Examining Machine Learning Strategies in Quelling Cyber Security Threats

Abstract

The alarming security threats in the internet world continually raisecritical concerns among individuals, organizations and governments alike. The sophistication of cyber-attacksmakes it imperative for a paradigm shift from traditional approaches and measures for quelling the attacks to modern sophisticated, digital and strategic ones, such as those involving machine learning and other technologies of artificial intelligence (AI). This study is aimed at examining machine learning (ML) strategies for effective cyber security.ML involves using algorithms and statistical models to enable computers learn from and make decisions or predictions based on data. The study relied on secondary data, which weresubjected to a systematic review. The results of itsthematic and qualitative analyses prove that majority ofthe literatures allude to the fact that the maximal performance abilities and tactics of the ML constitute its strategies for quelling cyber security. These include its:early detection of threats that are tackled before they cause damages; ability to analyze huge quantity of data quickly and accurately; and processing of datasets in real-time. The study argues that the noted abilities and tactics constitute ML strategies for quelling cyber security, regardless of its challenges like data quality, security vulnerabilities and possible incidences of bias. The study concludes that ML can indeed be used to detect and respond to threats in real-time, ascertain patterns of malicious behavior, and improve on internet security, which thereby prove it to be a viable tool for quelling cyber security.

Keywords: Machine learning, Strategies, Quell, Cyber security, Artificial intelligence

Introduction

The rising issues confronting the use of information and communication technologies have necessitatedglobal concerns about cyber security (Njoku et al., 2024; Bulama&Shrivastava, 2023).Cyber security refers to all kinds of actions, measures and activities geared toward attaining safety in the internet world. It involves protecting individuals, groups and nations alongside their sites, web applications and other digital property from external and internal cyber threats (Akintoye, 2022).The internet offers huge benefits to society in various regards. With the internet, activities are carried out seamlessly, easily and fast. In this era of digitalization, businesses, public service delivery, communication, interpersonal and intergroup relations, administration and so on are all done more on the internet. However, the use of internet has been characterized and threatened by a lot of crimes, known as cybercrimes.The crimes, which are of different forms and patterns, constitute the theme of cyber security. The threats have made government and organizations of different countries to make concerted efforts toward ensuring cyber security by watching against cyber security threats (CST henceforth), also known as cybercrimes.

Additional to projects and programs on cyber security, nations like US, Australia, Indonesia, UK, South Africa, India and Nigeriahave made laws against cybercrimes. Yet,heinous crimes on the internet persist (AL-Hawamleh, 2023). Halting the persistent continuity of the dreaded ills of the internet requires the application of strong strategic measures. This study is an attempt in that direction. The theme of cyber security has gainedscholarly attention and exploration in recent

times. However, most of the extant studies focus on the effects of cyber security threats on various facets of society–economy, governance, social life, education, polity, etc. This study uniquely draws attention to how machine learning (ML) strategies can help to quell cyber security threats. In other words, the present study seeks to examine and show the ML strategies that can help quell cyber security threats.ML refers to artificial intelligence statistical models and algorithms that make it possible for computers to learn from data for efficiency in certain activities.As a way of making scholastic contribution to addressing issues of cyber security, the study proposes the use of ML strategies to quell the threats to cyber security.

Issues and Trends in Cyber Security

Just as countries like US, UK, South Africa, India, China, etc. have been gaining millions of Dollars, Pounds and other currencies from the internet so also they have been losing huge amounts to cyber security threats (Njokuet al., 2024; Chitimira&Ncube, 2021). The losses are of two kinds. First, whooping amounts of money are lost to cyber-attacks. Second, huge amounts are spent consistently on devising and putting in place measures for detecting, preventing and tackling cyber-attacks. Money that ought to be spent on national and international projects and programs are looted by cyber criminals, and rather spent by governments on building as well as ensuring strong cyber security.Cybercrime, according to Vidya (2014), is the act of perverting a criminal act online by erasing a database while using a digital device or the internet. This study adds that cybercrime is not just about erasing a database. Rather, it is a term that describes all kinds of criminal acts one can think of, which are perverted online to harm the victims, while the criminal benefits from the digital theft or criminality.

As Snehi and Bhandari (2021) rightly note, online services have got proliferated and diversified, spreading to all endeavors. The services are presenting new challenges to the different fields. This study considers the challenges as being new because they are mostly the results of the use or adoption of the information and communication technology cum its associated innovations.Billions of dollars are being lost to cybercrimes (Bulama&Shrivastava, 2023). Kshetri (2017) reports that Nigeria, Kenya and South Africa suffer $649 million, $210 million and $157 million losses to cybercrimes each year, stressing that African economy as a whole suffers around $3.5 billion losses to cybercrimes yearly. Banks across the globe are reported to be losing $114 billion USD to cybercrimes, while around 274 billion USD is spent on quelling CST in the banking sector (Raghava et al., 2014).It is reported that $4 billion is spent on recovering $3.6 billion (Raghava et al., 2014). This report highlights the need to be proactive and prevent the activities of cyber criminals. It is better to prevent the attacks from occurring than waiting to spend huge amountsof money on recovering attempts. In some cases, recovery attempts are even futile.

Sule et al. (2021) report that Nigeria loses at least 127 billion Naira (about $328,842,878 million US Dollars) to cybercrimes per year in recent times. Awhefeada (2020) and Dauda et al. (2020) note that the loss of N127 billion to cybercrimes warranted the Central Bank of Nigeria to promulgate laws governing online transactions in the country, as the loss adversely affected the Gross Domestic Product (GDP). In 2015 alone, Nigeria lost $400 Billion to cybercrimes (Dauda et al., 2020). The implication of the foregoing is that any country that fails to take decisive

actions and measures to quell CST, there is the possibility of experiencing such huge losses that Nigeria has been going through. That is the essence of stressing the cases of Nigeria and several other African countries.Almomoni et al. (2021) note that given the huge expenses on quelling CST, institutions, organizations and countries have to be decisive and proactive to avoid spending huge amount like the $ 124.25 million at NSF for cyber security.

Poor awareness, lack of technical-know-how, technical faults or lapses in developing websites and applications, and poor user education account for the possibility of the cyberattacks users receive from cyber criminals (Gkioulos& Chowdhury, 2021; Mohammad & Reza, 2017). Over 4.95 billion people across the world use the internet for different activities involving the ICT cum new media (Okusi, 2023). The usage is consistently threatened by different cyberattacks, such as cross site scripting (XSS). XSS involves a code injection attack, whereby attackers inject malicious script code into web applications, hacking applications and stealing and manipulating the private or security data of the victims (Okusi, 2023; Chen et al., 2019; Marashdih et al., 2019).XSS attacks caused the British Airways loss of millions of Dollars in September 2020, with the booking transactions of 380,000 passengers affected (Anderson, 2020; Rodriguez et al., 2020).XSS attacks on the websites of UK Parliament, Yahoo and Hotmail are in record (Chaudhary et al., 2016). Chaudhary et al. (2016) are of the opinion that the devastating effects of XSS have drawn significant attention of researchers in a view to finding tangible solutions to the menace.

Given the rising issues and trends, AI technologies and techniques have to be leveraged accordingly for a range of efficacious solutions. Mohammad (2020) situates artificial intelligence (AI) in ICT, pointing out that the various concepts of ICT characterize AI. AI technologies include Machine Learning (ML), Deep Learning (DL), Natural Language Generation (NLG), Robotics, Speech Recognition (SR), and Biometrics or Biometric Identification (Jhaveri et al., 2022; Mohammad, 2020). According to Mohammad (2020), technologies can perform many jobs at once. This highlights the fastness, efficiency, performance, problem-solving and result-oriented capacities of AI technologies, including ML. This paper avers that among the many jobs is that of ensuring cyber security.The study by Alamleh et al. (2023) demonstrates that different techniques of the ML can help quell CST, particularly those associated with smart phones. Their study lends credence to the standpoint of this study that ML techniques can be used to quell CST. Medida et al. (2023) aver that deep learning (DL) techniques have the potentials to quell CST, as they can be used to detect and prevent cyberattacks like denial of service (DoS). They argue that classifying incoming packets into benign and malicious categories, DoS can be quelled using Dique, a technique of DL for detecting and preventing DoS.

Cyber Security and National Concerns

Cyber security threats are the different attacks and criminal activities on the internet, which disrupt virtual assets, harm essential information of organizations and nations.They taint the image of a nation or an organization, following the illegal activities carried out by internet thieves (cyber criminals or attackers). Their families and other dependents follow suit in suffering the effects of the attack. Institutions of different countries, including the US, have been attacked and harmed by different cyber criminals. Multinational companies like Sony and

Hollywood have been attacked by cyber criminals, causing them huge losses in Dollars. Employees of such companies are the first sufferers of the attacks. Of course, an attack on Hollywood of the US implies an attack on the nation itself on one hand and those in the industry on the other.

Cybercrimes are of global concerns, not just national concerns. The consequences of cyber security threats (CST) cannot be quantified. Although US governments have been making concerted efforts to quell CST cyber since the 1980s, there is need to do more becauseas new measures are taken to quell them, cyber criminals also devise new means of perverting the criminality consistently. That is why this study argues that being proactive and using AI technologies and techniques like the Machine Learning would help a lot in quelling the rising security threats. In what lends credence to the foregoing, Raghava et al. (2014) note that cybercriminals continually develop more advanced techniques for foiling the efforts and mechanisms of states and organizations against them. Thus, there is need for the US Government alongside its citizenry to remain resilient and proactive against cyber criminals cum their activities.

Governments and organizations need not wait until cyber criminals strike before they wedge war against them as well as their criminal activities. The counterfeit access devices and computer fraud Abuse Act (18USC & 1030-1984) and the Electronic Communication Privacy Act (18USC 88 2500-2711-1986) are ample examples of statutory efforts made by US Governments to quell CST in the country. This paper advocates the proactive use of ML techniques to wedge more war against cyber security threats in the US in particular and other countries in general. The need for cyber security cannot be overemphasized because it is of great relevance to national concerns. This is because the threatsto cyber security adverselyaffectthe national wellbeing of a nation or an organization.National capacity is weakened by cyber threats. These threats pose serious security challenges to nation's military and paramilitary, thereby increasing their functions and worsening the state of affairs for them.

Also, the privacy of individuals, organizations and nations remains threatened or in shambles as a result of CST.Social life is punctured and free association or interaction on the internet ceases. Economic losses are countless. Also, the adoption of technologies becomes questionable or contended.Bulama and Shrivastava (2023) argue for the creation of frameworks for combating cyber security threats. It recommends the use of effective techniques, such as developing and using sustainable trackers of IP address, cryptography, establishing cyber security police stations, digital right management, interactive voice response, and introducing cyber education ethics across the three tiers of education, to pursue the realization of cyber security.

Bulamaand Shrivastava(2022) propose biometric as a mechanism for quelling cyber security, stressing that it has the capacity to identify and verify millions of individuals on the basis of unique biometric data. Although this study agrees with them that biometric can be used to quell cyber security threats, it observes that only those whose details are captured and stored in national and organizational identity databases can be proven to be inolved in a crime or not. Regardless of the limitation of biometrics, it is capable of reducing crimes because most of those whose data had been captured and stored can rarely indulge in cybercrimes. This is because they

know and remain conscious of being caught and dealt with.Zwilling et al. (2022) are of the opinion that good as well as ethical cyber practices are some solutions to CST. That is because with such practices, threats can be easily detected and prevented. As Zwilling et al (2022) note, such practices can help in identifying and reporting phishing attempts. Thus, they lend credence to the present study that right actions taken against cyber criminality can be result-oriented.

For Motiwala(2017), the security agents of different nations of the world have to be empowered and fully re/trained consistently and armed with sophisticated resources for security operations, including advanced weapons, detective machines, ICT devices, etc., so as to be well informed and conversant with the trends of cyber security and readily take justified actions against criminal acts. Training security personnel repeatedly on how to detect and handle all forms of cyber and conventional security threats can make them become capable of combating the challenges posed by cyber criminals, who unleash mayhems on society as a result of their criminal acts.Vidya (2014) are of the view that cybercrimes need to be quelled or reduced significantly through measures like functional security agencies and the establishment of cyber ethics. As Adewole (2011) warns, any nation that fails to take decisive and workable measures against the activities of cyber criminals would keep on losing most of its resources and security details to them. The losses include losing some development funds and resources to cybercrimes.

Theoretical Framework

As Wang (2010) notes, in AI discipline, a theory concerns the concept of intelligence in human and computer and in the combined context: human intelligence, computer intelligence, and general intelligence. The human intelligence is natural, while computer intelligence is artificial, which is why it is regarded as artificial intelligence. General intelligence includes human and computer intelligence, animal intelligence, collective intelligence, alien intelligence and what have you (Wang, 2010). The current trend is that "in mainstream AI, projects are guided by one or more of these three considerations: practical problem-solving demands, knowledge about human intelligence, and available normative models" (Wang, 2012, p. 3).Based on practical problem-solving demands, the theory of computation is often considered to suffice for any other or a new theory of AI and its integration in or application to any project (Hayes & Ford, 1995; Marr, 1982).

This study is anchored on the Unified Theory of Acceptance and Use of Technology (UTAUT). As Moheb (2021) and Tamilmani et al. (2021) note, UTAUT is more encompassing and integrative than the other theories of AI, Computer, Information and Communication Sciences. The noted reason is why UTAUT is adopted for a theoretical framework. UTAUT is championed by Venkatesh et al. (2003) to explain how to comprehend the process of accepting an innovation like the AI. As identified by Venkatesh et al. (2003), the UTAUT has the following key dimensions:

- Behavioral intention and use, which drives (the realization of) job performance (p. 447).
- Expectancy effort, which concerns the extent to which the use of the system is easy (p. 450).

- Social influence, which refers to the individual's consideration of the new system on the basis of the importance others accord the system (p. 451).
- Facilitating conditions,whichconcern the enablers or support systems with which adopting and using the new system is possible and easy (p. 453).
- Behavioral intention, which concerns the individual's intention to use a given system–technology (p. 453).

Again, the dimensions of the theory, according to the exponents, are influenced and moderated by experience, age, gender, and usage voluntariness (Venkatesh et al., 2003). They later added three factors to the ones identified earlier, which are hedonic motivation, price value, and habit (Moheb, 2021; Tamilmani et al., 2021). Venkatesh's et al. (2003) UTAUT unifies the eight previous models: Theory of Reasoned Action (TRA), Technology Acceptance Model (TAM), Theory of Planned Behavior (TPB), Motivational Model (MM), the combined TAM and TPB (C-TAM-TPB), the Model of PC Utilization (MPCU), the Diffusions of Innovations Theory (DOIT), and the Social Cognitive Theory (SCT). From the above brief on UTAUT,it is substantial to assert that the theory aptly theorizes the acceptance of AItechnologies and techniques in cyber security.

Machine Learning and Cyber Security

The study done by Thakkar and Lohiya (2021) shows that Machine Learning techniques can be leveraged for XSS attacks and address other cyber security challenges. Zhang et al. (2021) are of the view that AI technologies and techniques are capable of tackling cyber security threats, particularly because of their computing power that makes them problem-solving. By implication, ML is affirmed by these scholars to be capable of tackling the rising cyber security across the globe. They mention that machine translation, robotics, cyber defense, language analysis, and speech recognition are some of the ways through which AI technologies and techniques solve different problems. ML and Deep Learning (DL) algorithms are proven by Jian-hua Li (2021) to be impacting internet world in a significant magnitude. For Jian-hua Li (2021), AI technologies are themselves vulnerable to cyber threats, but there are ways of deploying their techniques to surmount the threats.For example, by encrypting the deep neural network, the potential attacks on AI technologies can be averted.

Jian-hua Li (2021) also observes that although the high time-consumption of Support Vector Machine (SVM) limits its detective capacity, AVL Tree can be used to reduce time and improve detection, prevention, and performance.The study carried out by Kaur et al. (2023) affirms that ML, deep neural networks, decision trees, and web-log-based detection models can detect and predict XSS attacks. They thereby lend credence to the position of the current paper that ML techniques can help in quelling cyber security, when deployed accordingly. Okusi (2023) shows that deep forest is a technique of the ML that can help detect and prevent XSSattacks and address the issues of class imbalance. His study also lends credence to the position of the present study that ML techniques can be leveraged for cyber security. Similarly, Zhang et al. (2019) demonstrate that Natural Language Processing (NLP) is an AI technology and technique that can be used to address cyber security concerns. They add that Word2vec is an ML technique that can

be used to learn word embedding from a text corpus, with which cyber security threats can be detected, predicted and even prevented.

The present study avers that reinforcement learning and other techniques of the ML algorithms allow systems to learn from data and improve overtime. This would breed efficiency in security. The improvement would lead to a reduction in cybercrime rates. Also, ML can be leveraged for the optimization of cyber security operations.Cyber security projects can be arranged, predicted, and planned using ML algorithms. By so doing, ML helps in fostering effective resource management. Also, the use of big data in cyber security expedites the whole process. This includesenabling effective decision-making that produces appreciable results. Thus, ML can be deployedto find lasting solutions to cyber security challenges.

Studies, such as Wusuet al.(2022), agree that various ML algorithms are used for analytic prediction. This means that ML can be used to predict cyber situations, for which the optimization of cyber security processes obtains. With the predictive analytics, quality control is achieved too.The predictive and decision-support algorithms of ML are advantageous because they proffer predictive insights, efficiency, save costs, time and resources, foster better utilization,andprevent the making of many mistakes. Their major disadvantages include incomplete data and scalability of models both in general and cyber security contexts.

Advantages and Disadvantages of ML

Bulama and Shrivastava (2023) observe that through the use of the internet, ICT offers society both advantages and disadvantages. The advantages include seamless transactions, interactions, communication, learning and teaching, culture contact, and exchange of information, ideas, thoughts, and so on. The disadvantages include phishing, spamming, email spam, online charity, identity theft, cyber defraud, and creating and spreading viruses.Although the general disadvantages of AI technologies and techniques apply to ML, ML has some disadvantages that are specific to it.Dixit and Silakari (2021), Luo et al. (2021), Onan and Tocoglu (2021), Onan (2019), Pavan Kumar et al. (2021), and Zhang et al. (2022) argue that ML and DL techniques can be leveraged for tackling cyber security challenges, including those posed by cross-site scripting (XSS). The aforementioned studies, among others, imply that ML is advantageous because its techniques can be leveraged for security purposes.

On the other hand, Jian-hua Li (2021) points at high time consumption for training as the major limitation of the Support Vector Machine (SVM), which makes it unable to tackle cyber security challenges effectively.The present study argues that both AI-based and conventional techniques and measures can be used to surmount the time constraint. This is to say that regardless of the time consumption, SVM can be leveraged for effective cyber security. The needful has to be done to make it as well as other AI technologies and techniques work and serve the purpose of ensuring cyber security accordingly.Tariq et al. (2021), Kaur and Singh (2019), and Zhou and Wang (2019) argue that ML techniques are inefficient in detecting and preventing cyber security threats, such as XSS attacks. This current paper argues otherwise that despite any affirmed and imagined limitations of AI technologies, they are capable of addressing cyber security challenges once leveraged accordingly.

Again, Machine Learning is specifically advantageous because it provides predictive insights and efficiency. The predictive insights and efficiency potentials of the ML are the base of the claim advanced by this study about its potentials fortackling cyber security threats. It follows that ML can predict cyber threats accurately and thereby help to avert cybercrimes. Also, this study argues that it is because ML detects that it can predict. It is upon detection that its predictability of threats and other issues rest. SVM can be used for separating multiple or dual web applications, software and other internet packages that are vulnerable to cyberattacks because of their nature. Through the application of Baye's theorem, NB can be used to calculate cyberattack attempts, upon which prevention takes effect against and foil the attempts.

The different techniques of ML, such as data-based method, SVM, NB, KNN, RF, AR algorithms, EL, k-Means clustering, and PCA, can be used for various security purposes. Thus, they can be used to quell cyber security threats. Databased techniques can be used to predict cyber threats and to train manpower personnel on how to tackle cyber security challenges.Their advantages, which are both respective and collective, revolve around efficiency, easiness, detection, prediction, enhancement, saving time and costs, solving problems, generating reliable data and reducing risks and inadequacies. On the hand, their disadvantages in broad terms include requiring large storage, intensive training, difficulty in interpretation and practice, high time consumption, variation and complexities. Generically, ML is constrained by data completeness and model scalability.

ML alongside other AI technologies and techniques offers efficiency, safety, innovation and enhancement of different activities for optimal performance, productivity and outcomes (Regona et al., 2022). Its affirmed potentials, which give rise to the aforementioned, are the base of its capacity in quelling cyber security threats. ML offers learning, innovation and career opportunities, including technology literacy skills. With these skills acquired, different persons involved in the task of quelling cyber security threats are bound to proficiently and significantly tackle the worrisome trends of cyber security threats. By guaranteeing safety, ML indeed has the potentials of quelling CST. Nevertheless, there is need for future deployment of analytics tools for effective integration of ML and other AI technologies into cyber security.

Conclusion

As shown variously in the body of the work, this study has proven its claim that ML techniques can serve as strategies for mitigating cyber security threats, drawing evidence from extant literatures. The study submits that ML can indeed be used to detect and respond to threats in real-time, ascertain patterns of malicious behavior, and improve internet security. Given these potentials or capacities of the ML,there is no gainsaying the fact that it is a viable tool for quelling cyber security. It is thus imperative for nations, organizations and even individuals to rightly leverage ML for the quelling of cybercrimes. Training, awareness, shouldering costs and the willingness to adopt innovations for positive and significant change are the panacea to the perceived and real challenges to adopting ML as well as other AI technologies for solutions to problems in different spheres.

References

Adewole, K. (2011). An inquiry into the awareness level of cyber security policy and measures in Nigeria. *International Journal of Science and Advanced Technology, vol.1, no.7,* 91–96.

Alamleh, A., Almatarneh, S., Samara, G.&Rasmi, M.(2023). Machine learning-based detection of smartphone malware: Challenges and solutions. *Mesopotamian Journal of Cybersecurity, vol.2023*, 134–157. DOI: https://doi.org/10.58496/MJCS/2023/017

AL-Hawamleh, A. M. (2023). Predictions of cybersecurity experts on futurecyber-attacks and related cybersecurity measures.*International Journal of Advanced Computer Science and Applications*, vol.14, no.2

Anderson, B. (2020, December). 3 dangerous cross-site scripting attacks of the last decade. *ReadWrite, 1*. Available from: https://readwrite.com/3-dangerous-cross-site-scripting-attacks-of-the-last-decade.

Bulama, L. &Shirivastata, M. (2022). The role of information & communication technology towards protection of lives and property in Northern Nigeria: A focus on Maiduguri Borno state. *International Interdisciplinary Research Journal, vol.14, no.1*, 1–9.

Bulama, L. &Shrivastava, M. (2023). Framework & techniques to improve cyber security in Nigeria. *Journal of Data Acquisition and Processing,vol.38, no.2*.

Chaudhary, P., Gupta, B. B. & Gupta, S. (2016). Cross-site scripting (XSS) worms in online social network (OSN): Taxonomy and defensive mechanisms.*3rd International Conference on Computing for Sustainable Global Development (INDIACom*), 2131–2136.

Chen, X., Li, M., Jiang, Y. U. & Sun, Y. (2019). A comparison of machine learning algorithms for detecting XSS attacks. *Artificial Intelligence and Security*, 11635, 214-224.

Chitimira, H.&Ncube, P. (2021). The regulation and use of artificial intelligence and 5G technology to combat cybercrime and financialcrime in South African Banks. *PER/ PELJ,*(24). DOIhttp://dx.doi.org/10.17159/1727-3781/2021/v24i0a10742

Dixit, P. &Silakari, S. (2021). Deep learning algorithms for cyber security applications: A technological and status review. *Computer Sci. Rev.*, 39, 100317. https://doi.org/10.1016/J. COSREV.2020.100317

Gkioulos, V. & Chowdhury, N. (2021). Cyber security training for critical infrastructure protection: A literature review. *ComputerSci Rev*, 40:100361. https://doi.org/10.1016/J. COSREV.2021.100361

Jhaveri,R. H., Revathi,A., Ramana, K., Raut, R. &Dhanaraj, R. K. (2022). A review on machine learning strategies for real-worldengineering applications. *Hindawi Mobile Information Systems*, vol. 2022. 26. https://doi.org/10.1155/2022/1833507

Jian-Hua, L. (2021). Cyber security meets machine learning. In cyber security meets machine learning. *Springer Singapore*. https://doi.org/10.1007/978-981-33-6726-5

Kaur, J., Garg, U. &Bathla, G. (2023). Detection of cross-site scripting (XSS) attacks using machine learning techniques: A review.*Artificial Intelligence Review*, https://doi.org/10.1007/s10462-023-10433-3

Kaur, S. & Singh, M. (2019). Hybrid intrusion detection and signature generation using deep recurrent neural networks. *Neural Computer App.*, 32(12), 7859–7877. https://doi.org/ 10.1007/S00521-019-04187-9

Luo, C., Tan, Z., Min, G., Gan, J., Shi, W. & Tian, Z. (2021). A novel web attack detection system for internet of things via ensemble classification. *IEEE Trans. Industry Inf.*, 17(8), 5810–5818. https://doi.org/10.1109/ TII.2020.3038761

Marashdih, A. W., Zaaba, Z. F., Suwais, K. &Mohd, N. A. (2019). Web application security: An investigation on static analysis with other algorithms to detect cross site scripting. *Procedia computer science*, 161, 1173–1181.

Medida,V.N. V. S. N. &Mathew, R. J. (2023). DeepGuard: Detecting and preventing DoS attacks using deep learning. *DogoRangsang Research Journal (UGC Care Group I Journal)*, vol-13, Issue-6,

Mohammad, S. M. (2020). Artificial intelligence in information technology. *International Journal of Innovations in Engineering Research and Technology [Ijiert]*,vol.7, iss.6.

Mohammad. G.&Reza, S. (2017). Software vulnerability analysis and discovery using machine-learning and data-mining techniques. *ACM Computer Survey (CSUR)*, 50(4). https:// doi. org/10. 1145/3092566

Motiwala,A. (2017). Cyber security in Ghana: Evaluating readiness for the future. *Annaar International Peacekeeping Training Centre Brief*, (1),1-4.

Njoku,D. O., Iwuchukwu,V. C.,Jibiri,J. E. Ikwuazom, C.T.,Ofoegbu,C.I.&Nwokoma, F. O. (2024). Machine learning approach for fraud detection system in financial institution: a web base application. *International Journal of Engineering Research and Development*, vol.20, iss.4. 01-121.

Okusi, O. A.(2023). An analysis of cross-site scripting and its preventive techniques. M.Sc. Cyber Security: CSCT Masters Project. Department of Computer Science and Creative Technologies, University of West England (UWE), Bristol.

Onan, A. &Tocoglu, M. A. (2021). A term weighted neural language model and stacked bidirectional LSTMbased framework for sarcasm identification. *IEEE Access*, 9.7701–7722. https:// doi.org/10.1109/ACCESS.2021.30497 34

Onan, A. (2019). Consensus clustering-based undersampling approach to imbalanced learning. *Sci Program*.https:// doi. org/ 10. 1155/ 2019/ 59010 87

Pavan, K. P., Jaya, T. &Rajendran, V. (2021). SI-BBA—a novel phishing website detection based on swarm intelligence with deep learning. *Mater Today*.https://doi.org/10.1016/J. MATPR.2021.07.178

Rodríguez, G. E., Torres, J. G., Flores, P. &Benavides, D. E. (2020). Cross-site scripting (XSS) attacks and mitigation:A survey. *Computer Networks*, 166:106960. https://doi.org/10.1016/J. COMNET.2019.106960

Snehi, M. Bhandari, A. (2021). Vulnerability retrospection of security solutions for software-defined cyber-physical system against DDoS and IoT-DDoS attacks. *Computer Sci Rev*. https://doi.org/10.1016/j.cosrev.2021.100371

Tariq, I., Sindhu, M. A.,Abbasi, R. A., Khattak, A. S., Maqbool, O. & Siddiqui, G. F. (2021). Resolving cross-sitescripting attacks through genetic algorithm and reinforcement learning. *ExpSyst App*., 168:114386. https://doi.org/10.1016/J.ESWA.2020.114386

Thakkar, A. &Lohiya, R. (2021). A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions. *Artificial Intell Rev. 55(1*), 453–563. https://doi.org/10.1007/S10462-021-10037-9

Vidya, P.M. (2014). Cyber security – trends and challenges. *International Journal of Computer Science and Mobile computing,vol.3, iss.2*, 586-590.

Wusu, G. E., Alaka, H., Yusuf, W., Mporas, I., Toriola-Coker, L.&Oseghale, R. (2022). A machine learning approach for predicting critical factors determining adoption of offsite construction in Nigeria. *Smart and Sustainable Built Environment*(ahead-of-print).

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F. & Choo, K. K. R. (2021). Artificial intelligence in cyber security: Research advances, challenges, and opportunities. *ArtifIntell Rev*. 55(2),1029–1053. https://doi.org/10.1007/S10462-021-09976-0

Zhou, Y. & Wang, P. (2019). An ensemble learning approach for XSS attack detection with domain knowledge and threat intelligence.*Computer Security*, *82*, 261–269. https://doi.org/10. 1016/J.COSE.2018.12.016