ISSN No:-2456-2165

Deep Learning Approaches in Cyber Security-A Comprehensive Survey

[1]V. Jayabharathi, [2]Dr. S. Sukumaran
[1]Ph.D Research Scholar, [2]Associate Professor
[1]Excel College for commerce and science, komarapalayam-638183, Tamilnadu, India
[2]Erode Arts and Science College (Autonomous), Erode-638009, Tamilnadu, India

Abstract:- Recent years have seen the successful application of deep learning techniques, an enhanced model of conventional machine learning, in a variety of fields, including banking, entertainment, coordinating, health care, and cyber security. The study concentrated on a thorough examination of deep learning techniques in cyber security. Adversarial attacks have emerged as a more significant security threat to many deep learning applications than machine learning in the real world as deep learning techniques have become the core components for many security-critical applications such as identity recognition cameras, malware detection software, intrusion detection, spam detection, and self-driving cars. Through a review of the literature and consideration of the important research topics, this paper gives a thorough study on the Deep Learning process, supervised, and unsupervised approaches. The survey also discusses important DL architectures used in cyber security applications.

Keywords:- *Deep learning, Cyber Security, Supervised learning, and Unsupervised learning.*

I. INTRODUCTION

For millennia, wise people had fantasised of creating a machine that could mimic human brain function. Since "associationism," a theory that required scientists to comprehend the workings of human recognition systems, was first put forward by Aristotle in 300 B.C., it is possible to trace the roots of deep learning all the way back to that time. The McCulloch-Pitts (MCP) model, also referred to as the Prototype of artificial neural networks, was first proposed in 1943, marking the beginning of the modern era of deep learning. Based on neural networks that functionally resemble the neocortex in human brains, they developed a computer model. They used "threshold logic," a mathematical and algorithmic mix, in their model to simulate human reasoning, but not learning. Since then, deep learning has continuously advanced, reaching a few major turning points [1].

Artificial Intelligence - Artificial intelligence is the study of creating computer systems that can simulate human intelligence. The terms "artificial" and "intelligence" make up this phrase.

Machine Learning- In the middle of the 1950s, machine learning was developed to generate artificial intelligence. Its emphasis shifted to developing programmes that were better than iteration but were created with a single objective in mind and could be broadly understood as a form of function optimization. As the 20th century drew to an end, artificial intelligence ultimately started to evolve into its own area, and machine learning started to develop into a more advanced and mature science. Since numerous disciplines, including computer science and statistics, contribute to and are inspired by machine learning, many statistics programmes frequently incorporate and encourage their students to become proficient in the techniques. AI and statistics are coupled with machine learning. [3, 5] Given that it combines AI heuristics with statistical analysis, it is an evolution of AI. Machine learning is to make it possible for computer systems to understand the data and make judgments based on its properties. As a result, it employs statistics for fundamental ideas and promotes more AI heuristics to achieve its goal. Supervised and unsupervised learning are the two main paradigms that make up machine learning. With contrast to unsupervised learning, in supervised learning we already know what the label/response variable Y is. As a result, we can efficiently assess a model's effectiveness. We lack this knowledge in unsupervised learning, making it impossible for us to gauge how accurate we are. It makes sense to talk about the history of this topic before examining the difficulties with both paradigms [3, 4].

A. Deep Leaning

A subset of machine learning called "deep learning" allows for highly computational models with numerous layers of abstraction. The state of the art in many fields, including the identification of illness treatments and genomes, voice recognition, visual recognition, object finding, and many others, has been greatly enhanced by these techniques. The primary characteristic of dl layers is that they were learned from the data using a general-purpose learning technique rather than being created by humans. Deep learning is making remarkable strides toward resolving issues that have long defied the best efforts of the AI community. In addition to multiplying the registers in picture recognition, it has shown to be particularly effective in detecting complex structures in high dimensional data and is thus useful to many fields of research, commerce, and government. [5].

ISSN No:-2456-2165

The three categories of DL approaches include supervised with labeled data, unsupervised without a label, semi-supervised, and reinforcement learning, which combines partially labeled data with additional unlabeled data.

Supervised learning: In order to train algorithms to correctly recognize input or predict outcomes, it has labeled datasets. Supervised education the dataset is separated into pieces for training, testing, and validation. The training dataset contains inputs as well as the desired outcomes. After receiving the input data, the model adjusts its weights until the error is properly reduced. Algorithms: Multilayer Perception, CNN, RNN, LSTM and GRU

Unsupervised learning: Unsupervised learning techniques identify patterns from unlabeled [9] data. Finding the underlying structure of data and representing it in a compressed manner require grouping data based on similarities. Association rule mining and clustering are examples of unsupervised algorithms. Algorithms: GAN, AE, SOM, RBM, and DBN

Semi-supervised learning - This strategy falls somewhere in the middle between supervised and unsupervised learning. Combining labeled and unlabeled data makes up training data. While there is a significant amount of unlabeled data, there is a relatively little amount of annotated data. There needs to be a relationship between the objects with assumptions in order to use the unlabeled dataset.

Algorithm: CNN+LSTM, GAN+CNN, DDL, DRL

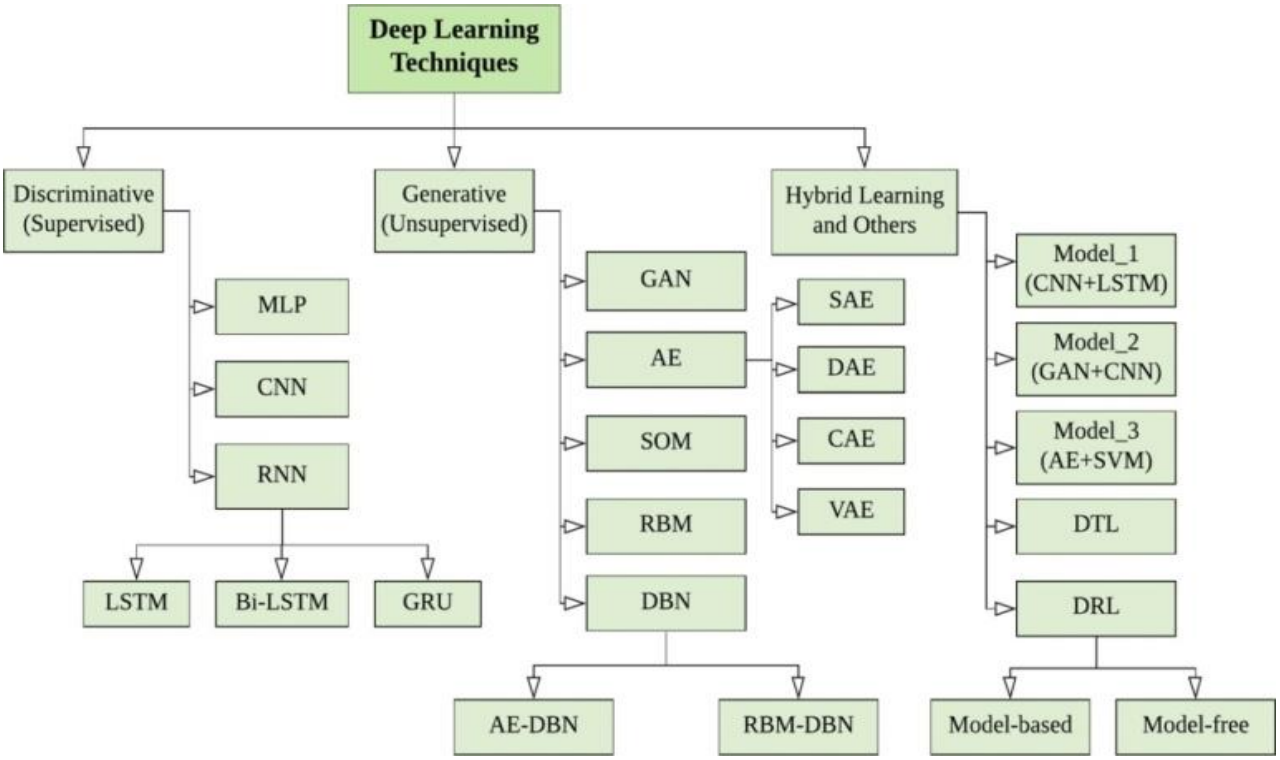

Fig 1:- Source: IBM Blog

B. Cyber Security

We are entering Industry 4.0 as a result of the rapid development of cyber physical systems (CPS), which are driven by technologies like cloud computing, mobile computing, edge computing, and the Internet of Things (IoT). However, as systems become more heterogeneous, sophisticated, and networked, the importance of cyber security in CPS is also expanding due to the inherent security risks and vulnerabilities. In 2018, there were 13% more vulnerabilities overall [10]. Zero-day exploits are expected to increase from one per week in 2015 to one per day by 2021 [12]. While the demand for cyber security specialists is rising globally to address this issue, there is a scarcity of qualified researchers and practitioners, with that number potentially reaching 25% [13]. A survey that acts as a lesson for cyber security experts is required. To assist in solving the significant issue of cyber security for upcoming ICT systems, it is crucial to identify the gaps in the body of literature. [14] With the aim of maintaining the confidentiality, integrity, and accessibility of information in the cyberspace, the term "cyber security" has developed to refer to a collection of principles and practices to safeguard ICT systems and networks. Cybercrime refers to illegal activities committed within the CPS that result in malicious attacks on computer hardware, networks, and software. What's more, the dangers to data integrity from un authorized access, theft, disclosure, and malicious or unintentional harm are becoming more significant. The broad threat categories have not changed over time, despite a rise in criminals and enemies in the field of cyber security. [15] The fundamental purpose of security research is to stop attackers from attaining their objectives, so it is crucial to have a thorough understanding of the many

ISSN No:-2456-2165

forms of attacks. Numerous cyber security strategies, including intrusion detection (ID), malware analysis, social network analysis, advanced persistent threats, online application security, and applied cryptography are being used to combat these dangers. An adaptive cyber security architecture that can proactively respond to changes in systems and physical processes is lacking, despite the massive rise of CPS towards Industry 4.0. The massive amounts of data collected by today's cyber security systems from network sensors, logs, and endpoint agents can be processed effectively utilizing data mining (DM) techniques to deliver timely information about harmful activity. By detecting network attacks, eliminating malware, finding vulnerabilities, and securing the system, deep learning opened up new security perspectives. Deep learning algorithms are able to identify more complex threats since they are not dependent on memory of well-known cues and typical assault patterns. Instead, they become familiar with the system and can see strange activity that could be a sign of malware or malicious actors.

➢ *Type of attackers*

The knowledge of the attacker can be divided into three categories. In the "black box" model, the attacker is completely unaware of the deep learning model and has no prior knowledge of it. In the grey box model, the attackers have a basic understanding of the model and are aware of information about certain of its components. In the white box model, the attacker is fully aware of the model, and this worst-case scenario is the only one that can occur.[15]

Based on their areas of operation, the following categories of cyber security can be made.

- Network security: These cyber security technologies protect businesses' networks and communications against unauthorized access.
- Applications and software are protected from any harmful activity that could result in data loss thanks to this cyber security protocol.
- End-user security: This procedure keeps system users informed so they may operate safely and stay safe from online risks.
- Operational security: Managing and moving huge amounts of data are typical requirements for business operations. The organisations' continued operation depends heavily on its safety, which is provided by cyber security.
- Informational security protects databases against unauthorized users and hackers who might try to access the data for their own or other people's financial gain.
- Disaster recovery and business continuity: This cyber security practise was developed in response to a cyber-security incident that would have resulted in data loss. Therefore, these techniques guarantee that all lost data is retrieved and that business operations return to normal.

Deep learning techniques are very successful at securing systems and data since they can carry out all the tasks listed under cyber security [16]. The employment of these cutting-edge techniques in cyber security helps to protect data, systems, users, and organizations from harmful attacks. Deep learning techniques are also very useful in the field of cyber security due to their great accuracy and efficiency as well as their capacity for autonomous improvement.

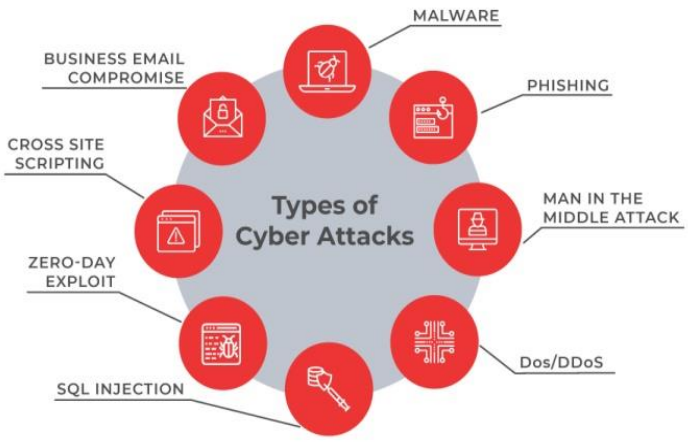

Fig 2:- Types of Cyber Attacks
Source: Blog Sites

This covers insider threat identification, spam and phishing detection, malware and botnet detection, network traffic analysis, and intrusion detection, among other things. With the advancement of technology, cyber security data is continuously expanding, and this growth has an impact on how well DL-based solutions work. Different DL architecture designs for cyber security have proliferated recently. On the other hand, attackers are employing the same resources to carry out more complex attacks. Today's DL has made major advancements in traditional signature- and rule-based systems as well as traditional machine learning-based solutions, and it can offer fresh perspectives on issues relating

to cyber security. It is difficult to make judgments regarding the effectiveness of any certain technique because different authors employed different datasets and measurements. However, there are certain broad tendencies that may be seen. So, across the many security areas, there was a noticeable variance in performance. With TPR ranging between 96.01% and 99.86%, FPR ranging between 1% and 1.95%, and accuracy ranging between 0.9959 and 0.9969, DL appears to have the most reliable performance among the domains using several techniques. The performance of methods for detecting network intrusions, however, showed broader variations, with TPRs ranging from 92.33% to 100%, FPRs from 1.58% to 2.3%, and accuracy from 44% to 99%. Due of the vast amounts of data and many sources present in the cyber world, DL can be successfully used to the field of cyber security. However, the lack of publicly accessible datasets is making this line of research increasingly challenging. These datasets are not shared among researchers and are small, outdated, or internally produced. To advance cyber security systems, it will be essential to create sizable benchmark datasets that are consistently updated. Additionally, the capability to evaluate proposed DL algorithms in actual operating scenarios is required for comparing detection rates, speed, memory utilization, and other performance indicators. The significance of DL has already been recognized by the cyber security sector, and as a result, new datasets are appearing.

II. RELATED RESEARCH WORKS

The most recent studies are geared toward readers who want to start researching deep learning (DL) for cyber security. DL is a subset of machine learning; however it differs from traditional learning in that it is more recent and complicated. As a result, emphasis is placed heavily on providing a comprehensive overview of the DL approaches and providing references to important works for each DL method. Examples that show how the techniques have been applied in cyber security are also provided. Highly cited papers were given extra attention because they describe common procedures. Some less-cited publications were also picked because it was understood that this emphasis could ignore important new and emerging strategies. Overall, articles were chosen so that each of the DL categories given below had at least one, but ideally several, representative papers. This section goes into great detail about the approach and limits of each paper.

Jianwensunetal[10]: This study suggests a Deep Belief Network-based approach for automatic fault identification for quality in section of electro motors. Results produced by the suggested strategy are quite precise.

Wei-longzhengetal [12]: In this study, two emotional categories based on EEG were classified using Deep Belief Networks. When compared to alternative State-of-the-art procedures, the suggested method produces findings that are more precise.

The impact of the maximising problem on social networks was discussed by the author. The main goal is to identify a limited group of nodes that will maximise influence. The issue of tackling the influence maximisation problem utilising greedy algorithms and stochastic optimization techniques like simulated annealing has also been studied. A unique GA is utilised to enhance influence while maintaining variety through the usage of many populations. The structure of modified GA is sometimes impacted, ensuring the diversity of the possible options and elevating the complexity of the optimization procedure. In the future, there might be a focus on how the makeup of a particular population has changed and how those changes have affected its attributes. OSN [13]

The author of [14] offered yet another set of attacks to violate user privacy. This cutting-edge assault type takes advantage of advertising platforms with the ability to microtarget audiences. One of the biggest and most well-known online social network systems in the world, Facebook, had its advertising system as the author's primary focus. Information leakage across different advertising campaigns has been linked to a number of design decisions made by advertising systems. It has also been explained why Facebook's remedies to the aforementioned vulnerabilities were insufficient to provide a defence. Nowadays, most people use many social media accounts.

The degree of security and privacy offered by any online network varies depending on the sort of service it offers. The author, Shuochao Yao and Yiran Zhao et al., discussed difficulties and recently developed solutions that point to the viability of creating dependable, efficient, and effective IoT systems that incorporate deep learning techniques [15].

CNNs and RNNs were utilised by Kolosnjaji et al. [16] to recognise malware. One-hot encoding is used to transform the list of call sequences to the API kernel into binary vectors. A method for storing categorical data that makes it easier for machine learning is one-hot encoding. The DL algorithm, which consists of a CNN and RNN, is trained using this data (consisting of an LSTM, and a softmax layer). This model achieves 89.4% accuracy, 85.6% precision, and 89.4% recall.

LEMNA, a novel technique to develop high-fidelity explanations for specific classification findings for security applications, is introduced in this paper[17]. A target deep learning model is treated as a "black box" by LEMNA, and its decision boundary is approximated using a mixed regression model improved by fused lasso. We demonstrate that the suggested strategy generates extremely accurate explanations by testing it on two well-known deep learning-based security applications. Additionally, we show how LEMNA may help security analysts and machine learning developers better understand classifier behavior, fix misclassification issues, and even apply automated updates to improve the initial deep learning model.

ISSN No:-2456-2165

In many applications, feature sequence extraction and data categorization using RNN and notably LSTM demonstrate excellent efficiency. Recurrent networks have the benefit of being able to process data sequences where a lengthy pattern of multidimensional features is modelled to place a specific sample in the proper class or map the entire sequence into a predicted scalar in regression issues. LSTM was shown to be effective in [18] for automatically extracting features for highly accurate solar array defect diagnostics.

The author [19] studied if deep learning models may be used for the security evaluation of cryptographic methods. In order to run the trials utilising technique 1 against S-DES and round reduced Speck32/64, a few neural network models have been constructed. The complete key space is utilised for S-DES and put to the test using MLP and CNN models. According to the results, CNN scored badly on this test, although several MLP models outperformed a random guess. The best model was accurate to within 0.2157. Compared to a random guess, which has an accuracy of 0.0009, it is substantially superior. This suggests that a neural network model can identify the right key for S-DES encryption in part. In 1-round Speck, technique 1 for Speck functioned admirably. However, when the key set nK is set to 2, 4, and 10, experimental results show that it is difficult to extend method 1 beyond 2-round Speck. Using MLP and LSTM models, we also used approach 2 against S-DES. MLP models have demonstrated comparatively greater performance and have a higher likelihood of recovering the random S-DES key than a random guess. However, LSTM models were unable to retrieve the S-DES random key.

To address privacy concerns about collected data used for deep learning training, Ma et al. [21] offer unique privacy preservation deep learning model, called PDLM. The PDLM uploads the encrypted data to service providers after applying deep learning on the data owners' encrypted data using multiple keys. The model is trained by service providers and the cloud platform using multi-key encrypted data and a toolbox for privacy preservation calculations.

A Deep feed forward Neural Collaborative Filtering was suggested by Farhan Ullah et al. [22] for the selection of educational services. The benchmark excellent books 10k was used as the basis for the experiments in Keras.

Modern deep learning classification techniques were used by the author [2] in comparison to traditional machine learning techniques. It constructed a corpus of cypher text for a multilingual dataset with 700 files on average, each with 4000 characters, and used our methods on this generated cypher text. They employed the cyphers AES and Blowfish.

As technology advances, the frequency and complexity of cyber-attacks are rising steadily today. Traditional cyber security solutions are unable to detect sophisticated unknown attacks like zero-day attacks and new malware variants in such a complicated technological environment. Cyber security systems have included ML techniques to address these issues, but they have had limited effectiveness in thwarting unexpected or unanticipated attacks. Meanwhile, DL methodologies enhance the learning process and show promising outcomes in a variety of applications, including cyber security. The significant developments in software engineering and the large production of training data are crucial to the success of DL. In order to do this, a thorough examination of DL approaches is performed, taking into account all facets of cyber security, including intrusion detection, software attack detection, and privacy protection. We examine the architecture of each of the works we have studied, paying close attention to the DL method(s) applied, how it was implemented, the test data sets used, and the outcomes obtained. We have, if feasible, compared the effectiveness of the various approaches. It is important to note that this was the most challenging portion because most studies do not use the same dataset for model testing.

The recent works on deep learning methods CCN, MLP, RNN, AE, LSTM, and, GAN Deep learning multi feed forward neural network, on the applications namely health care, self-driving cars, coordination, entertainment, and finance and cyber security, Text classification, image identification and some are implemented on heterogeneous data. Although many research studies have been published on attacks and the defense of the security and privacy of deep learning, they are still fragmented

Author, Year	Method	Merits	Demerits
Daniel S. Berman, Anna L. Buczak *, Jeffrey S. Chavis and Cherita L. Corbett, 2019	RNN, RBM, AUTO ENCODER	Reduce risk.	Performance varies for different authors.
Jollanda Shara,2021	CNN, RNN,RBN, GAN, AUTO ENCODER	Accuracy and performance is high.	Performance vary for different authors
Aarontuor,2017	RNN-TUNING LSTM	Good potential	insider threat only detect
Yue-JieHou,aZai-XinXie,a Jian-Hu,a,1 Yao-Shen,b,2 and Chi-Chun Zhoua,3,2021	CONVOLUTIONAL AUTOENCODER(CCAE)+HYBRID CLUSTERING ALGORITHM	High Accuracy, Robustness	It Also Have Incomplete Structural Characteristic
Tausiajansaleemmohammedahsanchisth,2021	DNN LSTM	Very good at analyzing time series data,	Dl requires comprehensive labeled data sets

		Tolerate noise, High accuracy	
Miki banarjee,2018	NEURAL NETWORK	More security	Data's are not necessarily originated from truth worth sources
Hardy et al,2016	CNN,AE,RBN	More security Boosting knowledge is highWide range of networks	Need lots of data set
Tausiajansaleem, mohammedahsan chisth,2019	CNN,RNN,LSTM,AE,RBM,GAN	More accurate prediction and effective results	High velocity, need large data set
Benchea and Gavrilu¸t,2017	DCAE,HAC	Reduce high dimensional information data	It pass number of requisite test
Kwon et al. 2017	CNN+CLOUDNET	Great accuracy High performance Efficient robustness	Some classification occurs.
Su et al.2018	AE, DAC	High accuracy	Need large data set

Table 1:- Summary of Related works

This work focus on specific environments or applications, Cloud, IoT, Cyber-Physical Systems (CPS), social networks, biometric and cryptography.

Authors	**Database**	**Methods**	**Results**
Alaa S. Al-Waisy, Rami Qahwaji,StanleyIpson, Shumoos Al-Fahdawi & Tarek A. M. Nagem,2018	SDUMLA-CASIA-,IRIS-V3 INTERVAL AND IITD HMT	CNN(IRIS)	99.82
LukeEverson,Dwaipayanbiswas,Madhuripanwar,2018	TROIKA	CNN+LSTM	96%.
Fabula AI ,USI Lugano, Imperial College,2019	YOUTUBE VIDEO DATASET	GDL	92.7%
Georgegkotsis1, Anikaoellrich1, Sumithravelupillai1,2, Maria Liakata3, Tim J. P. Hubbard4, Richard J. B. Dobson1,5 &Rina Dutta1,2017	REDDIT	FF CNN LINEAR SVM	70.82% 71.37% 58.72% 64.02%
Owusu-AgyemangKwabena, Zhen Qin , TianmingZhuang, And Zhiguang Qin,2019	DATA SET	DNN+HOMOMORPHIC ENCRYPTION	93.42
Yanshengli[a]weichen[a]yongjunzhang[a]chaotao[b]ruixiao[a]yihuatan[c],2020	DATA SET	1(WDCD) 2. GCP 3. CAM 4. LPP	96.66
MohamedEsmailkarar[ab]fahadalsunaydi[a]sultanalbusaymi[a]sultanalotaibi,2012	DATA SET	R-CNN	99.0%
Alaa S. Al-WaisyRami Qahwaji, Stanley Ipson, Shumoosal-Ahdawi & Tarek A. M. Nagem,2018	SDUMLA-CASIA-,IRIS-V3 INTERVAL AND IITD HMT	CNN(IRIS)	99.82

ISSN No:-2456-2165

Giovanni Apruzzese,2018	DATA SET	SUPERVISED AND UNSUPRVISED (ML+DL) ALGORITHM	Both Are Have Pros &Cons
Zhiqiang Wang , 1,2,3 Gefei Li , 2 Zihanzhuo , 4 Xiaoruiren , 1 Yuheng Lin , 1 And Jieminggu 4,2021	KITHUB.COM	CNN	99.3538

Table 2:- Comparison of Various Deep Learning Methods in Cyber Security.

III. CONCLUSION

It is crucial to comprehend the importance of the data provided on any social media platform in the age of the internet and how to keep it safe and secure. Many privacy settings and policies in the literature are offered by service providers as well as created by researchers. It is necessary to compare the current models in order to adopt ones that are more reliable and secure, along with the creation of new models and procedures. Attacks on cyber networks continue to develop at a rate that exceeds the capacity of cyber defenders to create and implement new signatures to stop these new attacks. The application of DL approaches to a wide range of these cyber security threat types that attacked networks, application software, host systems, and data was described in this survey report. Additionally, it gave a thorough analysis of the ways that DL techniques have been used to identify these cyber-attacks in the past. Describe the various criteria employed to assess DL performance for applications related to cyber security. However, a fair comparison between all of the various methodologies was not possible due to the use of various datasets for training and testing. As a result, benchmark datasets are essential for developing DL in the field of cyber security.

REFERENCES

[1]. Yue-JieHou, Zai-XinXie, Jian-Hu, Yao-Shen, And Chi-Chun Zhoua, “An Unsupervised Deep- Learning Method For Fingerprint Classification”, The CCAE Network And The Hybrid Clustering Strategy”-2019 .

[2]. Amine Boulemtafes, Abdelouahid Derhab, Yacine Challal,“A Review of Privacy-Preserving Techniques For Deep Learning”.

[3]. Techniques Muhammad Imran Tariq, Nisar Ahmed Memon, Shakeel Ahmed, Shahzadi Tayyaba, Muhammad Tahir Mushtaq,Natash Ali Mian, Muhammad Imran. “A Review Of Deep Learning Security And Privacy Defensive ”.-2018

[4]. Aaron Tuor and Samuel Kaplan And Brian Hutchinson Western Washington University Bellingham, WA Nicole Nichols And Sean Robinson Pacific Northwest National Laboratory Seattle, “Deep Learning for Unsupervised Insider Threat Detection in Structured Cyber Security Data Streams” -2017

[5]. Jollanda Shara, "Deep Learning Methods For Cyber security" Some Of The Authors Of This Publication Are Also Working On These Related Projects: Application Aspects Of Ml And Dl In Cryptography, Steganography And Cyber Security View Project Conference Paper - June 2021 Citations 0 Reads 328

[6]. Daniel S. Berman, Anna L. Buczak, Jeffrey S. Chavis And Cherita L. Corbett Johns “A Survey Of Deep Learning Methods For Cyber Security” Hopkins University Applied Physics Laboratory (JHU/APL1), Laurel, MD 20910, USA;

[7]. Tausifa Jan Saleem, Mohammad ahsanchisht, “Deep Learning For Internet Of Things Data Analytics” -2019 Pp381-389

[8]. Tausifa Jan Saleem, Mohammad ahsanchisht, “Deep Learning For Internet Of Things Data Analytics”- 2021, Pp526-542

[9]. Online Social Network Security: “A Comparative Review Using Machine Learning and Deep Learning” (2021) 53:843–861

[10]. Chanchal Kumar, Taran Singh Bharati, Shiv Prakash Online Social Network Security: “A Comparative Review Using Machine Learning And Deep Learning” 2021 PP 843-861

[11]. Mohaisen A, Alrawi O, Mohaisen M AMAL: High-Fdelity, "Behavior-Based Automated Malware Analysis And Classification". Computer Secure - 201552:251–266

[12]. Savage D, Zhang X, Yu X, Chou P, Wang Q “Anomaly Detection In Online Social Networks”. Social Network-2014 39:62–70

[13]. LEMNA: Explaining Deep Learning Based Security Applications,2018

[14]. "Deep learning through LSTM classification and regression for transmission line fault detection, diagnosis and location in large-scale multi-machine power systems",2021

[15]. A.Y. Appiah, X. Zhang, B.B.K. Ayawli, F. Kyeremeh, "Long Short-Term Memory Networks Based Automatic Feature Extraction for Photovoltaic Array Fault Diagnosis", IEEE Access 7 (2019) 30089–30101,https://doi.org/10.1109/ACCESS.2019.2902949 .

[16]. McDermott, C.D.Majdani, F.Petrovski, "Botnet detection in the internet of things using deep learning approaches". In Proceedings of the 2018 International Joint Conference on Neural Networks (IJCNN), Rio de Janeiro, Brazil, 8–13 July 2018; pp. 1–8.

[17]. G. D. Hill and J. A. Bellekens, "Deep learning based cryptographic primitive classification", ArXiv, September 2017, pp. 1-9.

[18]. T. Kim, B. Kang, M. Rho, S. Sezer and E. GyuIm, "A multimodal deep learning method for Android malware detection using various features", IEEE Transactions on Information Forensics and Security, vol. 14, no. 3, March 2019, pp. 773-788
[19]. Q. Feng, Y. Zhang, C. Li, Z. Dou and J. Wang, "Anomaly detection of spectrum in wireless communication via deep auto-encoders", The Journal of Supercomputing, vol. 73, no. 7, July 2017, pp. 3161-3178.
[20]. SourceFire, Inc., "Snort: An open source network intrusion detection and prevention system". [Online] Available: http://www.snort.org. Accessed on: Feb. 2, 2021.
[21]. AbdelBassetM,HawashH,ChakraborttyRK,RyanM, " A Deep learning approach for smart energy management in IoT-based smart cities ". IEEE Internet of Things J.2021.
[22]. "A Review on Security Threats and Vulnerabilities in Cloud Computing". International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 IJERTV4IS070073 www.ijert.org Vol. 4 Issue 07, July-2015