International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2019): 7.583

# AI - Enhanced Systems for Early Detection of Cybersecurity Threats

**Aakash Aluwala**

Email: *akashaluwala[at]gmail.com*

**Abstract:** ***The paper aims to explore the AI - enhanced system for the early detection of cybersecurity threats. In addition, the paper discusses how AI can identify and protect against cybersecurity threats and comparatively provide more effective results than conventional methods. Moreover, by addressing the challenges of artificial intelligence in cybersecurity, the study aims to provide potential solutions that can enhance the early detection method.***

**Keywords:** Cybersecurity, Detection, Threats, AI - Enhanced Systems, Cyberspace, Artificial Intelligence, Phishing

## 1. Introduction

Since the turn of the millennium, technology has advanced the way persons, enterprises and authorities work and perform routine tasks thereby enhancing the extent to which cyber threats are available and the network's exposure. Through this social transformation, networks, systems, homes, and businesses have been interwoven to reflect the current understanding of twenty - first - century cyberspace. Many of these advances, including mobile computing, improved processing capacities, IoT, and infusing technology into the daily lives of a person, have positively changed how people live and work, though it has not been without its problems [1].

Furthermore, through technological progression and application, it has also exposed individuals, companies, and governments to the new possibilities of threats in cyberspace. On the other hand, the main question emerging around AI and cyberspace is whether AI would allow more extensive and frequent attacks by an attacker with the set level of skills and resources compared to what such an attacker can do now. The last few years have witnessed some rather impressive and ominous demonstrations of AI capabilities in potential uses in cyber war.

For instance, investigators from ZeroFox proved that it was possible to use a fully automated spear phishing system to post tweets on the Twitter social platform based on a user's interests with more than 60% of the link clicks [2]. Therefore, the purpose of the paper is to explore the AI - enhanced system of AI to access the early detection and prevention of cybersecurity threats.

## 2. Literature Review

The field of cybersecurity is rapidly merging with AI - enhanced systems since the technology is being implemented to enhance cybersecurity systems. In particular, AI can improve cybersecurity since it can identify, protect against, and mitigate cyber threats at a higher level than conventional approaches [5]. DeepPhish is an artificial intelligence experiment that was carried out by Cyxtera Technologies and it illustrated how AI can be used in phishing.

The first experiment involved two threat actors and the results brought a considerable enhancement of the possibility of beating phishing filters in comparison with conventional phishing [4]. In one of the attacker's containers, a threat actor raised the engagement of the phishing link from 4.91% to 36.28% using AI technology. Google's study described further the escalating danger from phishing to cloud data centers and this was backed by the Phishing Trends and Intelligence, also it has revealed that phantom phishing attacks, specifically on SaaS, were up by 237% in 2018 [4].

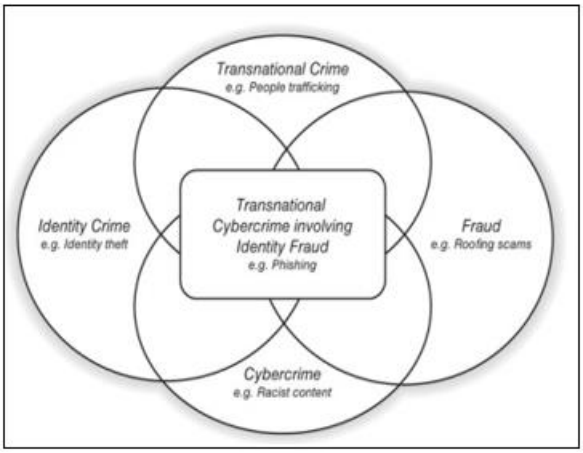


**Figure 1:** Interrelationship between the Transactional, Identity, Cybercrime and Fraud Crime
(Source: Peter, 2019) [3]

The above figure shows how these crimes overlap with the reporting needs of the organization and the data necessary for the CompStat model. In the third case, spear phishing is performed by Rick, and he targets seven potential victims. Police forces must analyze the results of the phishing attack to discover positive or negative indicators of criminality [3].

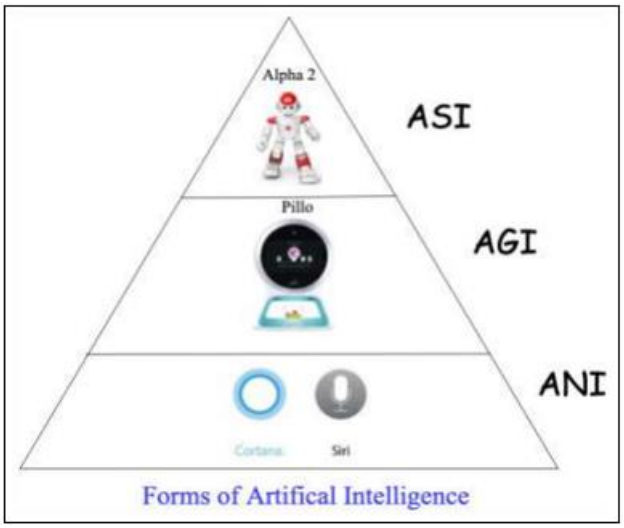


**Figure 2:** Forms of Artificial Intelligence
(Source: Tolani, 2019) [5]

In addition, based on the above figure forms of artificial intelligence high - risk behavior on a system or network are now being discovered through new security technologies with AI programs. The relationships in the form of similarities and differences within a given set of data are being identified and reported concerning anomalies by artificial intelligence that incorporates aspects of machine learning. Machine learning is one of the subsets of artificial intelligence that assist in identifying and analyzing of impacts of these patterns drawn from experience and data.

As has been observed in most applications, the results of an AI system are concerned with some aspect of human functioning and are obtained through the use of machine learning algorithms. One of the advantages of applying AI in cybersecurity is the generation of cyber courses of action (COAs) in the detection of cyber threats [5].

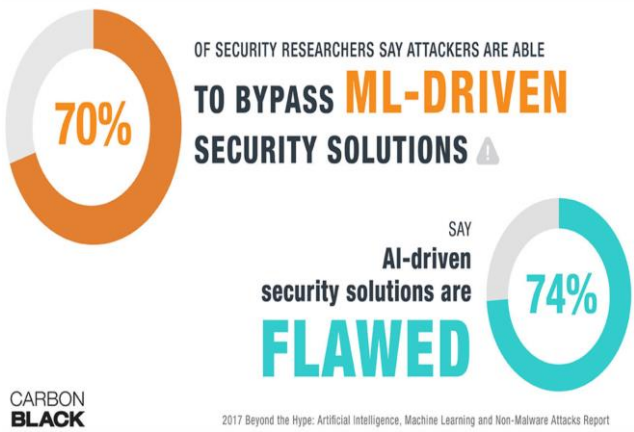


**Figure 3:** Ml - Driven Security Solutions
*(Source: Tara, 2018) [11]*

On this note, given the amount of data enumerated above, it can be asserted that no machine can be perfect and address all behavioral possibilities out there. This means it still needs a human response, and the best that can be used are algorithms, and they are improved over time but, the attacks become better, and devise ways of beating the learning algorithms to get in. " [11].

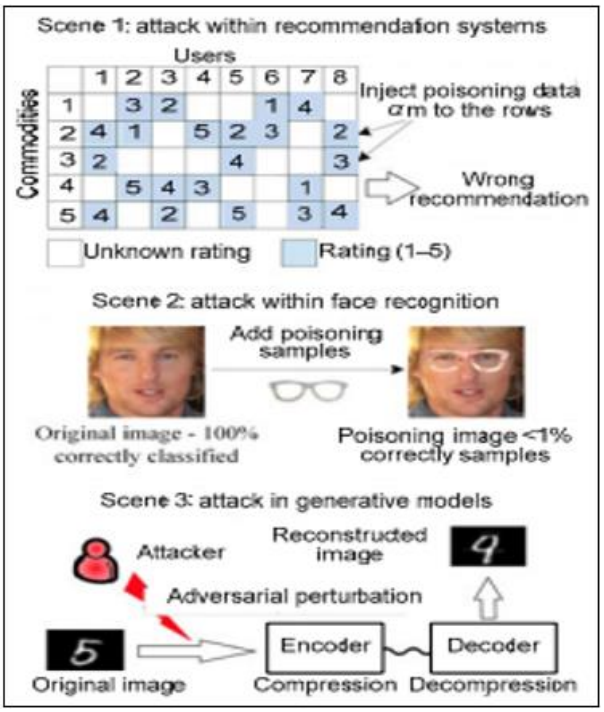


**Figure 4:** Attack of Adversarial in Various Ways
(Source: Li, 2018) [6]

The three typical adversarial attacks are illustrated in Fig in different application scenarios. In recommendation systems, the injection of poisoning data might lead to making wrong recommendations. Finally, it has also experimented with facial recognition. Even by adding a few modified images the application nearly provides the wrong classification. Just in the case of generative models, it may achieve rather poor results even for a small adversarial perturbation.

The researcher also presented another framework of algorithms to make classifiers unstable by changing a limited number of pixels rather than changing the entire image. Their scheme is therefore grounded on the ability to analyze the mapping of the inputs of a deep neural network and the outputs. They also experimented with a typical application of computer vision. The findings proved that calculating the same of the proposed algorithm would generate an output sample that humans normally labeled differently from that of the deep network with a rate of 97% based on only four. An average of 2% of the input features per sample were changed [6].

## 3. Monitoring Tools Impacted

The application of AI - enhanced systems in monitoring tools can early detection and response in the field of cybersecurity and has been revolutionized concerning monitoring tools. These tools employ the use of machine learning to process data within a short period to look for tendencies that are suggestive of risk. The ability of these AI systems to learn from new data means that it is a continually evolving system especially when encountering new threats, providing a more fluid means of defending against cyber - attacks. The subject area also reveals improvement in threat detection compared to classical systems.

Traditional security solutions mostly work based on periodic updates of standards and codes, which cannot be efficient against new threats. At the same time, AI systems can identify new threats previously unknown to them where the patterns of behavior are anomalous and therefore are more suited to an environment characterized by constant changes.

Also, the conventional monitoring tools are hastened by artificial intelligence which shortens the time it takes to identify and address the threats. For example, typical monitoring solutions can produce a great number of false positives and can overload analysts and escalations, if used with high frequencies. Better pattern recognition makes filtering out false positives easier for the AI systems, which frees up the security teams' time to deal with the actual threats. Since accuracy and efficiency increase when these characteristics are used for creating the system, threat mitigation happens faster and potential loss decreases due to cyber - attacks.

AI - based monitoring tools are also efficient in large and complicated networks. When organizations experience growth in network complexity, the traditional ways of practicing cybersecurity management prove to be quite difficult. AI systems can scale with the network, so he or she will not be overwhelmed with details and can monitor all the endpoints. This capability guarantees even maximal and intricate networks' protection against cyber threats.

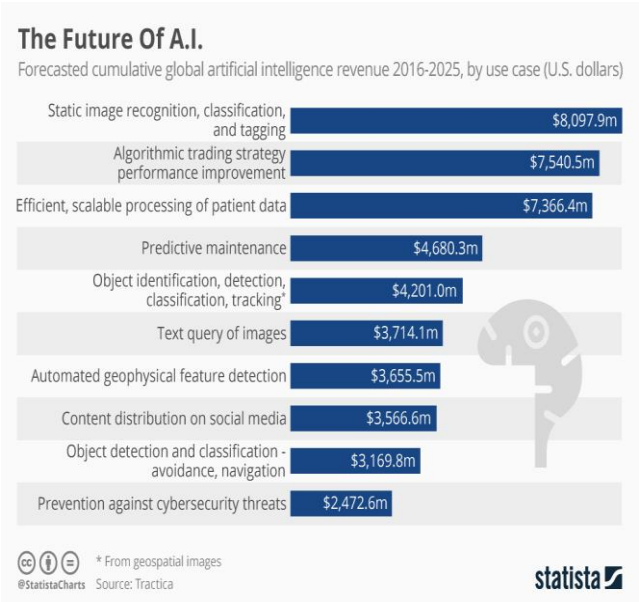


**Figure 5:** Future of AI
(Source: Tara, 2018) [11]

Moreover, the above figure shows the AI future, research suggests that if that same user behaves unlike the last time identified on the same eCommerce site, then, it raises the alarms as a likely security event [11].

## 4. Tasks

AI - enhanced systems and machine learning techniques show great promise for enhancing cybersecurity systems and enabling early detection of threats. By analyzing vast amounts of data on network traffic patterns, user behavior, and known malicious signs, AI can potentially spot anomalies and threats that may go unnoticed by traditional rule - based detection systems [7]. As cybercriminals continue developing novel attacks, the ability of AI to learn from data and adapt over time may allow it to identify new or modified threats that evade standard signatures and rules.

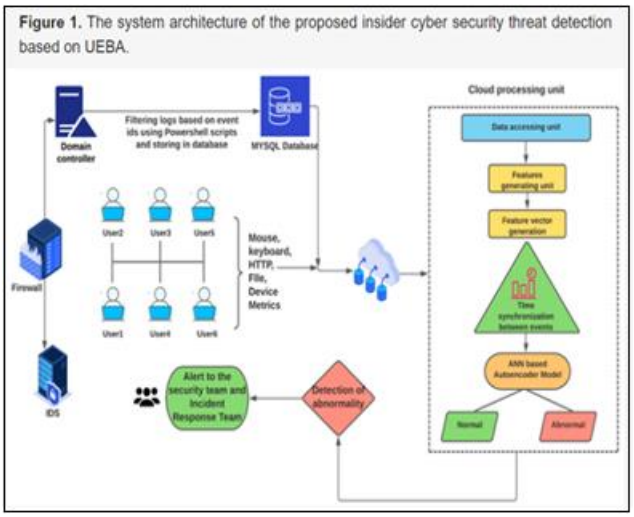


**Figure 6:** Insider cyber security threat detection
(Source: Swaminathan et al., 2019) [10]

However, several challenges remain. For AI systems to achieve their potential, they need access to comprehensive, high - quality datasets encompassing a wide range of normal and abnormal behaviors across different environments. This poses data collection and privacy issues. The systems also require extensive training to minimize false positives and negatives when detecting new behaviors. Insufficient or biased training data could render the systems ineffective at generalization.

Moreover, as AI is now being used offensively in attacks through techniques like deep fakes and personalized phishing, attackers may find ways to evade or fool AI - based defenses as well. Adversarial examples have shown that only small perturbations can cause AI models to misclassify malicious inputs as benign. Attackers could craft inputs tailored to trick specific detection systems over time. Defenders would need to continually evaluate and improve their AI to resist such adaptive assaults. Interpretability is another concern with deep learning techniques often used in AI/ML systems [8]. The complex models may detect threats but provide little visibility into the reasoning behind particular outcomes. Privacy is a significant consideration, as AI systems will require access to vast amounts of personal and organizational data for training and monitoring. Protections need to be put in place regarding appropriate data usage and access to build user trust. Technical methods like federated and differential privacy can help minimize privacy risks from such data collection. Careful system design and testing are prudent steps to maximize AI benefits securely.

Here are some strategies to enhance systems' early detection of cybersecurity threats using AI:

- One strategy is to employ machine learning techniques like anomaly detection models to learn patterns of normal

network traffic and behavior over time. Any significant deviations could flag potential threats [8].

- Another approach is to develop supervised learning models using comprehensive, labeled datasets of known malicious and benign samples. This helps systems generalize to new threats.
- As shown in the figure below systems could also leverage unsupervised techniques like clustering to group similar network events, files, or users to discern outliers or anomalies that may warrant closer inspection.
- Multi - stage detectors combining different AI techniques may also improve detection rates. For instance, an unsupervised auto - encoder could initially filter alerts, with a supervised classifier further analyzing notable anomalies [9].
- Federated learning helps overcome data privacy challenges by training models across decentralized edge devices without exchanging private data.
- Finally, techniques like adversarial training make systems more robust by challenging them with carefully constructed adversarial examples during development.

## 5. Solution and Implementation

To implement the AI - enhanced systems for early detection of cybersecurity threats, the researchers have initially introduced the idea of constructing privacy - preserving DL under the distributed training platform as shown in the figure, where it is possible to make use of the distributed learning technique to allow the various parties share a trained neural network model without disclosing the input datasets [6]. The main idea of this work is to allow parameter sharing of specific, deep neural networks during model training, and this results in making the described scheme efficient and resistant because the training process could be performed asynchronously.

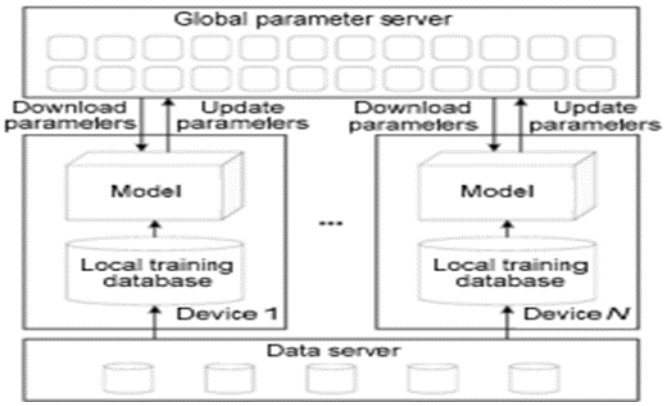


**Figure 7:** Deep Learning system
(Source: Li et al., 2018) [6]

In the cases when two datasets Modified National Institute of Standard and Technology (MNIST) and Street View House Number (SVHN) were used based on the above experiments, the performance of the proposed system was tested.

The results indicated relatively high classification accuracy in both datasets while restricting the participants to share up to 10% of their parameters. Nevertheless, they revealed that in the system gradients belonging to the cloud server may be intercepted, in such a way, that local data leakage can occur. However an unusual server guarantees the correctness of training, researcher resorted to additive homomorphic encryption to allow cipher computation on the gradients. The drawback of this scheme is that there will be additional communication costs between the cloud server and the DL participants [6].

Further, it proposed a down - to - earth secure aggregation scheme for the consideration of high - dimensional data in PML. This aggregation protocol enables the parameters received from many mobile devices to be added without being transmitted to the server from where they would be found. They also delivered some launches and compared this scheme with other protocols through secure multi - party computation. The measurements of experiments proved that the proposed protocol has less overhead more tolerance to faults and possesses higher robustness. As a result, with the advanced development of AI and cyberspace security, these two subjects appear more and more application prospects. One tried to incorporate biologically detailed characteristics of the perceiver into the model of perceived temperature.

## 6. Results

The cases implicated by the use of AI - enhanced systems in the domain of cybersecurity have stronger substantiations of the effectiveness of threats in early detection and prevention. Due to the integration of AI into such systems, it was indicated that it performs even better than traditional approaches in proving that emerging and complicated cyber threats can indeed be detected and handled.

Deep AI proved its effectiveness in detecting phishing through experiments like DeepPhish and established better user behavior as an efficient approach through deep learning models while addressing data privacy. These findings thus highlight the possibilities of the application of AI in the improvement of cybersecurity through accurate, timely, and adaptive means of the threat identification processes while at the same time demanding policymakers to address concerns such as data privacy and adversarial attacks issues that surround the application of AI in cybersecurity.

## 7. Conclusion

The study concludes that the increased use of AI - enhanced systems has brought major changes in the protection of cybersecurity through the early detection of threats. These systems have benefited from the use of machine learning and AI to examine patterns and styles that offer a much more proactive mechanism for protecting the business against cybersecurity threats. In addition, in data privacy, AI poses various problems that are intrinsic to the whole concept of artificial intelligence including, high - quality datasets and adversarial attacks. However, the flexible learning and adaptability of AI are a plus as it continues to learn. The subsequent studies ought to be directed toward increasing the stability and credibility of AI models, data protection, and clear AI decision - making to achieve better results with new types of cybersecurity threats.

## References

[1] Kreinbrink, Justin L. Analysis of artificial intelligence (AI) enhanced technologies in support of cyber defense: Advantages, challenges, and considerations for future deployment. MS thesis. Utica College, 2019.
[2] Brundage, Miles, et al. "The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. " arXiv preprint arXiv: 1802.07228 (2018).
[3] Peters, Kevin. "21st century crime: How malicious artificial intelligence will impact homeland security. " Homeland Security Affairs (2019).
[4] Varney, Adam. Analysis of the impact of artificial intelligence on cybersecurity and protected digital ecosystems. MS thesis. Utica College, 2019.
[5] Tolani, Monica G., and Harsha G. Tolani. "Use of artificial intelligence in cyber defense. " International Research Journal of Engineering and Technology (IRJET) 6.7 (2019): 3084 - 3087.
[6] Li, Jian - Hua. "Cyber security meets artificial intelligence: a survey. " Frontiers of Information Technology & Electronic Engineering 19.12 (2018): 1462 - 1474.
[7] Chaterji, Somali, et al. "Resilient cyberphysical systems and their application drivers: A technology roadmap. " arXiv preprint arXiv: 2001.00090 (2019).
[8] McGough, Andrew Stephen, et al. "Detecting insider threats using Ben - ware: Beneficial intelligent software for identifying anomalous human behavior. " Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications 6.4 (2015): 3 - 46.
[9] Moustafa, Nour, Jiankun Hu, and Jill Slay. "A holistic review of network anomaly detection systems: A comprehensive survey. " Journal of Network and Computer Applications 128 (2019): 33 - 55.
[10] Tara, Seals. Artificial Intelligence: A Cybersecurity Tool for Good, and Sometimes Bad (2018).
[11] Plan, Strategic. "The national artificial intelligence research and development strategic plan. " National Science and Technology Council, Networking and Information Technology Research and Development Subcommittee (2016).