Journal of Scientific & Industrial Research
Vol. 82, December 2023, pp. 1316-1330
DOI: 10.56042/jsir.v82i12.1702

A Review of Deep Learning Strategies for Enhancing Cybersecurity in Networks

Bhuvaneshwari A J* & P Kaythry

Department of ECE, Sri Sivasubramaniya Nadar College of Engineering, Kalavakkam, Chennai 603 110, India

Received 19 May 2023; revised 12 September 2023; accepted 19 October 2023

Rapid technological improvements have brought significant hazards to sensitive data and information. Cyberspace has connected various data structures, ranging from private communications/transactions to government activities. Cyberattacks are growing more complex which emphasizes the need to improve cybersecurity. Cyber security is more crucial as everything becomes more digital and as the number of connected devices keeps increasing. Cyber security techniques are used to keep networks, applications, and devices safe from intruders. Cloud and IoT technologies have expanded the complexity of computing, communication, and networking infrastructures, making cybercrime prevention more difficult. It takes a long time to develop threat recognition algorithms by the existing methods. Innovative strategies, like employing deep learning tools for cybersecurity, are anticipated to provide a solution to the issue. Deep learning approaches have many benefits which include the ability to solve complex problems quickly, high levels of automation, the best use of informal information, the capacity to generate excellent results at a lower cost, and the ability to recognize complex interactions. A diverse range of applications can be employed in deep learning models to make decisions based on predictions in the daily routine. The significant benefits of deep learning-enabled cyber security have improved security and reduced risks. The intensity of this systematic study provides consolidated knowledge about recent trends and serves as a foundation for future research in Deep learning-enabled Cybersecurity. This paper highlights the potential challenges and current cybersecurity issues with cutting-edge Deep Learning technologies.

Keywords: Cyber attacks, Deep learning models, Network vulnerabilities, Security solutions, Threats

Introduction

The advancement of digitization in all aspects of civilization has enabled the storage of a wide range of information.[1,2] The sensitivity of digitally stored data makes it increasingly vital to assure security. The internet and a range of digital technologies have made contemporary life incredibly comfortable. Everything beneficial has downsides, and the current technological world is no exception. While the use of the web has simplified our daily tasks, it also represents a tremendous challenge to data security which leads to online attacks. Data loss from intruders or software invasions, which can have considerably severe repercussions, might come from insecure data. Threats are rising at a much faster rate than in the past. Threats are frequently transient, but they can sometimes be severe and enduring. Cyberattacks are extremely difficult to detect and anticipate. Cyber Security in information technology needs to safeguard systems from cyberattacks.[3] Its intended goals are to mitigate the likelihood of cyberattacks and to safeguard against unauthorized utilization of science and skill, as well as web and network devices.

Cyber security has become essential to protect core ideals like fairness, tolerance, liberty, and user or organization privacy while preserving confidence and dependability in the digital infrastructure. Several technologies and methods have been developed under the cybersecurity umbrella to protect communication networks, end-to-end systems, and data logs from attacks, and unprivileged access. Cyber-defense pathways exist in almost all the layers of the Internet network Model.[3,4] Experts have attempted to address various network security issues such as denial of service, phishing, website incursions, viruses, and routing attacks. The focus is on developing tools and strategies such as firewalls, anti-virus software, Detection Systems, online application security, and so on. Attackers often respond with even more sophisticated tactics to bypass the proposed defenses whenever an intelligent solution is introduced to address network vulnerabilities. Current security systems struggle to keep pace with these evolving and advanced attack strategies. The need to bolster cybersecurity remains constant, driven by the ongoing proliferation of end-user devices and networks.

*Author for Correspondence
E-mail: bhuvaneshwariaj@ssn.edu.in

Emerging approaches, like the utilization of Artificial Intelligence (AI) tools for cybersecurity, are anticipated to provide solutions to this challenge.[5] It would contain a substantial amount of training data with the same pattern as test data for learning. However, acquiring relevant training data will typically take much time or even be impossible in the field of cybersecurity, where new attacks are discovered every day.[6–9]

Deep Learning (DL) is a type of AI that's pushing the high-tech industry ahead. It helps devices and networks learn from messy data and solve complex problems.[7] Intelligent DL machines can train continuously to stay up with real-world scenarios. Deep learning autonomously extracts valuable insights from vast amounts of raw network data, reducing the need for human experts and saving time and resources.[8] These learned features are then used in a learning algorithm to perform classification tasks, resulting in highly accurate threat detection. In DL, a shortage of labeled data is not an issue. The use of DL algorithms in cyber security will guarantee the safety of machines throughout their lifetime. Deep learning with cyber security empowers and enhances systems efficiency, safety, and security.[9] The intersection of DL and Cybersecurity with its sources of literature is shown in Fig. 1.

Some fascinating DL applications in cybersecurity are discussed in this paper as how deep learning might be used to improve security measures. It also interrogates the various defending measures from dangers including phishing, session hijacking, drive-by attacks, routing attacks, denial of service, etc. The article examines the previous advancements and contemporary cybersecurity techniques based on deep learning, thereby a valuable resource for safeguarding cyberspace. This work stands out for its emphasis on the transformative potential of deep learning in cybersecurity, offering a systematic study that consolidates knowledge about current trends and lays a foundation for future research. It highlights the convergence of deep learning technologies with cybersecurity, addressing potential challenges and current issues, ultimately aiming to improve security and reduce risks.

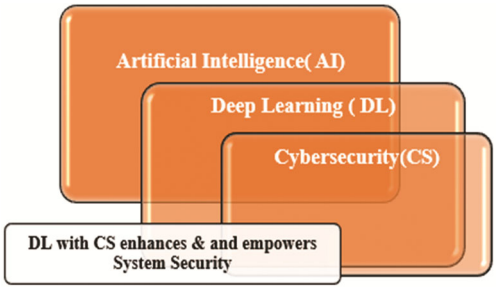

Fig. 1 — Convergence of deep learning and cybersecurity

Literature Review

Deep learning and cybersecurity have both garnered significant research attention, often treated as distinct domains with unique challenges and methods. Recently, there has been a significant merging of DL and cybersecurity. The new trend is altering how we respond to cyber threats and improve cybersecurity. This merging of expertise is reshaping the landscape of cyber defense and threat mitigation. Hence this integration promises more proactive and adaptable cybersecurity solutions as both domains continue to intertwine and advance. In review[1], the author's primary focus was to explore the realm of quantum cybersecurity, and the capabilities of quantum computing for mitigating cyber threats. The survey[3] offers an extensive examination of machine learning techniques applied to cybersecurity intrusion detection systems and its performance was analyzed with benchmark datasets. The authors of survey[4] have provided methods for edge intelligence and intelligent edge deployment with DL. The survey papers[4,5] contributed insights to both domains but did not specifically delve into the security challenges and vulnerabilities within these areas. To the best of our knowledge, the most relevant existing articles to our work encompass the following papers.[2–10] The literature sources have been categorized and assessed for this study, as depicted in Fig. 2.

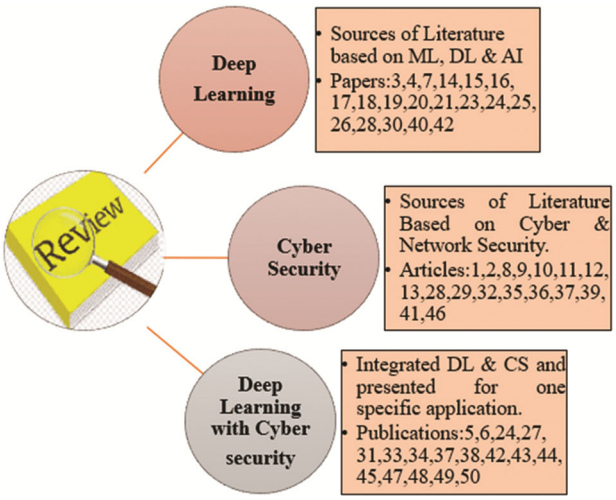

Fig. 2 — Categorized literature review

Integration Problems

The incorporation of deep learning into cybersecurity encounters several challenges and obstacles. Researchers are working to fully realize the potential of deep learning in enhancing cybersecurity by addressing issues including data privacy, model interpretability, and adversarial attacks.

Limitations

Recent studies have looked at deep learning models used for automating diverse security operations such as malware inspection and identifying breaches. However, these surveys exhibit certain limitations: They lack coverage of various cyberattacks in different network settings, and they primarily focus on general deep learning without delving into cyberattack specifics. Additionally, they don't provide guidance on selecting appropriate deep learning models for security or datasets tailored to specific use cases. Moreover, they concentrate on unencrypted traffic and traditional network configurations while neglecting areas like fraud detection and encrypted traffic. Finally, they fall short of delivering clear insights into cyberattacks, vulnerabilities, and mitigation strategies.

Cyber Security Probabilities

Organizations, as well as individuals, should make efforts to counteract cyber-warfare. Background knowledge must be included to give an overview of efficient attack detection based on deep learning techniques.[2,10] Some of the important security domains where cybersecurity is needed are listed in Table 1. Fraudsters are inventing more innovative ways to assault systems as technology advances.

Attacks from nodes that are already members of the network are called internal attacks.[11,12] An attack carried out by an unauthorized node is referred to as an outsider attack. The different kinds of cyber-attacks are illustrated in Fig. 3. These assaults can be divided into active and passive forms. An active attacker can transmit new packets to disrupt the network channel or misrepresent valid information, whereas a passive attacker can simply snoop on the channel and acquire sensitive details. It is broadly categorized based on how they compromise network security features. This section discusses some significant hacks on automobile networks, routing, and cyber attacks due to authentication.

Automotive Networks-related Attacks

With the proliferation of automation in automotive networks, there is a growing reliance on additional sensors, controllers, and interfaces. Reliable and secure connectivity is continuously needed for high-speed transmission. Considering the inherent vulnerabilities of automotive networks and their external interface connections, there is a heightened susceptibility to various potential attacks. These attacks pose a substantial risk to the security and privacy of the automotive network. Listed below are several significant vehicular network attacks, which are also illustrated in Fig. 3(a).

Sybil Attack

A node pretends to be numerous nodes by adopting false identities. It could be possible if the victim possesses false credentials or has their identity stolen. An attacker uses numerous identities to send multiple messages while announcing its positions concurrently. Node duplication confuses the topology, so they all assert their fictitious and illegal authority.[12] These attacks damage network topology and use more bandwidth.

Impersonation Attack

The attacker poses the privileged node identity. The motive is to obtain administrative privileges and disrupt the flow of data.[12] Possession of bogus attributes or identity theft could make these assaults conceivable. Attackers may provide false or spurious details to the nodes to gain an advantage. For example, to clear a route, an attacker feeds false

Table 1 — Various security domains

Domain	Foreword
Network security	Hackers target networks as one of the most susceptible systems. They intend to gain access to computers and other electronic devices to obtain personal information.
Data security	Hackers gain access to data that are exchanged between two or more nodes.
Application security	On the internet, there are a plethora of developers, each with its own set of applications for users. Thus, attackers can get information about the users from devices.
Mobile security	Mobile device security is to shield and rid devices of threats, risks of asset loss, and data loss when utilizing portable computers and communication equipment.
Cloud security	Anyone who wishes to keep their data safe does so through the cloud. Data can easily get into the wrong hands if this is not secure.

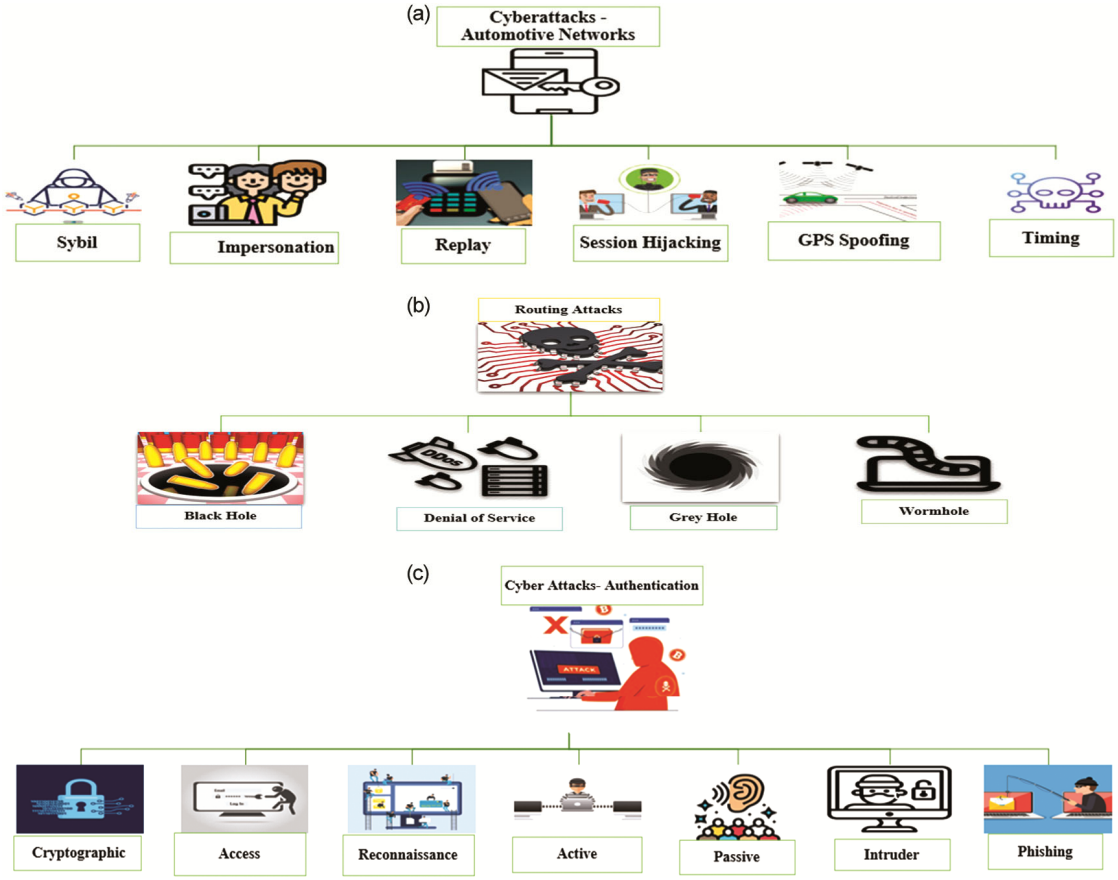

Fig. 3 — Various cyber attacks: (a) Cyberattacks in automotive networks, (b) Routing attacks, (c) Cyberattacks –Authentication

information about a significant traffic jam caused by an accident on a specific road. These threats jeopardize the vehicular network's authentication requirements.

Session Hijacking

It occurs when a hacker attempts to seize ownership of the distinct Session Identifier (SID) provided for every new session. An attacker can exploit the fact that internet layer authentication is only performed once. Attackers can take advantage of this functionality because no authentication is performed once the SID is generated and allocated.

Replay Attacks

The intruder impersonates a legitimate vehicle or Railcar to collect information datagrams before broadcasting a duplicate of the intercepted signal to another node for profit. These attacks cause serious issues to the system's secrecy and authenticity.[12]

GPS Spoofing

Vehicles' identities and geographic coordinates are stored in a database by a Global Positioning System (GPS) satellite. An RF transmitting device deliberately causes a GPS receiver to calculate a false position. The main aim is to disrupt vehicular networks and may feed fake information to the system.

Timing Attacks

To delay communication, an attacker modifies the time slot of a packet that has been received. This modification may prevent the malicious node's neighbors from receiving urgent messages on time. Due to the sensitive nature and urgency of the information in automobile networks, even a small delay could lead to serious congestion or accidents.

Routing Attacks

Many hackers penetrate the server or router of the network and send bogus data to the routing network. Routing attacks rely on holes and gaps in the routing protocols of the network.[11,12] Some of these assault types are discussed below and shown in which is shown in Fig. 3(b).

Black Hole

An attack called the "blackhole" involves a malicious node sending a fake route with fewer hops

in an effort to trick the source node into passing packets through it. Data packets are discreetly dropped by the attacker node after they have been transmitted to the route by the source node. It leads to unreliable network transmission.

Denial of Service (DoS)

The attacker streams the network with too many joining message request and gain the network credentials. Thereby, can significantly affect the effectiveness and performance of a network. Flooding, jamming, or a distributed DoS attack are used to flood the network with fake messages and block legitimate users from accessing a target node.

Grey Hole

Hacked cluster nodes may lose packets intentionally during transmission. However, the attacker chooses only specific packets based on their current requirements & aims.[12] These attacks may cause integrity issues in the routing network.

Wormhole Attack

Attackers construct a tunnel by two or more nodes in the existing topology. Then the packets are received by the node that is acting maliciously and sent to the destination end tunnel. The excavating technique lowers the number of hops along the path, which draws packets to the compromised nodes.

Authentication Related Cyberattacks

An attacker uses an automated process of trial and error to guess the network login credentials or cryptographic key. Thereby, unauthorized access to networks is thus made possible by this method. The attacker accesses private information and changes the original network data. Some of the cyberattacks related to authentication are shown in Fig. 3(c).

Cryptographic Attack

An attempt to recover the plaintext without the key by using practical cryptographic methods. By finding the weakness in a code or cipher, attackers obtain sensitive information and do unnecessary modifications.

Access Attack

The attackers gain access to the network and modify the stored confidential information. Attackers use web apps and file transfer services to gain access to databases, e-mail accounts, and other sensitive information. It may end up in data breaches, which can result in data loss or data content alteration.

Reconnaissance Attack

A reconnaissance attack is a type of security breach in which an attacker collects an extensive amount of information about the target network. The culprit authenticates to the targeted systems to look for any vulnerabilities. With the actual acquired information, hackers cause serious damage to the network.

Active Attack

The hacker actively tries to alter or manipulate the content of messages or information. These assaults endanger the system's integrity and availability. Illegal authentication interferes with the system processes and causes serious issues to the network.

Passive Attack

The attacker's primary objective is to obtain network-sensitive information by listening to the conversations between hosts. The attacker simply checks the target's capability to view the data during transmission rather than breaking into or altering the database.

Intruder Attack

In an intrusion assault, an unidentified device or service attempts to get into the network, in order to disrupt it or collect false attributes. The intruder is a vulnerability to the network and gains access to the stored data. It causes customized threats and potential attacks on many networks.

Phishing Attack

An act of deceiving users and obtaining sensitive and personal information-including payment card numbers and account credentials by delivering false communications through various channels such as emails, text messages, and social media.[13]

Deep Learning Methods

The term "Deep" refers to the number of computation levels that information can pass through. DL includes statistics and predictive modeling. Deep learning accelerates and streamlines the system process, which is highly useful for data analysis.[1–9] Unlike conventional machine learning algorithms, DL procedures excel at handling complex problems. The DL algorithm nonlinearly adjusts its input to what it has learned to build a statistical model. Many iterations are carried out to get satisfactory results. Deep learning has the advantage of allowing the software to independently expand its feature set. Unsupervised deep learning is often more rapid and precise for any application.

Strategies in Deep Learning

A wide range of DL approaches are accurate and effective in handling difficulties that are too difficult

for the human mind to comprehend.[7,8] Some of the traditional DL methods with their advantages are depicted in Fig. 4.

Convolutional Neural Networks (CNN)

CNN is a more sophisticated and incredibly promising version of the traditional artificial neural network concept. CNN excels in tasks involving data preprocessing, compilation, and intricate operations, yielding impressive outcomes.[8] It is based on how neurons in the nervous system are structured. Among its capabilities, CNN excels in tasks such as image recognition, fragmentation and video review.

Deep Reinforcement Learning (DRL)

The DRL empower systems by allowing agents to make independent decisions based on unstructured input data (by Reinforcement learning techniques), eliminating the need for manual interpretation. These agents can observe the situation while taking actions that contribute to the network's overall objectives. The current environment state is encapsulated within the input layer of the network architecture. This concept hinges on repetitive attempts to predict the potential rewards associated with each decision made under particular conditions.[13,14]

Recurrent Neural Networks (RNN)

The Long Short-Term Memory (LSTM) method is employed in RNN. It can foresee data in temporal sequences with accuracy. It employs prior condition knowledge for an input parameter.[15] As a result, it can assist a network in constructing poor memory, allowing it to successfully handle fluctuations in stock prices or any other time-based data systems.

Generative Adversarial Networks (GAN)

Classifier helps distinguish between accurate information and fraudulent details produced by the Generator Network. Instead of using real photographs, an image bank might be built from simulated information generated by the Generator network.[15] A convolutional neural network would be built in the first stage. A system comprising image indicators would subsequently be deployed to differentiate between authentic and counterfeit pictures. The effectiveness and speed of the network would ultimately benefit from this competition.

Self-Organizing Maps (SOM)

SOM is trained using competitive learning rather than error-control learning. Here unsupervised learning data are used to reduce the number of unpredictable elements. This technique produces a resultant model with a dimension of two and links to both input and output nodes. The SOM alters the corresponding weights of the adjacent units in accordance with the weight of the Best Matching Unit (BMU). Since those particular weights can be considered significant unit attributes as a whole, their significance indicates the node's position in the structure of the network.

Boltzmann Machines (BM)

The network architecture incorporates circular connections among its nodes due to its absence of a fixed direction. Once the connectivity is properly constrained, BM learning methods are good enough for problem-solving. This method is used to create model parameters due to its uniqueness. Boltzmann Machines is a stochastic network model, in contrast to all previous deterministic network models.

Auto Encoders (AE)

AE learns efficient codings of unlabeled data (unsupervised learning). They achieve this by employing an encoding function to condense the input data and a decoding function to reconstruct it. It operates independently using every input it receives before requiring an activation function and processing

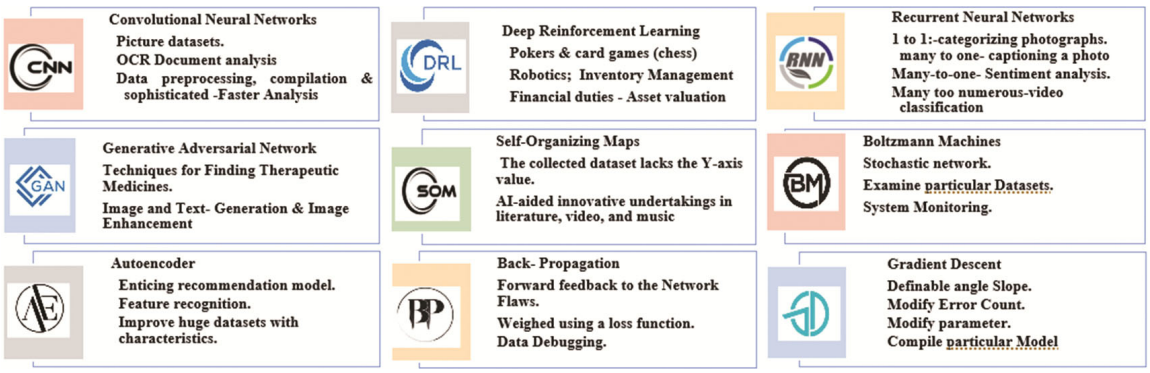

Fig. 4 — Traditional DL methods

the result.[15] Fewer data categories are formed, and all the data structures are used.

Back Propagation (BP)

The back propagation method learns from incorrect data prediction. Data flow in a given direction over a predetermined channel is referred to as propagation. When a choice is made, the entire system is capable of moving forward and feeds back any information about network flaws in reverse. The network first considers the parameters and makes a decision regarding the data. Secondly, it is weighed using a loss function. Finally, any erroneous parameters are self-corrected as a result of the discovered problem being transmitted backward.

Gradient Descent (GD)

A mathematical relationship between variables can be used to represent a gradient, which is a slope with a definable angle. The link between the artificial neural network's prediction error and the data settings may be expressed as the value of x & y in this deep learning approach. The error can be raised or lowered by making small changes in the dynamic network. Data trapping in the neural pathways would slow reconstructions and reduce their accuracy.

Deep Learning Model for Cyberattacks

An overview of conceivable cyberattacks in the context of digital network scenarios. Alongside these potential threats, Table 2 also presents a comprehensive set of countermeasures based on Deep Learning (DL) models. These countermeasures are designed to enhance the security and resilience of digital communication networks by leveraging the power of DL algorithms to detect, prevent, and respond to cyber threats effectively. This table serves as a valuable reference for understanding the range of cyber risks associated with Networks with their target area and security violations.

Advancement of DL in Security

Deep learning techniques have recently evolved to use larger datasets and more complex architectures, as well as to interact between various neural network types.[15] Some of the important recent developments in Deep learning methods are listed in Fig. 5.

Transfer Learning (TL)

Transfer learning improves the earlier learned model and connects it to its current network. TL aims to improve the effectiveness of the right particular population on targeted domains.[16] Transfer learning in cybersecurity involves leveraging knowledge from one domain or dataset to enhance cybersecurity tasks in another domain. This approach enables more efficient and accurate cybersecurity solutions, even when labeled data is limited in specific domains. Transfer learning become a suitable methodology for cybersecurity applications where acquiring training data is difficult.[17] Autoencoders with adapted TL are more effective for cybersecurity in automotive networks. It helps in feature extraction, threat intelligence integration, malware and intrusion detection, behavior analysis, adversarial attack

Table 2 — DL solutions for cyberattacks

Cyberattacks	Target Area		Security Violation	DL Methods
	Threats	Action/Vulnerable		
Sybil	User identity	Network bandwidth	Illegal Authority/Privacy	DRL/RNN
Impersonation	Privileged node	False information	Authorization/Privacy	CNN
Session hijacking	New sessions	Seize session identifier	Authentication/Secrecy	CNN/RNN
Replay	Legitimate node	Duplicates information	Secrecy/Authenticity	CNN/AE
GPS spoofing	Geographic data	GPS satellite signal	Authentication /Security	CNN/AE
Timing	Time slots	Missed deadline	Connectivity/Congestion	CNN/BM
Denial of service	Legitimate node	Flooding & blocking	Privacy/Availability	DRL/RNN
Black hole	Root node	Fake route	Availability/Confidentiality	CNN/GAN
Gray hole	Packet datagram	Packet loss	Authentication/Integrity	CNN/GAN
Wormhole	Network path	Malicious packet	Authentication/Connectivity	CNN/AE
Cryptographic	Data	Message modification	Privacy/ Secrecy/Security	CNN/GAN
Access	Login node	Data/Database	Secrecy/Security	CNN/AE
Reconnaissance	Machine/System	Data/Database	Secrecy /Confidentiality	CNN/AE
Active	Process	System data	Integrity / Availability	CNN/BP
Passive	Legitimate node	Eavesdropping	Privacy/ Secrecy/Security	CNN
Intruder	Service attempt	Disrupt network	Authenticity / Integrity	RNN/AE
Phishing	End user	False information	Availability / Authentication	DRL/RNN

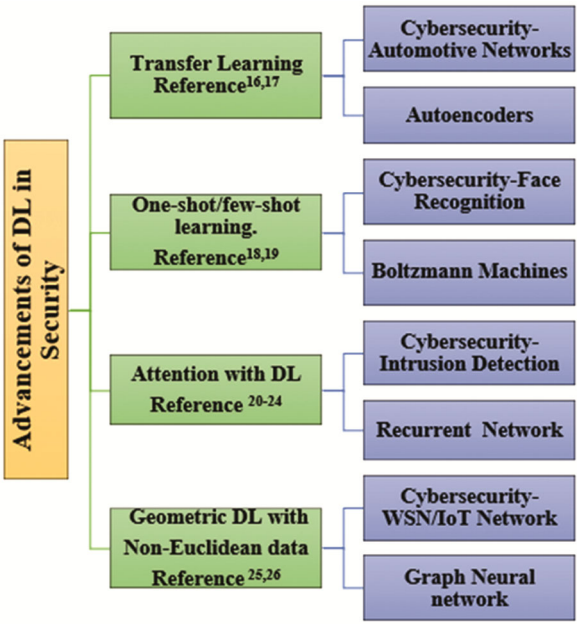

Fig. 5 — Recent DL methods

detection, real-time monitoring, and zero-day attack detection.

One-Shot/Few-Shot Learning

One-shot learning uses existing data to complete categorization problems. One-shot learning is commonly used in the recognition of facial features, particularly for verification & identification.[18] Face embedding constitutes a haze low-dimensional description of features that facial recognition systems learn. The Siamese network technique has found application in one-shot learning. It now utilizes contrastive and triplet loss functions to generate high-quality face embeddings.[19] Instead of relying solely on previous training data, it leverages the category's meta-description and connections. Deep one-shot learning paradigms have tremendous potential for identifying novel threats or intrusions. One-shot/few-shot learning avoids the requirement to collect and train models using a large dataset. Few-shot learning makes use of a limited number of instances from fresh data to teach itself a new task. When there is insufficient information to create a believable model, a few-shot learning approach at the data level is effective. The data-level method leverages a large base dataset for additional features and minimizes the overfitting and underfitting functions.[19] The overfitting issue in few-shot learning must be solved using parameter-level methods. These techniques encompass regularization, appropriate loss functions, and constraints within the parameter space. By doing so, the limited training samples can be effectively generalized even with a smaller dataset.

Attention-Based DL

The attention-based DL strategy emphasizes the importance of certain elements or parts within data sequences.[20] They enable the model to extract meaningful patterns and relationships from the input, enhancing its performance in various tasks.[21] Usually, recurrent networks (such as LSTM, Bi-LSTM, and others) are utilized in conjunction with such attention processes.[22] attention-based Deep Learning in cybersecurity allows for a more precise and efficient analysis of security data, helping organizations to detect and respond to threats effectively while minimizing false positives. It enables a deeper understanding of complex patterns within data, making it a valuable tool in the ongoing battle against cyber threats.[23] The field of cybersecurity has demonstrated the use of attention techniques to achieve outstanding accuracy in intrusions and threats.[24]

Geometric DL with Non-Euclidean Data

Non-Euclidean data is data in which the underlying domain does not use Euclidean distance as a metric between domain points. Geometric Deep Learning (DL) with non-Euclidean data is a burgeoning field with significant applications in cybersecurity. This approach allows for the analysis and modeling of complex data structures that do not adhere to traditional Euclidean geometries, such as graphs, networks, and irregularly shaped data.[25] Combining these applications with enlarged graph learning makes a thorough grasp of diverse subjects. Graph neural networks (GNNs) are starting to be applied in the context of cybersecurity.[26] It enables the modeling and analysis of complex data structures commonly encountered in this domain, leading to more accurate threat detection, anomaly identification, and enhanced security measures.

Deep Learning in Cyber Security

Deep learning in cybersecurity enables networks to learn from unstructured data and tackle complex problems.[2] Deep learning-based defense systems automate cyberattack detection.[3] The DL-based cybersecurity systems' key performance indicators are speed detection. Deep learning offers several significant advantages in the realm of network security, making it a valuable tool for safeguarding

digital assets and defending against cyber threats.[4] DL results are more accurate and reliable for known and unknown threats. It executes at a faster rate and achieves appropriate results. This section discusses the DL techniques for intrusion detection, malware analysis, spam detection, fraud identification and traffic analysis. The various deep learning applications for cybersecurity are illustrated in Fig. 6.

Intrusion Detection System

An intrusion detection system, whether in the form of hardware or software, is a vigilant entity that closely observes networks or systems for any breaches of established policies. The primary type of this system is a Network Intrusion Detection System (NIDS). NIDS manages and tracks network datagrams at several locations for any suspected intrusions as well as anomalies. It could be made up of equipment (detectors) and software (consoles).[27] The Host Intrusion Detection System (HIDS) monitors activities in the host system. Despite being limited to a single system, it is more capable than NIDS since it can retrieve secret messages heading across the various subnets.

A cloud intrusion detection system has an exclusive layer for the cloud. The fog layer enables demand-based authentication within an Application Programming Interface (API), concurrently establishing a connection between the existing system and hyper-virtualization. In the assessment of network traffic flow, detection systems utilize a variety of detection techniques such as Knowledge-based, activity-based, anomaly-based, and signature-based methods. Knowledge-oriented detection entails inspecting network data for patterns that fit known or pre-existing fingerprints. This method of detection looks at active attacks that exhibit specified fingerprints, but it must be updated regularly to accommodate evolving trends in attacks. In contrast, activity-oriented detection entails analyzing network data to find patterns that differ from conventional or benchmark behavior. When data traffic surpasses a predefined threshold, this form of inspection scrutinizes the data and applies analytical methods to detect anomalies. Subsequently, it notifies the administrator or supervisor about these deviations. Anomaly-oriented detection would detect fresh deviations, it requires significantly more computing power in real-time. Furthermore, very minor deviations from the starting point could activate a warning signal, raising the likelihood of false positive results. The signature-oriented analysis compares known protocol characteristics to network congestion. Using predetermined, vendor-supplied profiles, it recognizes an unpredictable series of instructions on the internet and application layer.[28]

Software Defined Networks (SDN)

It separates the system's centralized unit from the network's nodes with a controller. Software-defined networks monitor the overall network and have the authority to thwart any incursions. Three models employed in an SDN infrastructure are Naive Bayes (NB), Nearest Centroid (NC), and Support Vector Machine (SVM). Flow characteristics are generated from network traffic traces and then supplied to the classifier for prediction. The real-time network data traffic acquisition and application categorization capabilities of the SDN platform provide challenges. One of the works in the literature [29] used a model with a unique softmax layer as the final layer. This layer could classify normal and abnormal traffic flows. The suggested model, once trained on the NSL-KDD dataset, is capable of identifying intrusion activities.[30] Subsequently, this model was subjected to reasonable testing in conjunction with a federal SDN manager, facilitating the analysis of arriving traffic.

The prediction was made by identifying abnormal traffic due to spyware. The test results demonstrated that their model used only six fundamental flow

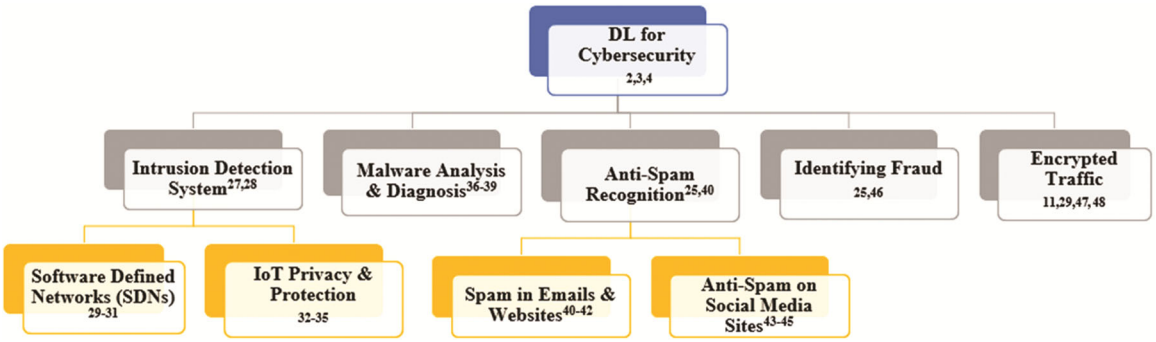

Fig. 6 — DL for cybersecurity

variables. However, noticeable overfitting evidence indicated that regularization procedures could improve results. Due to the constraints faced by RNN, the anticipated method falls short when dealing with network link records that exhibit strong temporal correlations. Consequently, the literature recommends an intrusion detection system that integrates RNN by autoencoder (AE) models. The work analyzed existing vulnerabilities in SDN networks and virtualization technologies. That could be used as part of a botnet with network function virtualization and to fight against DoS assaults in an SDN. Most experiments achieved an Area Under the Curve (AUC) of 0.988, which is a deep learning evaluation statistic.[31]

Deep Learning for IoT Privacy and Protection

The Internet of Things (IoT) comprises several kinds of smart and sensing devices. IoT devices can exchange, collect and send data between connected networks. IoT communication networks could be an infrastructure-less environment with minimal human intervention.[32] According to the application environment, IoT systems are self-configuring and self-adapting. Ensuring top-level protection for IoT systems with portable or wireless networks is a major concern. This IoT systems deployment could face new security issues. Although it is a centrally administered device that anybody may access, IoT must take security measures against assaults like botnets, malicious attacks, and DoS.[33]

Security Breach for IoT

- Heterogeneity- each IoT device has its own set of Standards. All devices must function together under the supervision of a centralized node. The network's security will suffer as a result of this variety.
- IoT devices are always low-power, low-energy efficient, and small in size, allowing a large amount of data to be transferred across the internet and making it easy for hackers to get access to the central system.

This study tries to give a comprehensive overview of deep learning techniques to address security and privacy issues in the IoT.[34] Deep learning for IoT systems requires the usage of the domain-specific dataset for effective training. The occurrence of lopsided datasets and unbalanced datasets may negatively affect learning performance.[35] The hybrid deep learning approach could be utilized to boost effectiveness without considerably increasing execution time. Deep learning-based blockchain technology may also be utilized to increase IoT stability. Blockchain technology is a new way of ensuring the safety and confidentiality of decentralized records.

Malware Analysis and Diagnosis

Malware can infiltrate gadgets and networks and is meant to cause harm to such devices and networks. This harm may manifest its own code distinctly for the end user or terminal according to which kind of virus and its intent. Traditional malware solutions like firewalls identify malware using a signature-based detection method.[36] When faced with complex threats, firewalls perform less than they do when dealing with simple ones. In contrast, DL procedures are more flexible to complicated security issues because they do not rely on the identification of pre-existing fingerprints or conventional patterns of attack. Complicated risks could be easily recognized by DL methods. All sorts of odd behavior can be observed in the system. The results of the analysis help in identifying and reducing the potential hazard. Threats can be identified more successfully by offering extensive behavioral analysis and finding related code, malevolent functionality, or infrastructure.

Artificially supervised sandbox software packages are used to analyze dynamic malware. The analysis entails observing how it operates and affects the host system. Despite its high resource use, it is good against viral concealment. The Sandbox can help security teams to overcome advanced malware attacks and boost their defenses.[37] Sandbox investigates discrete and unforeseen threats deeply and supplements its findings with security intelligence. However, hackers are aware of the conventional protection schemes and the existence of sandboxes. Because of this acquired knowledge, dynamic malware analysis fails to protect the system. Static analysis is also ineffective for detecting advanced malware.[38] Hybrid analysis is useful, especially for detecting malicious code. It could be useful for extracting many more Indications Of Compromise (IOCs) and unknown code. Hybrid inspection aids in the detection of unknown threats. It takes a long time and needs a manual component in practice. These tactics are problematic to implement with the increase in the quantity, intricacy, and sophistication of the virus. Deep learning-based systems are suggested to overcome this problem. Scalability is addressed by

numerous DL-based solutions that automate various stages of malware detection and categorization procedures.[39] It has been shown that DL-based techniques have good accuracy rates and can categorize malware more quickly than human analysis.

Anti-Spam Recognition

The term "Spam" can also refer to "Simultaneously Posted Advertisement Message communication". It is unprompted information circulated in large numbers. Spam is typically sent via email, although it can also be distributed via text message, social media, or phone calls. Spam mailings are frequently disguised as legitimate marketing emails. However, spam can occasionally be an erroneous or harmful plan. In the instance of finding spam, a well-trained Deep Learning model must be able to assess if the pattern of words contained in an e-mail is more prevalent in spam emails or those found in safe emails. Spam is the most widespread cyber-attack and a big problem for a wide range of online users. Deep Learning techniques have recently been utilized to build spam prevention filtration systems, and their effectiveness has been shown.

Spam in Emails & Websites

Email spam is the unwanted sending of email communications. Spam emails overload the inbox and divert the focus away from the emails we truly want to read. Deep learning models were suggested in the work to address emails that contain visuals and spam content.[40] The suggested architectures generated an output class by combining text and image classifiers to determine if it is spam or not. The initial design incorporated feature fusion, but the enhanced version leveraged constraints across both classification algorithms, achieving a remarkable 98.11% accuracy rate through the utilization of probabilistic classes. However, the limited dataset size, comprising only 1500 photos, posed a challenge of overfitting. This research identified spam hosts with 95.25% accuracy using the WEBSPAM-UK2007 dataset.[41] In the literature, a particular deep learning-based model was proposed for screening internet data and recognizing spam. The model consists of three layers, each with its specific role.[42] The model was in response to spotting internet spam, with the spam detector built using the LSTM and CNN models. Layers were responsible for the successful digital data retention in a remote cloud environment.

Anti-Spam on Social Media Sites

Social Media Sites, which grant clients to broadcast messages and discuss ideas globally, have gained in popularity. Hackers tend to be fast to grab abuzz with all the interest on social media platforms, flooding their spam via chatbots as well as dodgy profiles. The study employed a deep-learning approach to detect spam in Twitter tweets.[43] On many tests, the proposed model outperformed traditional classifiers with a success rate of over ninety percent. The authors proposed a multiple-phase anti-spam analyzer for cellular social media platforms using deep learning techniques.[44] The authors developed a top-computing framework with an accuracy of 88.62%, through which initial observation was performed on a portable device and the outcomes were then uploaded to an online server for extra processing. Researchers delved into the realm of IoT-based social media applications, specifically focusing on spam-related concerns in the literature.[45] They introduced Co-Spam, a spammer detection solution designed for use in Internet of Things applications. The results of their investigation demonstrated that Co-Spam achieved a commendable level of accuracy, albeit it required the incorporation of multiple hyper-parameters and a meticulously fine-tuned set of features.

Identifying Fraud

A series of actions are conducted in the name of fraud detection to stop the theft of financial resources or other valuables. The identification of fraud refers to the methods and information analytics that enable firms to detect as well as avoid illegal monetary transactions. This encompasses activities such as fraudulent credit card operations, personality theft, cyber hewing, insurance coverage scams, and related illicit actions.[46] Such types of crimes cause significant financial losses for people, companies, and the government. To combat criminals by adapting to their tactics, detection techniques are always being improved. These methods often employ information mining techniques, facts, and algorithmic learning. Offenders do not need to physically hold the card or pretend to be the cardholder to use it; they only require the data associated with the card. One of the studies discussed in the paper intended a structural-secular attention-oriented graph network using a real-world dataset of card transactions from a commercial bank.[25] Identity fraud is being stopped with the aid of deep learning to inspect the threats in milliseconds. The following issues should be covered by DL-driven fraud detection models.

- Provide trustworthy scores to fraud detection specialists for use in digital transactions.
- Give the detailed information needed for user identification, recognizing the fraud and identity proving.
- More real-time anomalies in authenticity-based behaviour are discovered.
- Should lessen clients' resistance when on boarding, reducing false positives.

Examination of Encrypted Communications/Traffic

Encrypted traffic inspection allows for the identification and detection of abnormal activity concealed in encrypted traffic.[11] It analyses the encrypted traffic before decryption using an amalgamation of algorithmic learning, and cognitive analytics. From ransomware to HTTPS, attackers have adapted cryptography techniques in their assaults to protect connections with compromised devices and evade discovery. It is expected to set the goal of detecting potential vulnerabilities as well as managing and safeguarding assets.[29]

The new applications employ renowned transport layer's port ID to conceal their connections or bypass standard enrollment Socket ID with good accuracy. The Deep Packet Inspection (DPI), concentrates on payloads for traffic classification. However, this method works with unencrypted traffic and is computationally expensive. As a result, new techniques emerged that rely on statistical or time-series aspects and can manage both encrypted and unencrypted traffic. It classifies encrypted traffic, detects encrypted malware, and inspects SSL/TLS traffic for threats while preserving privacy. Fingerprinting is based on interpersonal likes and dislikes. A fingerprint can be made by using any of the user's settings, for example, the display, the installed typefaces, along a browser's settings. Website fingerprinting refers to the practice of tracing internet congestion from websites using software such as The Onion Router (TOR). A few works investigated the effectiveness of webpage fingerprinting with DL filters. The authors demonstrated that stacked denoising AEs can successfully identify webpages exploiting merely the path (inbound or outbound) and integrate-arrival durations of TOR packets.[47] The work projected in the literature was an automated website fingerprinting model that uses TOR datagrams and has a 95.3 success rate which is more accurate than the state-of-the-art assault.[48]

Ransomware Case Study

Ransomware attacks have become a significant cybersecurity threat, causing substantial financial losses and data breaches. Creating a DL model specifically for detecting ransomware cyberattacks involves training a neural network to recognize patterns and behaviors associated with ransomware activities. A suitable DL architecture must be chosen for this task and the steps involved are given in Table 3. It may be efficient to use CNN, RNN, or both. Additionally, users can test with more sophisticated topologies like LSTM networks. Expertise in DL and cybersecurity, as well as a dedication to moral and legal compliance, are required for creating and maintaining an efficient DL model for ransomware detection.

This case study delves into the world of ransomware, exploring the nature of these attacks, their impact on organizations, and effective mitigation strategies. When the Darkside ransomware organization targeted one of the significant petroleum pipelines in the United States in May 2021, it resulted in the Colonial Pipeline ransomware assault. Due to the attack's considerable damage to the Atlantic Coast's gasoline supply, several states experienced fuel shortages and panic buying. Analyzing real-

Table 3 — DL approaches for ransomware

S. No	Flow process	Methods
1	Data collection	Collect Network traffic or logs with both normal and ransomware-related, labeled accordingly.
2	Data preprocessing	Clean and preprocess the data, extracting relevant features if needed
3	Model selection	Choose an appropriate deep learning architecture (e.g., RNN, CNN, LSTM) for the task
4	Feature extraction	Convert data into a suitable format for deep learning, using embeddings or other techniques
5	Model training	Train your model on the dataset, adjusting hyperparameters and addressing overfitting
6	Anomaly detection	Do real-time monitoring to detect anomalies in network traffic or logs (may ransomware)
7	Real-time monitoring	Use streaming data processing frameworks for efficient real-time monitoring
8	Alerting and response	Develop mechanisms to respond to ransomware detection, and initiating incident response procedures
9	Model updates	Continuously update and fine-tune the model to adapt to evolving ransomware threats
10	Evaluation and testing	Regularly assess the model's performance, ensuring it detects ransomware while minimizing false positives

world incidents, this case study intends to offer valuable insights for businesses and individuals to enhance their defenses against the increasing threat of ransomware attacks. Essentially, the aim of this case study is to educate readers about the anatomy of ransomware attacks, their severe consequences, and practical strategies for prevention and recovery. The author's works in the literature make it possible to identify a known ransomware sample by achieving an impressive accuracy rate of 99.3%.[49] The suggested DL model with LSTN detected ransomware and achieved the best performance at a 99.8% accuracy rate.[50]

Conclusions

All the possible cyberattacks in the networks and essential topics in the cybersecurity field are studied. Deep Learning is becoming more and more significant in the field of cybersecurity. Almost all the fundamental DL models and the vital resources that include a standardized structure and data sources are covered. This paper comprehensively discusses and reviews all relevant research on the applications of DL in cybersecurity. This paper will be a reference for investigators, programmers, and safety professionals interested in using algorithms driven by DL to address cyberspace security. This study focuses on the analysis of ransomware cyberattacks and their mitigation through the application of DL strategies. Lastly, there is a need to be cautious about a potential trap. Even though DL has enormous promise, it is not to be employed in all scenarios. It needs to be applied to problems that involve huge volumes of data with significant multiple properties. Future research should pay more attention to DL designs that have been adapted to portable networks and can overcome the shortcomings of traditional approaches.

Acknowledgment

The authors are grateful to Sri Sivasubramaniya Nadar College of Engineering, Chennai, for the support and cooperation they provided throughout this research project.

Conflict of interest

The authors declare that they have no financial or other conflicts of interest.

References

1 Mijwil M, Unogwu O J, Filali Y, Bala I & Al-Shahwani H, Exploring the top five evolving threats in cybersecurity: An in-depth overview, *Mesopotamian J Cybersecur*, **2023** (2023) 57–63, https://doi.org/10.58496/MJCS/2023/010.

2 Rajasekharaiah K M, Dule C S & Sudarshan E, Cyber security challenges and its emerging trends on latest technologies, in *IOP Conf Series: Materials Sci Eng*, **981(2)** 2020, 022062, doi:10.1088/1757-899X/981/2/022062.

3 Gümüşbaş D, Yıldırım T, Genovese A & Scotti F, A comprehensive survey of databases and deep learning methods for cybersecurity and intrusion detection systems, *IEEE Syst J*, **15(2)** (2020) 1717–1731, doi:10.1109/JSYST.2020.2992966.

4 Wang X, Han Y, Leung VC, Niyato D, Yan X & Chen X, Convergence of edge computing and deep learning: A comprehensive survey, *IEEE Commun Surv Tutor,* **22(2)** (2020) 869–904, doi:10.1109/COMST.2020.2970550.

5 Macas M, Wu C & Fuertes W, A survey on deep learning for cybersecurity: Progress, challenges, and opportunities, *Comput Netw*, **212** (2022) 109032, https://doi.org/10.1016/j.comnet.2022.109032.

6 Mahdavifar S & Ghorbani A A, Application of deep learning to cybersecurity: A survey, *Neurocomputing*, **347** (2019) 149–176, https://doi.org/10.1016/j.neucom.2019.02.056.

7 Santhosh Kumar S V, Selvi M & Kannan A, A comprehensive survey on machine learning-based intrusion detection systems for secure communication in internet of things, *Comput Intelligence Neurosci*, **2023** (2023) 1–24, doi.org/10.1155/2023/8981988.

8 Liu L, Lin J, Wang P, Liu L & Zhou R, Deep learning-based network security data sampling and anomaly prediction in future network, *Discrete Dyn Nat Soc*, **2020** (2020) 1–9, https://doi.org/10.1155/2020/4163825.

9 Kaur J & Ramkumar K R, The recent trends in cyber security: A review, *J King Saud Univ - Comput Inf Sci*, **34(8)** (2022) 5766–81, https://doi.org/10.1016/j.jksuci.2021. 01.018.

10 Wu Y, Wei D & Feng J, Network attacks detection methods based on deep learning techniques: A survey, *Secur Commun Netw*, **2020** (2020) 1–7, https://doi.org/10.1155/2020/8872923.

11 Jadoon A K, Wang L, Li T & Zia M A, Lightweight cryptographic techniques for automotive cybersecurity, *Wirel Commun Mob Comput*, **2018** (2018) 1–15, https://doi.org/10.1155/2018/1640167.

12 Park S, Aslam B, Turgut D & Zou C C, Defense against Sybil attack in vehicular ad hoc network based on roadside unit support, in *Proc- IEEE Mil Commun Conf* (IEEE) 2009, 1–7, doi:10.1109/MILCOM.2009.5379844.

13 Do N Q, Selamat A, Krejcar O, Herrera-Viedma E & Fujita H, Deep learning for phishing detection: Taxonomy, current challenges and future directions, *IEEE Access* **10** (2022) 36429–36463, doi:10.1109/ACCESS.2022.3151903.

14 Liu X, Xie L, Wang Y, Zou J, Xiong J, Ying Z & Vasilakos, A V, Privacy and security issues in deep learning: A survey, *IEEE Access **9*** (2020) 4566–4593, doi:10.1109/ACCESS.2020.3045078.

15 Goodfellow I, Bengio Y & Courville A, *Deep learning* (Cambridge, MA, USA: MIT Press), 2017) doi:https://www.deeplearningbook.org/.

16 Vu L, Nguyen Q U, Nguyen D N, Hoang D T & Dutkiewicz E, Deep transfer learning for IoT attack detection, *IEEE Access, **8*** (2020) 107335–107344, doi:10.1109/ACCESS.2020.3000476.

17 Zhao J, Shetty S, Pan J W, Kamhoua C & Kwiat K J, Transfer learning for detecting unknown network attacks, *Eurasip J Inf Secur* (2019) 1–13, https://doi.org/10.1186 / s13635-019-0084-4.

18 Gu Y, Yan H, Dong M, Wang M, Zhang X, Liu Z & Ren F, WiONE: One-shot learning for environment-robust device-free user authentication via commodity Wi-Fi in man–machine system, *IEEE Trans Comput Soc* **8(3)** 630–642, doi:10.1109/TCSS.2021.3056654.

19 Hindy H, Tachtatzis C, Atkinson R, Brosset D, Bures M, Andonovic I, Michie C & Bellekens X, Leveraging Siamese networks for one-shot intrusion detection model, *J Intell Inf Syst*, **60(2)** (2022) 407–436, https://doi.org/10.1007/s10844-022-00747-z.

20 Gao Y, Gong M, Xie Y & Qin A K, An attention-based unsupervised adversarial model for movie review spam detection, *IEEE Trans. Multimedia*, **23** (2021) 784–796, doi:10.1109/TMM.2020.2990085.

21 Cao R, Liu G, Xie Y & Jiang C, Two-level attention model of representation learning for fraud detection, *IEEE Trans Comput Soc Syst*, **8(6)** (2021) 1291–1301, doi:10.1109/TCSS.2021.3074175.

22 Chaudhari S, Mithal V, Polatkan G & Ramanath R, An attentive survey of attention models, *ACM Trans Intell Syst Technol*, **12(5)** (2021) 1–32, https://doi.org/10.1145/ 3465055.

23 Cheng J, He R, Yuepeng E, Wu Y, You J & Li T, Real-time encrypted traffic classification via lightweight neural networks, in *GLOBECOM 2020–2020 IEEE Glob Commun Conf* (IEEE) 2020, 1–6, doi:10.1109/GLOBECOM42002. 2020.9322309.

24 Li Y, Zhang L, Lv Z & Wang W, Detecting anomalies in intelligent vehicle charging and station power supply systems with multi-head attention models, *IEEE Trans Intell Transp Syst*, **22(1)** (2020) 555–564, doi:10.1109/TITS.2020. 3018259.

25 Cheng D, Wang X, Zhang Y & Zhang L, Graph neural network for fraud detection via spatial-temporal attention, *IEEE Trans Knowl Data Eng*, **34(8)** (2020) 3800–3813, doi: 10.1109/TKDE.2020.3025588.

26 Bowman B & Huang H H, Towards next-generation cybersecurity with graph AI, *ACM SIGOPS Oper Syst Rev,* **55(1)** (2021) 61–67, https://doi.org/10.1145/3469379. 3469386.

27 Tang T A, Mhamdi L, McLernon D, Zaidi S A & Ghogho M, Deep learning approach for network intrusion detection in software defined networking, *IEEE Inter conf on WINCOM'16,* (IEEE) 2016, 258–263, doi: 10.1109/ WINCOM.2016.7777224.

28 Otoum S, Kantarci B & Mouftah H T, On the feasibility of deep learning in sensor network intrusion detection, *IEEE Netwo L*, **1(2)** (2019) 68–71, doi: 10.1109/LNET. 2019.2901792.

29 Raikar M M, Meena S M, Mulla M M, Shetti N S & Karanandi M, Data traffic classification in software defined networks (SDN) using supervised learning, *Procedia Comput Sci*, **171** (2020) 2750–2759, https://doi.org/10.1016/ j.procs.2020.04.299.

30 Tavallaee M, Bagheri E, Lu W & Ghorbani A A, A detailed analysis of the KDD CUP 99 data set, *2009 IEEE Int Symp Comput Intell Inform Secur Defen App* (IEEE) 2009, 1–6, doi: 10.1109/CISDA.2009.5356528.

31 Elsayed M S, Le-Khac N A, Dev S & Jurcut A D, Ddosnet, A deep-learning model for detecting network attacks, *IEEE 21st Inter Symp WoWMoM* (IEEE) 2020, 391–396, doi: 10.1109/WoWMoM49955.2020.00072.

32 Pa Y M, Suzuki S, Yoshioka K, Matsumoto T, Kasama T & Rossow C, IoT POT: A novel honeypot for revealing current IoT threats, *J Inf Process*, **24(3)** (2016) 522–533, https://doi.org/10.2197/ipsjjip.24.522.

33 Yao H, Gao P, Zhang P, Wang J, Jiang C & Lu L, Hybrid intrusion detection system for edge-based IIoT relying on machine-learning-aided detection, *IEEE Netw*, **33(5)** (2019) 75–81, doi: 10.1109/MNET.001.1800479.

34 Yue Y, Li S, Legg P & Li F, Deep learning-based security behavior analysis in IoT environments: A survey, *Secur Commu Netw*, (2021) 1–13, https://doi.org/10.1155/ 2021/8873195.

35 Hassan & W H, Current research on Internet of Things (IoT) security: A survey, *Comput Netw*, **148** (2019) 293—294, https://doi.org/10.1016/j.comnet.2018.11.025.

36 Faruki P, Bharmal A, Laxmi V, Ganmoor V, Gaur M S, Conti M & Rajarajan M, Android security: A survey of issues, malware penetration, and defenses, *IEEE Commun Surv Tutor*, **17(2)** (2014) 998–1022, doi: 10.1109/COMST.2014.2386139.

37 Feng R, Chen S, Xie X, Meng G, Lin S W & Liu Y A, A performance-sensitive malware detection system using deep learning on mobile devices, *IEEE Trans Inf Forensics Secur*, **16** (2021) 1563–1578, doi: 10.1109/TIFS.2020. 3025436.

38 Jeon J, Park J H & Jeong Y S, Dynamic analysis for IoT malware detection with convolution neural network model, *IEEE Access*, **8** (2020) 96899–96911, doi: 10.1109/ACCESS. 2020.2995887.

39 Zhou Y & Jiang X, Dissecting android malware: Characterization and evolution, *IEEE Symp Secur Priva* (IEEE) 2012, 95–109, doi: 10.1109/SP.2012.16.

40 Seth S & Biswas S, Multimodal spam classification using deep learning techniques, *IEEE 13th Inter Conf SITIS* (IEEE) 2017, 346–349, doi: 10.1109/SITIS.2017.91.

41 Castillo C, Donato D, Becchetti L, Boldi P, Leonardi S, Santini M & Vigna S, A reference collection for web spam, in *ACM Sigir Forum*, **40(2)** (2016) 11–24, https://doi.org/10.1145/1189702.1189703.

42 Makkar A, Ghosh U & Sharma P K, Artificial intelligence and edge computing enabled web spam detection for next-generation IoT applications, *IEEE Sens J*, **22** (2021) 25352–25361, doi: 10.1109/JSEN.2021.3066492.

43 Wu T, Liu S, Zhang J & Xiang Y, Twitter spam detection based on deep learning, in *Proc Int Multiconf Australasian Comput Sci* 2017, 1–8, https://doi.org/10.1145/3014812. 3014815.

44 Feng B, Fu Q, Dong M, Guo D & Li Q, Multistage and elastic spam detection in mobile social networks through deep learning, *IEEE Netw*, **32(4)** (2018) 15–21, doi: 10.1109/MNET.2018.1700406.

45 Guo Z, Shen Y, Bashir A K, Imran M, Kumar N, Zhang D & Yu K, Robust spammer detection using collaborative neural network in Internet-of-Things applications, *IEEE Internet Things J*, **8(12)** (2021) 9549–9558, doi: 10.1109/JIOT.2020. 3003802.

46 Kou Y, Lu C T, Sirwongwattana S & Huang Y P, Survey of fraud detection techniques, in *IEEE Inter Conf NSC* (IEEE) 2004, 749–754, doi: 10.1109/ICNSC.2004.1297040.

47 Abe K & Goto S, Fingerprinting attack on Tor anonymity using deep learning, *Proc APAN*, **42(0)** (2016) 15–20.

48 Rimmer V, Preuveneers D, Juarez M, Van Goethem T & Joosen W, Automated website fingerprinting through deep learning, in *25th Annual Netw Distri Syst Secur Symp* (San Diego, California, USA, ISOC) 18–21 February 2018, http://dx.doi.org/10.14722/ndss.2018.23105.

49 Zhang H, Xiao X, Mercaldo F, Ni S, Martinelli F & Sangaiah A K, Classification of ransomware families with machine learning based on n-gram of opcodes, *Future Gener Comput Syst*, **90** (2019) 211–221, https://doi.org/10.1016/j.future. 2018.07.052.

50 Alsaidi R A, Yafooz W M, Alolofi H, Taufiq-Hail G A M, Emara A H M & Abdel-Wahab A, Ransomware detection using machine and deep learning approaches, *Int J Adv Comput Sci Appl*, **13(11)** (2022), https://doi.org/10.3390/bdcc7030143.