CONVOLUTIONAL LONG SHORT-TERM MEMORY FOR FILELESS MALWARE DETECTION

© COPYRIGHT UPM

By

KUNAPRASAN A/L KAREEGALAN

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Master of Science

April 2024

FSKTM 2024 9

All material contained within the thesis, including without limitation text, logos, icons, photographs and all other artwork, is copyright material of Universiti Putra Malaysia unless otherwise stated. Use may be made of any material contained within the thesis for non-commercial purposes from the copyright holder. Commercial use of material may only be made with the express, prior, written permission of Universiti Putra Malaysia.

Copyright © Universiti Putra Malaysia

© COPYRIGHT UPM

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Science

CONVOLUTIONAL LONG SHORT-TERM MEMORY FOR FILELESS MALWARE DETECTION

By

KUNAPRASAN A/L KAREEGALAN

April 2024

Chairman : Aziah binti Asmawi, PhD
Faculty : Computer Science and Information Technology

In the realm of cybersecurity, the rise of fileless malware presents a significant challenge to endpoint security. Traditional malware detection methods often fall short against these sophisticated attacks, necessitating the use of advanced techniques such as deep learning models. This study addresses the limitations of Bi-Directional Long Short-Term Memory (BLSTM) models in dynamic malware analysis and proposes enhancements through the Convolutional Long Short-Term Memory (ConvLSTM) architecture. BLSTM models are commonly used in dynamic malware analysis, where they process input sequences in both forward and backward directions, combining the results into a single output. This dual-layer approach enhances the model's ability to analyze data from multiple perspectives. However, the process is time-consuming, potentially increasing the window for successful fileless malware attacks.

© COPYRIGHT UPM

A key limitation of BLSTM models is the lack of parameter sharing between the forward and backward directions. This absence of shared parameters can restrict the model's ability to capture spatial and temporal features simultaneously, potentially reducing its effectiveness in detecting fileless malware attacks. To address these challenges, this study introduces the ConvLSTM model, which optimizes malware analysis by consolidating feature extraction within a single LSTM cell layer. ConvLSTM employs a two-dimensional approach, breaking down samples into subsequences and leveraging timesteps for additional feature extraction. This strategy enables the analysis of spatial-temporal data, enhancing the prediction accuracy of true malware instances.

Unlike traditional LSTM models, ConvLSTM integrates convolutional layers within its architecture, allowing for parameter sharing across both spatial and temporal dimensions. This approach reduces computational complexity and improves the model's performance in understanding multidimensional data structures. The research involved re-simulating existing work with the BLSTM model using the same malware dataset. The Spyder app was used to run the event simulator, and the results from previous work were replaced with those from the ConvLSTM model, applying the same parameters. Time, accuracy, and loss were selected as the primary performance metrics to assess the model's effectiveness. The ConvLSTM model demonstrated superior performance in detecting fileless malware, achieving a detection accuracy of 98% compared to BLSTM's 90%. ConvLSTM also significantly reduced processing time, averaging 10 seconds per completion, while BLSTM took 22

© COPYRIGHT UPM

seconds. Furthermore, ConvLSTM experienced lower losses, averaging 10% per epoch compared to BLSTM's 20%.

In conclusion, ConvLSTM represents a promising advancement in fileless malware detection, offering superior performance over traditional BLSTM models. Its ability to accurately identify and swiftly mitigate threats, coupled with enhanced computational efficiency, makes it a robust solution for fortifying endpoint security against evolving cyber threats. As the cybersecurity landscape continues to evolve, ConvLSTM holds significant potential in bolstering defense mechanisms against sophisticated malware attacks, providing a proactive approach to safeguarding enterprise networks and data assets.

Keywords: Fileless Malware Detection, Convolutional LSTM (ConvLSTM), Bi-Directional LSTM (BLSTM), Cybersecurity & Dynamic Malware Analysis

SDG: GOAL 9: Industry, Innovation, and Infrastructure

© COPYRIGHT UPM

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains

MEMORI PENJANAAN PANJANG PENDEK UNTUK PENGESANAN PERISIAN HASAD TANPA FAIL

Oleh

KUNAPRASAN A/L KAREEGALAN

April 2024

Pengerusi : Aziah binti Asmawi, PhD
Fakulti : Sains Komputer dan Teknologi Maklumat

Dalam bidang keselamatan siber, peningkatan perisian hasad tanpa fail memberikan cabaran besar kepada keselamatan titik akhir. Kaedah pengesanan perisian hasad tradisional sering gagal dalam menghadapi serangan canggih ini, yang memerlukan penggunaan teknik lanjutan seperti model pembelajaran mendalam. Kajian ini menangani batasan model Memori Jangka Pendek (BLSTM) Dwi Arah dalam analisis perisian hasad dinamik dan mencadangkan penambahbaikan melalui seni bina Memori Jangka Pendek Konvolusi (ConvLSTM). Model BLSTM biasanya digunakan dalam analisis perisian hasad dinamik, di mana ia memproses urutan input dalam kedua-dua arah ke hadapan dan ke belakang, menggabungkan keputusan menjadi satu output. Pendekatan dwi-lapisan ini meningkatkan keupayaan model untuk menganalisis data daripada pelbagai perspektif. Walau bagaimanapun, proses itu memakan masa, berpotensi meningkatkan tetingkap untuk serangan perisian hasad tanpa fail yang berjaya.

Had utama model BLSTM ialah kekurangan perkongsian parameter antara arah hadapan dan belakang. Ketiadaan parameter dikongsi ini boleh menyekat keupayaan model untuk menangkap ciri spatial dan temporal secara serentak, yang berpotensi mengurangkan keberkesanannya dalam mengesan serangan perisian hasad tanpa fail. Untuk menangani cabaran ini, kajian ini memperkenalkan model ConvLSTM, yang mengoptimumkan analisis perisian hasad dengan menyatukan pengekstrakan ciri dalam satu lapisan sel LSTM. ConvLSTM menggunakan pendekatan dua dimensi, memecahkan sampel kepada urutan dan memanfaatkan langkah masa untuk pengekstrakan ciri tambahan. Strategi ini membolehkan analisis data spatial-temporal, meningkatkan ketepatan ramalan kejadian perisian hasad sebenar.

Tidak seperti model LSTM tradisional, ConvLSTM menyepadukan lapisan konvolusi dalam seni binanya, membolehkan perkongsian parameter merentas kedua-dua dimensi spatial dan temporal. Pendekatan ini mengurangkan kerumitan pengiraan dan meningkatkan prestasi model dalam memahami struktur data berbilang dimensi.

Penyelidikan itu melibatkan simulasi semula kerja sedia ada dengan model BLSTM menggunakan set data perisian hasad yang sama. Apl Spyder telah digunakan untuk menjalankan simulator acara dan hasil daripada kerja sebelumnya telah digantikan dengan hasil daripada model ConvLSTM, menggunakan parameter yang sama. Masa, ketepatan dan kehilangan telah dipilih sebagai metrik prestasi utama untuk menilai keberkesanan model. Model ConvLSTM menunjukkan prestasi unggul dalam mengesan perisian

© COPYRIGHT UPM

hasad tanpa fail, mencapai ketepatan pengesanan sebanyak 98% berbanding 90% BLSTM. ConvLSTM juga telah mengurangkan masa pemprosesan dengan ketara, dengan purata 10 saat setiap selesai, manakala BLSTM mengambil masa 22 saat. Tambahan pula, ConvLSTM mengalami kerugian yang lebih rendah, dengan purata 10% setiap zaman berbanding 20% BLSTM.

Kesimpulannya, ConvLSTM mewakili kemajuan yang menjanjikan dalam pengesanan perisian hasad tanpa fail, menawarkan prestasi unggul berbanding model BLSTM tradisional. Keupayaannya untuk mengenal pasti dengan tepat dan mengurangkan ancaman dengan pantas, ditambah dengan kecekapan pengiraan yang dipertingkatkan, menjadikannya penyelesaian yang teguh untuk mengukuhkan keselamatan titik akhir terhadap ancaman siber yang berkembang. Memandangkan landskap keselamatan siber terus berkembang, ConvLSTM mempunyai potensi besar dalam memperkukuh mekanisme pertahanan terhadap serangan perisian hasad yang canggih, menyediakan pendekatan proaktif untuk melindungi rangkaian perusahaan dan aset data.

Kata Kunci: Pengesanan Perisian Hasad Tanpa Fail, LSTM Konvolusi (ConvLSTM), LSTM Dwi Arah (BLSTM), Keselamatan Siber, Analisis Perisian Hasad Dinamik

SDG: MATLAMAT 9 Industri, Inovasi, dan Infrastruktur Industri, Inovasi, dan Infrastruktur

© COPYRIGHT UPM

ACKNOWLEDGEMENTS

I would like to express my deepest appreciation to my supervisor Dr. Aziah Asmawi for helping me with this thesis. Her invaluable insights and expertise have been instrumental in shaping the direction and outcome of this research.

I would also like to extend my appreciation to my committee members wholeheartedly. Finally, I am deeply grateful to my family and friends for their unwavering support and encouragement throughout the course of this project.

© COPYRIGHT UPM

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Master of Science. The members of the Supervisory Committee were as follows:

Aziah binti Asmawi, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Mohd. Izuan Hafez bin Ninggal , PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Muhammad Daniel Hafiz bin Abdullah, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Mohd Taufik bin Abdullah, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

ZALILAH MOHD SHARIFF, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 7 November 2024

© COPYRIGHT UPM

Declaration by the Graduate Student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any institutions;
- intellectual property from the thesis and the copyright of the thesis are fully-owned by Universiti Putra Malaysia, as stipulated in the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from the supervisor and the office of the Deputy Vice-Chancellor (Research and innovation) before the thesis is published in any written, printed or electronic form (including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials) as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld in accordance with the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2015-2016) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software

Signature: ________________________ Date: ________________

Name and Matric No: Kunaprasan Kareegalan

© COPYRIGHT UPM

TABLE OF CONTENTS

© COPYRIGHT UPM

© COPYRIGHT UPM

© COPYRIGHT UPM

© COPYRIGHT UPM

LIST OF TABLES

© COPYRIGHT UPM

LIST OF FIGURES

© COPYRIGHT UPM

© COPYRIGHT UPM

LIST OF ABBREVIATIONS

BPTT	Backpropagation Through Time
BSLTM	Bi-Directional Long short-term memory
BYOD	Bring Your Own Device
CNN	Convolutional Neural Network
CNN-BLSTM	Convolutional neural network - Bi-Directional Long short-term memory
ConvLSTM	Convolutional Long short-term memory
EDR	Endpoint Detection & Response
FCLSTM	Fully Connected Long short-term memory
GRU	Gated Recurrent Unit
IDS	Intrusion Detection System
LAN	Local Area Network
LSTM	Long short-term memory
PS	PowerShell
RAM	Random Access Memory
RNN	Recurrent neural network
SAE	Security Architecture Environment
WMI	Windows Management Interface

© COPYRIGHT UPM

CHAPTER 1

INTRODUCTION

1.1 Endpoint Security

Endpoint Security protects endpoint devices such as laptops, mobile devices, desktops, and others, which serve as gateways to the enterprise network and can be exploited by attackers. Endpoint Security solutions defend entry points from vulnerable activities or harmful attacks. When organizations ensure endpoint compliance with data security standards, they also maintain greater control over the increasing number and various types of access points in the network. Devices like tablets, smartphones, or laptops are significant entry points for threats. The goal of endpoint security is to protect every endpoint connecting to the network, capable of blocking access and other vulnerable actions at these entry points.

As many organizations implement enterprise practices such as BYOD (Bring Your Own Device) and enable mobile/remote work, the boundary of Enterprise Network Security is fundamentally blurred. The requirement for active endpoint security methodologies has significantly increased, particularly with the rise of mobile threats. When employees depend on mobile devices, home personal computers, and laptops to establish connections to the organization's network and conduct business, centralized security measures are no longer sufficient for the current undefined security perimeter. This is why Endpoint Security has increased as a centralized security solution with additional

© COPYRIGHT UPM

defense at entry points for attacks and exit points for sensitive data. By ensuring that endpoint devices meet security standards before accessing the network, enterprises can exert greater control over the number of access points and more efficiently mitigate threats and attempts to gain unauthorized access. In addition to monitoring access, endpoint security tools offer capabilities such as monitoring and blocking vulnerable malicious activities.

1.2 Fileless Malware

In today's interconnected digital landscape, a significant and evolving threat to the integrity of endpoint security is presented by the rise of fileless malware. Unlike traditional malware variants, which rely on the presence of executable files stored on disk, fileless malware is operated entirely within a system's volatile memory, exploiting legitimate system processes and applications to execute malicious activities. This stealthy approach allows fileless malware to evade detection by conventional antivirus solutions, posing a formidable challenge to organizations seeking to safeguard their digital assets. The occurrence of fileless malware attacks continues to grow, driven by the increasing complexity of cybercriminals and their ability to exploit vulnerabilities in software and hardware ecosystems. These attacks target a wide range of endpoints, including desktops, laptops, mobile devices, and servers, making them particularly difficult to defend against. Moreover, fileless malware often exhibits polymorphic and obfuscated characteristics, further complicating detection and analysis efforts.

© COPYRIGHT UPM

Recognizing the urgent need for enhanced endpoint security, novel approaches to fileless malware detection and mitigation are being explored in this research. By dissecting the structure of fileless malware attacks and understanding their behavior patterns, proactive defense mechanisms are aimed to be developed that can identify and neutralize these threats in real-time. Through an in-depth analysis of fileless malware attack vectors and the development of innovative detection algorithms, organizations are required to be empowered with the tools and insights needed to bolster their cybersecurity posture. By cracking the nature of fileless malware and proposing effective countermeasures, efforts are being made to cover the way for a more strong and secure digital ecosystem.

In the following chapters, the methodology used to conduct this research will be delved into, detailing the experimental setup, data collection techniques, and analytical frameworks utilized. The findings of the investigation will also be presented, discussing their implications for endpoint security, and recommendations for future research and industry best practices will be proposed. Through this comprehensive exploration, contributions are aimed to be made to the ongoing efforts to combat fileless malware and fortify the defenses of organizations against emerging cyber threats. As the digital landscape continues to evolve, organizations face mounting pressure to safeguard their sensitive data and critical infrastructure from malicious actors. In recent years, fileless malware has emerged as a potent weapon in the arsenal of cybercriminals, enabling them to bypass traditional security measures and infiltrate networks with unprecedented stealth and

© COPYRIGHT UPM

sophistication. The insidious nature of fileless malware lies in its ability to exploit legitimate system processes and applications, making detection and remediation challenging for even the most advanced cybersecurity solutions. By residing solely in a system's memory and leveraging built-in functionalities, fileless malware can execute malicious code without leaving any traces on disk, thereby evading traditional signature-based detection mechanisms.

In response to this escalating threat landscape, this research seeks to delve deep into the mechanisms and behaviors of fileless malware, aiming to uncover vulnerabilities and develop effective mitigation strategies. By analyzing real-world attack scenarios and studying the tactics, techniques, and procedures (TTPs) employed by fileless malware actors, the study aims to provide organizations with actionable insights and best practices for defending against these stealthy threats. Through a combination of empirical research, data-driven analysis, and machine learning techniques, this study aims to advance the state-of-the-art in fileless malware detection and prevention. By leveraging cutting-edge technologies and methodologies, the study endeavor to equip organizations with the knowledge and tools needed to stay one step ahead of cyber adversaries and safeguard their digital assets in an increasingly hostile threat landscape.

Dynamic malware analysis is a crucial component of modern cybersecurity strategies, aimed at identifying and mitigating the ever-evolving threats posed by malicious software. Unlike static analysis techniques that examine the code of a program without executing it, dynamic analysis involves the live execution of malware within a controlled environment. This allows security analysts to

© COPYRIGHT UPM

observe the behavior of the malware as it interacts with a simulated system, providing valuable insights into its functionality and potential impact.

By analyzing the runtime behavior of malware, security professionals can better understand its capabilities, detect evasion techniques, and develop effective countermeasures to protect against future attacks. In this chapter, will be explore the principles, methodologies, and significance of dynamic malware analysis in safeguarding digital assets and networks against cyber threats.

1.3 Research Problem

Despite traditional malwares being expired, fileless malware has emerged as a more extensive threat to current network infrastructure, leveraging its ability to remain undetectable by modern security protections. Malicious payloads are injected directly into the memory (RAM) using JavaScript to execute malware code in web browsers without relying on common legitimate tools and applications. This susceptibility can lead to zero-day attacks, as the code and programs can be easily manipulated. To address this issue, dynamic malware analysis is conducted to gather data on malware behavior, running in isolated virtual environments to execute suspicious code captured from real users and test its impact on the host system using sandboxing.

Dynamic malware analysis typically employs deep learning models, such as Long Short-Term Memory (LSTM), for malware classification. LSTM is an artificial recurrent neural network (RNN) architecture commonly used in the field of deep learning. This approach analyzes past and future malware behavior sequences to classify possible zero-day attacks. Despite the success achieved using LSTM models in dynamic malware analysis, such as the Bidirectional LSTM model used by Weizhong Qiang, Lin Yang, Hai Jin (2022), but there are several unresolved challenges persist.

The BLSTM model reads input sequences in both forward and backward directions, combining the analyzed results into an output. This is achieved by combining two LSTM cells with opposite timings to the same output, creating a dual layer between the sequences. However, this process consumes more time to complete the analysis, potentially increasing the likelihood of successful files malware attacks. (Weizhong Qiang, Lin Yang, Hai Jin 2022).

The BLSTM model operates on spatial-temporal data structured in a 3D format: [samples, time steps, features]. It processes data both forward and backward using separate LSTM networks, but parameters are not shared between directions. This lack of parameter sharing may limit the model's effectiveness in capturing spatial and temporal features simultaneously, potentially impacting its accuracy in understanding data across both dimensions especially in detecting fileless malware attacks. (Weizhong Qiang, Lin Yang, Hai Jin 2022).

© COPYRIGHT UPM

1.4 Research Objective

1) We used ConvLSTM Model which shorten the process of malware analysis and reduce the time taken to increase the number of malware detectable.

2) We used four-dimensional approach which able to run the samples into single sequence input and produce output in accurate and better results on the prediction.

1.5 Research Scope

The scope of this research is:

This study aims to investigate the efficacy of Convolutional Long Short-Term Memory (ConvLSTM) architecture in enhancing dynamic malware analysis, particularly in detecting fileless malware threats. The research will focus on addressing the limitations of traditional Bi-Directional Long Short-Term Memory (BLSTM) models in capturing spatial and temporal features simultaneously. The scope encompasses the development and implementation of ConvLSTM-based malware detection models, alongside a comparative analysis with existing BLSTM models.

Key performance metrics such as detection accuracy, processing time, and loss rates will be evaluated to assess the effectiveness of ConvLSTM in mitigating fileless malware attacks. The research will utilize real-world malware datasets and employ simulation tools to conduct experiments and validate the findings. Additionally, the study aims to explore the potential of

© COPYRIGHT UPM

ConvLSTM in improving endpoint security measures and contributing to the advancement of cybersecurity technologies.

1.6 Research Questions:

1) Why Fileless Malware attacks are hard to detect and vulnerable?

Fileless Malware is hard to detect because usually the payload is the medium to execute a traditional malware attack but this attack directly injected the malicious code into the victim machine's memory. There is no code placed in the victim's machine. Besides, this attack using legitimate programs. There is nothing there to find but still, attack takes place. Current EDR solutions can detect malicious activity done by Fileless Malware through behavior scanning. Behavior scanning scans the legitimate programs that running or used for malicious activity but still fails when comes to the latest attack.

2) Does the current Fileless Malware solutions like Sandboxing is real-time?

Only known malwares are can be real real-time detection but for zero-day malware only can be detected using analyzing type detecting. Attackers are working to take over the machine as fast as they can so their malware injection and execution timing will try to archive maximum 99% real-time attack.

1.7 Research Contribution

This research makes significant contributions to the field of cybersecurity by addressing the escalating threat of fileless malware, which poses a formidable

© COPYRIGHT UPM

challenge to endpoint security. Traditional malware detection methods have proven ineffective against these sophisticated attacks, necessitating the exploration of advanced techniques. In response, this study introduces the Convolutional Long Short-Term Memory (ConvLSTM) architecture, a novel approach designed to enhance dynamic malware analysis. By consolidating feature extraction within a single LSTM cell layer, ConvLSTM aims to overcome the limitations of existing Bi-Directional Long Short-Term Memory (BLSTM) models.

The primary contribution of this research lies in its endeavor to optimize malware analysis processes through the implementation of ConvLSTM. By leveraging this innovative architecture, the study seeks to reduce processing time while simultaneously improving prediction accuracy for identifying genuine malware instances. Through a comparative evaluation between ConvLSTM and BLSTM models, the research aims to provide insights into the performance differences and efficacy of ConvLSTM in detecting fileless malware instances.

The findings of this study demonstrate promising results, indicating that ConvLSTM outperforms BLSTM in key metrics such as detection completion rate, processing time, and loss minimization. These results underscore the potential of ConvLSTM as an advanced solution for mitigating the threat of fileless malware and strengthening endpoint security measures. Overall, the contributions of this research lie in its innovative approach to addressing the challenges posed by fileless malware and advancing the capabilities of dynamic malware analysis through ConvLSTM architecture.

© COPYRIGHT UPM

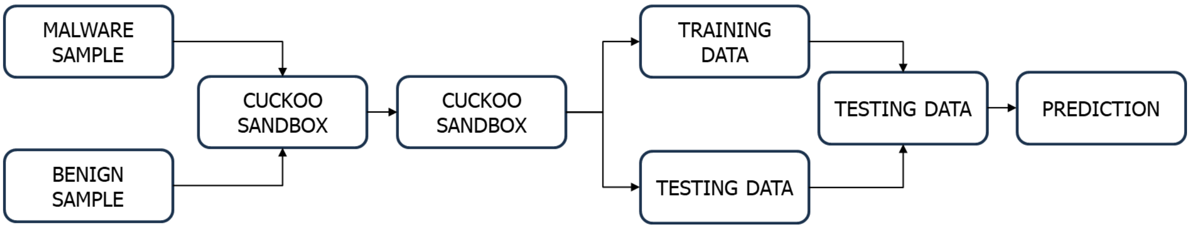

Figure 1.1: Overall Framework

From the framework, this research should be able to:

i. This able to increase layers in an LSTM capture progressively higher higher-level features in Deep Learning Dynamic Malware Analysis.

ii. Increase handling spatiotemporal correlations for malware behavior sequence.

iii. Archive more accuracy on malware behavior detection on zero-day attack.

iv. Reduce Overhead on entire analysis proceed and increase the response time.

© COPYRIGHT UPM

1.8 Thesis Organization

The remainder of the thesis is organized as follows:

Chapter 2: Presents a literature review, which includes an overview Types, Strength and Weakness of Fileless Malware, Deep Learning Techniques for mitigation. This chapter also discusses related research concerning the proposed ideas.

Chapter 3: Describes the research methodology, beginning with an overview of the research framework. It includes details on the experimental setups, topologies, requirements, performance metrics, and validation procedures.

Chapter 4: Details the Hybrid Deep Learning Approach by comparing existing/used models and explain how it works including flow of the design with Python Script explanation.

Chapter 5: Execute experiments with BLSTM and ConvLSTM, then discuss and compare the results with those from previous studies.

Chapter 6: Concludes the thesis and provides recommendations for potential future research directions.

© COPYRIGHT UPM

REFERENCES

Abdel-Hamid, O., Mohamed, A., Jiang, H., Deng, L., Penn, G., & Yu, D. (2014). Convolutional neural networks for speech recognition. *IEEE/ACM Transactions on Audio, Speech, and Language Processing, 22*(10), 1533-1545. https://doi.org/10.1109/TASLP.2014.2339736

Ahmad, R., Aslam, M., Ishfaq, M., & Hameed, S. (2023). An insight into the machine-learning-based fileless malware detection. *Sensors, 23*(2), 612. https://doi.org/10.3390/s23020612

Ahmad, R., et al. (2023). An Insight into the Machine-Learning-Based Fileless Malware Detection. *Sensors, 23*(2), 612. https://doi.org/10.3390/s23020612

Anderson, B., & McGlohon, M. (2018). Machine learning for malware detection. In *Journal of Computer Virology and Hacking Techniques* (Vol. 14, No. 1, pp. 33-54).

Anon. (2021). Classification Metrics Can’t Handle A Mix Of Multiclass And Continuous Targets - Design Corral. [online] Available at: https://designcorral.com/blog/classification-metrics-can-039-t-handle-a-mix-of-multiclass-and-continuous-targets/ [Accessed 29 Oct. 2022].

Arbelle, A., Cohen, S., & Raviv, T. R. (2022). Dual-Task ConvLSTM-UNet for instance segmentation of weakly annotated microscopy videos. *IEEE Transactions on Medical Imaging*, 1–1. https://doi.org/10.1109/tmi.2022.3152927

bio-protocol.org. (n.d.). BLSTM Architecture. [online] Available at: https://bio-protocol.org/bio101/r9316115 [Accessed 29 Oct. 2022].

Blisk1 (2019). powershell script in task manager. [online] Available at: https://www.reddit.com/r/PowerShell/comments/dtexun/powershell_script_in_task_manager/ [Accessed 29 Oct. 2022].

BLSTM recurrent neural network for object recognition. (2016). *Journal of Artificial Intelligence Practice*. https://doi.org/10.23977/jaip.2016.11005

Brownlee, J. (2017a). CNN Long Short-Term Memory Networks. [online] Machine Learning Mastery. Available at: https://machinelearningmastery.com/cnn-long-short-term-memory-networks/#:~:text=The%20CNN%20Long%20Short%2DTerm [Accessed 29 Oct. 2022].

Brownlee, J. (2017b). How to Develop a Bidirectional LSTM For Sequence Classification in Python with Keras. [online] Machine Learning Mastery. Available at: https://machinelearningmastery.com/develop-bidirectional-lstm-sequence-classification-python-keras/ [Accessed 29 Oct. 2022].

© COPYRIGHT UPM

Brownlee, J. (2018). How to Develop LSTM Models for Time Series Forecasting. [online] Machine Learning Mastery. Available at: https://machinelearningmastery.com/how-to-develop-lstm-models-for-time-series-forecasting/ [Accessed 29 Oct. 2022].

Brownlee, J. (2020). How to develop LSTM models for time series forecasting, MachineLearningMastery.com. Available at: https://machinelearning mastery.com/how-to-develop-lstm-models-for-time-series-forecasting/ (Accessed: 14 July 2023).

Chaudhary, S., Gautam, A., & Sharma, A. (2021). Deep learning-based malware detection: A review. *Journal of Information Security and Applications, 58*, 102820.

Chaudhary, S., Gautam, A., & Sharma, A. (2021). Deep learning-based malware detection: A review. *Journal of Information Security and Applications, 58*, 102820.

Chauhan, N. S. (2022). Introduction to RNN and LSTM. *The AI dream*. Retrieved from https://www.theaidream.com/post/introduction-to-rnn-and-lstm

Cho, K., Van Merriënboer, B., Bahdanau, D., & Bengio, Y. (2014). On the properties of neural machine translation: Encoder-decoder approaches. *arXiv preprint* arXiv:1409.1259.

Coleman, S.-P. W., & Hwang, Y.-S. (1970). Malware detection by Merging 1D CNN and bi-directional LSTM utilizing sequential data. *SpringerLink*. Retrieved from https://link.springer.com/chapter/10.1007/978-981-33-6385-4_16

Coleman, S.-P.W., & Hwang, Y.-S. (1970). Malware detection by merging 1D CNN and bi-directional LSTM utilizing sequential data. In *Proceedings of the International Conference on Artificial Intelligence and Computer Science* (pp. 16). Springer, Singapore. https://doi.org/10.1007/978-981-33-6385-4_16

Cybereason. (2019). Fileless Malware 101: Understanding Non-Malware Attacks. Retrieved June 6, 2024, from https://www.cybereason.com/blog/fileless-malware-101-understanding-non-malware-attacks

Dalal, K. R., & Rele, M. (2018). Cyber security: Threat detection model based on machine learning algorithm. In *2018 3rd International Conference on Communication and Electronics Systems (ICCES)* (pp. 239-243). IEEE. https://doi.org/10.1109/CESYS.2018.8724096

Deep Instinct. (2022). Prevent fileless malware. Retrieved June 6, 2024, from Deep Instinct website.

© COPYRIGHT UPM

Dey, P. et al. (2021) Comparative analysis of recurrent neural networks in stock price prediction for different frequency domains, MDPI. Available at: https://www.mdpi.com/1999-4893/14/8/251 (Accessed: 14 July 2023).

Dobilas, S. (2022). LSTM Recurrent Neural Networks — How to Teach a Network to Remember the Past. [online] Medium. Available at: https://towardsdatascience.com/lstm-recurrent-neural-networks-how-to-teach-a-network-to-remember-the-past-55e54c2ff22e [Accessed 29 Oct. 2022].

Fang, W., Pang, L., Yi, W., & Sheng, V. S. (2021). AttEF: Convolutional LSTM encoder-forecaster with attention module for precipitation nowcasting. *Intelligent Automation & Soft Computing, 29*(3), 453–466. https://doi.org/10.32604/iasc.2021.016589

ForcePoint (2018). What is Sandbox Security? [online] Forcepoint. Available at: https://www.forcepoint.com/cyber-edu/sandbox-security [Accessed 29 Oct. 2022].

Frontiers. (2023). Deep learning-powered malware detection in cyberspace: A contemporary review. *Frontiers in Artificial Intelligence and Applications*. Retrieved June 6, 2024, from Frontiers website.

Gers, F. A., Schmidhuber, J., & Cummins, F. (2000). Learning to forget: Continual prediction with LSTM. *Neural Computation, 12*(10), 2451-2471. https://doi.org/10.1162/089976600300015015

GitHub. (n.d.). Error: Classification metrics can't handle a mix of binary and continuous targets · Issue #169 · autonomio/talos. [online] Available at: https://github.com/autonomio/talos/issues/169 [Accessed 29 Oct. 2022].

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. In *Advances in Neural Information Processing Systems* (pp. 2672-2680).

Guo, F., Yang, J., Li, H., Li, G., & Zhang, Z. (2021). A ConvLSTM conjunction model for groundwater level forecasting in a karst aquifer considering connectivity characteristics. *Water, 13*(19), 2759. https://doi.org/10.3390/w13192759

He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 770-778).

Hinguruduwa, L. (2020). Setting up Cuckoo Sandbox For Dummies (Malware Analysis). [online] Medium. Available at: https://medium.com/@oshara.16/setting-up-cuckoo-sandbox-for-dummies-malware-analysis-3daa99e950b5 [Accessed 29 Oct. 2022].

© COPYRIGHT UPM

Hinton, G. E., & Salakhutdinov, R. R. (2006). Reducing the dimensionality of data with neural networks. *Science, 313*(5786), 504-507. https://doi.org/10.1126/science.1127647

Hinton, G. E., & Salakhutdinov, R. R. (2006). Reducing the dimensionality of data with neural networks. *Science, 313*(5786), 504-507.

Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural Computation, 9*(8), 1735-1780. https://doi.org/10.1162/neco.1997.9.8.1735

Hu, X., Liu, T., Hao, X., & Lin, C. (2022). Attention-based Conv-LSTM and Bi-LSTM networks for large-scale traffic speed prediction. *The Journal of Supercomputing*. https://doi.org/10.1007/s11227-022-04386-7

Huang, X., Xie, W., & Ma, J. (2019). Malware traffic classification based on temporal and spatial features. *Security and Communication Networks, 2019*, 1-13. https://doi.org/10.1155/2019/8312179

Infocyte. (2019). Why Traditional Endpoint Detection and Response (EDR) Platforms Can’t Detect File-less Malware. [online] Available at: https://www.infocyte.com/blog/2019/12/04/why-traditional-endpoint-detection-and-response-edr-platforms-cant-detect-file-less-malware/ [Accessed 29 Oct. 2022].

Intezer. (2023). What is Fileless Malware? Explained, with Examples. Retrieved June 6, 2024, from https://www.intezer.com/blog/malware-analysis/what-is-fileless-malware-explained-with-examples/

Ioffe, S., & Szegedy, C. (2015). Batch normalization: Accelerating deep network training by reducing internal covariate shift. In *Proceedings of the 32nd International Conference on Machine Learning* (Vol. 37, pp. 448-456).

ISACA. (2023). Understanding the threat of fileless malware. Retrieved June 6, 2024, from https://www.isaca.org/resources/news-and-trends/industry-news/2023/understanding-the-threat-of-fileless-malware

Ito, R., & Mimura, M. (2019). Detecting unknown malware from ASCII strings with natural language processing techniques. In *2019 14th Asia Joint Conference on Information Security (AsiaJCIS)* (pp. 1-8). IEEE. https://doi.org/10.1109/AsiaJCIS.2019.00-12

Jamalpur, S., Navya, Y. S., Raja, P., Tagore, G., & Rao, G. R. K. (2018). Dynamic malware analysis using Cuckoo Sandbox. In *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)* (pp. 1056-1060). IEEE. https://doi.org/10.1109/ICICCT.2018.8473346

Jason, K. (2014). What is Endpoint Security? Data Protection 101. [online] Digital Guardian. Available at: https://digitalguardian.com/blog/what-endpoint-security-data-protection-101 [Accessed 29 Oct. 2022].

© COPYRIGHT UPM

John (2019). Traditional Antivirus vs. EDR (Endpoint Detection and Response). [online] Cybriant. Available at: https://cybriant.com/antivirus-vs-edr/ [Accessed 29 Oct. 2022].

Kara, B., & Tjahjadi, T. (2022). Efficient and robust malware detection based on control flow traces using deep neural networks. *Computers & Security, 124*, 102871. https://doi.org/10.1016/j.cose.2022.102871

Keydana, S. (2020). RStudio AI Blog: Convolutional LSTM for spatial forecasting. blogs.rstudio.com. [online] Available at: https://blogs.rstudio.com/ai/posts/2020-12-17-torch-convlstm/ [Accessed 29 Oct. 2022].

Kim, K.-J. and Tagkopoulos, I. (2019a) Application of machine learning in rheumatic disease research, The Korean journal of internal medicine. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6610179/ (Accessed: 23 September 2023).

Kim, K.-J., & Tagkopoulos, I. (2019a). Application of machine learning in rheumatic disease research. *The Korean Journal of Internal Medicine*. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6610179/

Kim, S., Kang, B., & Kang, S. (2018). A study on a CNN-LSTM based model for detecting anomalous network traffic. *International Journal of Advanced Computer Science and Applications, 9*(4), 37-42. https://doi.org/10.14569/IJACSA.2018.090406

Kishore, P., Barisal, S. K., & Mohapatra, D. P. (2020). JavaScript malware behaviour analysis and detection using sandbox assisted ensemble model. In *2020 IEEE Region 10 Conference (TENCON)* (pp. 864-869). IEEE. https://doi.org/10.1109/TENCON50793.2020.9293847

Kohavi, R. (1995). A study of cross-validation and bootstrap for accuracy estimation and model selection. In *Proceedings of the 14th International Joint Conference on Artificial Intelligence* (Vol. 2, pp. 1137-1143).

Kolosnjaji, B., Zarras, A., Webster, G., & Eckert, C. (2016). Deep learning for classification of malware system call sequences. In B. H. Kang & Q. Bai (Eds.), *AI 2016: Advances in Artificial Intelligence* (Vol. 9992, pp. 137-153). Springer, Cham. https://doi.org/10.1007/978-3-319-50127-7_11

Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). Imagenet classification with deep convolutional neural networks. *Advances in Neural Information Processing Systems* (pp. 1097-1105). MIT Press.

Kumar, N., Mukhopadhyay, S., Gupta, M., Handa, A., & Shukla, S. K. (2019). Malware classification using early stage behavioral analysis. In *2019 14th Asia Joint Conference on Information Security (AsiaJCIS)* (pp. 16-23). IEEE. https://doi.org/10.1109/AsiaJCIS.2019.00-10

© COPYRIGHT UPM

Kurakin, A., Goodfellow, I., & Bengio, S. (2016). Adversarial examples in the physical world. *arXiv preprint* arXiv:1607.02533.

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature, 521*(7553), 436-444. https://doi.org/10.1038/nature14539

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature, 521*(7553), 436-444.

LeCun, Y., Bottou, L., Bengio, Y., & Haffner, P. (1998). Gradient-based learning applied to document recognition. *Proceedings of the IEEE, 86*(11), 2278-2324. https://doi.org/10.1109/5.726791

Li, D., Sun, L., Xu, X., Wang, Z., Zhang, J., & Du, W. (2021). BLSTM and CNN Stacking Architecture for Speech Emotion Recognition. Neural Processing Letters, 53(6), pp.4097–4115. doi:10.1007/s11063-021-10581-z.

Lipton, Z. C. (2016). The mythos of model interpretability. *Queue, 14*(3), 31-57. https://doi.org/10.1145/3236386.3241340

Lipton, Z. C., Berkowitz, J., & Elkan, C. (2015). A critical review of recurrent neural networks for sequence learning. *arXiv preprint* arXiv:1506.00019.

Liu, Y., & Wang, Y. (2019). A robust malware detection system using deep learning on API calls. In *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)* (pp. 1456-1460). IEEE. https://doi.org/10.1109/ITNEC.2019.8728992

LSTM RNN in tensorflow - javatpoint (no date) www.javatpoint.com. Available at: https://www.javatpoint.com/long-short-term-memory-rnn-in-tensorflow (Accessed: 23 September 2023).

LSTM RNN in TensorFlow (n.d.). *javatpoint*. Retrieved from https://www.javatpoint.com/long-short-term-memory-rnn-in-tensorflow

Matrix Education (2019). Validity vs Reliability vs Accuracy in Physics Experiments. [online] Matrix Education. Available at: https://www.matrix.edu.au/the-beginners-guide-to-physics-practical-skills/physics-practical-skills-part-2-validity-reliability-accuracy-experiments/ [Accessed 29 Oct. 2022].

Menahem, E. (2020). Sandboxing is Limited. Here’s Why and How to Best Stop Zero-Day Threats. [online] Cato Networks. Available at: https://www.catonetworks.com/blog/sandboxing-is-limited-heres-why-and-how-to-best-stop-zero-day-threats [Accessed 29 Oct. 2022].

Miguel, T. (2021). How the LSTM improves the RNN. [online] Medium. Available at: https://towardsdatascience.com/how-the-lstm-improves-the-rnn-1ef156b75121 [Accessed 29 Oct. 2022].

© COPYRIGHT UPM

Mittal, A. (2019). Understanding RNN and LSTM. [online] Medium. Available at: https://aditi-mittal.medium.com/understanding-rnn-and-lstm-f7cdf6dfc14e [Accessed 29 Oct. 2022].

Norton. (2018). What is fileless malware and how does it work? Retrieved June 6, 2024, from https://us.norton.com/blog/how-to/what-is-fileless-malware-and-how-does-it-work

O'Connor, F. (2017). Fileless Malware 101: Understanding Non-Malware Attacks. [online] Cybereason.com. Available at: https://www.cybereason.com/blog/fileless-malware [Accessed 29 Oct. 2022].

Ocatak, O. (2019). LSTM Malware Detection Dataset [Data set]. GitHub. https://github.com/ocatak/lstm_malware_detection

Olah, C. (2015). Understanding LSTM Networks -- colah's blog. [online] Github.io. Available at: https://colah.github.io/posts/2015-08-Understanding-LSTMs/ [Accessed 29 Oct. 2022].

Pan, S. J., & Yang, Q. (2010). A survey on transfer learning. *IEEE Transactions on Knowledge and Data Engineering, 22*(10), 1345-1359. https://doi.org/10.1109/TKDE.2009.191

Panda, R. (2022). ConvLSTM. [online] GitHub. Available at: https://github.com/rohitpanda2022/ConvLSTM [Accessed 29 Oct. 2022].

paperswithcode.com. (n.d.). Papers with Code - ConvLSTM Explained. [online] Available at: https://paperswithcode.com/method/convlstm#:~:text=ConvLSTM%20is%20a%20type%20of [Accessed 29 Oct. 2022].

Qiang, W., Yang, L., & Jin, H. (2022). Efficient and robust malware detection based on control flow traces using deep neural networks. *Computers & Security, 122*, 102871. https://doi.org/10.1016/j.cose.2022.102871

Quora.com. (2015). What is the difference between ConvLSTM and CNN LSTM? - Quora. [online] Available at: https://www.quora.com/What-is-the-difference-between-ConvLSTM-and-CNN-LSTM [Accessed 7 Sep. 2019].

Raff, E., Barker, J., Sylvester, J., Brandon, R., Catanzaro, B., & Nicholas, C. (2018). Malware detection by eating a whole EXE. In *Proceedings of the AAAI Conference on Artificial Intelligence* (Vol. 32, No. 1).

Rahman, S. A., & Adjeroh, D. A. (2019). Deep learning using convolutional LSTM estimates biological age from physical activity. *Scientific Reports, 9*(1). https://doi.org/10.1038/s41598-019-46850-0

Ray, A., Rajeswar, S., & Chaudhury, S. (2015). Text recognition using deep BLSTM networks. 2015 Eighth International Conference on Advances in Pattern Recognition (ICAPR). doi:10.1109/icapr.2015.7050699.

© COPYRIGHT UPM

Saxe, J., & Berlin, K. (2015). Deep neural network based malware detection using two-dimensional binary program features. In *Proceedings of the 10th International Conference on Malicious and Unwanted Software (MALWARE)* (pp. 11-20).

Scherer, D., Müller, A., & Behnke, S. (2010). Evaluation of pooling operations in convolutional architectures for object recognition. In *International conference on artificial neural networks* (pp. 92-101). Springer, Berlin, Heidelberg.

Sciencedirect.com. (2022). [online] Available at: https://www.sciencedirect.com/science/article/pii/S2212827122003948/pdf?md5=0a961940f59df7ec048691115c84b271&pid=1-s2.0-S2212827122003948-main.pdf [Accessed 29 Oct. 2022].

Server Fault. (n.d.). windows server 2012 r2 - powershell scheduled task always shows running even once completed. [online] Available at: https://serverfault.com/questions/798093/powershell-scheduled-task-always-shows-running-even-on [Accessed 29 Oct. 2022].

Sharma, P. (2023) Training neural network with Keras and basics of Deep Learning, Analytics Vidhya. Available at: https://www.analyticsvidhya.com/blog/2021/11/training-neural-network-with-keras-and-basics-of-deep-learning/ (Accessed: 23 September 2023).

Sharma, P. (2023). Training neural network with Keras and basics of Deep Learning. *Analytics Vidhya*. Retrieved from https://www.analyticsvidhya.com/blog/2021/11/training-neural-network-with-keras-and-basics-of-deep-learning/

Shi, X., Chen, Z., Wang, H., Yeung, D.-Y., Wong, W.-K., Woo, W.-C., & Kong Observatory, H. (n.d.). Convolutional LSTM Network: A Machine Learning Approach for Precipitation Nowcasting. [online] Available at: https://proceedings.neurips.cc/paper/2015/file/07563a3fe3bbe7e3ba84431ad9d055af-Paper.pdf [Accessed 29 Oct. 2022].

Shin, H. C., Roth, H. R., Gao, M., Lu, L., Xu, Z., Nogues, I., ... & Summers, R. M. (2016). Deep convolutional neural networks for computer-aided detection: CNN architectures, dataset characteristics and transfer learning. *IEEE transactions on medical imaging, 35*(5), 1285-1298.

Singh, J., & Singh, J. (2018). Challenges of malware analysis: Obfuscation techniques. Retrieved from https://api.semanticscholar.org/CorpusID:53572683

Sinha, N. (2018) Understanding LSTM and its quick implementation in Keras for sentiment analysis., Medium. Available at: https://towardsdatascience.com/understanding-lstm-and-its-quick-implementation-in-keras-for-sentiment-analysis-af410fd85b47 (Accessed: 14 July 2023).

Sinha, N. (2018). Understanding LSTM and its quick implementation in Keras for sentiment analysis. *Medium*. Retrieved from https://towardsdatascience.com/understanding-lstm-and-its-quick-implementation-in-keras-for-sentiment-analysis-af410fd85b47

Soni, M. (2018) Understanding architecture of LSTM cell from scratch with code., HackerNoon. Available at: https://hackernoon.com/understanding-architecture-of-lstm-cell-from-scratch-with-code-8da40f0b71f4 (Accessed: 14 July 2023).

Soni, M. (2018). Understanding architecture of LSTM cell from scratch with code. *HackerNoon*. Retrieved from [https://hackernoon.com /understanding-architecture-of-lstm-cell-from-scratch-with-code-8da40f0b71f4](https://hackernoon.com/understanding-architecture-of-lstm-cell-from-scratch-with-code-8da40f0b71f4)

SpringerOpen. (2019). An emerging threat: Fileless malware: A survey and research challenges. *SpringerOpen*.

Srivastava, N., Hinton, G., Krizhevsky, A., Sutskever, I., & Salakhutdinov, R. (2014). Dropout: A simple way to prevent neural networks from overfitting. *Journal of Machine Learning Research, 15*(1), 1929-1958.

Stack Overflow. (n.d.). python - Confusion Matrix ValueError: Classification metrics can’t handle a mix of binary and continuous targets. [online] Available at: https://stackoverflow.com/questions/69875073/confusion-matrix-valueerror-classification-metrics-cant-handle-a-mix-of-binary [Accessed 29 Oct. 2022].

Stack Overflow. (n.d.). python - Keras AttributeError: ‘Sequential’ object has no attribute ‘predict_classes’. [online] Available at: https://stackoverflow.com/questions/68836551/keras-attributeerror-sequential-object-has-no-attribute-predict-classes [Accessed 29 Oct. 2022].

Syed, F., Di Sipio, R., & Sinervo, P. (2019). Bidirectional Long Short-Term Memory (BLSTM) neural networks for reconstruction of top-quark pair decay kinematics. arXiv:1909.01144 [hep-ex, physics:physics]. [online] Available at: https://arxiv.org/abs/1909.01144 [Accessed 29 Oct. 2022].

© COPYRIGHT UPM

Szegedy, C., Liu, W., Jia, Y., Sermanet, P., Reed, S., Anguelov, D., ... & Rabinovich, A. (2015). Going deeper with convolutions. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 1-9).

Tan, M., & Le, Q. (2019). EfficientNet: Rethinking model scaling for convolutional neural networks. In *International Conference on Machine Learning* (pp. 6105-6114).

TechAdvisory. (2023). The stealthy intruder: Understanding fileless malware. Retrieved June 6, 2024, from https://www.techadvisory.org/2023/01/understanding-fileless-malware/

TensorFlow. (n.d.). tf.keras.layers.ConvLSTM2D | TensorFlow v2.10.0. [online] Available at: https://www.tensorflow.org/api_docs/python/tf/keras/layers /ConvLSTM2D [Accessed 29 Oct. 2022].

The format provided earlier includes elements from APA but needs some corrections to fully comply with APA standards. Below is the corrected version in APA format with access dates:

Verma, Y. (2021). Complete Guide to Bidirectional LSTM (with python codes), Analytics India Magazine. Available at: https://analyticsindiamag.com/complete-guide-to-bidirectional-lstm-with-python-codes/ (Accessed: 13 July 2023).

Wang, Y., Sun, L., & Peng, D. (2022). A multihead ConvLSTM for time series classification in eHealth Industry 4.0. *Wireless Communications and Mobile Computing, 2022*, 1–7. https://doi.org/10.1155/2022/4457448

Warden, P. (2016). TensorFlow for Poets. [online] Available at: https://petewarden.com/2016/02/28/tensorflow-for-poets/ [Accessed 29 Oct. 2022].

Wills, J. (2018). The Rise of Fileless Malware and How to Protect Against It. [online] Security Intelligence. Available at: https://securityintelligence.com/the-rise-of-fileless-malware-and-how-to-protect-against-it/ [Accessed 29 Oct. 2022].

Xavier, A. (2019) An introduction to convlstm, Medium. Available at: https://medium.com/neuronio/an-introduction-to-convlstm-55c9025563a7#:~:text=ConvLSTM%20theory&text=In%20this%20kind%20of%20architecture,data%20order%20is%20extremely%20important (Accessed: 23 September 2023).