BULLET: Jurnal Multidisiplin Ilmu
Volume 03, No. 05, Oktober,Novemeber 2024
ISSN 2829-2049 (media online)
Hal 749-758

Role of Artificial Intelligence in Enhancing Information Assurance

Nahid Neoaz

Wilmington University, USA

nahidneoaz@yahoo.com

Abstract: The unveiling of AI in the supplement of Information assurance is revolutionizing practice of Cybersecurity in organization. Derived from AI enablers of ML and DL, NLP makes a significant contribution in the construction of threat perception, risk management, immediate response, and recovery to incidents than the conventional security. Executive Summary Machine Learning Employment A raw feed of a vast volume of data in advance technology can be fed in on a continuous basis, these data can be filtered, analyzed, verified, interpreted, patterns can be generated, threat identification and threat handling can be done on an automated basis and time loss to threats and time taken for rectifications can be minimized. The value of AI can consequently be justified on the basis of further details within the vulnerability management on the basis of risk prioritization, the analytical approach of patch metallization as well as the detection of new vulnerability, the so-called zero-day-vulnerability; for incident response, AI is of relevance because it uses the analytical potentials of AI in order to immediately contain the event, to drive the recovery process, and during findings analysis. That is why its constant supervision is one of the activities that make AI enhance one or another stabilization of the organizational systems, and provides the prognosis of dangers and the implementation of numerous rehearsing. Therefore, AI as the potential future solution in the sphere of cybersecurity needs to be discussed in connection with the data safety concerns, as well as ethical issues and roles of people. The principal concern of this paper is therefore, on how convenient on information assurance is, with point reference to the aspect of how it can be convenient in helping to elucidate threats, for the purpose of responding independently and in improving the recovery process; notwithstanding, like everything in this world, AI has both advantages and disadvantages that require reconsideration. Which is why AI is a strategic asset that needs to be used to protect organizations and their systems against today's and tomorrow's cyber threats.

Keywords

Theoretical plane, AI, differences, self-governing systems, risks, adaptive systems, Bit coin, safety language, armor against cyber criminality, constant vigil, isolation, data clone, data purity.

INTRODUCTION

Information assurance (IA) is one of the capabilities that is very crucial for the purpose of guarding information systems and embraces confidentiality integrity availability and authenticity as well as non-repudiation. Given the fact that in recent years there is growing tendency towards usage of digital solutions for management and operation of business, the protection of the data that is critical to an organization and assurance of the security of the system against the threats of cyber-attacks is today more critical than ever [1]. For this reason, Information assurance is held to assure that these systems are reliable, safe and, in the best of ways, safeguarding the valuable data from any intrusion or threats. AI has recently been adopted in information assurance because it is likely to improve the conventional security measures. Gradually, machine learning, natural language processing and neural networks are incorporated into cybersecurity as more effective, more adaptable and, perhaps most significantly, as more scalable as the threat actors become smarter and more numerous and the methodologies broader and deeper in scale. AI has the capability of optimizing a greater extent of data than possible by humans and at much brisker and exacting speeds therefore; AI is a force to reckon * within the combat against even more heinous cyber-crimes [2].

In the subsequent segment, the author plans to demonstrate how the use of AI can bring several advantages for information assurance work. Unluckily AI technologies proves most beneficial when in searching for abnormality and possible areas of vulnerability in real time this way an organization can prevent an increasing weaknesses before they even happen. Furthermore, the threat detection, incidence response, vulnerability scan, and others gathering the amount of large overload of data may help to decrease the workload for a security team to define the strategic directions of the security operations [3]. The other positive of applying AI in the area of information assurance is the fact that it can be trained while in service as you do not train it for it before particular risks take place. The more the traffic in front of an AI system and new threats and more introduce, the better the models themselves are and the better the systems are to detect the threats. It is particularly useful when hackers are creating new brilliant and unethical scenarios. Sometimes people also able to overlook some relations between data points while AI systems always able to identify them and hence the risk assessment will be more correct and the decision making will be completely correct [4].

The objective of this paper is to critically analyse the improved use of Artificial Intelligence in improving information assurance. The key emerging AI technologies that will be discussed further in relation to cybersecurity are the technologies classified as key defining the field at the current stage: machine based threat prognostic system, other systems for predictive effective threat assessments, automated vulnerability management system, and AI-based systems for incident management on preventive basis [5]. The paper will also look at the challenges that come with implementation of AI to information assurance including ethical challenges, rights challenges on data and technical challenges of AI. The paper will also describe what is expected next for the AI application in the information assurance area, the ongoing advancements and the potential that more can the AI bring to the information assurance and cybersecurity fields. As the shape of digital landscape becomes more mature and is at the same level as harm risks information assurance should be enhanced by AI. Using AI will enable organizations to come up with even more promising, precise and faster – evolving security strategies, as this is necessary because threats have started to evolve [6].

OVERVIEW OF INFORMATION ASSURANCE

Information assurance can be therefore defined as IA risk management with regard to information security and protection of the information system, its confidentiality, integrity, availability and authenticity, and non-repudiation. They occupy a huge manpower for protecting an organizations information from any threatened either from within or outside or whether as a result of a deliberate act or an incidence that was unforeseen. Corresponding to growing digitization of business processes, IA is the protector of data, valuable resources and the client, customer and company's interest [7]. At its core, information assurance focuses on five key principles known as the CIA triad—confidentiality, integrity, and availability—along with authenticity and non-repudiation

Security means that only the necessary individuals or other systems must receive the necessary information. This principle protects information from some of the risks such as hacking, theft or even loss of information that leads to severe financial and reputation loss in organizations/best. With regard to the elements for evaluation, integrity refers to the extent of relevant, valid, complete and consistent data. It still permits original data to be believed and affirm that the data is not misunderstood by some detrimental participants in the wrong approach. Accessibility means that the data and systems have to be available to be used on demand [8]. In its simplest and most obvious form this principle states that it could not exist without standby systems, plan B's and C's, very high system availability are completely necessary to make it making system uptime as a key parameter. It gives the guarantee of the uniqueness of the user or a system which utilizes this information. This ensures that a user of an information system inputs credible data from a certain source, secondly this ensures the authenticity of a form of communication that a user has with an information system [9].

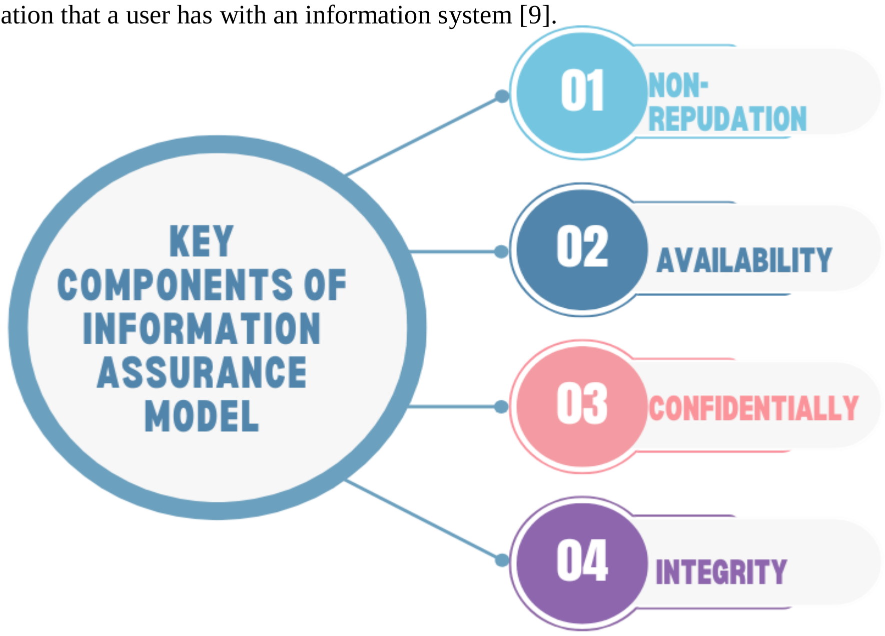


Figure: 1 showing key components of information assurance model

Non-repudiation reduces the likelihood of its magnanimity ensuring that it is very clear that an action or a transaction has occurred, performed by a particular person or technology such that an individual cannot dispute it. This is crucial for the legal enforcement and adaption of the laws and regulations for the automated implementation and fulfill some requirements to prove that the actions implemented In a system cannot be undone or deleted by the authorities concerned. One of the biggest goals of information assurance is to level the increasing threat factor that exists for the organizations. Included among these are; Data breaches, Ransom ware, DoS attacks, and insiders attacks all which are slowly turning into more complex and disastrous. IA strategies have thus endeavored at putting measures that can assist one to detect risks that are likely to occur or are likely to occur and respond to them amount adequate systems to be prepared for adversity in the future as embraced by the information systems [10]. In addition, introduction of new trends of commerce use of different technologies in business processes facilitated creation of new digital platforms, cloud environment, connected control devices and all of the above mentioned create high levels of difficulty in information security. For example, the IoT, cloud and big data connections are blending issues concerning the privacy, interoperability and security of big data in distributed environments. Consequently, it looks like organizations simply have to protect not only their transportation hubs, but also be confronted with the cyber threats in virtual and cloud in many cases, which seems to call for another toolbox and strategy [11].

Information assurance also requires the managerial level risk management inside an organizational while trying to demarcate the risk and threats in a bid to align to some standard, the same organizational will also seek to identify how it can manage the identified risk. IA is integrated in a larger IA programmer in the organization consisting of inter alia risk evaluation, reviews at regular intervals, and operation in the Standards and Laws framework. It could have been used ensuring information is protected enough, while at the same growing with new threats and growing technological input [12]. Information assurance is an all-encompassing and fundamental security science concerned with the confidentiality, integrity, availability, authenticity and non-repudiation of organizational information. If the presented Principles of IA are applied, risks can be avoided or at least effects of those risks can be minimized, threats can also be dealt in the similar manner and secure surroundings can be developed which will improve the level of credibility and higher organizational robustness within the framework of NWI_TE [13].

AI AND ITS APPLICATIONS: CYBERSECURITY

AI refers to the ability of the machines to process information to enable them to think as humans, learn, reason, solve problems and most of the time, make decisions. In various trade and professions, cognitive technology in general, and especially AI, has become the new insurgent, and this was used by cybersecurity to strengthen assurance. Subdomains such as Machine learning (ML), natural language processing (NLP) or neural networks are used for enhancing the detection, prevention or reaction in regard to information assurance threats [14]. As for AI in cybersecurity, one of the key modeling utilization is big data analyzing in real time. Standard security measures might work for days analyzing the flow of data and do not always recognize patterns, seize on discrepancies, and forecast potential threats whereas AI systems do that within seconds. For example if it is a machine learning algorithm the AI system will be able to adapt using past events, new attack changes and trends in cybersecurity [15].

The use of AI instruments is also valuable to execute ordinary safety work. For example, certain AI systems can be designed to perform vulnerability assessment and possible threats on their own, annotate threats and may seek or request for redress, thus they help relieve the pressure off security component's teams and enable them to review more serious issues. Also, there are costs in increase of the response time on incidents through the use of AI to identify and manage threats such as self- applied patches, and hunting for threats. A major domain where AI gives its assistance is with the ability to identify phishing [16]. Methods from the sphere of natural language processing allow to give more accurate evaluations of the content of the inbox and to select a correct or to refuse a wrong message which is a phishing attempt. Duration and types of user authentication are also enhanced hereby, as well as continuous check methods applied along with biometric and behavioral data. Indeed, AI is a tool, identified as one of the most potent weapons in the enhancement of cybersecurity in general, and information assurance in specific. That it can evaluate volumes of information, do recurrent work, and get better and better as the computer teaches it, where the computer gives it new data, tell a lot about how it could be used in countering new and emerging cyber threats [17].

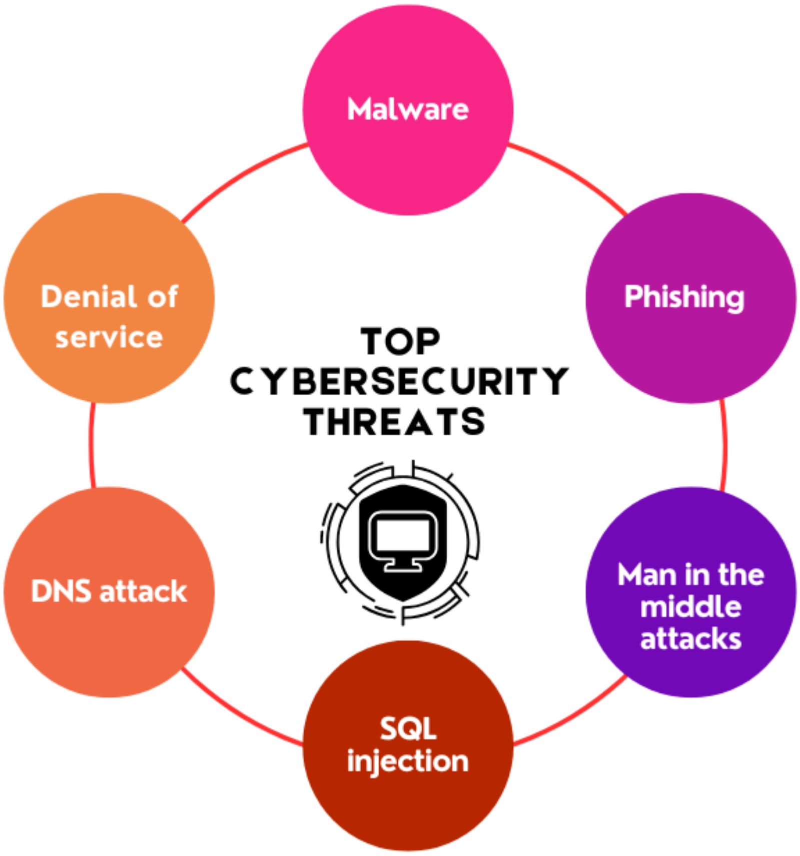


Figure: 2 showing top cyber security threats

THE ROLE OF AI IN THREAT IDENTIFICATION AND CONTROL

This is so because of AI which enhance mostly the threats detection and prevention in information assurance lately. Traditional approaches and security technologies, as useful and effective as they are, have several problems with timely dynamic responses. On balance, AI, particularly, the ML and DL, is like a video game because it has to provide a constantly responsive, adjustable, and effective system in combating cyber tip in real-time [18]. AI threat identification mainly uses the AI and Machine learning techniques in the detection of the anomalies within the network traffics and the systems data. Often, such algorithms need extremely huge data volumes, by which they are able to learn the normal behavior of a system so as to alert of any anomaly that might depict a security threat. This capability makes an AI solution capable of detecting new threat types that might not have been previously identified or have been insufficiently researched and that could attack fresh or so-called zero-day flaws. This is especially so if the AI-based systems have access to new information so they can keep updating themselves about a new threat that might still be out of the range of the signature-based detections [19].

Moreover, AI optimizes threat prevention in light of the fact that the answers to the enthused threats are mechanical. In other words, an AI system can contain infected devices, filter out malicious traffic and apply patches and upgrades with input frequency so low that the AI system does all that way faster than a human, thus minimizing the impact of cyber-attacks. At this level of automation, organizations remain alert for the security threats that develop inside an organization while at the same time increasing an organization’s capability to fight both internal and external security threats [20]. AI therefore also has a role to play in the counteraction of risks and extends beyond risk prediction which then uses historical attacks to build even more accurate models. Using methodologies from existing security failures, as well as from planning risks and possibilities in earlier cyber-attacks artificial intelligence can predict what areas and how newer threats can strike which assists organizations in strengthening their strategies against such threats. The establishment of solutions in threat detection and prevention by means of AI is provoking growth and transformation of polytechnics in information assurance through offering; real-time, automatic, and adaptive methodologies to tackle new cyber threats while enhancing the efforts of anchored teams for the best means of system protection [21].

AI FOR VULNERABILITY MANAGEMENT AND FOR PATCH AUTOMATION.

Vulnerability management as a task of information assurance entails assessment of potential risks, and their remediation for use by hackers. Due to increasing size and complexity of the IT infrastructures vulnerability management have become very difficult and time consuming when done manually. This is where Artificial Intelligence (AI) is going to come in handy to be especially applied to vulnerability scanning, risk assessment, and patching. When it comes to the identification of vulnerabilities in large-scaled networks and systems, AI driven vulnerability management systems however can operate faster than usual [22]. Technologies consisting on machine learning are capable of interacting a large amount of data, which can include settings and configurations, code and behavior to discover flaws. Unlike other current systems that use hard-coded signature database, the present AI systems will be useful to detect new/unknown signatures or method used in the attacks. AI systems learn from experiences of security attacks and increase the confidence of organizations about the patterns of vulnerability that they previously did not recognize [23].

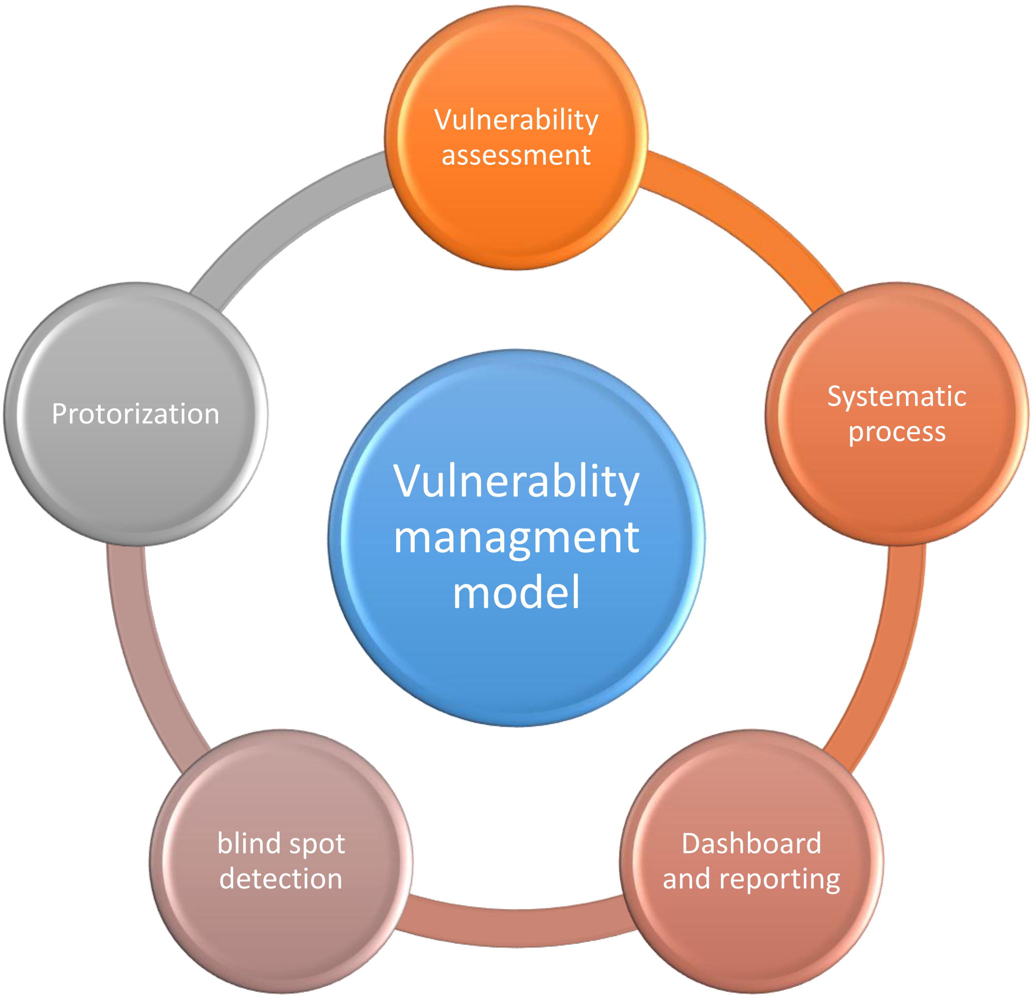


Figure: 3 showing vulnerability management model

Another advantage that comes with using AI in this area of work is that it can quickly sort the vulnerabilities hence assigning them risk levels. The vulnerabilities are again not scored in the same way that traditional CVSS does; the traditional scoring does not consider or treat each vulnerability the same whereas, AI systems firstly define risk factors such as the exploitability of the vulnerability and its criticality to the particular system and also the organizational risk profile. It means that, for example, security teams address the worst issues as first in order to make a necessary number of responses to the problem. Aside from risk analysis and risk categorization, AI is also introduced with respect to the process of patch management. The major advantage that the check point of the AI driven systems provides to the patch Management is that the Management of patch can go through its life cycle commencing with the check that patches are needed, passing through the test phase, through deployment of the patches to other systems and up to the validation of the patches [24]. The benefit include; It minimizes the occasion whereby human interrupt the process or apply unnecessary patch, therefore, it patches the network on time thereby reducing the hole which the hacker can exploit. Furthermore, the previously mentioned AI system can also help accelerate the creation of synthetic patches for the vulnerabilities for which patches cannot be prepared at the moment, but their protection can be ensured by a synthetic patch until an effective one is developed [25].

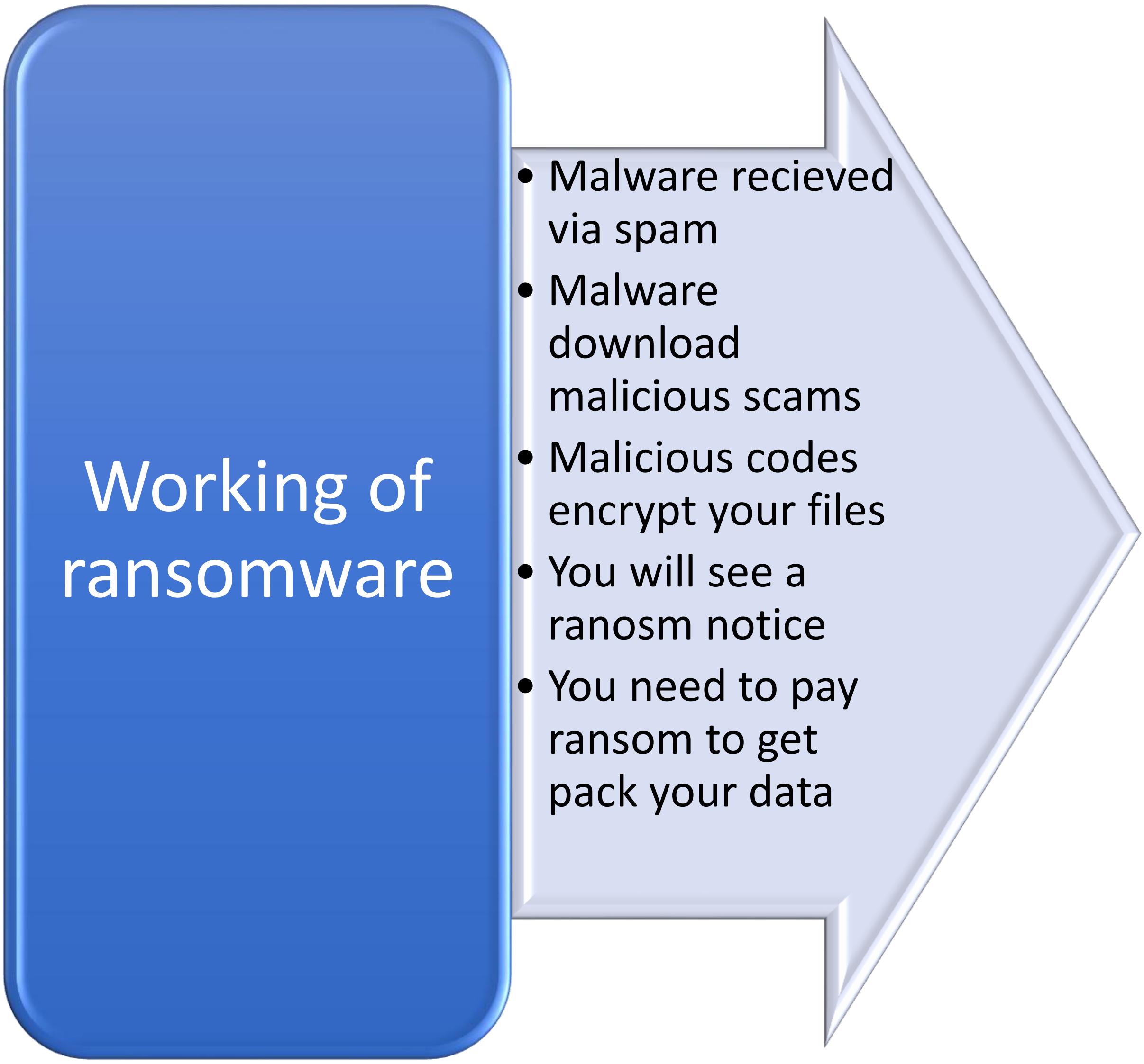
For more frequent perusing susceptibilities, AI also foresees and identifies them. Since the AI systems focus on threats and constantly verify the network activity, security cannot be lower than the level of the environment. This capability of real-time is especially important in the context of constant emergence of new vulnerabilities and the inability of traditional methods to cope with them efficiently. Besides that, implementing AI in vulnerability management and patching does not only enhance the process but also shares some burden for security professionals. This makes it possible to distribute the human resource to accord issues such as response to security incidences and system improvement [26]. Moreover, since AI can assist in making the detection and patching activities faster and more accurate it also assists in the creation of safer and more secure systems – all of these contribute to the overall information assurance of an organization. Many are already saying that AI is revolutionizing the way vulnerability management and patch automation are consumed because it takes less time and is often more accurate than conventional means of risk identification and risk prioritization. Because of its capability to learn from experience, change and address emerging threats it is a critical weapon in the quest for security and sound information systems [27].

USE OF AI IN MANAGING INCIDENTS: RESPONSE AND RECOVERY.

In relation to increased complexity of threats in the cyber space, the two are the primary activity jurisdictions for information assurance in the organization. The level of response by an organization to a security matter is much a measure of the type and level of calamity that an organization is likely to suffer. Analyzed methods that were utilized towards handling those incidents although have proved helpful, are conventional, were pre-planned, and followed causal model and consist mainly of Human intervention key factors which may delay the whole process. Advanced technologies, including AI, are revolutionizing how incident response and recovery take place in order to enhance the possibility of early identification, response, and recovery from adverse occurrences in any organization [28]. AI plays an effective role within the detection and prevention of an incident from happening within its infancy. Machine learning or more specifically, Artificial intelligence (AI) can analyses a great deal of networking traffic, user actions and behavior, system logs and application data, to look for trends and identify potential threats. Several issues are inherent to traditional security mechanisms, one of which is that the known threats use signatures to identify them which are not so effective when dealing specifically with unknown, new, or zero-day threats. However, AI systems use real time data to decide newly arriving behaviors that can be potentially dangerous even if never seen as threats before [29].

For instance, it can follow a botnet attack by being able to distinguish a pattern of extension or transmission of messages or traffic by bot-infected tools in a network. Similarly exclusion criteria in relation to phishing case, it is possible for AI to detect phishing messages through analyzing the text of the message, sifting through the authenticity of the sender, and detecting links or attachments that may be malicious through textual analysis. When applied AI can also help to recognize such threats at an early stage to build the required response to the risk or to decrease a cyber-event [30]. Automated actions are a great place for AI once an incident has raised its head; as it is seen a lot of the mitigation and containment actions can be fully automated. In fact, in traditional protective measures, the operator has to count on personnel support to isolate infected apparatus, apply countermeasures, and prevent Workflow malfunctions. As you could expect this process could be quite slow if made within a big complex network; therefore is allowing the attackers to cause more damage. AI based systems can respond to these indicators also in real time in order to manage and reduce the further threat [31].

For instance during an occurrence of ransom ware attack, AI is able to identify infected endpoints and reject it from the network to avoid further coverage of the malware. Similarly, in case the anomaly detector of the AI system discovers a denial-of-service (DoS) attack, the model is capable of automatically rerouting traffic so as to effectively mitigate the impact of an attack and at the same time inform the security team for further action [32]. AI can also use ‘virtual’ or ‘soft’ patches if it can neutralize a risky path toward the program until the security team constructs a physical one. These virtual patches can be of more help especially if patching cannot happen because of such cases as for instance in cases where the patching process might disrupt very essential business operation. Recovery phase of an incident can be explained as the activity by which the involved system, data and other services are restored back to an active state [33]. AI does help to accelerate this phase because several recovery processes can be automated, to retain all servers and functionalities with minimal to no disruptions. For instance, it can instantly pinpoint the most current clean backup images and start the restoration process, across the compromised computers. AI can also monitor the recovery process to check if every system has been fully recovered, in case of any inefficiency in the process, action can then take to correct the issues [34].



Working of ransomware

- Malware recieved via spam
- Malware download malicious scams
- Malicious codes encrypt your files
- You will see a ranosm notice
- You need to pay ransom to get pack your data

Figure: 4 showing working of ransom ware

On the other hand, with AI systems it is always possible to look for the rest of the attacker's assets to make sure that all inherent conditions have been addressed, and the attacker cannot take the chance to tap into the network again. Not only can the machine learning models provide how the attack on various parts of the system could be and in turn decide which of the numerous systems should be restored first based on their importance. But when an event has been managed, functions service recall have been resumed, AI among them participates actively in investigation. In case with helping AI-tools one can find the root cause of the given case, analyze the sequence of the events and find out more about the risks and weak points in the security system of the particular company leading to the given leakage [35]. While performing such analysis is useful for predicting improvement of the future response plan, it is also important to drive up the level of information assurance in general. These systems are informed by tests, and can, therefore, recognize similar threats inside an organization, improving the organization's ability to contain unpleasant events. In the future, AI can also be of assistance when it comes to reporting of the incident in question or when giving recommendations concerning modifications of the security policies and practices after the examination of the findings of an incident [36].

Another potential utility of AI in cyberspace is in creating reconstructed likely future attacks that the hackers may stage in order to get a higher understanding of the current vulnerabilities and defects that are synonymous with the current safety frameworks, and in validating the effectiveness of current safety standards in dealing with possible future attacks [37]. Thus, organizations can get advantage of such simulations as these will improve the models used in following attacks and develop the incident response frameworks. However, for reporting, escalation or even for decision making insofar as a response to an incident is concerned there is need for AI, but to decide on the data, qualitative or quantitative, there is need for human analyst [38]. AI is not a competitor to human analysts who may analyze intelligence information but rather complements their work by providing analysis and forecast in the timely fashion and helps respond to intelligence information. That means security analysts are now available to do higher level tasks like threat modeling, seeking out threats proactively, and estimating the exact extent of damage during an attack because these are tasks at the lower levels that an AI system is capable of handling [39].

In this case, security teams have a large number of tasks, so the use of AI systems may be useful in such cases, reduce the response time, and bring some rationality to work with incidents. In totality, the use of AI within incident response and recovery has opened avenue to real-time, sophisticated and self-learning solutions to enhance an organization's ability to achieve practical detection, prevention and recovery from cyber threats [40]. Optimizing what AI is best suited for such as threat identification, first reaction, mitigation, and diagnosis, organizations can reduce the impact of cyber threats. Therefore, to apply AI for handling over incidents improves information assurance but also improves the preparedness of an organization for the diverse and evolving threat threats.

CONCLUSION

It has raised proactive security and reactive security to an incident in organizations and cybersecurity has benefited positively from the integration of Artificial Intelligence into information assurance. The roles that it has provided for enhancing the concepts of confidentiality, integrity, availability, authenticity and non-repudiation of systems are central with a increasing spectrum and magnitude of threats. The ability to protect organizations' weaknesses; the ability to recognize threats on the fly and act automatically when security breaches do happen – all of these characteristics that AI delivers, equip organizations with what they need to secure their networks as increasingly segments of their structure become connected. Technologies like machine learning, Deep learning, and natural language processing enable organizations better on threat detection and able to even distinguish prospective threats and can respond to threats by itself. All these technologies do not only enable the organizations to protect themselves from understood as well as unknown threats However, they also support the organizations to handle the risks, automate patches besides supporting the organizations to recover from the events while at the same time keeping human errors minimum and at the same time improving the use of the system's efficiency.

The potential of utilizing AI we can see as data learning makes system changes dynamically for instance; in response to incidents, we can enhance response and reduce the time taken to counter new threats. AI therefore simplifies the mundane and repetitive activities out of the function from the security teams and actually improves the function since it becomes a nuisance. On one hand, the integration of AI has received so many benefits in its application, but on the other hand, it comes with some limitations when it comes to implementation in cybersecurity. Issues which include privacy and security, data privacy legal issues and potential adversarial exploits of AI models are still among the issues that ought to be solved by the organizations. Further, such adaptation should assist I and not compete it with intelligence. However, high automatization and prognosis potential of AI, people's intervention is crucial to dive deeper into the interpreting process and use the results for strategic decision-making. AI has significant contribution on the information assurance is by adding a better explanation of the detection and prevention of cyber threats and handling or recovering from them. The ability to take large data flows, calculate operations, and develop in response to the continuously evolving tendencies in threats makes it valuable in the modern world. This paper has postulated and defended the proposition that as computerized milieu continue to grow and interconnect, AI will continue to be an essential tool for organizations, safeguarding them against, and providing timely and efficient means of managing risks and strengthening organizational defenses against cyber threats.

REFERENCES

1. Zheng, Q., Yu, C., Cao, J., Xu, Y., Xing, Q., & Jin, Y. (2024). Advanced Payment Security System: XGBoost, LightGBM and SMOTE Integrated. arXiv preprint arXiv:2406.04658.
2. Song, X., Wu, D., Zhang, B., Peng, Z., Dang, B., Pan, F., & Wu, Z. (2023). Zeroprompt: streaming acoustic encoders are zero-shot masked lms. arXiv preprint arXiv:2305.10649.
3. Lyu, W., Zheng, S., Pang, L., Ling, H., & Chen, C. (2023). Attention-enhancing backdoor attacks against bert-based models. arXiv preprint arXiv:2310.14480.

4. Yu, C., Jin, Y., Xing, Q., Zhang, Y., Guo, S., & Meng, S. (2024). Advanced User Credit Risk Prediction Model using LightGBM, XGBoost and Tabnet with SMOTEENN. arXiv preprint arXiv:2408.03497.
5. Peng, H., Xie, X., Shivdikar, K., Hasan, M. A., Zhao, J., Huang, S., & Ding, C. (2024, April). Maxk-gnn: Extremely fast gpu kernel design for accelerating graph neural networks training. In Proceedings of the 29th ACM International Conference on Architectural Support for Programming Languages and Operating Systems, Volume 2 (pp. 683-698).
6. Lyu, W., Dong, X., Wong, R., Zheng, S., Abell-Hart, K., Wang, F., & Chen, C. (2022). A multimodal transformer: Fusing clinical notes with structured EHR data for interpretable in-hospital mortality prediction. In AMIA Annual Symposium Proceedings (Vol. 2022, p. 719). American Medical Informatics Association
7. Weng, Y., & Wu, J. (2024). Big data and machine learning in defense. International Journal of Computer Science and Information Technology, 16(2), 25-35.
8. Yu, C., Xu, Y., Cao, J., Zhang, Y., Jin, Y., & Zhu, M. (2024). Credit card fraud detection using advanced transformer model. arXiv preprint arXiv:2406.03733.
9. Jin, C., Peng, H., Zhao, S., Wang, Z., Xu, W., Han, L., & Metaxas, D. N. (2024). APEER: Automatic Prompt Engineering Enhances Large Language Model Rerunning. arXiv preprint arXiv:2406.14449.
10. Lin, Z., Wang, Z., Zhu, Y., Li, Z., & Qin, H. (2024). Text Sentiment Detection and Classification Based on Integrated Learning Algorithm. Applied Science and Engineering Journal for Advanced Research, 3(3), 27-33.
11. Zhu, A., Li, J., & Lu, C. (2021). Pseudo view representation learning for monocular RGB-D human pose and shape estimation. IEEE Signal Processing Letters, 29, 712-716
12. Liu, T., Cai, Q., Xu, C., Hong, B., Ni, F., Qiao, Y., & Yang, T. (2024). Rumor Detection with A Novel Graph Neural Network Approach. Academic Journal of Science and Technology, 10(1), 305-310.
13. Lipeng, L., Xu, L., Liu, J., Zhao, H., Jiang, T., & Zheng, T. (2024). Prioritized experience replay-based DDQN for Unmanned Vehicle Path Planning. arXiv preprint arXiv:2406.17286.
14. Luo, H., Wu, T., Han, C. F., & Yan, Z. (2022, December). IGN: Implicit Generative Networks. In 2022 21st IEEE International Conference on Machine Learning and Applications (ICMLA) (pp. 560-566). IEEE.
15. Jin, C., Che, T., Peng, H., Li, Y., & Pavone, M. (2024). Learning from teaching regularization: Generalizable correlations should be easy to imitate. arXiv preprint arXiv:2402.02769.
16. Peng, H., Ran, R., Luo, Y., Zhao, J., Huang, S., Thorat, K., & Ding, C. (2024). Lingcn: Structural linearized graph convolutional network for homomorphically encrypted inference. Advances in Neural Information Processing Systems, 36. ISSN: 3006-4023 (Online), Journal of Artificial Intelligence General Science (JAIGS) DOI: 10.60087 398
17. Yan, C., Weng, Y., Wang, J., Zhao, Y., Zou, Y., Li, Z., & Baltimore, U. S. Enhancing Credit Card Fraud Detection Through Adaptive Model Optimization.
18. Liu, T., Cai, Q., Xu, C., Hong, B., Xiong, J., Qiao, Y., & Yang, T. (2024). Image Captioning in News Report Scenario. Academic Journal of Science and Technology, 10(1), 284-289.
19. Deng, T., Shen, G., Qin, T., Wang, J., Zhao, W., Wang, J., & Chen, W. (2024). Plgslam: Progressive neural scene represenation with local to global bundle adjustment. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 19657-19666).
20. Sun, C., Li, S., Lin, Y., & Hu, W. (2022). From Visual Behavior to Signage Design: A Wayfinding Experiment with Eye-Tracking in Satellite Terminal of PVG Airport. In Proceedings of the 2021 DigitalFUTURES: The 3rd International Conference on Computational Design and Robotic Fabrication (CDRF 2021) 3 (pp. 252-262). Springer Singapore
21. Desyatnyuk, O., Naumenko, M., Lytovchenko, I., & Beketov, O. (2024). Impact of digitalization on international financial security in conditions of sustainable development. Problemy Ekorozwoju, 19(1), 104-114.
22. Evren, R., & Milson, S. (2024). The cyber threat landscape: understanding and mitigating risks (No. 11705). EasyChair.
23. George, A.S., Baskar, T., & Srikaanth, P.B. (2024). Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. Partners Universal International Innovation Journal, 2(1), 51-75.
24. George, A.S., Baskar, T., & Srikaanth, P.B. (2024). Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities across Key Sectors. Partners Universal International Innovation Journal, 2(1), 51-75.
25. Gounari, M., Stergiopoulos, G., Pipyros, K., & Gritzalis, D. (2024). Harmonizing open banking in the European Union: an analysis of PSD2 compliance and interrelation with cybersecurity frameworks and standards. International Cybersecurity Law Review, 1- 42.

26. Groenewald, E., & Kilag, O.K. (2024). E-commerce Inventory Auditing: Best Practices, Challenges, and the Role of Technology. International Multidisciplinary Journal of Research for Innovation, Sustainability, and Excellence (IMJRISE), 1(2), 36-42.
27. Gupta, V.P., & Arora, A.K. (2024). FinTech: the Financial Sector's Digital Reformation. Revolutionary Challenges and Opportunities of Fintech.
28. Hassan, A.O., Ewuga, S.K., Abdul, A.A., Abrahams, T.O., Oladeinde, M., & Dawodu, S.O. (2024). Cybersecurity in banking: a global perspective with a focus on Nigerian practices. Computer Science & IT Research Journal, 5(1), 41-59.
29. Huang, H., Jiang, N., Chen, W., Tang, Y., & Li, N. (2024). A call to rethink the necessity of and challenges facing academic research organizations in the new era of drug innovation in China. Drug Discovery Today, 103925.
30. Judijanto, L., Kaaffah, F.M., Muthmainah, H.N., & Vandika, A.Y. (2024). Literature review on computer network security in the financial sector in indonesia challenges and Finance & Accounting Research Journal, Volume 6, Issue 4, April 2024 Farayola, P.No. 501-514 Page 514 solutions in facing digital security threats. Sciences du Nord Nature Science and Technology, 1(01), 20-27.
31. Corine Boon, Deanne N. Den Hartog, David P. Lepak, A systematic review of human resource management systems and their measurement, J. Manag. 45 (6) (2019) 2498–2537.
32. Ashlea C. Troth, David E. Guest, The case for psychology in human resource management research, Hum. Resour. Manag. J. 30 (1) (2020) 34–48.
33. Maria Panayiota Markoulli, Mapping human resource management: reviewing the field and charting future directions, Hum. Resour. Manag. Rev. 27 (3) (2017) 367–396.
34. Orhan Yabanci, from human resource management to intelligent human resource management: a conceptual perspective, Hum. Intell. Syst. Integr. 1 (2) (2019) 101–109.
35. Karen Pak, Human Resource Management and the ability, motivation and opportunity to continue working: a review of quantitative studies, Hum. Resour. Manag. Rev. 29 (3) (2019) 336–352.
36. Samuel Roscoe, Green human resource management and the enablers of green organisational culture: enhancing a firm’s environmental performance for sustainable development, Bus. Strat. Environ. 28 (5) (2019) 737–749
37. Stefan Strohmeier, Smart HRM–a Delphi study on the application and consequences of the internet of things in human resource management, Int. J. Hum. Resour. Manag. 31 (18) (2020) 2289–2318.
38. Yishu Liu, An optimized human resource management model for cloud-edge computing in the internet of things, Cluster Comput. 25 (4) (2022) 2527–2539.
39. Kambur Emine, Yildirim Tulay, from traditional to smart human resources management, Int. J. Manpow. 44 (3) (2023) 422–452.
40. Mohammed Mohammed Sadeeq, Nasiba M. Abdulkareem, Subhi Rm Zeebaree, Dindar Mikaeel Ahmed, Ahmed Saifullah Sami, Rizgar R. Zebari, IoT and Cloud computing issues, challenges and opportunities: a review, Qubahan Acad. J. 1 (2) (2021) 1–7.