European Journal of Molecular & Clinical Medicine

ISSN 2515-8260 Volume 09, Issue 07, 2022

SURVEY ON CYBER SECURITY THROUGH WATERMARKING AND DEEP LEARNING TECHNIQUES

[1]M.Bommy, [2]Paritala Jhansi Rani, [3]Thomas Abraham J V, [4]Gunjan Chhabra, [5]Suresh Kumar Sharma, [6]MK Jayanthi Kannan

[1]Assistant Professor, Department of Computer Science & Engineering, Madanapalle Institute of Technology & Science, Madanapalle, Andhra Pradesh, India.
[2]Associate Professor, Department of Computer Science and Engineering, Koneru lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India.
[3]Associate Professor, School of Computer Science and Engineering, Vellore Institute of Technology Chennai Campus, Vandalur Kelambakkam Road,Chennai, India.
[4]Associate Professor, Department of Computer Science and Engineering, Graphic Era Hill University, Dehradun, Uttarakhand, India
[5]Assistant Professor, Department of Statistics, Mathematics and Computer Science, Sri Karan Narendra Agriculture University, Jobner, Jaipur, Rajasthan, India.
[6]Professor and HOD of Information Science and Engineering, Department of Computer Science Engineering, Faculty of Engineering and Technology, JGI Campus, JAIN (Deemed-To-Be University), Bangalore, Karnataka, India.

[1]bommym@mits.ac.in, [2]jhansirani@kluniversity.in, [3]thomasabraham.jv@vit.ac.in, [4]chhgunjan@gmail.com, [5]suresh.cs@sknau.ac.in, [6]dr.mkjayanthi.ju@gmail.com

ABSTRACT

With the growth of the Internet, cyberattacks are evolving quickly, and the state of cyber security is not promising. Cyber security is often an extension of traditional information technology (IT) security that aims to safeguard systems, applications, and data that are vulnerable to various online assaults, such as data theft and espionage as well as data manipulation and denial of service attacks. Due to the losses incurred by countries, companies, and people as a result of numerous cybercrime assaults, there is a need for an increase in cyber security research. This study examines deep learning (DL), watermarking techniques for cyber security applications and illustrates how deep learning and water making is used in cybersecurity and how state-of-the-art solutions may be outperformed by deep learning ones. We advise professionals to think about integrating deep learning into security systems.

Keywords: Cyber Security, Deep Learning, Watermarking, Cyber Attacks.

ISSN 2515-8260 Volume 09, Issue 07, 2022

I. Introduction:

The Internet is transforming how people learn and work as a result of the deeper integration of the Internet and social life, but it also exposes us to more significant security risks. A major problem that needs to be resolved quickly is how to recognise different network assaults, especially those that have never been seen before. Computers, networks, programmes, and data are all protected by a variety of technologies and procedures called "cybersecurity" in order to prevent assaults and illegal access, modification, or destruction [1]. Network security systems and computer security systems make into a network security system. Firewalls, antivirus programmes, and intrusion detection systems are all features of these systems (IDS). Unauthorized system behaviour, such as usage, copying, modification, and destruction, may be found, ascertained, and identified with the use of IDSs [5].

Both internal and external invasions constitute security breaches. For IDSs, there are three basic categories of network analysis: hybrid, anomaly-based, and misuse-based (also known as signature-based). Utilizing the hallmarks of known attacks, misuse-based detection approaches seek to identify known attacks [9]. They are utilised for recognised attack types and don't cause a lot of phoney alerts. The database rules and signatures, however, must frequently be updated manually by administrators. It is impossible to identify fresh (zero-day) threats with improper technology. By examining the typical network and system behaviour, anomaly-based approaches can spot departures from the norm.

They are desirable due to their ability to recognise zero-day assaults. Another benefit is that each system, application, or network's regular activity profiles are unique, making it harder for attackers to predict which actions they can carry out covertly. Additionally, it is possible to define the signatures for abuse detectors using the data that anomaly-based approaches (new attacks) warn on. Because previously unknown system actions might be classified as anomalies, the fundamental drawback of anomaly-based approaches is the possibility for high false alarm rates. Misuse and anomaly detection are combined in hybrid detection [13]. It is used to boost the rate of known intrusion detection and decrease the number of false positives for unidentified assaults. Hybrid approaches to ML/DL are the norm.

Since form the begining, Deep Learning has been more and more popular for use in applications of artificial intelligence thanks to the range of neural networks in many fields of study. Deep Learning is important because it can process both labelled and unlabeled data, as well as other kinds of data like numbers, text, or pictures. AI solutions, such as anomaly detection, malware identification, intrusion detection systems, etc., are very useful in the realm of cybersecurity. These programmes operate as analyst agents when human analysis is insufficient and assist in reducing the demand for human labour.

A subset of machine learning techniques built on artificial neural networks is known as deep learning (DL). Input and output layers are included in these networks' many levels, and each layer comprises several units known as neurons that carry out weighted operations. For

diverse purposes, DL uses a variety of designs, including feedforward, convolutional, and recurrent networks. Deep learning's use was recently realised in the years 2011–2012, when a quick GPU implementation of CNNs [2] was made possible and it established records in computer vision competitions. After the CNN architecture Alexnet [6] won the "ImageNet Large Scale Visual Awareness Challenge" by a huge margin in comparison to other models, CNNs received global recognition.

Deep Learning applications have also been used for activities related to cybersecurity operations, such as sequential data analysis, pattern identification, and natural language processing (NLP). The International Telecommunication Union (ITU) has the following definition of cybersecurity (or information security): "Cybersecurity is the collection of tools, policies, security principles, safeguards, rules, actions, risk management strategies, best practises, assurance, and technology that may be used to secure an organization's and user's assets as well as the cyber environment. The assets of an organisation or user comprise its staff, infrastructure, applications, services, telecommunications systems, and any information that is transported and/or stored in the cyber environment.

The demand for protecting them and finding new methods to take use of them have both increased with the proliferation and diversity of computer devices worldwide. The applications of artificial intelligence have grown significantly along with technology. Several security applications have been constructed around AI, many real-world applications employ AI, which creates security problems, and there are a number of ways that AI may be exploited for immoral cyber activities. AI has a significant role to play in cyber security.

In this article, the role of deep learning in cybersecurity is examined, along with the security concerns of deep learning applications. We also discuss the usefulness of deep learning as well as the harmful ways that it may be used to damage individuals and organisations. The following is a description of the following sections: The second section reviews the works that are relevant to this study; the third section lists useful applications of various DL architectures; the fourth section explores misuses of AI and demonstrates its dual nature as being both beneficial and potentially harmful.

In addition to outlining some practical ways that security processes might be automated, the article intends to emphasise the major concerns that automated cybercrimes may cause in the near future. The study only discusses Deep Learning applications, their uses and abuses in the field of cybersecurity, as well as the security problems associated with actual systems.

II. Literature Review

Several articles have highlighted the use of deep learning and artificial intelligence as security measures as well as harmful cyberweapons. [10] lists the many AI applications for cyber-security, including but not limited to Intelligent Agents and Neural Networks. It provides examples of how AI may be used in security applications. [14] focuses solely on deep learning

ISSN 2515-8260 Volume 09, Issue 07, 2022

techniques that strengthen defences against cyberattacks. After defining terms for various cyberthreats and DL architectures, they examined many models and presented them under the headings of various security applications, such as ransomware, spam categorization, and malware detection.

The malevolent uses of AI are described in [17] along with methods to anticipate, stop, and mitigate them. It takes into account problems with and assaults on three main forms of security: social, digital, and physical. Each security category is covered in detail in the study, along with dangers that may exist in that area and control points and mitigation strategies that should be taken into account while doing security analysis. Additionally, it provides guidelines for using AI and a strategic study of AI's potential impact on security in the future.

[20] examines several machine learning methods, including deep learning, that can be used to cyber security applications. The researchers also emphasised the necessity for accurate parameter adjustment and re-training in order to get better outcomes, as well as the machine learning algorithm's susceptibility to adversarial assaults.

[23] discuss several machine learning algorithm threats and provide countermeasures. The paper discusses strategies for defending against two types of attacks—evasion and poisoning. These categories are then broken down into other sorts, each of which is explained in depth. Data privacy is also covered in relation to AI applications.

[26] discusses the adversarial assaults used against systems using deep learning models for image processing. They evaluate the designs, examine the situation, and suggest countermeasures. The study exclusively discusses adversarial attacks on computer vision networks like generative networks and convolutional neural networks (variational autoencoders and GANs).

Deep Learning models have practical security uses, but they also bring with them potential dangers, which must be considered when integrating them into a security system. Additionally, as noted in section B, deep learning models also have several characteristics that enable the use of them for destructive purposes.

Digital Watermarking: Although China was the first country to master the skill of making paper, it wasn't until 1282 in Italy that paper watermarks made their debut. Thin wire designs were added to the paper moulds to create the markings [3]. According to [17], digital watermarking is the technique of embedding data into digital media in a way that makes it difficult for humans to notice but simple for computers to detect. A digital watermark is a transparent, undetectable information pattern that is added using a particular computer method to an appropriate part of the data source [11].

Digital watermarks are additional signals that may be recognised or retrieved afterwards to provide information about the digital data (audio, video, or still photos). Digital watermarking is used to guard against unauthorised copying and alteration of digital files without the owners'

ISSN 2515-8260 Volume 09, Issue 07, 2022

consent. This review will concentrate on digital watermarking and look at how it may be used in cyber security. Earlier Works The design and prototype implementation of an image verification server employing digital watermarking are proposed by [15] to stop scammers from utilising a picture saved from social networks to create a fake user's profile.

The Discrete Wavelet Transform, or DWT, uses the watermark algorithm. A bit stream is used as the watermark. In order to create a low-frequency approximation representation, the algorithm deconstructed the image. Low-frequency approximation representation contains the watermark (LL). Each time, a non-overlapping 3x1 sliding window's coefficient triple is chosen and adjusted. The watermark is embedded by altering three coefficients while sliding a non-overlapping 3x1 window across them three times. To represent one bit of watermark data, the median of the three coefficients is quantized to produce a multiple of "space". In order to create a reconstruction point for watermark extraction, the sliding window's median is calculated and quantized.

The retrieved watermark sequence is given the bit value related to that rebuilt location. Users have more privacy control thanks to the server. The work in [18] outlines a watermarking-based strategy and how to put it into practise to protect against phishing assaults, a type of online identity theft (ViWiD). An integrity verification system called ViWiD is based on the obvious watermarking of logo pictures. It does not need the installation of any software or the storing of any data, such as keys or history logs, on the computers of users. All calculation is done on the company's web server. In order to fend off "one size fits all" assaults, the watermark is created to be distinct for each user and to carry a shared secret between the business and the user.

The biggest problem in adding a visible watermark to logo pictures is preserving the beauty of the watermarked logo while yet being able to add a strong and legible watermark to it. To explore potential connections between digital picture watermarking and data integrity or more general data security, [21] looks at digital watermarking and current advancements in the field. They examine the two fundamental techniques for digital picture watermarking and talk about shared architectural aspects. A watermark embedder and a watermark detector make up the two primary parts of the architecture of digital watermarking. Some digital data and hidden information are combined in the embedder, with the data serving as the carrier and the hidden information as the watermark.

The application situation has a significant impact on the architecture's specifics. A watermark detector's functions include recovering watermarks from damaged data and spotting data integrity issues. Further consideration of the potential applications of such a diverse variety of scenarios reveals that they generate divergent needs for the architecture. Digital watermarking was used to copyright-protect scalar and multimodal sensor network data in Applications of Digital Watermarking to Cyber Security. In order to ensure that the proprietary information is kept secure between the sensor nodes, this research investigates various watermarking techniques

to address the issue of copyright protection of the scalar data in wireless sensor networks (WSNs) and image data in wireless multimedia sensor networks (WMSNs).

For the purpose of copyrighting scalar data in WSNs, they create the Linear Feedback Shift Register (LFSR) and Kolmogorov Rule (LKR) watermarking technology. While it is useless against false data insertion, data alteration, and selective forwarding, the developed LKR watermarking technology can guard against copyright data erasure, packet replication, and multiple data identities (data Sybil attack). By using Digital Audio Sampling Analysis - Identification, [24] provided forensic proof of copyright violation. They discussed audio analysis techniques that included the use of watermarking for copyright-protected music. Use of Digital Watermarking Generally Numerous applications employ digital watermarking.

III. Comparison of ML and DL

The link between machine learning, deep learning, and artificial intelligence is a complex one (AI). A new technical science called artificial intelligence (AI) researches and creates theories, methodologies, techniques, and software applications that mimic, enhance, and extend human intelligence [4]. It is a field of computer science that aims to comprehend the fundamentals of intelligence and create new breeds of intelligent machines that behave similarly to humans.

Robotics, computer vision, natural language processing, and expert systems are all being studied in this field. Artificial intelligence (AI) is capable of simulating human awareness and thought. Although thinking like a human could be more intelligent than human intelligence, AI is not human intelligence. Computational statistics, which likewise focuses on creating predictions with computers, is a subfield of AI that is closely connected to (and frequently overlaps with) machine learning. It is closely related to mathematical optimization, which provides the discipline with methods, theory, and application fields. ML and data mining are sometimes confused [8], although the latter subject is also known as unsupervised learning and focuses more on exploratory data analysis.

Unsupervised machine learning (ML) may also be used to discover significant abnormalities after learning and establishing baseline behavioural profiles for different entities [12]. A "field of research that offers computers the ability to learn without being explicitly taught," according to the father of machine learning, Arthur Samuel The primary objective of machine learning (ML) is classification and regression using pre-learned known characteristics from training data. DL is a recent area of study in machine learning. The creation of a neural network that mimics the human brain for analytical learning is the driving force behind it. It imitates the way the human brain interprets data like sights, sounds, and words [16].

The idea of deep learning (DL) was put out by Hinton [19] based on the deep belief network (DBN), where a hope-filled unsupervised greedy layer-by-layer training algorithm is given to address the optimization issue of deep structure. Next, a multi-layer automated encoder's

ISSN 2515-8260 Volume 09, Issue 07, 2022

deep structure is suggested. A true multilayer structure learning approach that employs a space relative relationship to minimise the number of parameters and increase training performance is the convolution neural network presented by LeCun et al. [22].

An observation, such as a picture, can be described in many different forms, such as a vector representing each pixel's intensity value or, in a more abstract form, as a collection of edges, an area with a certain shape, or something similar. The learning of tasks from cases is facilitated by the use of specialised representations. DL approaches have supervised learning and unsupervised learning much like ML methods. Different learning frameworks have produced learning models that are very dissimilar. The advantage of DL is the effective replacement of features manually using hierarchical feature extraction and unsupervised or semi-supervised feature learning [25]. The following are some of the distinctions between ML and DL:

Depends on data: Deep learning and conventional machine learning differ mostly in how well they perform as the volume of data grows. Due to the fact that deep learning algorithms need a lot of data to fully grasp the data, they do not perform as well when the data volumes are minimal. On the other hand, in this instance, the performance will be greater when the conventional machine-learning algorithm follows the specified principles [16].

Hardware requirements: There are several matrix operations needed by the DL algorithm. The GPU is frequently utilised to effectively optimise matrix computations. Therefore, the hardware required for the DL to function effectively is the GPU. Compared to conventional machine-learning techniques, DL makes more use of high-performance computers with GPUs [27].

Processing of features: Feature processing is the practise of incorporating subject expertise into a feature extractor to simplify the data and provide patterns that improve the performance of learning algorithms. The process of processing features takes time and requires expertise. In ML, the majority of an application's attributes need to be specified by a professional before being encoded as a data type. Pixel values, forms, textures, positions, and orientations are all examples of features. The precision of the characteristics gathered determines how well most ML systems function. The main distinction between typical machine-learning algorithms and deep learning (DL) is the attempt to directly extract high-level characteristics from data [25]. As a result, DL lessens the effort required to create a feature extractor for each issue.

Way for resolving issues: Traditional machine learning algorithms often divide an issue into several smaller problems, solve the smaller problems, and then combine the results to get the desired outcome. Deep learning, on the other hand, supports direct, end-to-end issue solutions.

Execution period: Because there are numerous parameters in a DL algorithm, it often takes a long time to train one; as a result, the training stage takes longer. The fastest DL algorithm, like ResNet, needs exactly two weeks to finish a training session, whereas ML training just takes a few seconds to a few hours. The exam time is the exact reverse, though. Running deep learning algorithms while testing takes relatively little time. As the amount of data rises, the test duration

increases in comparison to certain ML algorithms. Due to the short test duration of some ML algorithms, this argument does not hold true for all of them.

Interpretability: Importantly, when contrasting ML vs DL, interpretability is a crucial consideration. The performance of DL in recognising handwritten numbers may be fairly impressive, coming close to meeting human standards. A DL algorithm won't, however, explain why it produced this outcome [16]. Naturally, a deep neural network node is activated from a mathematical perspective. But how should neurons be represented mathematically, and how do these layers of neurons interact? As a result, it is challenging to describe how the outcome was produced. On the other hand, the machine-learning algorithm makes clear criteria for why it makes a certain conclusion; as a result, the decision's justification is simple to understand.

An essential component of the machine learning mission is the assessment model. While the same sort of machine-learning missions also have distinct evaluation indicators, each with a different emphasis such as classification, regression, clustering, and the like, different machine-learning have a variety of evaluation indicators [28].

IV. Conclusion

In this study, we first discussed the several ways that deep learning techniques and water marking have been used to cybersecurity. Additionally, we demonstrated the security risks associated with deep learning, including how their applications might be abused and used maliciously. The purpose of the study was to illustrate how deep learning and watermaking is used in cybersecurity and how state-of-the-art solutions may be outperformed by deep learning ones. We advise professionals to think about integrating deep learning into security systems. Future research in this field might concentrate on the impact of emerging technologies like 5G, IoT, blockchain, quantum computing, and edge computing on deep learning. There will be security concerns specific to these new technology. Future developments in novel and intricate deep learning systems would likewise require evaluation. This research, we hope, will inspire more investigation into deep learning's and watermark uses in cybersecurity.

References

[1]. S. Aftergood, “Cybersecurity: The cold war online”, Nature, vol. 547, no. 7661, pp. 30-31, 2017.

[2]. Schmidhuber, J. “Deep learning in neural networks: An overview of Neural networks”, 61, pp. 85-117, 2015.

[3]. Cox, J., Miller, et. al., “Digital watermarking and steganography”, Morgan Kaufmann, Publisher, Elsevier Inc., 2008.

[4]. R. G. Smith and J. Eckroth, ‘‘Building AI applications: Yesterday, today, and tomorrow,’’ AI Mag., vol. 38, no. 1, pp. 6–22, 2017.

[5]. A. Milenkoski, et. al., “Evaluating computer intrusion detection systems: A survey of common practices”, ACM Computer Survey, vol. 48, no. 1, pp. 1-41, 2015.

[6]. Krizhevsky, A., Sutskever, I., & Hinton, G. E, "Imagenet classification with deep convolution neural networks", Advances in neural information processing systems, NeurIPS Proceedings, pp. 1097-1105, 2012.
[7]. Megías, D., Serra-Ruiz, J., & Fallahpour, M, "Efficient self-synchronised blind audio watermarkingsystem based on time domain and FFT amplitude modification", Signal Processing, 90(12), 3078-3092, 2010.
[8]. P. Louridas and C. Ebert, ''Machine learning,'' IEEE Software, vol. 33, no. 5, pp. 110-115, 2016.
[9]. C. N. Modi and K. Acha, "Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: A comprehensive review", Journal of supercomputing, vol. 73, no. 3, pp. 1192-1234, 2017.
[10]. Dilek, S., Çakir, H., & Aydin, M, "Applications of Artificial Intelligence Tech-niques to Combating Cyber Crimes: A Review", International Journal of Artificial Intelligence & Applications, 6(1), 21, 2015.
[11]. Katzenbeisser, S., & Petitcolas, F. A. P, "Information hiding: Techniques for steganography anddigital watermarking", Information Hiding First International Workshop Proceedings, 295-315, 2000.
[12]. M. I. Jordan and T. M. Mitchell, ''Machine learning: Trends, perspectives, and prospects,'' Science, vol. 349, no. 6245, pp. 255–260, 2015.
[13]. E. Viegas, et. al., "Towards an energy-ef_cient anomaly-based intrusion detection engine for embedded systems", IEEE Transaction Computing, vol. 66, no. 1, pp. 163-177, 2017.
[14]. Berman, D. S., et. al., "A survey of deep learning methods for cyber security", Information, 10(4), 122, 2019.
[15]. Prakobphol, K., & Zhan, "Alleviating identity theft in social networks", pp. 1-4, 2002.
[16]. Y. LeCun, Y. Bengio, and G. Hinton, ''Deep learning,'' Nature, vol. 521, pp. 436–444, May 2015.
[17]. Brundage, M., "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mit-igation", arXiv preprint arXiv:1802.07228, 2018.
[18]. Topkara, M., et. al., "ViWiD: Visible watermarking based de-fence against phishing" Digital watermarking, Lecture Notes in Computer Science, 3710, 470-483, 2005.
[19]. G. E. Hinton, ''Deep belief networks,'' Scholarpedia, vol. 4, no. 5, p. 5947, 2009.
[20]. Apruzzese, G., et. al., "On the effectiveness of machine and deep learning for cyber security", in 2018 10th International IEEE Conference on Cyber Conflict (CyCon), pp. 371-390, 2018.
[21]. Sztipanovits Mate, et. al., "Watermarking Methods for Cyber Security", 2014.
[22]. Y. LeCun, et. al., ''Gradient-based learning applied to document recognition,'' Proc. IEEE, vol. 86, no. 11, pp. 2278–2324, Nov. 1998.
[23]. Bae, H., et. al., "Security and Privacy Is-sues in Deep Learning", arXiv preprint arXiv:1807.11655, 2018.
[24]. Braun, S. K., "Forensic evidence of copyright infringement by digital audio sampling analysis - iden-tification marking", International Journal of Cyber-Security and Digital Forensics (IJCSDF), 3(3),170-182.
[25]. L. Deng and D. Yu, ''Deep learning: Methods and applications,'' Found. Trends Signal Process., vol. 7, nos. 3-4, pp. 197-387, Jun. 2014.

[26]. Akhtar, N., & Mian, A., Threat of adversarial attacks on deep learning in comput-er vision: A survey. IEEE Access, 6, 14410-14430, 2018.

[27]. I. M. Coelho, et. al., ‘‘A GPU deep learning metaheuristic based model for time series forecasting,’’ Appl. Energy, vol. 201, no. 1, pp. 412-418, 2017.

[28]. I. Zliobaite, et. al., ‘‘Evaluation methods and decision theory for classification of streaming data with temporal dependence,’’ Mach. Learn., vol. 98, no. 3, pp. 455-482, 2015.