Rivista Italiana di Filosofia Analitica Junior Vol 14, No. 1 (2023)
ISSN: 2037-4445

Role of Machine Learning Applications in Enhancing Cyber Security Effectiveness: An Empirical Study

Parul Chaudhary

Assistant professor

Maharaja Surajmal Institute of Technology

Rohit Sharma

Asst. Professor

Panipat Institute of Engineering and Technology

Meena Rao

Associate Professor

Maharaja Surajmal institute of technology

Mohit Tiwari,

Assistant Professor,

Department of Computer Science and Engineering,

Bharati Vidyapeeth's College of Engineering, Delhi, India

Abstract

In the modern era, the internet has become a necessary component of daily life. People use the internet more and more often in daily life all around the world. The likelihood of harmful attacks has also increased as a result of growing internet dependence. As a result of rising cyber security concerns, cyber security has become a critical component of the fight against all online threats, frauds, and assaults. As the internet expands, there is an increasing chance that you may be the target of ongoing cyber-attacks. In this digital era, machine-learning techniques are an essential tool for fending off threats from the internet. Various machine-learning techniques are used to identify the risk associated with cyber security. For creating a system that adapts to the data source, machine learning is a valuable method. Machine learning techniques may be used to classify hazards and identify compromised endpoints in order to handle massive volumes of data more successfully and precisely.

Keywords: Machine Learning Techniques, Cyber Security, Effectiveness of Cyber Security, Online Threats, Cyber Attacks

Introduction

The common usage of network, connected device and the disproportionate reliance on ICTs has increased globally. Many malicious individuals try to attack host data or breach credentials. Various proofs of concept and real assaults have occurred during the past few years. Cyber security practices are employed to safeguard electronic devices and computer programmers against unauthorized entry, hostile incursions, and damage, as well as to safeguard the services they provide against interruption or misdirection. These assaults usually aim to access, alter, delete, and steal critical information while defrauding users. They also attempt to disrupt corporate operations. The topic of cybersecurity has gained importance recently because of the advancement of computing technology, the accessibility of smart devices, our reliance on them, and the ease with which we may access the Internet. The foundations of cyber security state that any cyber security strategy must have several levels of security

and that any cyber security system comprised of people, processes, and technology must function effectively as a unit to provide a strong defense against cyber-attacks. The two technical advancements have significantly affected current cyber-attacks and accompanying countermeasures. These include the explosion of digital data, which keeps data on devices and in clouds, and the Internet of Things, which links objects to a network or the internet. The Internet has considerably contributed to the growth of the digital world and has established itself as a necessary aspect of modern living (Ali, Nameen, Anam, Ahmed, 2022 and Virmani, Choudhary, Pillai, & Rani, (2020).

The growth of the technological world is contributing to an increase in internet addiction. Although these technologies have a wide range of positive effects on people and communities, they also present several problems. For instance, hackers could use security flaws to harm individuals worldwide by stealing from them and destroying their property. Cyberattacks may result in consequences for organizations, such as monetary losses and reputational damage. As a result, network security has become a significant issue. Firewalls, encryption, and antivirus software applications, among other conventional security measures employed by enterprises, play a vital part in securing. There are many kinds of cyberthreats in cyberspace. Every day, many new hazards materialize. In the field of cybersecurity, the balance between attackers and defenders is still far from being established. Dangers are becoming more difficult to avoid in the ever-expanding online world, and they are continuously changing in nature. It becomes challenging to identify dangers as a result (Kumar, Singh, & Kumar, 2021 and Sreekanth, Dr. Kurian, Jibin, Sajay, Dijesh, 2023).

Without ever concluding a contract, machine learning, a form of artificial intelligence, allows computers to build and practise using data. To forecast training data, it makes use of digital simulation, which is received via primary collection processing. The broad range of industries including e-commerce employs the artificial intelligence technologies. This technology is very effective when judgments are based on customer activities, hobbies and healthcare requirements. Machine learning techniques are needed to increase security precautions. The two types of machine learning algorithms are controlled and unsupervised. They are distinct from the information they are gathering. A community with expertise in labelled teaching may offer simulations as a component of a controlled learning strategy to assist learners in understanding the differences between the labels. Uncontrolled learning is a tactic for employing elusive knowledge equations that are intended to inflate courses on their own. In many cases, the indicated information is quite uncommon. Automated learning from examples and experience without explicit programming is the foundation of machine learning. Machine learning techniques have recently been used in a variety of fields, including malware analysis, industrial control systems, intrusion detection, power system security, etc. Any technology that has the ability to learn from experience, much like individuals do, can be used in machine learning. It searches for patterns and develops itself to apply them in future assessments, just like the human brain does. It thus opposes the archaic practises of teaching by doing and data programming into the systems. Machine learning, in contrast to many other technologies attempting to provide cyber security, bases its decisions on data rather than algorithms and changes its behaviour in response to new information. Machine learning, to put it simply, is an advancement in artificial intelligence that enables the system to learn without being directly programmed (Shaukat, Luo, Varadharajan, Hameed, Chen, Liu, & Li, 2020).

Machine learning is a potent technique for overcoming the difficulties of identifying and preventing cyberattacks. In order to discover patterns and anomalies that can point to an attack, machine learning algorithms can analyse complicated and vast amounts of data. These algorithms are a powerful tool for boosting cyber security since they can be taught to learn from past data and identify new assaults in real-time. Anomaly detection, intrusion detection, malware categorization, and phishing detection are just a few of the cyber security applications that employ machine learning. Searching for unexpected patterns of behaviour that might be indicators of an assault is known as anomaly detection. Finding unauthorised entry is required to identify network or system intrusions (Vadivelan, Bhargavi, Kodati, & Nalini, 2022 and Bhutada, Bhuatada, 2018).

Literature Review

According to research there are different types of cyber security issues one can face. First is Cybercrime detection. Intrusion monitoring strategies are exposed when hostile software or policy breaches damage protected knowledge. There are several ways to find infiltration. Whether based on signatures or abnormalities, the procedures are categorized extensively. Using the signature approach, both packets are connected to the IDs of acknowledged insider activities. Another type of cyber security challenge is the study and identification of malware. Malicious software is an easy way to get malware. Malicious software in particular is a type of cyberattacks tool. It is frequently seen when illegal operations like data theft, access control, host computer damage, and other comparable things are taking place. Malicious is a general phrase that encompasses a wide range of destructive software, including worms, trojans, viruses, bugs, spyware, root kits, and adware. There are several families of both of these virus categories. Because Android is the most widely used smartphone operating system, malware infection makers severely penalise it. Because there are more and more Android application variations every day, it has become more difficult to identify and classify harmful mobile variations. Companies use a variety of techniques to scan cellphones for harmful software. Fraud detection is currently one of the major difficulties with data management. Spam is usually portrayed in advertisements as an unwanted package message. Spam is a phrase that is frequently used to describe spam, but it may also describe a message on a social networking site or another posting channel. Spam messages use a significant amount of time. Spam mail that impersonates official bank communications is routinely sent to customers in an effort to trick them. Many incur a significant financial loss if they reply to these text filters (Singh, Wazid, Das, Chamola, & Guizani, 2022).

According to a research, there are various types of cyber-attacks. Middle in aman attack is one of them. Every time a reliable user connects to the database, this assault takes place. The interruption of a conversation is one instance of this attack. In such an attack, the attacker conceals or links the victim to the database. The attachments remove the victim's IP, but the conference goes on as planned because the server still uses the suspect's IP. To put it another way, the company and brand suffer when the victim's computer separates from itself. It's usual to utilise User Access Compromise. The login information and other personal information of the compromised user are attacked. Unencrypted passwords can improve security, democratic password management can be thwarted, and people have the ability to establish forceful movements and encyclopaedias. They are common techniques for obtaining private information from customers. The most effective ways to get user data are through ransomware and harpoon threats. A malware attack forces or humiliates victims into accepting an address in order to acquire marked document. Root access compromise is another type of cyberattack. This invasion resembles a user exploitation attempt, however instead of accessing a genuine server, the attackers have access to a user's accounts, which have exclusive permissions in comparison to those on the list. The manipulation of web flaws is used to compromise web access. Cross-site scripting and the incursion of Structured Query Language appear to be some common sorts of network breach threats. In essence, malicious software is a piece of code that has not been approved. For instance, hostile hackers may use ransomware to steal personal data, penetrate systems or infrastructure, temporarily shut down or destroy a platform for computer crimes, install dangerous scripts, etc. Malicious software comes in many different forms, mostly depending on the objectives of the perpetrators and the rate at which each spreads. They are few examples of cyber attacks which are changing their nature with the advent of technology. Day by day they are becoming more powerful (Kumar, & Pande, 2022 and Handa, Sharma, & Shukla, 2019).

In a research it was estimated that One of the essential components for enabling greater levels of cyber security and defending next-generation cyber systems is machine learning. The most recent cyber security systems are being updated to include enhanced versions of artificial intelligence and machine learning. Through improving the knowledge of Artificial Intelligence, security of the online safety of various datasets, groups, or even physical realities can be improved. In contrast to a reality that does not depict or exhibit a reality, companies involved in cyber security are primarily concentrating on

Artificial Intelligence and general behaviour. For a range of applications, including security, organisations from throughout the world have shown a strong interest in using ML models. The main goal of ML applications in the cybersecurity framework is to increase the automation and efficiency of security analysis in comparison to current cybersecurity systems. However, due to the changing nature of cyber threats, security experts find it difficult to thoroughly examine all potential vulnerabilities to cybersecurity systems. The results show that machine learning (ML) models presently used in conventional security designs outperform conventional rule-based or signature-based strategies in a variety of domains. Numerous businesses throughout the world generate a significant amount of data each day as a consequence of numerous user activities, network data traffic, and countless other electronic transactions. A security analyst's responsibility is to look for trends in this data that could indicate any suspicious or out-of-the-ordinary activities. The major issue with this approach is that security experts may find it time-consuming and challenging to manually evaluate such a large volume of data in order to look for suspicious and abnormal trends. On the other side, ML enables a digital gadget to learn and grow more intelligent since robots are far better than people at identifying patterns (Gupta, Gupta, & Kukreja, 2021 and Gupta, Johri, Srinivasan, Hu, Qaisar, & Huang, 2022).

According to a research Anti-virus software packages employ their signatures to find malware and viruses. As a result, AVS may only identify malware that matches a viral signature in the database. On the other hand, ML-based cybersecurity systems are capable of learning from data and are able to differentiate between known and unknown threats. The findings of ML algorithms show extraordinary effectiveness in recognising and preventing various threats, and they are now being employed broadly in cybersecurity. Without ML algorithms, it is challenging to construct effective first-level cybersecurity solutions. In contrast to traditional cybersecurity systems, ML tends to make cybersecurity computer processes more actionable and intelligent even in novel settings. The basis for machine learning's efficacy in cybersecurity systems is its capacity to assess patterns, which enables speedy decision-making and ultimately stops all probable known and unknown assaults. The ability of ML technology to manage massive amounts of data created by several networks offers a solid security solution for problems like user authentication, access control, firewall filtering, etc. ML-based security systems may scan for possible risks, do predictive analysis, and forecast the next assault by correlating and arranging incoming data flow into a certain pattern. By using ML in cybersecurity applications, a corporation may significantly save the time and money it would otherwise spend on recruiting cybersecurity specialists. Security professionals were free to concentrate on more crucial strategic concerns since machine learning techniques have been shown to be more successful in the cybersecurity market for repetitive automated tasks. According to experts, the best strategy to prevent zero-day attacks is to use machine learning since it enables security professionals to possibly close vulnerabilities and thwart exploits before they lead to a data breach. The quality of data used in training and testing phase strongly influences the effectiveness of Machine Learning. If the data supplied to the models provides an accurate representation of the environment, ML generally has the potential to make cybersecurity more responsive, affordable, and substantially more successful (Mangalraj, 2019 and Iyer, & Rajagopal, 2020 and Geetha, & Thilagam, 2021).

Objective

1. To explore the role of machine learning applications in enhancing cyber security effectiveness
2. To know the influence of machine learning applications in enhancing cyber security effectiveness

Methodology

In this study 242 respondents were surveyed to know the factors that determine the role of machine learning applications in enhancing cyber security effectiveness. The study was conducted with the help of a structured questionnaire. Also, researchers used a convenient sampling method for collecting the primary data. After the completion of the fieldwork, the data was analyzed and evaluated by mean and t-test.

Findings

Table below is sharing respondent's general details in which it is found that in total 242 respondents males are 47.1% and females are 52.9%. 25.6% are in the age group of 18 – 24 years, another 27.2% are between 25 – 34 years of age, 23.6 % are in the age group of 35 – 44 years and the remaining 23.6% are above 45 years of age group. 22.3% of the respondents are single, 61.1% are married with kids and the remaining 16.6% are married without kids. Talking about their monthly income, 21.5% have monthly income between INR 25,000 – INR 50,000, 28.1% have monthly income between INR 50,001 – INR 100,000 and the rest 50.4% have monthly income above INR 100,000.

Table 1 General Details

Variables	**Respondents**	**Percentage**
Gender		
Female	128	52.9
Male	114	47.1
Total	**242**	**100**
Age (years)		
18 – 24	62	25.6
25 – 34	66	27.2
35 – 44	57	23.6
Above 45	57	23.6
Total	**242**	**100**
Marital Status		
Single	54	22.3
Married with kids	148	61.1
Married without kids	40	16.6
Total	**242**	**100**
Monthly Income (INR)		
25,000 – 50,000	52	21.5
50,001 – 100,000	68	28.1
More than 100,000	122	50.4
Total	**242**	**100**

Table 2 Role of Machine Learning Applications in Enhancing Cyber Security Effectiveness

S. No.	**Statements**	**Mean Value**	**t value**	**Sig.**
1.	Machine learning helps in automating the process of finding and contextualizing relevant data at any stage	4.18	15.188	0.000
2.	ML helps to understand previous cyber-attacks and develops effective defence response	3.86	11.140	0.000
3.	ML can be used in various domains within cyber-security to increase security processes	4.29	16.975	0.000
4.	ML helps to automize repetitive and time consuming tasks such as triaging intelligence	3.74	9.541	0.000
5.	ML algorithms are used to identify and counter attacks	3.79	10.353	0.000
6.	ML detects the threats much faster than any manual process	3.93	11.983	0.000

7.	ML develops predictive forecasting models that builds threat profiles to prevent before it happens	4.07	13.917	0.000

The table above shows the factors that determine the role of machine learning applications in enhancing cyber security effectiveness. The respondent says that ML can be used in various domains within cyber-security to increase security processes with mean value 4.29, Machine learning helps in automating the process of finding and contextualizing relevant data at any stage with mean value 4.18 and ML develops predictive forecasting models that builds threat profiles to prevent before it happens with mean value 4.07. The respondent also believes that ML detects the threats much faster than any manual process with mean value 3.93, ML helps to understand previous cyber-attacks and develops effective defense response with mean value 3.86. The respondent also says that ML algorithms are used to identify and counter attacks with mean value 3.79 and ML helps to automize repetitive and time consuming tasks such as triaging intelligence with mean value 3.74. Further t-test shows that all the statements are significant (with the value below 0.05).

Conclusion

Deep learning and machine learning techniques are influenced by the human brain's quick ability to recall information from the past. These techniques have been applied to tackle problems in several different study domains. Cyber security is now more known than ever because to rising internet usage and a wide range of network applications. A variety of businesses can reduce labour expenses while performing more accurate data analysis than human analysts thanks to automated cybersecurity solutions based on machine learning. The significance of data preparation in machine learning modelling is looked at together with the benefits of appropriately trained ML models on the detection of contemporary cyberattacks and the reduction of false-positive rates. The automated capability of ML should not be exaggerated, even when key security concerns, where domain expertise is vital, cannot be addressed without human involvement. Machine learning techniques have shown a lot of promise for detecting and stopping invasions. Spam filtering, virus analysis, and intrusion detection are just a few of the cyber security applications that have successfully leveraged a variety of machine learning approaches. The well-known machine learning techniques used in cyber security includes deep learning and artificially generated neural networks. However, each algorithm has benefits and drawbacks, and selecting the best algorithm for a given task depends on a number of variables, including the data available, the nature of the threat, and the necessary level of accuracy. By identifying risks that had not yet been discovered, lowering false positives, and delivering rapid and precise responses to attacks, machine learning algorithms can enhance cyber security. Artificial intelligence and critical thinking advancements provide intriguing answers to network security problems. However, it is crucial to determine which approach is suitable for each job. To get extremely accurate results and have a comprehensive model guarded from malicious software. Given how rapidly viruses and cyberattacks are evolving, the modern environment demands an intelligent protection solution. AI techniques are more adaptable and resilient when compared to current cyber security solutions, widening security execution and enhancing protection against a growing number of sophisticated cyberthreats.

References

1. Geetha, R., & Thilagam, T. (2021). A Review on the Effectiveness of Machine Learning and Deep Learning Algorithms for Cyber Security. *Archives of Computational Methods in Engineering*, *28*(4), 2861–2879.
2. Virmani, C., Choudhary, T., Pillai, A., & Rani, M. (2020). Applications of Machine Learning in Cyber Security. In *Advances in information security, privacy, and ethics book series* (pp. 83–103).
3. Ali, A., Nameen, S., Anam, S., Ahmed, M.M (2022). Machine Learning for Intrusion Detection in Cyber Security: Applications, Challenges and Recommendations. *Innovative Computing Review*. 2(2), 41-64.

4. Bhutada, S., Bhuatada, P. (2018). Applications of Artificial Intelligence in Cyber Security, *International Journal of Engineering Research in Computer Science and Engineering*, 5(4), 214-219.
5. Handa, A., Sharma, A., & Shukla, S. K. (2019). Machine Learning In Cybersecurity: A Review. *Wiley Interdisciplinary Reviews-Data Mining And Knowledge Discovery*, *9*(4), 1-7.
6. Gupta, C., Johri, I., Srinivasan, K., Hu, Y., Qaisar, S. M., & Huang, K. (2022). A Systematic Review on Machine Learning and Deep Learning Models for Electronic Information Security in Mobile Networks. *Sensors*, *22*(5), 2017.
7. Sreekanth, D., Dr. Kurian, M. J., Jibin, N., Sajay, K. R., Dijesh, P. (2023). An Analysis Of The Effectiveness Of Machine Learning Algorithms In Detecting And Preventing Cyber-Attacks, *Eur. Chem. Bull.* 12 (S3), 234 – 241.
8. Iyer, S., & Rajagopal, S. (2020). Applications of Machine Learning in Cyber Security Domain. In *Advances in information security, privacy, and ethics book series* (pp. 64–82).
9. Kumar, K., & Pande, B. P. (2022). Applications of Machine Learning Techniques in the Realm of Cybersecurity. *Cyber Security and Digital Forensics*, 295–315.
10. Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, S., Liu, D., & Li, J. (2020). Performance Comparison and Current Challenges of Using Machine Learning Techniques in Cybersecurity. *Energies*, *13*(10), 2509.
11. Singh, J., Wazid, M., Das, A., Chamola, V., & Guizani, M. (2022). Machine Learning Security Attacks And Defense Approaches For Emerging Cyber Physical Applications: A Comprehensive Survey. *Computer Communications*, *192*, 316–331.
12. Gupta, A., Gupta, R., & Kukreja, G. (2021). Cyber Security Using Machine Learning: Techniques and Business Applications. In *Springer eBooks* (pp. 385–406).
13. Mangalraj, P. (2019). *Implications of Machine learning in Cyber Security*, WI '19 Companion, 142-143.
14. Vadivelan, N., Bhargavi, K., Kodati, S., & Nalini, M. (2022). Detection Of Cyber Attacks Using Machine Learning. In *AIP Conference Proceedings*. American Institute Of Physics. 2405(1), 030003.
15. Kumar, S., Singh, B. P., & Kumar, V. (2021). A Semantic Machine Learning Algorithm for Cyber Threat Detection and Monitoring Security. In *2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*.