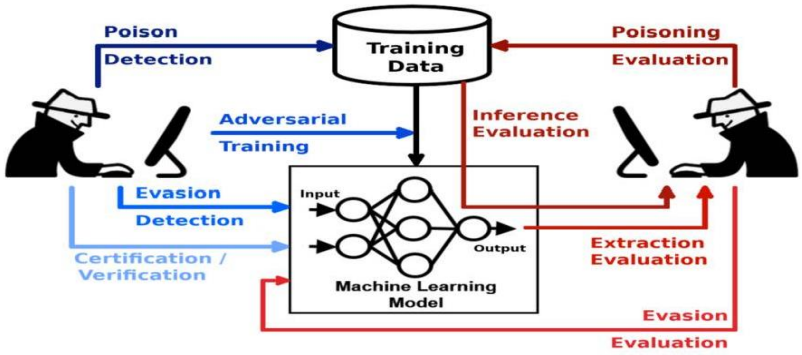

Figure 1: Adversarial Attacks in Machine Learning

For instance, adversarial attacks on image recognition systems can cause the model to misclassify an image by introducing minor perturbations that are imperceptible to the human eye but lead to significant errors in the AI model's output. In cybersecurity, similar techniques to evade malware detection systems or to bypass intrusion detection systems (IDS). Attackers can craft inputs that are specifically designed to exploit the vulnerabilities in the AI model, leading to false negatives where malicious activity goes undetected.

Moreover, AI models themselves can become targets for attacks. Model poisoning, for example, occurs when an attacker corrupts the training data used to develop an AI model, leading to the deployment of a compromised system. This type of attack is particularly concerning in cybersecurity, where the integrity of the AI model is crucial for its effectiveness. Defending against adversarial attacks requires developing models that can withstand such manipulations, which is an ongoing area of research.

Ethical Challenges

However, implementing AI into security comes with many ethical and legal issues. A key concern in this regard is that AI systems could be used to make decisions that impact on individuals' rights and freedoms without appropriate oversight and accountability. For instance, AI systems that automatically block access to resources or mark people for security risks have significant privacy and civil liberty implications.

Moreover, in the context of decision making can cause bias and unfairness. The algorithms used to train models are subject to biases in the data, and this can be shown in the decisions of the AI system. In the realm of cybersecurity, this may lead to a disproportionate focus on or exclusion of specific groups or individuals due to the use of biased data. Ensuring AI systems are fair to address bias is essential to cybersecurity.

AI also introduces challenges in the field of cybersecurity. There are also legal issues regarding the use of AI in the field of cybersecurity. The lack of regulations and standards for security systems can lead to uncertainty and potential liability issues. The AI system may not be able to identify a cyber-attack, resulting in a data breach, and it can be difficult to determine who the developers of the AI were at fault?

Whether it is the AI system, the organisation that adopted it or the end users? It is crucial to establish legal obligations and liabilities of AI-driven cybersecurity systems to boost their adoption.

The complexity of integration and implementation

Another challenge is integrating AI with current cyber security and network solutions. Many organizations have their own security measures and systems in place and integrating AI into these systems can involve significant changes. This may include network reconfiguration, security policy adjustments and training staff on the new systems.
AI systems are also complex, so specialized knowledge and expertise are needed to implement them. The creation and implementation of AI models requires knowledge of both cyber security and machine learning, and there is a lack of professionals with the skills in both domains. One thing that hinders the use of AI-powered security solutions is its skill gap. Furthermore, with the nature of security threats, systems need to be constantly updated and adapted to new threats. This demands investments in R&D and continual maintenance and improvement of the AI systems over time. But in order to ensure their AI-powered cybersecurity solutions remain effective and updated, organisations must be ready to allocate resources.

Conclusion

Considering that the global population is close to 8 billion, this indicates that the predicted proportion is 75%. Furthermore, they expect that by the year 2030, the percentage may have increased to ninety percent of the world population. This growth indicates that there will be an increase in the connectivity of enormous amounts of data and services, which will become a primary worry. Additionally, it will present as a genuine target to those who seek to assault it in cyberspace through the use of malevolent actions that are referred to as cyber-attacks. From the perspective of the contemporary threat landscape, the infrastructure of networks has been a particularly significant area of concern in terms of cyber security throughout the course of the past two decades. A significant increase in the number of people using the internet has been the primary driver of the development of services that provide significant advantages, such as online banking, e-commerce, and the revolution brought about by the Internet. This trend of services has attracted a large number of cyber-attackers, who have developed programs that have the potential to lead to the activities, including purposeful ones, such as the theft of sensitive information from systems, network, and data storage. In the realm of cyber security, which is one of

the most significant problems to be observed, the role of the security is represented in the protection of data from cyber-attacks, which have grown even more harmful for the stability of the economy and the national security. Over the course of 2017, the Australian Cyber Security Centre conducted an in-depth analysis of a number of different levels of threats that were generated by the attackers in order to break into the network. In the majority of instances of electronic piracy and cyber threats, the individuals who commit the acts of piracy are typically thought to be socially isolated, and this inclination will push them to engage in activities that are illegal. They are skilled and motivated to carry out hostile actions such as looking for money and other novel attacks. They are not only talented but also motivated. Furthermore, according to the Report, million sensors to record thousands of attacks that threaten in countries every second, and attacks are increasing in number and the majority of these attacks typically last for thirty minutes or less. This is indicated by the fact that the majority of these attacks are typically for less than thirty minutes. The survey discloses that cybercriminals make money through the use of form jacking and web attacks. These attacks involve malicious acts carried out on websites in order to obtain card payment details and important information regarding the checkout page of the customer. The cyber-scientists presented a number of security tools that can be utilized for the purpose of monitoring, detecting, and blocking the activities. These tools include monitoring, intrusion detection systems, and penetration testing methodologies.

References

[1] Singh, K., Yadav, M., Singh, Y., & Barak, D. (2024). Finding security gaps and vulnerabilities in IoT devices. In Revolutionizing Automated Waste Treatment Systems: IoT and Bioelectronics (pp. 379-395). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-6016-3.ch023

[2] Hajimahmud, V. A., Singh, Y., & Yadav, M. (2024). Using a smart trash can sensor for trash disposal. In Revolutionizing Automated Waste Treatment Systems: IoT and Bioelectronics (pp. 311-319). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-6016-3.ch020

[3] Singh, K., Yadav, M., & Yadav, R. K. (2024). IoT-Based automated dust bins and improved waste optimization techniques for smart City. In Revolutionizing Automated Waste Treatment Systems: IoT and Bioelectronics (pp. 167-194). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-6016-3.ch012

[4] Yadav, M., Hajimahmud, V. A., Singh, K., & Singh, Y. (2024). Convert waste into energy using a low capacity igniter. In Revolutionizing Automated Waste Treatment Systems: IoT and Bioelectronics (pp. 301-310). IGI Global. https://doi.org/10.4018/979-8-3693-6016-3.ch019

[5] Khwaldeh, S., Mohit, Y., & Khushwant, S. (2024, May). Defensive auto-updatable and adaptable bot recommender system (DAABRS): a new architecture approach in cloud computing systems. In 2024 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1-6). IEEE. https://doi.org/10.1109/HORA61326.2024.10550519

[6] Singh, K., Yadav, M., Singh, Y., & Moreira, F. (2025). Techniques in reliability of internet of things (IoT). Procedia Computer Science, 256, 55-62. https://doi.org/10.1016/j.procs.2025.02.095

[7] Singh, K., Yadav, M., Barak, D., Bansal, S., & Moreira, F. (2025). Machine-Learning-Based Frameworks for Reliable and Sustainable Crop Forecasting. Sustainability, 17(10), 4711. https://doi.org/10.3390/su17104711

[8] Singh, K., & Yadav, M. (2025). Prognosis of artificial intelligence in education. LatIA, 3, 107-107. https://doi.org/10.62486/latia2025107

[9] Yadav, M., Singh, K., Thukral, K., Kwatra, S., & Barak, D. (2025). Intelligent Electronic Ticketing Platform in Smart Transportation Ecosystem. In Driving Green Transportation System Through Artificial Intelligence and Automation: Approaches, Technologies and Applications (pp. 581-601). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-72617-0_30

[10] Singh, K., Yadav, M., & Abdullayev, V. H. (2024). Prediction of Flight Areas using Machine Learning Algorithm. LatIA, (2), 13. https://doi.org/10.62486/latia202493

[11] Singh, K., Yadav, M., Singh, Y., Malik, P. S., Siwach, V., Khurana, D., ... & Elngar, A. A. (2024). IoT Networks: Integrated Learning for Privacy-Preserving Machine Learning. In Artificial Intelligence Using Federated Learning (pp. 250-275). CRC Press. https://doi.org/10.1201/9781003482000-13?urlappend=%3Futm_source%3Dresearchgate.net%26utm_medium%3Darticle

[12] Singh, K., Yadav, M., Yadav, R. K., Naib, B. B., Bhatia, S., & Panda, D. K. (2024, December). Prognosis of Relocation Disease in Animals using Aggregation Method with Optimization Techniques. In 2024 Eighth International Conference on Parallel, Distributed and Grid Computing (PDGC) (pp. 15-20). IEEE.

https://doi.org/10.1109/PDGC64653.2024.10984354

[13] Khang, A., Singh, K., & Yadav, M. (2026). Anomaly Detection Driven by Machine Learning: Enhancing SIEM Tools for Sturdy Cyber Defense. In AI-Powered Cybersecurity for Banking and Finance (pp. 338-361). Productivity Press. https://doi.org/10.4324/9781003596875-14?urlappend=%3Futm_source%3Dresearchgate.net%26utm_medium%3Darticle

[14] Ngoc, A. P. T., Abdullayev, V., Khang, A., Ragimova, N., & Yadav, M. (2026). Identify and classify brain tumors using deep learning techniques and magnetic resonance imaging. In Revolutionizing Digital Healthcare Through Artificial Intelligence and Automation (pp. 333-346). Academic Press. https://doi.org/10.1016/C2024-0-02016-18

[15] Ngoc, A. P. T., Singh, K., & Yadav, M. (2026). New neural network methods for the detection of heart diseases. Revolutionizing Digital Healthcare Through Artificial Intelligence and Automation, 289-298. https://doi.org/10.1016/B978-0-443-36434-1.00034-3