International Journal of Management, IT & Engineering
Vol. 9 Issue 4, April 2019,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Deep Learning For Cybersecurity: Developments, Issues, And Possibilities

Reetu Kumari Assistant Professor
KalpnaChawala College of Education for Women
Hissar ,Haryana Pincode-125001

Abstract

This article summarises the expanding scientific literature on DL's effects on cybersecurity, conducts a thorough and methodical examination of the many methods for detecting cyberattacks, and categorises the various DL-based cyberattack detection systems now in use. We investigate methods for using GANs to attack deep learning infrastructures. It describes the datasets used to assess the effectiveness of the cyberattack detection system suggestions made by researchers. We compile a comprehensive database of all the articles ever published regarding applying DL to the topic of cybersecurity and analyse their trends over time. While deep learning has been around for a while in the realm of data science, new technological trends and improvements have given it a chance to really take off in the world of cyber security. This article provides a brief overview of some of the commercially available deep learning-based cybersecurity solutions. There will be almost 15% more data breaches and cyberattacks in 2021 than in 2020. It is predicted that attacks like ransomware and social engineering schemes would rise as a consequence of IT faults including poorly built networks, poor maintenance practises, human error, and an unclear IT asset set. With the advent of deep learning technology, however, firms may take preventative measures against cyberattacks.

Keyword:*Cyber World, Proactive Nature,****Cybersecurity. Hardware Maintenance,Virus***

Introduction

Significant cyber security difficulties have emerged as a result of the increasing frequency of network attacks in recent years. Even more so now, with the advent of cutting-edge smart network technologies, cyber security is of paramount importance in the defence of critical infrastructure against attacks and unauthorised access. Cybersecurity relies on a wide variety of methods and resources. Application security, information security, network security, disaster recovery, operational security, end-user education, and so on are only some of the many subsets of cybersecurity. Cyberspace is one of the most significant challenges to national security and economic stability in the twenty-first century (Cyberspace Policy Review, 2009). There is an urgent need to learn why certain individuals launch cyberattacks. With devastating effects like the exposure of private information, the suspension of essential services, the introduction of new vulnerabilities, and the theft or illegal use of hardware and software, cyberwarfare, fought without conventional weapons, is among the most destructive forms of modern conflict. The majority of respected organisations, including banks, retailers, critical infrastructures like SCADA and power grids, etc., continue to face cybersecurity challenges. A cyberattack is any hostile act committed against a computer system, network, or individual user's device. Cyberattacks may be launched by anyone from a nation-state to an individual, a small group, a community, or a large organisation. A cyberattack might be initiated by a party still in the shadows. Any computer system vulnerable to hacking is at danger of being used in an attack that might steal from, alter, or destroy its intended target. **(Lin, 2016)**

While numerous attack detection systems exist already, the exponential growth in attack volume and the development of hacking tactics need the development of new detection technologies. Although existing machine learning techniques have proven useful over the last several decades, they currently have limited scalability over a vast network and have difficulty detecting cyberattacks in large, scattered settings. Traditional machine learning approaches have the drawback of requiring human generated characteristics to do the recognition work. Although having a computer that can automatically recognise and categorise the features required for attack detection is ideal, it is not essential. **(Imamverdiyev & Abdullayeva, 2018)**

Deep learning is now one of the most active research fields in the field of artificial intelligence, providing significant new possibilities for going beyond the limitations of classic machine learning approaches. Features are often retrieved by humans in classic machine-learning methods. Specifically, scientists are looking at "feature engineering." However, deep neural networks do feature extraction more effectively than humans do in huge data processing. **(Imamverdiyev & Abdullayeva, 2018)**

Objectives of Paper

- Disscuss about Cybersecurity in India: Background
- Disscuss about Proactive Nature Of Deep Learning
- Disscuss about **Protection from Malicious Software and External Attack**
- **Disscussabout** Dangerous Cybersecurity

Review of literature

Dewar (2014) One of the goals of cyber security is "to allow cyberspace activity without worry of physical or digital harm" (p. 18). Diverse countries use different approaches to cyber security due to their differing perspectives on the attribution issue and the accumulation of interplays across securitization components. The three main approaches to cyber defence that Dewar describes using the triptych concept are Active Cyber Defense (ACD), which "focuses on identifying and neutralising threats and threat agents both inside and outside the defender's network," Fortified Cyber Defense (FCD), which "builds a protective environment," and Resilience Cyber Defense (RCD), which "focuses on ensuring system continuity" (Ibid). He also shows that the United States and the United Kingdom have consistently opted for the ACD, while Germany has settled on the FCD, and the European Union and Japan have opted for the RCD (Ibid).

Dunn-Cavelty (2010, p. 363)refers to "the insecurity caused by cyberspace and the technological and non-technical ways of making it (more) secure." According to this definition, unlike many of the cyber security-related studies mentioned in recent years, cyber security is more than just a "technical" concern linked to computer science, encryption, or IT (e.g. Vacca 2013, McLean 2013). As it turns out, cyber security is a vast and intricate field. She goes on to classify what she calls "three interlocking cyber-security discourses," which include the "technical discourse" of "viruses, worms, and other bugs," the "crime-espionage discourse" of "cyber-crooks and digital spies," and the "militarycivil defence discourse" of "cyber(ed) conflicts and vital system security" (pp. 364-369).

(Baskerville, 2016) Many people in the contemporary world have been negatively impacted by the lack of cyber security. The proliferation of new apps made possible by rapid technical advancement is largely to blame for this rise in cybercrime, which threatens the safety of millions of internet users. Information security refers to the practise of using appropriate technical and operational safeguards to protect many types of information systems, including but not limited to applications, data centres, databases, computers, and networks. Computer networks and sensitive data may be better protected thanks to anti-virus programmes, firewalls, and other technical solutions. They aid in safeguarding online users and computer systems, but nevertheless present significant risks to those who use and manage such systems. The primary goal of increasing network security necessitates that many companies upgrade their network architecture to guarantee the continued safety of their computer systems and networks.

(Simon, 1996) Considering that people are the most vulnerable part of any computer system, how can we lessen the impact of this weakness? Phishing emails and accidental misuse of USB flash drives are just two examples of the kinds of dangers that a company faces, and unfortunately, there aren't many safeguards in place to fight against them save ongoing training and awareness programmes. If even a single phishing email is able to breach the network perimeter and deliver a malicious payload, then the most advanced defense-in-depth model in the world is useless. Both scenarios result in the same loss of IT expertise for the company. There is no such thing as a foolproof security instrument, and it is ludicrous to expect any security software to intercept every possible security risk. Understanding and controlling the human element of computer security is essential, as shown by the notions of limited rationality and satisficing decision making

Cybersecurity in India: Background

Policymakers in India have paid so little attention to cybersecurity that the government is struggling to meet people' demands for increased safety measures. India has pathetically weak defences against modern cyberthreats like Stuxnet, Flame, and Black Spectre. As a result, compared to other wealthy countries, India has far less strategies and actions related to cybersecurity. As a result, the Indian government has been unable to go forward with a number of vital measures. Both the National Critical Information Infrastructure Protection Centre (NCIPC) and the National Cyber Coordination Centre have been approved but none has been implemented in India (NCCC). India established its National Cyber Security Policy in 2013, however its execution has been lacking in a number of important areas, such as the protection of personal data and the upholding of civil liberties. India is home to a number of crucial infrastructure nodes, including monetary institutions, satellites, automated power networks, and thermal power plants. The government of India has highlighted the worrying rise in cyberattacks on banks and other financial institutions. India has encountered a wide variety of Internet-based threats, including viruses, hacking, identity theft, spamming, email bombing, website defacement, online defamation, and service outages. In spite of being ranked #81 for internet access, the nation is #7 for cybercrime. The alarming increase of cyberattacks, from 23 in 2004 to 62,000 by mid-2014, is a major cause for worry. There was a 136% rise in cyber threats and assaults against government entities in 2013, with attacks on Indian financial services businesses increasing by 126%. About 69% of breaches have targeted enterprise-level organisations (IANS 2014). Symantec, a security software provider, stated that in 2014, 40% of assaults were directed against business and commercial services, hotel and individual services. India needs a comprehensive strategy for dealing with cybercrime so it can battle these and other threats.**(Verma & Sharma, 2014)**

Deep Learning Plays a Role in CyberSecurity

Deep learning (DL) is a subfield of machine learning (ML) that can learn to become better on its own by poring through existing computer programs. Deep learning is the process of using artificial neural networks to achieve cognitive and learning capabilities that are similar to those of a person. Recently, advances in computing power have allowed neural networks to surpass previous limits on their complexity. However, advancements in big data analytics have made it possible for neural networks to be considerably larger and more complex, potentially allowing computers to surpass humans in situations involving observation, learning, and fast reaction. The dynamics of today's assaults are always shifting, and the solutions we have for cyber security today can't keep up. This is particularly true in terms of their capacity to identify novel threats, analyse intricate pathways and events, and scale to handle massive quantities of assaults. Many of these problems may be handled by applying deep learning to conventional cyber security activities including DDoS detection, anomaly detection, malware and botnet detection, and voice recognition. **(Aditham, Ranganathan, & Katkoori, 2017)**

The Proactive Nature Of Deep Learning

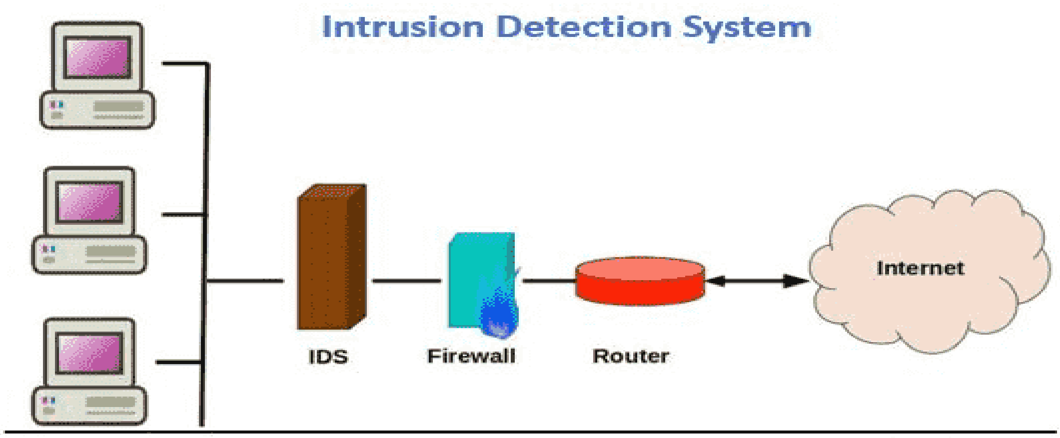
The vast majority of current cybersecurity tools are symptom-based, meaning they can only be used to locate potential dangers after they have already been seen. Most of the time, they can only detect threats they have already seen, rendering them ineffective against brand-new, never-before-seen hazards, often known as "zero-day" threats. Deep learning algorithms employ neural networks to simulate the human brain's ability to "learn" and change in response to new information. That makes it more capable of automatically adjusting to the wide variety of threats in the world. In contrast to ML, which requires human assistance to adapt fast enough, DL is continually becoming better at what it does thanks to its capacity to learn, making it more adept at preventing potential threats before they ever arise. It's possible that DL will work very well for ID/IP, the process by which malicious network activity is identified and bad actors are prevented from accessing a network. Too many false positives were produced when machine learning (ML) was used for this purpose, making it more difficult for security teams to detect and eradicate true threats. Better able to differentiate between benign and malicious traffic, ID/IP systems might benefit from DL neural networks' improved traffic analysis.(Teyou & Ziazet, 2018)

Behavior Analysis

In order to ensure the success of a deep learning-based security approach, it is essential to constantly monitor and analyse user behaviour and patterns. Bypassing security measures and, at times, without producing any signals or alerts makes it more harder to detect than more conventional hostile activities against networks. For instance, many forms of cyber defence are helpless in the face of insider attacks, which occur when employees use their legitimate access to the system for nefarious ends rather than using an external hacking technique. Analytics of User and Entity Behavior may be used to defend against such attacks (UEBA). Following an initial period of setup, it has the potential to learn to recognise regular patterns of employee behaviour and to signal any abnormalities that might suggest an insider attack. **(Lee, 2015)**

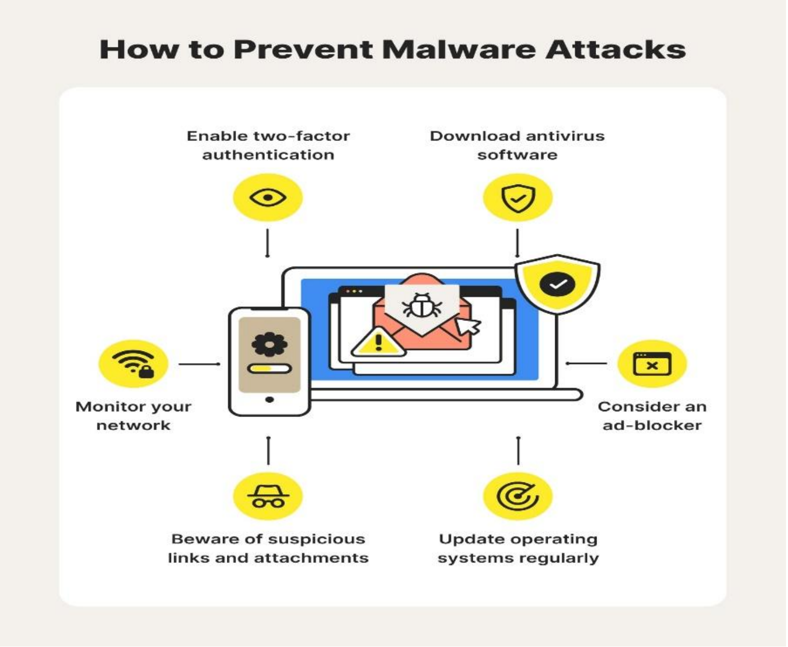
Detection of Intrusion

An IDS/IPS may monitor a network for suspicious activity, block it if it's about to happen, and notify users. They have commonalities and extensive patterns of violence that make them easy to identify. This way, hackers and other malicious actors are less likely to compromise sensitive information. Previously, this duty was handled by machine learning techniques. However, numerous false positives were generated by the system due to the algorithms, making the work of security experts much more taxing than it already was. Smarter ID/IP systems can be created with the help of deep learning, convolutional neural networks, and recurrent neural networks, all of which improve the accuracy with which traffic is analyzed, reduce the number of false alerts, and aid security teams in distinguishing between malicious and lawful network activity. ***(P. W & Friedman, 2014)***



Dealing with Malware

Signature-based detection is often used by traditional malware solutions like standard firewalls to identify malicious software. The business maintains a dossier of possible dangers and regularly updates it to account for new dangers. This tactic is useful against less sophisticated threats but fails miserably when facing more sophisticated adversaries. Because they don't depend on a library of previously recorded signatures and standard attack tactics, deep learning algorithms can spot more nuanced threats. Instead, they get to know the system *inside and out, keeping an eye out for anything out of the ordinary that may be malicious software.**(Dilipraj, 2013)***



Email Monitoring

Emails sent and received from official company accounts must be inspected often in order to prevent hacking of any kind. Phishing attacks, for instance, often involve sending emails to workers in an organisation with the express purpose of obtaining personal details. Such assaults may be thwarted with the use of deep learning and cybersecurity programmes. Emails might be screened for suspicious behaviour using NLP.**(Verma A. K., 2014)**

Cybersecurity

The goal of data security is to prevent unauthorised parties from accessing or modifying your data, whether they are within or outside of your organisation. Computers, networks, programmes, and data are all examples of digital resources, and there are many different ways to protect them from destruction. Privacy, data, and system availability must all be at the forefront of any comprehensive cybersecurity strategy. Cybersecurity issues may have far-reaching consequences for a firm, including damage to its brand and disruptions to its daily operations. Credit card and bank account data may be easily hacked. This kind of personal data is a hot commodity on the "dark web," where it can be bought and sold with relative ease. If this information falls into the wrong hands, the business might lose access to banking and credit card services and perhaps violate data protection laws. Every month, news of a major security breach involving personal information is reported somewhere in the globe. A distinct but related issue is the potential harm to the company's image should hackers get access to sensitive information. The effects of data loss on a company's reputation may be severe. The loss of goodwill and reputation might be far more devastating than the data itself. The firm might be subject to legal or regulatory action in the case of a data breach. A claim may be filed against a business by a third party that has experienced some kind of damage. In many nations, businesses may face significant penalties and even legal action if they are found to have violated privacy laws. Ransomware is the latest and most dangerous cyber menace, wreaking havoc on organisations of all sorts.

Since at least 2012, stories have surfaced of ransomware attacks with a business motivation. Malicious software may remain hidden until the victim opens a certain file. If the virus is running, it may encrypt the company's data using a key that is only known to the hackers, or it could connect to a command and control site and wait for orders. If an attacker gains access to encrypted data after a breach, that material will remain unavailable to the firm until the attacker gives over the key. Worries about data loss arise when an adversary encrypts all accessible data, which often includes backup data and systems. The data has been taken hostage by the attacker, who demands a ransom in exchange for its release. To decode the data using a standard desktop computer is estimated to take five quadrillion years if the user does not pay the ransom. Researchers may have found a means to decrypt the data by exploiting a vulnerability in the encryption's architecture, giving hope to the impacted organisation. Organizations have two options: pay the required ransom or attempt to recover their data and systems by reverting to an earlier backup. Unless the integrity of the environment is restored, restoring the data does not eliminate the risk of the ransomware being reactivated or reappearing.. **(Daniel, Rabih, & Julie, 2017)**

Protection from Malicious Software and External Attack

A company's preparedness is essential in the face of a dynamic threat landscape where new risks are continually emerging. The following are some of the most vital system tools and approaches for warding against such attacks: Firewalls are a kind of security software (and hardware) that blocks unauthorised users from entering a network. Malicious software, such as malware, spyware, and web proxies, may arrive through pop-up windows and may have more nefarious goals, such as capturing credentials for fraudulent use, therefore taking precautions against it is essential. Email inboxes may be protected against unwanted, mass-distributed communications with the use of anti-spam software. By using anti-phishing software, users are protected against bogus websites that seek to steal personal information. There can be no reliable system with several layers of defence without all of these components. The price of security measures should be assessed against the potential costs of an attack, which might include the loss of data, fraud, and the cost of rebuilding systems. You should do business with a reputable, established company. Some companies advertise themselves as providing these services, but their products might really be malicious software. Never download software from an unknown source, no matter how tempting it may seem. Since they will be responsible for implementing and maintaining the company's chosen tools, the systems integration (technical support) departments are the best persons to consult with about the equipment the business should acquire. Maintaining current versions of these applications is essential. Unfortunately, malicious software is spreading at a frightening pace. Most software companies provide updates to their databases on a daily basis to keep the system safe. Accurate implementation of these adjustments is essential. **(Thomas J, 2016)**

International Journal of Management, IT & Engineering
Vol. 9 Issue 4, April 2019,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Hardware Maintenance Plans

Hardware vendors should be kept on a maintenance contract in case of hardware breakdown. Service level agreements (SLAs) should detail the minimum standards to which a provider must adhere in the case of a service interruption. Immediate maintenance is required for mission-critical gear such servers, switches, and backup systems. In the event of a breakdown of these parts, many contracts require a response time of no more than four hours. For less crucial equipment, such individual workstations, response times might be longer. In order to quickly replace a faulty component in the event of a failure, some firms, particularly those in remote areas, invest in several copies of critical components like their power supply. The company must ensure the support company has sufficient replacement components on available to meet the SLAs.. **(Eldad, 2005)**

Dangerous Cybersecurity Myths

- ***Cybercriminals are outsiders***. In fact, hostile insiders, either acting alone or in collaboration with hackers from the outside, are typically to blame for cybersecurity breaches. These insiders may be affiliated with well-structured organisations supported by governments.
- ***Risks are well-known***. In reality, the threat landscape is growing as hundreds of previously unknown security flaws in both legacy software and cutting-edge hardware are discovered and published. However, the number of potential entry points for human error, in the form of careless workers or contractors that accidentally create a data breach, is growing.
- ***Attack vectors are contained***. Cybercriminals are finding new attack vectors all the time - including Linux systems, operational technology (OT), Internet of Things (IoT) devices, and cloud environments.
- ***My industry is safe***. Cybersecurity threats affect every sector of the economy, as hackers target the communication infrastructures of both public and private institutions. Supply chains, ".gov" websites, and key infrastructure are all more at risk, and ransomware attacks are now targeting a wider variety of organisations, including local governments and non-profits. **(Bendovschi, 2015)**

Conclusion

Cyber security is becoming more important as the frequency of cyberattacks and data breaches increases. In 2016, 46% of organisations, up from 28% in 2015, reported a "problematic absence" of cybersecurity skills, according to research from Enterprise Strategy Group. Experts in cyber security are in high demand from a variety of sectors, including corporations, governments, and non-profits. The demand for qualified cybersecurity workers is growing rapidly across several industries, including the financial industry, healthcare, and retail. In official contexts, however, the term "cybersecurity" is more often employed. Analyzes and assesses infrastructure vulnerabilities; investigates how to best make use of existing tools and countermeasures to address identified flaws and recommends improvements (software, hardware, networks). Assesses the level of harm to data and infrastructure caused by security incidents, weighs available recovery solutions, and suggests improvements. Control tests of the current safety procedures. Possible involvement in planning, implementing, or monitoring safety procedures.

References

Aditham, S., Ranganathan, N., & Katkoori, S. (2017). LSTM-based memory profiling for predicting data attacks in distributed Big Data systems. In Proccedings of the IEEE international parallel and distributed processing symposium workshops.

Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures". Procedia Economics and Finance. doi:10.1016/S2212-5671(15)01077-1.

Dilipraj, E. (2013). India's Cyber Security 2013: A Review." Centre for Air Power Studies. 97 (14): 1–4.

Daniel, S., Rabih, B., & Julie, W. (2017). Security", Towards a More Representative Definition of Cyber. *Journal of Digital Forensics, Security and Law*, 12 (2). ISSN 1558-7215.

Imamverdiyev, Y., & Abdullayeva, F. (2018). Deep Learning method for Denial of Service Attack Detection based on restricted Boltzmann machine. Big Data. doi:10.1089/big.2018.0023 PMID:29924649.

Eldad, E. (2005). Reversing: secrets of reverseengineering. John Wiley & Sons. ISBN 978-0-7645-7481-8.

P. W, S., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press. ISBN 978-0199918119.

Lee, N. (2015). Counterterrorism and Cybersecurity: Total Information Awareness. (2nd ed.) Springer. ISBN 978-331917243.

Lin, T. (2016). Financial weapons of war. Minnesota Law Review .

Teyou, G., & Ziazet, j. (2019). Convolutional neural network for intrusion detection system in cyber physical systems.

Thomas J, M. (2016). Computer Security Discourse at RAND, SDC, and NSA (1958-1970). In *IEEE Annals of the History of Computing* (pp. 38 (4): 12–25). doi:10.1109/MAHC.2016.48. S2CID 17609542.

Verma, A. K. (2014). Cyber Security Issues and Recommendations. *" International Journal of Advanced Research in Computer Science and Software Engineering*, 4 (4): 629–634.

Verma, A., & Sharma, A. (2014). Cyber Security Issues and Recommendations. *International Journal of Advanced Research in Computer Science and Software Engineering*, 4 (4):629–634.