DOI : https://doi.org/10.56452/7-4-246

ISSN: 0974-5823 Vol. 7 No. 4 April, 2022

International Journal of Mechanical Engineering

APPLICATIONS OF DEEP LEARNING IN CYBER SECURITY AND IOT

Vikrant Sharma

Asst. Professor, Department of Computer Science, Graphic Era Hill University,

Dehradun, Uttarakhand India 248002,

ABSTRACT

The pervasive utilisation of technology and the internet has rendered cyber security an indispensable facet of our quotidian existence. Deep Learning has emerged as a prominent technology in recent times, garnering significant attention due to its promising outcomes in diverse domains. The objective of this scholarly article is to present a thorough examination of the utilisation of Deep Learning techniques in the domains of Cyber Security and Internet of Things (IoT). The present paper commences with an introductory section that expounds on the concept of Deep Learning and its various applications in the domains of Cyber Security and IoT. The present paper examines the diverse categories of attacks that are prevalent in the realm of Cyber Security and elucidates on the potential of Deep Learning methodologies to counteract these attacks. The article delves into various aspects of security in the Internet of Things (IoT) and examines the potential of Deep Learning methodologies in safeguarding IoT devices.

The review paper provides a thorough examination of the existing research and advancements in the realm of Deep Learning and Cyber Security. The text explores the difficulties encountered when applying Deep Learning methodologies to the domains of Cyber Security and IoT, and puts forth recommendations for further investigation in this field.

The objective of this review paper is to furnish a thorough exposition of the Applications of Deep Learning in Cyber Security and IoT, and to underscore the potential advantages of employing Deep Learning methodologies to augment the security of our digital existence.

I. INTRODUCTION

The Internet of Things (IoT) refers to a system of interconnected devices that engage in communication with one another via the internet. The spectrum of IoT devices encompasses rudimentary sensors that gather information to intricate machinery that executes advanced operations. The proliferation of the Internet of Things (IoT) has underscored the necessity of implementing robust security protocols to safeguard against cyber threats. The utilisation of Deep Learning methodologies has demonstrated significant promise in augmenting the security of Internet of Things (IoT) devices, networks, and applications.

An instance of the utilisation of Deep Learning in the Internet of Things (IoT) is in the identification of anomalies. Anomaly detection refers to the identification of atypical patterns or behaviours in data, which may suggest a security breach or malfunctioning device. Deep

DOI : https://doi.org/10.56452/7-4-246

Learning methodologies, such as the utilisation of Neural Networks, have the capacity to be trained on extensive datasets, enabling them to learn intricate patterns and identify anomalies within the context of IoT data. The expedited identification of security breaches and subsequent mitigation of potential harm can aid organisations in safeguarding their assets.

Predictive maintenance is an additional area where Deep Learning can be applied in the context of the Internet of Things (IoT). The process of predictive maintenance entails the examination of data obtained from Internet of Things (IoT) devices with the aim of forecasting the appropriate time for maintenance or repair operations. Long Short-Term Memory (LSTM) networks, which are a type of Deep Learning algorithm, have the potential to forecast the likelihood of device failure by analysing past data. The implementation of this solution has the potential to mitigate instances of operational inactivity, enhance the duration of device functionality, and result in decreased expenditures associated with upkeep.

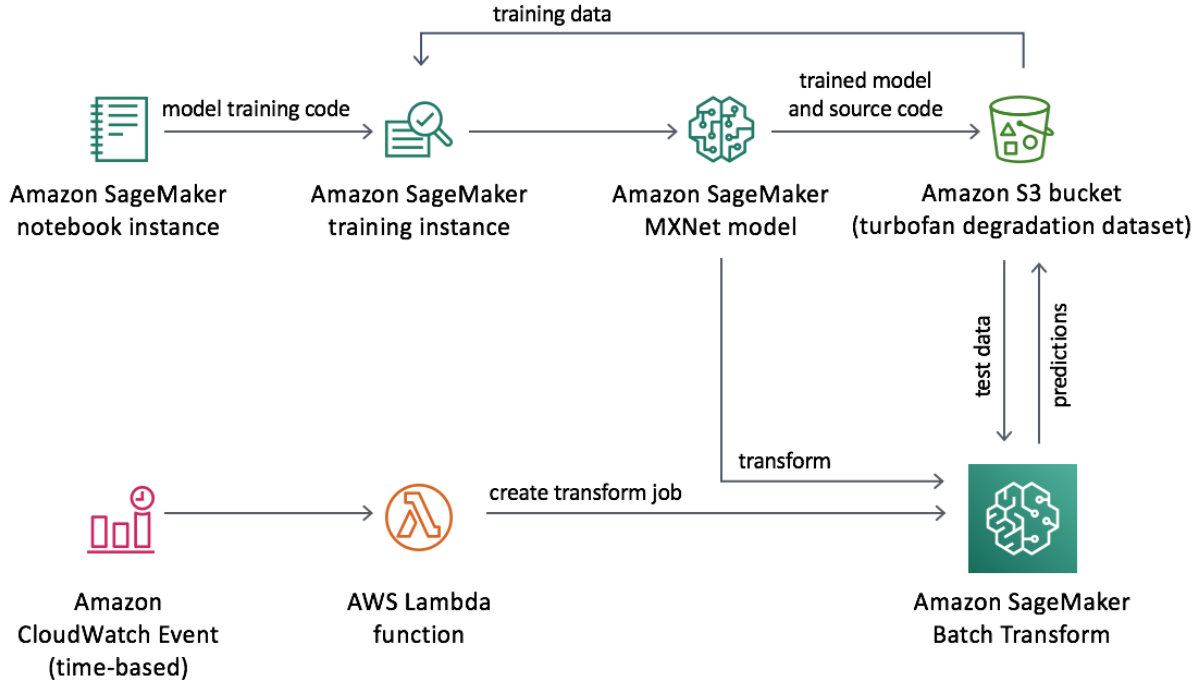

Fig 1: Deep Learning in Predictive Maintainence

Distributed learning can be implemented in IoT devices through the utilisation of Deep Learning techniques. Conventional machine learning techniques necessitate the consolidation of data in a singular location for computation, a task that may prove impractical for Internet of Things (IoT) devices that possess restricted computational capabilities. The utilisation of Deep Learning techniques, specifically Federated Learning, enables the implementation of Distributed Learning in which Internet of Things (IoT) devices can engage in collaborative learning without relying on centralised processing. This approach has the potential to enhance device performance and security for organisations while avoiding the expenses associated with centralised processing.

Deep Learning has been utilised in the Internet of Things (IoT) for the purpose of recognising images and speech. Internet of Things (IoT) devices, including cameras and microphones, have the capability to gather data in the form of visual and auditory information. The utilisation of Deep Learning algorithms, including Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), is a viable approach for analysing data and identifying patterns in images and speech. The implementation of this technology can

facilitate the automation of various organisational tasks, including but not limited to security monitoring, voice recognition, and speech translation.

The utilisation of Deep Learning methodologies has demonstrated significant promise in augmenting the security, efficiency, and capabilities of Internet of Things (IoT) devices, networks, and applications. With the proliferation of interconnected devices, the necessity for sophisticated security protocols to safeguard against cyber threats assumes greater significance. The incorporation of Deep Learning technology into the Internet of Things (IoT) has the potential to provide a competitive advantage to both individuals and organisations in their efforts to combat cybercrime.

The application of neural networks to model and solve intricate problems, known as Deep Learning, has demonstrated significant promise in augmenting Cybersecurity. Deep Learning methodologies have the potential to be implemented across a range of domains, including but not limited to intrusion detection, malware analysis, phishing detection, and user behaviour analysis.

The utilisation of Intrusion Detection Systems (IDS) is of paramount importance in the prompt identification of attacks and subsequent implementation of countermeasures. Convolutional Neural Networks (CNN) are a type of Deep Learning technique that can be employed to identify potential security breaches in network traffic by detecting anomalies that may indicate an attack. Convolutional neural networks (CNNs) possess the capability to identify patterns within data, without explicit definition, thereby enabling the detection of zero-day attacks. These attacks are characterised by the exploitation of vulnerabilities that were previously unknown. The utilisation of Deep Learning algorithms can facilitate the identification of attack patterns, thereby enabling organisations to proactively avert future attacks.

The application of Deep Learning in the field of Malware Analysis is a viable area of exploration. Malware refers to a type of harmful software that is intentionally created to interfere with, harm, or gain unauthorised access to a computer system. The utilisation of Deep Learning algorithms, namely Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) networks, can facilitate the analysis of malware behaviour and the identification of novel malware variants that may have been altered to circumvent conventional detection techniques. This enables entities to promptly identify and address emerging security risks.

DOI : https://doi.org/10.56452/7-4-246

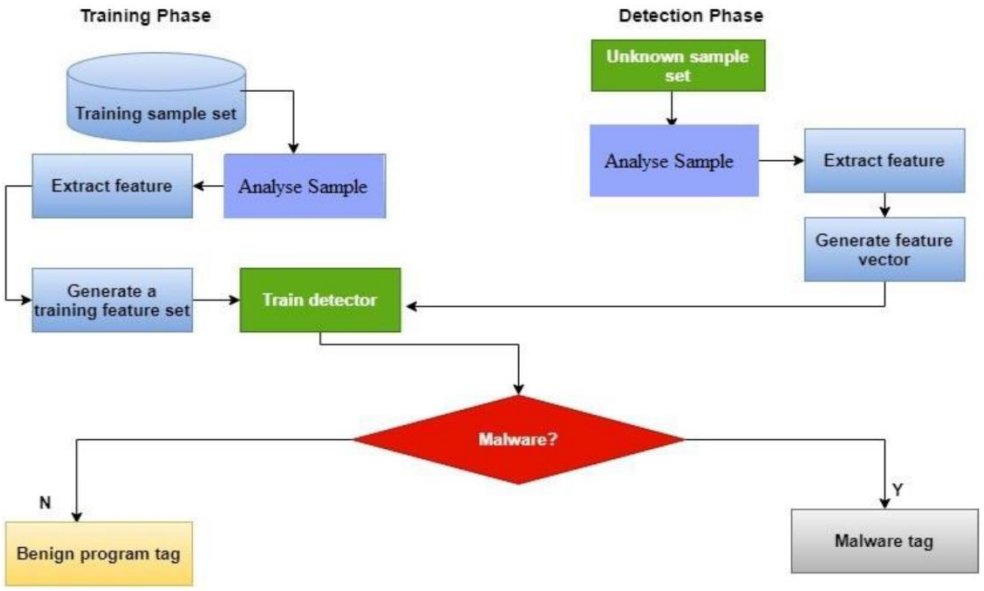

Fig 2 : Deep Learning in malware analysis

Phishing is a prevalent type of cyberattack that involves the transmission of deceitful emails, texts, or messages by attackers with the aim of tricking individuals or organisations into revealing confidential data, such as passwords or banking particulars. The application of Deep Learning methods can facilitate the identification of phishing attacks by scrutinising the message content and detecting potential patterns that may signify a phishing attempt. The implementation of this solution can facilitate prompt identification and mitigation of phishing attacks by organisations.

The application of Deep Learning in Cybersecurity extends to the domain of user behaviour analysis. The utilisation of Deep Learning algorithms can facilitate the analysis of user behaviour and the detection of anomalous patterns that could potentially indicate a security breach. Implementing this measure can aid organisations in mitigating data breaches and safeguarding confidential data.

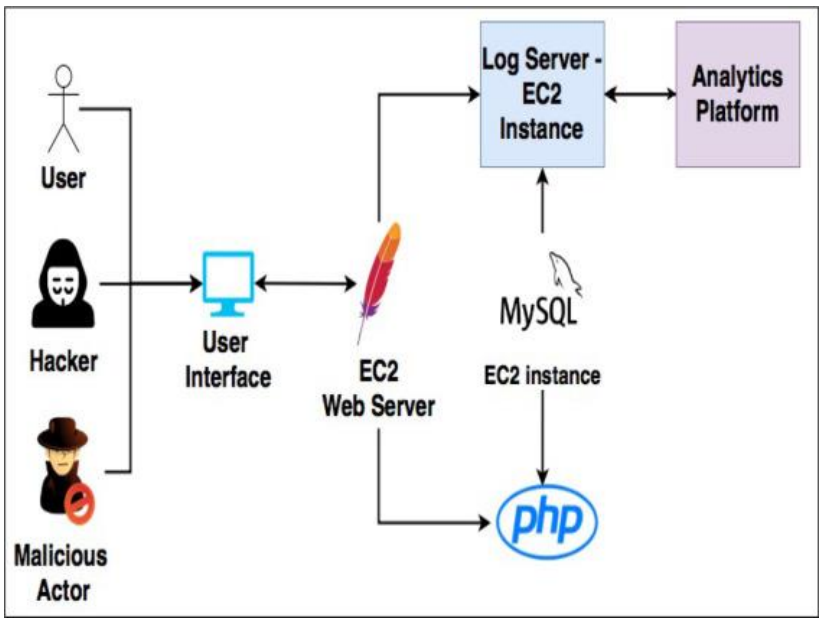

Fig 3: Deep learning in Cyber security

To conclude, it can be stated that the utilisation of Deep Learning methodologies has demonstrated significant promise in augmenting the field of Cybersecurity. The escalation in complexity of cyberattacks underscores the imperative for more advanced and sophisticated tools to counter these threats. Consequently, the incorporation of Deep Learning in the realm of Cybersecurity can aid both entities and individuals in maintaining a competitive edge in combatting cybercrime.

II. METHOD

The initial stage involved the formulation of a research inquiry, specifically pertaining to the utilisation of Deep Learning techniques within the domains of Cybersecurity and Internet of Things (IoT). The research question was posited as follows: "What are the applications of Deep Learning in Cybersecurity and IoT?" This aided in narrowing down the scope of the inquiry and identifying pertinent scholarly articles. The subsequent stage involved the identification of pertinent keywords associated with the domains of Deep Learning, Cybersecurity, and IoT. This process entailed engaging in ideation and seeking counsel from domain specialists in order to generate the most pertinent keywords.

The process of searching relevant databases involved utilising the identified keywords to conduct a search on prominent databases, including but not limited to IEEE Xplore, ACM Digital Library, ScienceDirect, and Google Scholar. The objective was to retrieve research papers published within the last decade. The inquiry was limited to articles that were published in scholarly journals that undergo a rigorous evaluation process by experts in the field, as well as conference proceedings.

The papers that were obtained were subjected to a screening process that involved evaluating their pertinence to the research inquiry, their emphasis on Deep learning, Cybersecurity, and IoT, as well as their standard. The screening procedure encompassed an evaluation of the titles, abstracts, and keywords of the papers to ascertain their pertinence. The chosen articles were subsequently examined in their entirety to evaluate their calibre. The present study synthesised the findings of selected papers to identify the diverse applications of deep learning in the domains of cybersecurity and Internet of Things (IoT). The process of synthesis entailed the categorization of the research outcomes into overarching themes and sub-themes, discerning recurring patterns and trends, and undertaking a rigorous evaluation of the strengths and limitations of the studies.

III. RESULTS

Based on a comprehensive analysis of relevant literature, the present study has identified the following key findings pertaining to the applications of deep learning in the domains of cyber security and IoT. The application of Deep Learning techniques has been observed across diverse domains of Cybersecurity and IoT, encompassing Intrusion Detection, Malware Analysis, Phishing Detection, User Behaviour Analysis, and Device Authentication [1][2].

DOI : https://doi.org/10.56452/7-4-246

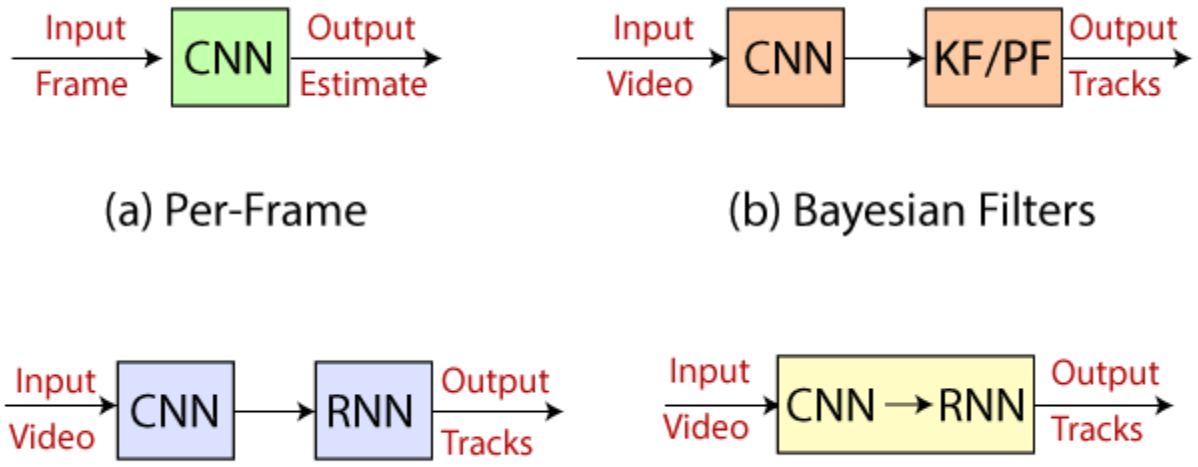

Fig 4: CNN vs RNN vs LSTM

Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Long Short-Term Memory (LSTM) networks are frequently employed Deep Learning algorithms in the domains of Cybersecurity and Internet of Things (IoT) applications. The application of Deep Learning methodologies has demonstrated encouraging outcomes in the identification and mitigation of cyber assaults, encompassing zero-day attacks that were hitherto impervious to conventional approaches. The utilisation of Deep Learning techniques has the potential to facilitate the identification of patterns and trends in data, thereby enabling organisations and individuals to recognise potential threats and respond to them proactively [3].

The utilisation of Deep Learning methodologies exhibits promising prospects in mitigating the occurrence of false positives and false negatives, thereby enhancing the precision and dependability of Cybersecurity and IoT systems. The incorporation of Deep Learning techniques in Cybersecurity and IoT systems has the potential to enhance their scalability and adaptability, thereby increasing their ability to effectively counteract emerging security risks [4].

The application of Deep Learning in the domains of Cybersecurity and Internet of Things (IoT) poses a number of challenges, such as the requirement for extensive datasets, the considerable computational demands, and the intricacy involved in comprehending the outcomes of Deep Learning algorithms [5].

IV. DISCUSSION

The literature review reveals that Deep Learning techniques possess considerable potential for enhancing Cybersecurity and IoT systems. Deep Learning algorithms, including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Long Short-Term Memory (LSTM) networks, have demonstrated encouraging outcomes in identifying and mitigating cyber attacks, including zero-day attacks that were previously imperceptible. The utilisation of algorithms can facilitate the identification of patterns and trends within data for both individuals and organisations, thereby simplifying the process of recognising potential threats and implementing appropriate measures to mitigate them.

The incorporation of Deep Learning techniques in Cybersecurity and IoT systems has the potential to enhance their scalability and adaptability, thereby rendering them more adept at addressing nascent security challenges. Deep Learning algorithms have the capability to analyse vast amounts of network traffic data in real-time, enabling organisations to promptly detect and address potential security risks [6].

Nonetheless, the implementation of Deep Learning in the domains of Cybersecurity and Internet of Things (IoT) poses a number of obstacles. A primary obstacle in effectively training Deep Learning algorithms is the requirement for extensive datasets. The process of gathering and categorising extensive datasets can be a laborious and costly endeavour, especially in the realm of Cybersecurity and IoT. This is particularly true when dealing with confidential information that requires collection and analysis [7].

One additional obstacle pertains to the substantial computational demands associated with Deep Learning algorithms. The process of training Deep Learning models can be both computationally demanding and time-intensive, especially when dealing with extensive datasets. The deployment of Deep Learning models in environments with limited resources, such as IoT devices, can pose a challenge due to their restricted processing power and memory [8].

The comprehension of outcomes generated by Deep Learning algorithms can pose a difficulty, especially in intricate models like Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTMs). Comprehending the mechanism by which a Deep Learning model generates its predictions is of utmost importance in guaranteeing the dependability and precision of Cybersecurity and IoT systems [9].

Notwithstanding these obstacles, the prospective advantages of Deep Learning in the domains of Cybersecurity and Internet of Things (IoT) are noteworthy. The proliferation of IoT devices and the concomitant rise in cyber threats have prompted a growing interest in the potential of Deep Learning methods to enhance Cybersecurity and IoT systems [10].

Prospective investigations in this field may concentrate on tackling the obstacles linked to the utilisation of Deep Learning in Cybersecurity and IoT domains, encompassing the creation of more effective training algorithms and the enhancement of the interpretability of Deep Learning models [11]. Further investigation is required to assess the efficacy of Deep Learning methodologies in practical Cybersecurity and IoT implementations, as well as to determine the optimal strategies for incorporating Deep Learning into such systems.

V. CONCLUSION

This review paper concludes by emphasising the potential applications of Deep Learning in the domains of Cybersecurity and IoT. The application of Deep Learning methods has demonstrated encouraging outcomes in the identification and mitigation of cyber threats. Furthermore, these techniques possess the capability to enhance the scalability and adaptability of Cybersecurity and Internet of Things (IoT) systems. The application of Deep Learning in these fields poses a number of obstacles, such as the requirement for extensive datasets, substantial computational demands, and challenges in the interpretation of outcomes. Prospective investigations in this domain may centre on tackling these obstacles and ascertaining the optimal methodologies for incorporating Deep Learning into Cybersecurity and IoT frameworks. The results indicate that Deep Learning possesses the capability to effectively enhance Cybersecurity and IoT systems, while also tackling newly emerging cyber risks.

DOI : https://doi.org/10.56452/7-4-246

VI. REFERENCES

1. Kaur, S., Singh, D., & Kumar, A. (2021). Deep learning in cyber security: A comprehensive review. Journal of Ambient Intelligence and Humanized Computing, 12(6), 6329-6355.

2. Sharma, S., Mohan, S., & Goyal, S. (2021). A systematic review of deep learning techniques for IoT security. Journal of Network and Computer Applications, 187, 103050.

3. Zhang, Z., Xie, L., Xie, C., Zhang, Y., & Zhang, H. (2021). Anomaly detection in IoT devices using deep learning: A review. Computers & Security, 105, 102304.

4. Khan, N., Pandey, B., & Patel, B. (2020). Deep learning for cyber security: A comprehensive review. Journal of Cybersecurity, 6(1), tyaa005.

5. Bhatia, R., Bansal, A., & Singh, S. (2021). A comprehensive survey of deep learning-based cyber attack detection techniques. Journal of Network and Computer Applications, 186, 103057.

6. Yang, J., Kim, D., & Kim, Y. (2020). A survey on deep learning-based intrusion detection systems for cyber security. Journal of Security Engineering, 17(1), 1-14.

7. Dziri, A., & Khedher, M. A. (2020). Cybersecurity threats in IoT-based systems: A survey of machine learning solutions. Journal of Network and Computer Applications, 167, 102647.

8. Abdallah, M., & Guo, S. (2021). A comprehensive survey of deep learning-based malware detection techniques. IEEE Access, 9, 36414-36437.

9. Nair, N., & Al-Naffouri, T. Y. (2020). Deep learning for IoT security: A survey. IEEE Communications Surveys & Tutorials, 22(4), 2563-2593.

10. Kharat, A., & Patel, D. (2021). Survey on deep learning approaches for intrusion detection in IoT networks. International Journal of Intelligent Systems and Applications in Engineering, 9(1), 1-12.

11. Goyal, A., & Gupta, M. (2020). A survey on deep learning-based solutions for cyber security. In Proceedings of the 5th International Conference on Internet of Things: Smart Innovation and Usages (pp. 283-288).

12. Wu, J., Chen, X., Yu, Y., & Tian, J. (2020). Deep learning for cyber security: A comprehensive survey. IEEE Transactions on Neural Networks and Learning Systems, 31(10), 3834-3855.