Unlocking the Coverts: How “Machine Learning” is Revolutionizing Covert Communication

Veena N D[1]**, Anitha Devi M D**[2]

[1]Research Scholar, Department of Computer Science and Engineering, Sri Siddhartha Academy of Higher Education, Tumakuru, Karnataka, India

[2]Research Supervisor, Sri Siddhartha Academy of Higher Education, Tumakuru, Karnataka, India
Email: *veenand[at]ssit.edu.in*

Abstract: ***In the contemporary era characterized by pervasive digitization, wherein the preservation of privacy assumes paramount significance, both individuals and organizations are perpetually engaged in the pursuit of secure communication methodologies. The advent of “machine learning” has significantly impacted the field of covert communication, bringing about a revolutionary transformation in its operational dynamics. “machine learning”, a subfield of artificial intelligence, possesses the capacity to effectively process and analyze extensive volumes of data, thereby enabling the identification of intricate patterns that may elude human perception. The advent of this technology has ushered in a plethora of opportunities in the field of encryption, facilitating the development of robust and highly impregnable security systems. The continuous evolution of “machine learning” algorithms has led to significant advancements in covert communication methods. “machine learning” has emerged as a powerful tool for various applications, including the encryption of text messages and the secure exchange of sensitive emails. This technology has revolutionized the field by providing unparalleled levels of precision and efficiency in covert operations. The incorporation of “machine learning” techniques into covert communication has demonstrated notable advantages in the realm of countering cyber threats and safeguarding against unauthorized breaches of privileged information. By leveraging the capabilities of “machine learning”, organizations can proactively mitigate the risks posed by malicious actors aiming to compromise their sensitive data. This article aims to provide an in - depth analysis of “machine learning” and its profound impact on Covert communication. By examining its revolutionary capabilities, we will uncover the transformative effects it has on this field.***

Keywords: Covert Communication, “machine learning”, SVM, CNN

1. Introduction

In the contemporary era characterized by pervasive digitalization, wherein the preservation of privacy assumes paramount significance, both individuals and organizations are perpetually engaged in the pursuit of secure communication methodologies. “machine learning” has emerged as a pivotal technology in transforming the landscape of covert communication.

What is “machine learning” and how does it work?

“Machine learning”, a subfield within the realm of artificial intelligence, encompasses the advancement and refinement of algorithms that empower computers to acquire knowledge and conduct analysis on data sets without the need for explicit instructions or programming. According to the provided reference [2], it is evident that the user is requesting a specific action to Statistical techniques are employed in order to discern patterns, make predictions, and enhance performance through iterative processes. Through the process of training models on extensive datasets, “machine learning” algorithms possess the capability to acquire knowledge and adjust their behavior in response to novel information. This ability empowers them to effectively make precise decisions and predictions. According to the available literature, the user has provided a text for the purpose of rewriting it in a “Machine learning” algorithms operate through a fundamental mechanism known as "training. " In the course of this procedure, a model is provided with labeled data, denoting data that has already been categorized or classified. The underlying objective of the model is to comprehend the intricate patterns and interconnections inherent in the dataset, thereby generating a comprehensive framework of rules or parameters. These rules or parameters enable the model to effectively forecast outcomes or categorize instances in novel, unobserved data.

“Machine learning” has been observed to have a noteworthy impact on covert communication, primarily through its ability to enhance existing encryption techniques and bolster the overall security systems in place. Traditional encryption methods are predicated on the utilization of mathematical algorithms to obfuscate data, thereby rendering it unintelligible to individuals lacking proper authorization. Nevertheless, it is worth noting that the ever - increasing computing power has introduced potential vulnerabilities to the aforementioned encryption methods, rendering them susceptible to brute - force attacks or intricate hacking methodologies. “machine learning” algorithms, conversely, possess the capacity to analyze extensive quantities of data and discern patterns that may elude human perception [4]. This capability enables researchers to develop encryption techniques with increased resilience against attacks, thereby offering heightened levels of security.

“Machine learning” algorithms used for Covert communication

In the realm of covert communication, a multitude of “machine learning” algorithms are employed to bolster encryption methodologies, thereby fortifying the safeguarding of sensitive data and upholding the principle of data confidentiality. The Support Vector Machine (SVM) algorithm is a highly regarded method that has gained significant popularity in the field of “machine learning”. It is particularly renowned for its effectiveness in classification tasks, where the goal is to assign data points to predefined categories or classes. SVM has been widely adopted and utilized across various domains due to its robustness and ability to handle complex datasets. Support Vector Machines (SVM) is a “machine learning” algorithm that aims to identify the optimal hyperplane in a high - dimensional feature space. This hyperplane is strategically positioned to effectively separate different classes of data points. SVM has gained popularity due to its ability to accurately categorize and classify sensitive information, making it a valuable tool in various domains. [4] [5] [7]

The Random Forest algorithm, a frequently employed algorithm, operates by amalgamating numerous decision trees to generate predictions. The Random Forest algorithm is widely recognized for its adeptness in managing intricate datasets and delivering precise outcomes. Consequently, it has garnered considerable attention in the realm of Covert communication applications, where the need for accurate classification is of paramount importance.

In recent years, there has been a surge in the utilization of “Deep Learning” algorithms, specifically “Convolutional Neural Networks (CNN)” and “Recurrent Neural Networks (RNN)”, within the realm of Covert communication. The utilization of algorithms in data analysis enables the automatic extraction of features and acquisition of intricate patterns. Consequently, these algorithms prove to be highly suitable for various applications, including but not limited to image encryption and speech recognition. According to the provided reference [4], it is evident that further investigation is required in order to [5] [9]. According to the provided reference [15], it can be inferred that there is additional information or context that the incorporation of “machine learning” techniques into covert communication systems offers numerous benefits that significantly bolster security and privacy measures. “Machine learning” algorithms have the capability to perform real - time analysis of extensive datasets, thereby facilitating expedited and enhanced encryption procedures. In various contexts, particularly those involving time - sensitive and confidential communication, such as military operations or emergency responses, the significance of ensuring both expeditiousness and security cannot be overstated.

Furthermore, it is important to note that “machine learning” algorithms possess the remarkable capability to adapt and acquire knowledge from novel data, thereby endowing them with a high degree of resilience in the face of ever - evolving cyber threats. As the evolution of hacking techniques persists, it is imperative to explore the potential of “machine learning” in swiftly adapting and enhancing encryption methodologies to effectively mitigate these security breaches.

In addition, it is worth noting that “machine learning” techniques have the capability to effectively identify anomalies and promptly detect potential security breaches in real - time. Through the systematic analysis of network traffic, user behaviour, and pertinent data, “machine learning” algorithms possess the capability to discern atypical patterns or activities that could potentially signify a breach in security. The implementation of a proactive approach enables organizations to promptly address and mitigate the risk of unauthorized access to sensitive information. The present study undertakes a comprehensive examination of various methodologies and cutting - edge advancements documented in the existing body of literature pertaining to the subject matter. Section 2 of this paper elucidates the diverse techniques and state - of - the - art approaches that have been explored. Additionally, section 3 delves into the intricacies of the challenges and limitations encountered within this domain. Session 4 provides a concise overview of the potential utilization of “machine learning” in the development of algorithms for clandestine communication. Section 5 of the paper elucidates various real - world applications and delves into the ethical considerations associated with the subject matter. The authors meticulously analyze the practical implications of their research findings and shed light on the potential impact of their work in diverse domains. Furthermore, section 6 provides a comprehensive overview of the future directions and avenues for further exploration in this field. The authors highlight the need for continued investigation and propose potential research areas that could enhance our understanding and application of the subject matter.

2. Related Literature

Samson Ho, along with several other individuals, Based on the user's input, it appears that they have provided a reference or citation in the form of " [6]". This suggests that the user is referring to a specific source or piece of information that they have encountered in their research. However, without additional The objective of this study is to propose an “Intrusion Detection System (IDS) ” that utilizes “Convolutional Neural Network (CNN) ” technology in order to enhance the level of internet security. The proposed paradigm for Intrusion Detection Systems (IDS) involves the classification of network packet traffic into two distinct categories, namely benign and malicious. The primary objective of this approach is to effectively identify and detect instances of network intrusions. The model employed in this study was trained and validated utilizing the CICIDS2017 dataset, which was obtained from the esteemed “Canadian Institute for Cybersecurity”. The model has been subjected to a thorough evaluation, which includes assessing its overall accuracy, attack detection rate, false alarm rate, and training overhead. The effectiveness of the proposed model has been evaluated through comparisons with nine other widely recognized classifiers.

Praneeth Narisetty and his colleagues, in their study, conducted an investigation into the subject matter at hand. The user's text, denoted as " [7]", appears to be a reference or citation. According to the most recent “CICIDS2017 dataset”, various “machine learning” algorithms, including “support vector machines”, “artificial neural networks”, “convolutional neural networks”, “random forests” and ensemble learning algorithms, have received favorable evaluations. The performance of significant learning estimation was observed to be comparatively lower when compared to other popular “machine learning” algorithms such as “Support Vector Machines (SVM) ”, “Artificial Neural Networks (ANN) ”, “Random Forests (RF) ”, and “Convolutional Neural Networks (CNN) ”. The dataset will be utilized for the purpose of conducting port scanning attacks. These attacks, like other types of attacks, will be executed by harnessing the power of artificial intelligence and “machine learning” algorithms. To facilitate this process, Apache Hadoop and Spark technologies will be employed. The primary objective of this study is to ascertain the algorithm that exhibits the most optimal accuracy rates in predicting the likelihood of a cyberattack. The study assesses the performance of four distinct algorithms, namely “Support Vector Machines (SVM)”, “Artificial Neural Networks (ANN) ”, “Random Forests (RF) ”, and “Convolutional Neural Networks (CNN) ”, in order to determine the algorithm that exhibits the highest level of effectiveness.

Emrah Tufan et al. [7], esteemed researchers affiliated with the “Institute of Electrical and Electronics Engineers (IEEE)”, The present study investigates the phenomenon of network infiltration attempts through the utilization of anomaly - based “machine learning” algorithms. These algorithms offer a higher level of security in comparison to traditional misuse - based techniques. The dataset used in this study was acquired from a real institutional production environment. It was employed to develop and deploy two models: an ensemble learning model and a “convolutional neural network” model. The employed models were utilized in conjunction with the “UNSW - NB15” benchmarking dataset to showcase their efficacy and dependability. To delimit the scope of the investigation, the focus of this study was restricted to exploratory assaults. Based on the empirical evidence gathered from the data, it can be observed that the “CNN” model exhibited marginally higher accuracy rates, thereby suggesting its comparative advantage in terms of performance.

In their scholarly publication, Sarker et al. (2018) present a novel security model named "IntruDTree" that utilizes “machine learning” techniques for the purpose of intrusion detection. The proposed model integrates the consideration of the relative significance of security elements in order to develop a tree - based generalized intrusion detection model. The constructed model exclusively incorporates the predetermined significant features. The utilization of this particular model offers notable advantages in relation to its ability to accurately predict outcomes for test cases that have not been previously observed. This is achieved by effectively minimizing the computational complexity through the reduction of feature size. The effectiveness of the “IntruDTree model” was evaluated through the utilization of cybersecurity datasets. Performance metrics such as precision, recall, fscore, accuracy, and ROC scores were computed to gauge its efficacy.

To assess the efficacy of the security model, a comparative analysis is conducted between the “IntruDTree model” and several widely employed “machine learning” methodologies, including the naive “Bayes classifier, logistic regression, support vector machines, and k - nearest neighbour”.

In a study conducted by Mohamed M. and his colleagues [9], The present article advocates for the adoption of a dual - layer approach in the implementation of “Intrusion Detection Systems (IDS) ”. The primary layer of the network architecture is responsible for classifying the network connection based on the specific service being utilized. Following a thorough investigation, a succinct compilation of attributes that augment the precision in discerning deleterious conduct on the aforementioned platform has been unearthed. The second layer utilizes the aforementioned traits in order to categorize each network connection as either an attack or regular activity. This is achieved through the application of pattern recognition technique. In the training phase, the generation of two multivariate normal statistical models takes place. These models are specifically referred to as the normal behaviour model and the attack behaviour model. In the context of “network security”, the classification of network connections as either attack or normal activity is achieved through the utilization of two multivariate normal statistical models. These models are employed during the testing and operating phases of the system. The classification process is based on the maximum likelihood estimate function, which enables the determination of the most probable classification for each network connection. The obtained testing results provide evidence of the superior performance exhibited by the suggested “Intrusion Detection System (IDS) ” in the domain of network intrusion detection, when compared to other IDSs with similar functionalities. The system achieves a high Detection Rate (DR) of 97.5%, indicating its ability to accurately identify positive instances. The “False Acceptance Rate (FAR) ” is impressively low at 0.001, indicating a minimal rate of falsely accepting negative instances. The Matthews Correlation Coefficient (MCC) is calculated to be 95.7%, indicating a strong overall performance in terms of both true positive and true negative predictions. Moreover, the system achieves an impressive overall accuracy of 99.8%, showcasing its ability to correctly classify instances across the board. Notably, these impressive results are achieved by utilizing only four carefully selected characteristics.

3. Employing “Machine learning” and “Cyber Security”:

“Machine learning” in cyber security:

Connected systems in cyberspace exhibit susceptibility to a multitude of attack vectors, encompassing replay attacks, “man - in - the - middle attacks (MiTM)”, impersonation, credentials leakage, password guessing, session key leakage, unauthorized data update, malware injection, flooding, “denial of service (DoS)”, and “distributed denial of service (DDoS) ”. Therefore, in order to effectively detect and mitigate these attacks, it is crucial to establish a robust security framework. “machine learning” models have the potential to gain insights into various cyber - attacks through the utilization of pre - processed datasets, both in offline and online modes. The “machine learning” algorithms employed in this study have the capability to promptly identify and discern any indications of unauthorized access or intrusion, such as a cyberattack, in a live or online environment. The illustration presented in Figure 1 portrays the scenario of "“machine learning” in the field of “cyber security. In the given context, it is noteworthy that a networked device, encompassing various forms such as laptops, desktops, smartphones, and “Internet of Things (IoT) ” devices, holds the potential to facilitate a diverse array of online activities. These activities encompass but are not limited to conducting financial transactions, accessing healthcare data, and managing sensitive information such as social security numbers. Cybercriminals are constantly engaged in the pursuit of identifying vulnerabilities within various systems. Once these vulnerabilities are detected, they proceed to launch an attack. The detection and mitigation of cyber - attacks can be facilitated through the utilization of diverse “machine learning” methodologies. These methodologies encompass “supervised learning, unsupervised learning, reinforcement learning, and deep learning”. Each of these approaches can be applied in various contexts to effectively address the challenges posed by cyber - attacks.

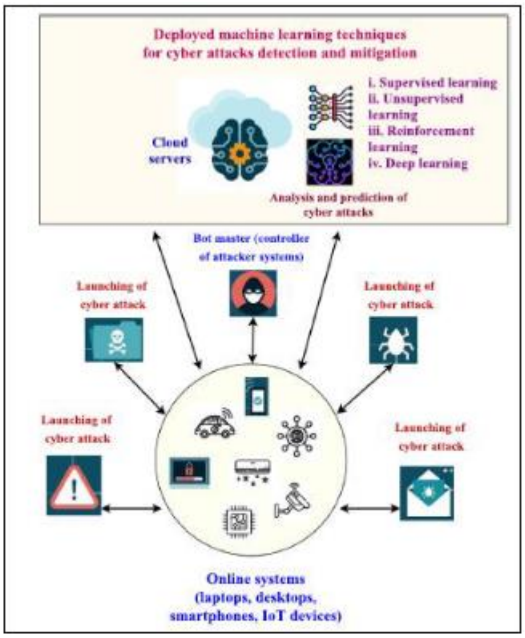
Deployed machine learning techniques for cyber attacks detection and mitigation
Cloud servers
i. Supervised learning
ii. Unsupervised learning
iii. Reinforcement learning
iv. Deep learning
Analysis and prediction of cyber attacks
Bot master (controller of attacker systems)
Launching of cyber attack
Launching of cyber attack
Launching of cyber attack
Launching of cyber attack
Online systems (laptops, desktops, smartphones, IoT devices)

Figure 1: Adoption of “machine learning” into cyber security

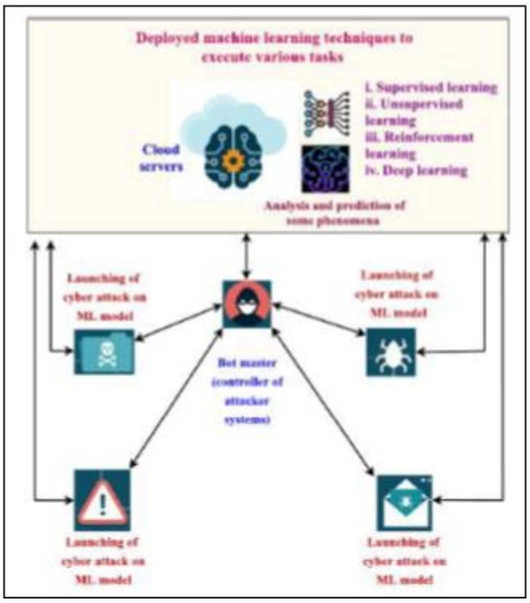
Deployed machine learning techniques to execute various tasks
Cloud servers
i. Supervised learning
ii. Unsupervised learning
iii. Reinforcement learning
iv. Deep learning
Analysis and prediction of some phenomena
Launching of cyber attack on ML model
Launching of cyber attack on ML model
Bot master (controller of attacker systems)
Launching of cyber attack on ML model
Launching of cyber attack on ML model

Figure 2: Adoption of cyber security in “machine learning”

The determination of the most appropriate technique, whether it be supervised learning, unsupervised learning, reinforcement learning, or deep learning, for a given system is contingent upon the characteristics of the communication environment and the availability of resources. Cloud servers provide a highly capable infrastructure for processing and storing data, thereby facilitating the application of “machine learning” methodologies to analyze and forecast potential security breaches.

“Cyber Security” in “Machine learning”:

Figure 2 presents an illustrative scenario that encapsulates the concept of “cyber security” in “machine learning”, commonly known as “machine learning” (ML) security. “machine learning” (ML) models are commonly employed in the field of research to analyze and make predictions about a wide range of events. However, it is important to note that certain categories of attacks, namely model poisoning disruption attacks and dataset poisoning attacks, possess the capability to significantly impair the effectiveness of “machine learning” models [6]. The potential consequences of these attacks encompass the capacity to induce inaccuracies in “machine learning” (ML) models, thereby affecting the predictive capabilities of said models in relation to the events in question. The phenomenon known as the "dataset poisoning attack" refers to a strategic approach employed by malicious actors to introduce adversarial samples, which are essentially modified values, into a given dataset. The primary objective of this attack is to deliberately manipulate the dataset in such a way that it leads to the production of inaccurate predictions by the “machine learning” (ML) model. The primary goal of the adversary in the context of the "model poisoning attack" is to compromise the integrity of the models by intervening in their internal mechanisms and modifying their configurations. The perpetrator is motivated to acquire valuable data from the model, while simultaneously endeavoring to expose confidential information through a "privacy breach attack. " The concept of a privacy breach encompasses the manifestation of a membership inference attack. In the context of “machine learning”, a “runtime disruption attack” refers to a malicious act where an attacker deliberately interferes with the execution process of a “machine learning” model. This interference is aimed at compromising the accuracy of the model's predicted results. Therefore, in order to mitigate these attacks, it is crucial to implement various cyber security methodologies, such as employing encryption techniques, utilizing signature generation and verification procedures, and employing hashing processes. The “machine learning” models and their corresponding datasets are protected through the implementation of robust cybersecurity measures, which are designed to maintain the integrity and confidentiality of the information. Moreover, the outcomes projected by these models demonstrate a notable level of precision and accuracy.

Challenges and limitations of “Machine learning” in “Covert communication”

“Machine learning”, as a cutting - edge technology, undoubtedly presents noteworthy benefits in the realm of covert communication. However, it is imperative to acknowledge and address the various challenges and limitations that accompany its implementation. One of the main challenges is the requirement for large amounts of labeled training data. Labeled data plays a crucial role in the efficacy of “machine learning” algorithms, as it serves as the foundation for the creation of accurate models. However, for “Covert communication”, obtaining large amounts of labeled data can be challenging due to the sensitive nature of the information being communicated. An additional constraint worth considering pertains to the possibility of adversarial attacks. Adversarial attacks encompass the deliberate manipulation of input data with the intention of deceiving “machine learning” algorithms and circumventing security measures. In the context of image encryption algorithms, it is plausible for an adversary to manipulate an image with the intention of deceiving said algorithm into performing decryption operations on it. The issue at hand is being actively addressed by researchers who are diligently working towards the development of robust “machine learning” models that exhibit resistance against adversarial attacks. In addition, it is worth noting that there exist valid concerns pertaining to the interpretability and explainability of “machine learning” algorithms. In the realm of “covert communication”, it is of utmost importance to possess a comprehensive understanding of the inner workings of encryption processes and to diligently ascertain their level of security. Nevertheless, it is worth noting that certain “machine learning” algorithms, particularly those based on deep learning architectures, have been commonly characterized as "black boxes" due to the inherent difficulty in comprehending the rationale behind their decision - making processes. The current focus of researchers centers around the advancement of explainable “machine learning” models, which aim to produce outcomes that are transparent and comprehensible.

4. Real - world applications and ethical considerations:

“Machine learning” has been widely utilized in various domains, including covert communication, leading to significant advancements in safeguarding sensitive data within organizations. An example of an application that can benefit from this technology is in the realm of email security. “Machine learning” algorithms have the capability to effectively analyze various components of emails, including their content, attachments, and metadata. This analytical process enables the detection and prevention of potentially harmful activities such as phishing attacks, malware infiltration, and other forms of malicious behaviour. Through the process of continuous learning, algorithms have the ability to assimilate knowledge from emerging threats, thereby enabling them to dynamically adjust and enhance security protocols. This adaptive approach empowers organizations to effectively safeguard themselves against the ever - evolving landscape of cyber threats.

An additional utilization of this technology pertains to the realm of secure messaging. “Machine learning” algorithms have the capability to perform text analysis on messages, enabling them to detect potential security risks. These risks may include the inadvertent sharing of sensitive information or the presence of suspicious language. The algorithms possess the capability to autonomously apply encryption to messages, utilizing predetermined rules or user - defined preferences, thereby guaranteeing the preservation of confidentiality for sensitive information.

Privacy is a prominent issue that has garnered significant attention and concern. The utilization of “machine learning” techniques has been demonstrated to have the potential to bolster security measures. However, it is important to acknowledge that the effective implementation of “machine learning” algorithms necessitates the availability of sensitive data for training purposes. It is imperative for organizations to prioritize the maintenance of data privacy and the safeguarding of individuals' personal information throughout their operations. An additional ethical consideration that warrants attention is the possibility of “machine learning” algorithms being misused. “Machine learning”, as a powerful tool, possesses the capability to safeguard sensitive information. However, it is important to acknowledge that it can also be employed in a manner that undermines privacy and security. It is imperative for organizations to exercise constant vigilance in order to ensure the responsible and legitimate utilization of “machine learning” algorithms.

Moreover, it is important to acknowledge that biases inherent in “machine learning” algorithms can give rise to significant ethical challenges when it comes to covert communication. When algorithms are trained using biased data, there is a potential for them to inadvertently perpetuate discriminatory practices or exhibit favoritism towards specific individuals or groups. It is imperative to undertake diligent measures in order to guarantee that “machine learning” models undergo training using datasets that encompass a wide range of variables and accurately represent the population. This is crucial in order to minimize bias and foster a sense of fairness within the models.

5. Conclusion

The advent of “machine learning” has brought about a significant transformation in the realm of covert communication, ushering in a new era of heightened security and privacy in the context of our modern digital landscape. Through the utilization of “machine learning” algorithms, organizations have the capacity to cultivate resilient encryption methodologies, identify and mitigate cyber threats, and guarantee the preservation of confidentiality for sensitive information. The incorporation of “machine learning” into “Covert communication”, nevertheless, presents a set of challenges and ethical considerations. The ethical and secure implementation of “machine learning” in Covert communication necessitates a meticulous consideration of data privacy, bias, and responsible use of algorithms.

The rapid advancement of “machine learning” techniques has opened up numerous opportunities for augmenting covert communication methods. The future holds promise for various exciting trends, including but not limited to quantum - safe encryption, integration with “blockchain technology”, and sentiment analysis. In summary, it can be stated that “machine learning” is playing a pivotal role in unraveling the intricacies of secure communication, thereby providing individuals and organizations with the means to safeguard their confidential data in the face of a progressively interconnected global landscape. By adopting this revolutionary technology, we can effectively protect privacy and guarantee the utmost confidentiality of our highly sensitive information.

6. Future trends and possibilities in “machine learning” for Covert communication

The domain of “machine learning” for covert communication is undergoing constant evolution, with numerous prospective trends and possibilities that exhibit potential for further advancements. An area of active investigation pertains to the advancement of quantum - safe encryption algorithms. As the capabilities of quantum computing continue to advance, there is a growing concern regarding the potential vulnerability of traditional encryption methods. The utilization of “machine learning” techniques holds promise in facilitating the advancement of encryption methodologies that exhibit resilience against quantum attacks, thereby guaranteeing enduring security measures. An additional emerging trend in the field of technology involves the amalgamation of “machine learning” techniques with other nascent technologies, notably “blockchain”. The utilization of “blockchain technology” offers a decentralized and immutable framework that ensures secure communication. By combining “machine learning” algorithms with “blockchain”, organizations can create robust and transparent security systems that ensure data integrity and confidentiality.

Moreover, it is worth noting that recent progress in the field of natural language processing and sentiment analysis holds great potential for bolstering the security of communication systems. This is achieved through the utilization of advanced algorithms and techniques that enable the analysis of the emotional tone and underlying intent conveyed within messages. By leveraging these advancements, it becomes possible to gain deeper insights into the true meaning and sentiment behind the exchanged information, thereby facilitating more effective and secure communication. “machine learning” algorithms have the capability to identify potential threats or suspicious behavior by analyzing linguistic cues, thereby offering an augmented level of security.

References

[1] Chauhan, D., and J. K. Jain. "A Journey from IoT to IoEA Journey from IoT to IoE. " International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278 - 3075.

[2] Z. Lv, L. Qiao, J. Li, H. Song, Deep - learning - enabled security issues in the internet of things, IEEE Internet Things J.8 (12) (2021) 9531–9538.

[3] Y. Wang, J. Yu, B. Yan, G. Wang, Z. Shan, BSV - PAGS: Blockchain based special vehicles priority access guarantee scheme, Comput. Commun.161 (2020) 28–40.

[4] N. Magaia, R. Fonseca, K. Muhammad, A. H. F. N. Segundo, A. V. Lira Neto, V. H. C. de Albuquerque, Industrial internet - of - things security enhanced with deep learning approaches for smart cities, IEEE Internet Things J.8 (8) (2021) 6393–6405.

[5] S. A. Parah, J. A. Kaw, P. Bellavista, N. A. Loan, G. M. Bhat, K. Muhammad, V. H. C. de Albuquerque, Efficient security and authentication for edge - based internet of medical things, IEEE Internet Things J.8 (21) (2021) 15652–15662.

[6] Ho, Samson, et al. "A novel intrusion detection model for detecting known and innovative cyberattacks using convolutional neural network. " IEEE Open Journal of the Computer Society 2 (2021): 14 - 25.

[7] Praneeth Narisetty, Pavan Narra "A “MACHINE LEARNING” APPROACH FOR DETECTING CYBERATTACKS IN NETWORKS", International Journal of Emerging Technologies and Innovative Research (www.jetir. org | UGC and issn Approved), ISSN: 2349 - 5162, Vol.9, Issue 6, page no. ppg26 - g31, June - 2022, Available at: http: //www.jetir. org/papers/JETIR2206605. pdf

[8] Tufan, Emrah, Cihangir Tezcan, and Cengiz Acartürk. "Anomaly - based intrusion detection by “machine learning”: A case study on probing attacks to an institutional network. " IEEE Access 9 (2021): 50078 - 50092.

[9] Sarker, Iqbal H., et al. "Intrudtree: a “machine learning” based cyber security intrusion detection model. " Symmetry 12.5 (2020): 754.

[10] Abdeldayem, Mohamed M. "Intrusion Detection System Based on Pattern Recognition. " Arabian Journal for Science and Engineering (2022): 1 - 9.

[11] Y. Sun, A. K. Bashir, U. Tariq, F. Xiao, Effective malware detection scheme based on classified behavior graph in IIoT, Ad Hoc Netw.120 (2021) 102558.

[12] J. Yang, Z. Bian, J. Liu, B. Jiang, W. Lu, X. Gao, H. Song, Noreference quality assessment for screen content images using visual edge model and AdaBoosting neural network, IEEE Trans. Image Process.30 (2021) 6801–6814.

[13] Y. Zhao, J. Yang, Y. Bao, H. Song, Trustworthy authorization method for security in industrial internet of things, Ad Hoc Netw.121 (C) (2021).

[14] T. S. Messerges, E. A. Dabbish, R. H. Sloan, Examining smart - card security under the threat of power analysis attacks, IEEE Trans. Comput.51 (5) (2002) 541–552.

[15] M. R. K. Soltanian, I. S. Amiri, Chapter 3 - problem solving, investigating ideas, and solutions, in: M. R. K. Soltanian, I. S. Amiri (Eds.), Theoretical and Experimental Methods for Defending Against DDOS Attacks, Syngress, 2016, pp.33–45.

[16] T. Lei, Z. Qin, Z. Wang, Q. Li, D. Ye, EveDroid: Event - aware android malware detection against model degrading for IoT devices, IEEE Internet Things J.6 (4) (2019) 6668–6680.

[17] J. Steinhardt, P. W. Koh, P. Liang, Certified defenses for data poisoning attacks, in: 31st International Conference on Neural Information Processing Systems, in: NIPS’17, Curran Associates Inc. Long Beach, California, USA, 2017, pp.3520–3532.

[18] M. Aladag, F. O. Catak, E. Gul, preventing data poisoning attacks by using generative models, in: 1st International Informatics and Software Engineering Conference, UBMYK, Ankara, Turkey, 2019, pp.1–5, http: //dx. doi. org/10.1109/UBMYK48245.2019.8965459.

[19] C. Huang, S. Chen, Y. Zhang, W. Zhou, J. J. P. C. Rodrigues, V. H. C. de Albuquerque, a robust approach for privacy data protection: IoT security assurance using generative adversarial imitation learning, IEEE Internet Things J. Volume 8, Issue 6, November - December - 2022 | http: //ijsrcseit. com

[20] Jay Kumar Jain et al Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., November - December - 2022, 8 (6): 374 - 385 385 (2021) 1, http: //dx. doi. org/10.1109/JIOT.2021.3128531.

[21] N. Papernot, P. McDaniel, X. Wu, S. Jha, A. Swami, Distillation as a defense to adversarial perturbations against deep neural networks, in: 2016 IEEE Symposium on Security and Privacy, 2016, pp.582–597, http: //dx. doi. org/10.1109/SP.2016.41.

[22] N. Papernot, A marauder’s map of security and privacy in “machine learning”, in: 11th ACM Workshop on Artificial Intelligence and Security, Toronto, Canada, 2018.

[23] S. Pirbhulal, W. Wu, K. Muhammad, I. Mehmood, G. Li, V. H. C. de Albuquerque, Mobility enabled security for optimizing IoT based intelligent applications, IEEE Netw.34 (2) (2020) 72–77.

[24] Chauhan, Dipti, Jay Kumar Jain, and Sanjay Sharma. "An end - to - end header compression for multihop IPv6 tunnels with varying bandwidth. " 2016 Fifth international conference on eco - friendly computing and communication systems (ICECCS). IEEE, 2016.

[25] Jain, Jay Kumar, Devendra Kumar Jain, and Anuradha Gupta. "Performance analysis of node - disjoint multipath routing for mobile ad - hoc networks based on QOS. " International Journal of Computer Science and Information Technologies 3.5 (2012): 5000 - 5004.

[26] Waoo, A., and Sanjay Sharma. "Threshold Sensitive Stable Election Multi - path Energy Aware Hierarchical Protocol for Clustered Heterogeneous Wireless Sensor Networks. " International Journal of Recent Trends in Engineering & Research 3.09 (2017): 158 - 16.

[27] Jain, Jay Kumar, and Sanjay Sharma. "Performance Evaluation of Hybrid Multipath Progressive Routing Protocol for MANETs. " International Journal of Computer Applications 71.18, 2023.

[28] Jain, Jay Kumar, and Akhilesh A. Waoo. "An Analytical Study of Energy Efficient Routing Approaches in Wireless Sensor Network. " THEETAS 2022: Proceedings of The International Conference on Emerging Trends in Artificial Intelligence and Smart Systems, THEETAS 2022, 16 - 17 April 2022, Jabalpur, India. European Alliance for Innovation, 2022.

[29] J. K. Jain, C. S. Dangi and D. Chauhan, "An Efficient Multipath Productive Routing Protocol for Mobile Ad - hoc Networks, " 2020 IEEE International Conference for Innovation in Technology (INOCON), 2020, pp.1 - 5, doi: 10.1109/INOCON50539.2020.9298291.