**The History and Future of Artificial Intelligence and Deep Learning**

**and their Applications in Cybersecurity**

Justin Mendes

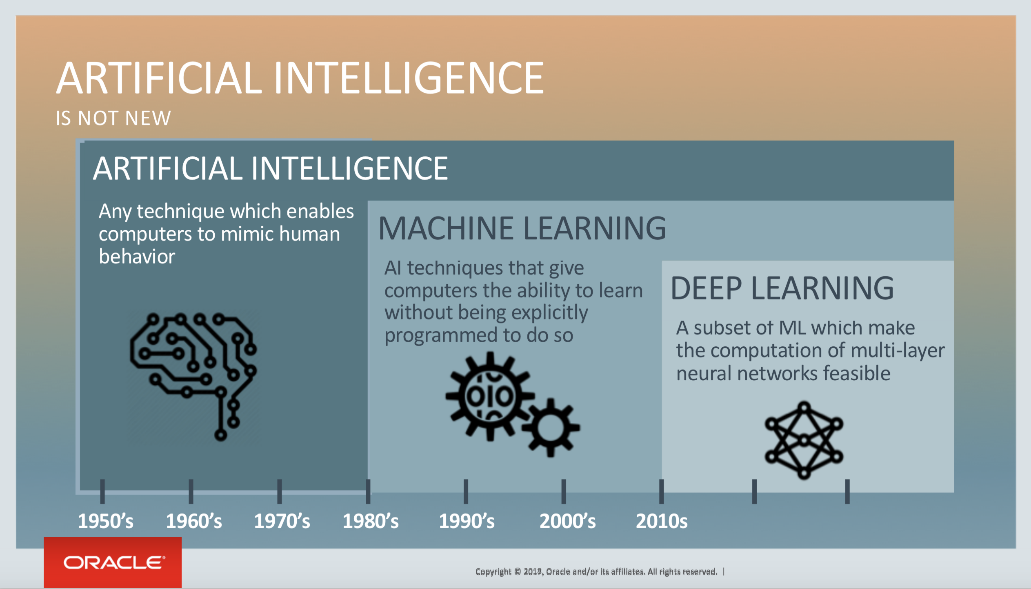
Advisor: Dr. Li Feng

**Abstract**

Artificial Intelligence (AI) and Deep Learning (DL) have made boundless advancements in the field of computer science, specifically in the area of cybersecurity. With the existing methods adopted in cybersecurity such as using a firewall, using strong, safe passwords, enabling two-factor authentication (2FA), updating systems and software, backing up data, and installing anti-malware software, AI and DL have solved the multitude of issues that have plagued these obsolete and archaic systems. AI and DL have made electronic data and information more safe and secure against criminals and unauthorized users who do not have the express permission to access that data and information. AI and DL were designed and developed to protect from these prohibited intrusions through taking extra precautionary measures to prevent it from occurring, compared to the approaches that are still in operation. The research and results of AI and DL have revealed that they are potential applications that will eventually and ultimately surpass the contemporary techniques practiced in cybersecurity. The determination and work that has been performed and attained from the research of AI and DL will have a prospective impact in cybersecurity, as well as the entire environment of computer science intrinsically in itself.

**1. Introduction**

AI is the concept and expansion of computer systems that perform assignments and responsibilities that would usually involve human intelligence, for instance language translation, decision-making, speech recognition, visual perception, etc. DL is the subsection of AI and Machine Learning (ML) that involve algorithms that are inspired via the brain which can learn from enormous quantities of data required to solve any problem through learning patterns. AI and DL have the appropriateness and qualifications to acquire optimal feature representation of basic input cases. It has been tested in innumerable use cases in cybersecurity for instance binary analysis, recognizing phishing and spam, recognizing android malware, malware allocation, and recognizing intrusions (Ismail). Figure 1below labeled Progression of AI, ML, DL illustrates the evolution from AI to DL beginning in the early 1950s to present day. The figure also defines and describes the difference of AI, ML, and DL from each other to get a better comprehension of the terminology moving forward in this research paper.



**Figure 1: Progression of AI, ML, DL**

This research paper will outline the work associated to AI and DL to replace and enhance the redundant and obsolete mechanisms that are presently implemented in cybersecurity for instance using a firewall, using strong, safe passwords, enabling 2FA, updating systems and software, backing up data, and installing anti-malware software (Donovan). There is an assortment of redundant and obsolete mechanisms that are presently implemented in cybersecurity that have not been familiarized and distinguished in this section. There is correspondingly more description and explanation of the different subgroups of processes that are administered in cybersecurity from what they are and how they work, their implementations and applications, complications and resolutions, and examples manifestations. The outline and organization of the research paper will be as indicated. Section 2 will grasp the background of the research paper, briefly explaining the existing solutions for cybersecurity more in depth. Section 3 will grasp the methodology, briefly explaining the current solutions and methods being developed for cybersecurity, which are AI and DL. The section will also explain the procedures used to identify and analyze the different solutions and evaluate the results of them and to explain how the data and information was collected and analyzed. Section 4 will grasp the results of the research paper, reporting the findings for the research paper based on the findings of how effective AI and DL is in cybersecurity. The final section will conclude the research paper, summarizing and synthesizing the key elements of the research paper to give a better understanding to the reader about the topic of AI and DL and their applications in cybersecurity and to recommend new areas of research for the future.

**2. History of Cybersecurity**

The existing solutions for cybersecurity as mentioned before including firewalls, using strong, safe passwords, enabling 2FA, updating systems and software, backing up data, and installing anti-malware software. Firewalls are network security systems which supervise any and all incoming and outgoing network traffic to determine whether explicit traffic should be accepted or rejected depending on a set of security instructions. Firewalls can be software, hardware, or both. They are internal networks which can be either credible or suspicious external networks as a barricade between ensured and guarded networks. Strong, safe passwords should be unique, complex, and long. 2FA(2FA) is an additional security layer to deny users from trying to gain access to personal online accounts that do not belong to other users. The premise of 2FA is that a user will enter their username and password but will also need to offer another piece of information to gain access. The second piece of information is requested when trying to gain absolute access to an account. Updating systems and software prevents malware from targeting unknown and contemporary security vulnerabilities. Data backup is the result of archiving and replicating folders and files for the purpose of restoring them if data is stolen or lost. Anti-Malware Software is a form of software program designed and developed to avoid, identify, and delete malware on computer devices (Donovan). This section will delve further into these methods through explaining more in depth about the different subgroups of what they are and how they work, their implementations and applications, and issues with the methods.

**2.1 Use a Firewall**

Firewalls are network security systems that observe and regulate arriving and departing network traffic to ascertain whether to permit or obstruct distinct traffic established through a series of security guidelines. They are the first line of network security fortification through constructing a barricade between the controlled and secured internal networks that are either reliable or defective external networks. Firewalls can be either software, hardware, or both. Examples of some categories of firewalls are proxy firewalls, stateful inspection firewalls, unified threat management (UTM) firewalls, and next-generation firewalls (NGFW) (CISCO).

Firewalls can be either software, hardware, or both. Examples of some categories of firewalls are proxy firewalls, stateful inspection firewalls, unified threat management (UTM) firewalls, and next-generation firewalls (NGFW). Proxy firewalls are an early type of firewall systems that served as a gateway for explicit applications from one server to another. They have supplementary functionality such as security and content caching to avert direct relations of external networks. The issues with proxy firewalls are that they impact the support of their applications and throughput capabilities. Stateful inspection firewalls accepts or rejects network traffic due to protocols, ports, and states. They supervise any and all activities from the initial relation to the final relation to filter inquiries made by means of context and defined rules by the administrator. UTM firewalls are systems that combine the functionalities of both stateful inspection firewalls with antivirus and intrusion prevention. They have cloud management and supplementary services to focus of ease of use and simplicity. NSGFW firewalls are the next-generation of firewalls meant to evolve stateful inspection and packet filtering to block application layer attacks and advanced malware. They must have the capabilities of standard firewalls, application awareness, integrated intrusion prevention, etc. Firewalls are mainly implemented and applied with the Internet of Things or the Internet (CISCO). Vulnerabilities and threats of firewalls are insider attacks, unexploited security patches, and configuration faults. If an attack happens inside a system, a perimeter firewall is inoperative since an attacker is already in the system. If a firewall is not properly managed, vulnerabilities in a system or software program may be exploited by attackers until it is patched. If the configuration settings of a firewall are incorrect, it can cause a loss in network performance and protection failures for the network (CISCO). Updating systems and software may fix these issues, which this section will confer later in the subheadings.

**2.2 Use Strong, Safe Passwords**

Strong, safe passwords, according to the Computer Emergency Response Team (CERT), must be unique, complex, and long. It is recommended that an individual should consider the following virtuous routines and behaviors when regarding password handling: never use common words found in any dictionary of any language, always use the longest form of password permissible by the system, never use personal information, always use different passwords on different accounts and systems, never forget and share passwords, always periodically change passwords, and always use uppercase letters, lowercase letters, numbers and symbols. It has been found that approximately 60% of data breaches happened from weak, stolen, or lost passwords (CISA). The issues with safe, strong passwords are preserving individual’s data since they can be negligible of their passwords and can be compromised by attackers. There are many attack styles that are used to compromise passwords. The most acclaimed of these attack styles are brute-force attacks. Brute-force attacks are a trial and error style of attack that compromise an individual’s passwords by contrasting the passwords with a database (CISA). Enabling 2FA may fix this issue, amongst other issues, which this section will confer in the next subheading.

**2.3 Enable Two-Factor Authentication**

2FAis an additional security layer to deny users from trying to gain access to personal online accounts that do not belong to other users. The premise of 2FA is that a user will enter their username and password but will also need to offer another piece of information to gain access. The second piece of information which is requested when trying to gain access to an account derives from something the user knows, something the user has, or something the user is. 2FA has a potential compromise of not allowing the account of the user to get unlocked through having one of the factors. If a device or password is stolen or lost, it is highly unlikely that another individual will have that users 2FA information. When 2FA is handled accurately and appropriately, then applications and websites will be more assured of the identity of the user will most expectedly unlock the account. Some common types of 2FAs are hardware tokens for 2FA, Short Message Service (SMS) text-message 2FA, voice-based 2FA, Software Tokens for 2FA, push notification for 2FA, etc. (AUTHY)

2FA is a tool to utilize with a password. The premise of 2FA is that a user will enter their username and password but will also need to offer another piece of information to gain access. The second piece of information which is requested when trying to gain access to an account derives from something the user knows, something the user has, or something the user is. Something the user knows could be a keystroke pattern, answers to secret questions, a password, or a personal identification number (PIN). Something the user has could be a hardware token, a smartphone, or a credit card in their possession. Something the user is could be a voice print, an iris scan, or a fingerprint pattern. If one factor is potentially compromised, it will not unlock a user’s account. If a user’s identity is used correctly, there will be more confidence by websites and apps to unlock their account. 2FAs are mainly implemented and applied with SMS text-messages, software tokens, push notifications, etc. Through SMS text-messages, a one-time passcode (OTP) is sent to a user’s smartphone, after a website or app receives their account username and password, which must then be inserted back into the website or app to get access. Through software tokens, a time-based, one-time passcode (TOTP) is sent to a 2FA app on a user’s smartphone, which is supported by the website or app, and must then be inserted back into the website or app to get access. Software tokens are only valid for a short period of time and remove the probability of attacks and interceptions since passcodes are generated and displayed on the same software system. Through push notifications, a website or app sends a push notification to a user which they can approve or deny the authentication attempt taking place (AUTHY). The issues with 2FAs are a user forgetting, losing, or changing something the user knows, something the user has, or something the user is. The user may forget their keystroke pattern, answers to secret questions, their password, or their PIN. The user may lose their hardware token, their smartphone, or their credit card. The user may have a change in voice print, iris scan, or fingerprint pattern. Attackers may also still be able to steal these items to enter a user’s account (AUTHY).

**2.4 Update Systems and Software**

Updating systems and software provides regular improvements and fixes to vulnerabilities in system and software products. The best chance in preventing attacks from manipulating vulnerabilities is to update to the most current patch and version of a system and software. Never ignore prompts to update systems and software since there are exploits to the antiquated system or software. The latest patches and versions of systems and software address well-known exploits. Malware does not exactly target unknown and contemporary security vulnerabilities in updated systems and software. Updating systems and software are mainly and most notably implemented and applied to firewalls as specified previously (Donovan). The issues with updating systems and software are relearning and readjusting to established processes of the newer versions with altered and removed functionality, complexity of updated processes, and may be unavailable or expensive. Attackers may also still find vulnerabilities in the new updates after a period, which they can exploit and will lead to a constant cycle of updates for systems and software with the issues listed in this subheading (Donovan).

**2.5 Back Up Data**

Data backup defends against ransomware (ransom software) to safely store data on-premise and off-site. Ransomware is a type of malicious software which encrypts an individual’s data to block access to it until the individual pays for a decryption key. Data backup also ensures that all data in the server environments is shielded with the same level of security, whether it is virtual or physical. The advent of ransomware has caused the full backup of any and all data to become a safeguard. It is simple to set up a cloud service application in a matter of minutes with little to no cost. The cloud service can be accessed from any system or software attached to the Internet in any location. Through data backup, individuals must not overlook file servers that are susceptible to attacks and should check their backups regularly to correctly ensure that the data is functioning. Data backup are mainly implanted and applied to cloud servers such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), and Recovery as a Service (RaaS) (Solomon). IaaS refers to a computing infrastructure that is an outsourced service and is the lowest level of cloud solution. Development and hosting environments are examples of IaaS. The benefits of IaaS are reduced cost and simple scalability requirements. PaaS is a more advanced cloud computing to IaaS in which solution stacks and computing platform services are apart of providing infrastructure. Operating systems, programming languages, libraries, and graphic user interfaces are examples of PaaS. The benefits of PaaS are the community, no upgrades, lower costs, and simplified deployment. SaaS provides full functionality of web applications. Time management, email, web conferencing, etc. are examples if SaaS. The benefits of SaaS are rapid scalability, accessibility, and maintenance. RaaS helps in disaster recovery, archiving, and backup in an integrated platform. Servers and data recovery centers are examples of RaaS. The benefits of RaaS are preventing loss of data, preventing loss of virtual and physical infrastructure, cost-effective, fast recovery and accuracy maintenance, and great flexibility for required backup. The issues with data backup are there may be network failures, hardware failures, software failures, human error, etc. Attackers may also still be able to attack cloud services to steal data with ransomware (Solomon).

**2.6 Install Anti-Malware Software**

Anti-Malware Software is a form of software program designed and developed to avoid, identify, and delete malware (malicious software) on computer devices. Anti-malware software applies three tactics to defend devices for malware, including sandboxing, malware detection, and signature-based malware detection. All these procedures defend against malware dangers in different manners. Anti-malware Software can assist in halting malware assaults through contributing real-time defense against the installation of devices through scanning each arriving network data for malware to deter any dangers that it discovers. It can also identify unconventional models of malware and propose defenses definitive to the ransomware assault. The basis for anti-malware software is because while malware is repetitively evolving, anti-malware software applies a manifold of identification procedures. With sandboxing, malware detection, and signature-based malware detection, anti-malware programs might also depend on reputation-based devices of recent data about malware in other devices (Rouse).

Installing anti-malware software can protect systems and software from malware using three strategies including sandboxing, behavior-based malware detection, and signature-based malware detection. Sandbox prevents unknown applications from affecting a system or software. Anti-malware software that has sandboxing runs suspicious unknown programs to monitor results in a sandbox. If there is malicious behavior, it will be terminated by the anti-malware software. Behavior-based malware detection is powered by ML algorithms. An anti-malware software can detect malware by identifying the threat with its behaviors and characteristics to evaluate the malwares intended actions before its behavior is executed. Signature-based malware detection uses databases of known malware to scan for the specific malware. When a malware signature is identified by the anti-malware software that matches the specific file, it is flagged as potential malware. Signature-based malware detection can only detect known malware. Anti-malware software is used for scanning files and folders for viruses. Installing anti-malware software will prevent individuals from visiting websites that distribute malware, prevents malware from spreading on an infected system or software, generates and tracks data on the amount of malware or infections are on a system or software and the required time to clean or destroy the malware or infections, and offers a report or insight to an individual on how the malware or infection has affected the system or software. Anti-malware software is needed to detect constantly developing and evolving malware (Rouse). The issues with anti-malware software are that there are a diverse number of malware software that steadily grow every year that anti-malware software cannot keep up with, anti-malware software may not be fast enough to deliver protection updates and may be too late, removing detected malicious code from an infected system or software consumes a lot of CPU resources that cannot be appropriated, and two or more anti-malware software cannot simultaneously run on a single system or software since they cannot get along (Rouse).

**3.1 Future of Cybersecurity**

With threats becoming more complex, moving from basic attacks against one system to complicated attacks against every system on a network, traditional security simply isn’t enough in the age of digitalization. Today, with the sharp increase in in use of digital technologies in the world, driven by the need to become more agile and adaptable, there has been a surge in the number of potential ways for cybercriminals to gain access to networks. As a result, the entire cybersecurity battlefield has evolved and become far more complex. Today’s security teams must come up with new tactics to fend off the advanced threats being levelled against increasingly interconnected networks. Security has become a worldwide issue that needs to be addressed and managed to prioritize risk. There have been three key shifts which have taken place in the wake of cybersecurity threats (Ismail). Security has moved beyond IT and has the power to break down barriers. Increasing interaction across the world has led to assets that need protecting and identifying to reduce the impact of a future attack. However, it has reached the stretches beyond the confines of the core of personal systems and out into the edge where data is transferred and potentially moved by cybercriminals targeting personal data. Adaptive systems and software are leveraging digital transformation which impacts how they also use security. They link it back to enabling disruptive models strengthen their focus on cybersecurity threats (Ismail).

Security is at the heart of innovation in which case cybersecurity is no longer a barrier to change or hinder the adoption of new processes and innovative technologies. Security is the center of the new digital age. It is accelerating the speed of services, embedding software-defined networks (SDN), enabling wider, seamless, and secure access to data in the Internet, etc. Security is now a pre-requisite, that is built into new technologies and systems from the inception (Ismail). Security is becoming smarter, better, faster, and stronger in the case that speed agility are not the only assets cybersecurity needs to harness. It also acts smarter and is more effective, since expenditures are reduced. Managing security in the digital age involves the gathering, synthesis and analysis of security data as a standard. It is no longer just about data, but what the data represents. These providers leverage insight to intelligence services within a global network which will be at the forefront of the next generation of cybersecurity services, improving cybersecurity threat visibility and mitigating any and all risks. This will separate individuals who are experts in protecting personal data with those who are collecting and stealing data with their own foresight (Ismail).

**3.1 Artificial Intelligence**

AI makes it conceivable for machines to learn from experience, adjust to new situations, and achieve human-like tasks. Most AI examples rely heavily on DL and natural language processing. Using these technologies, systems and software can be proficient in achieving explicit responsibilities by processing large quantities of data and recognizing and classifying patterns in data. AI is important because it automates repetitive learning and discovery through data, adds intelligence, adapts through progressive learning algorithms, analyzes more and deeper data, achieves incredible accuracy, and gets the most out of data. AI works by joining large amounts of data with fast, iterative processing and intelligent algorithms, allowing systems or software to learn mechanically from patterns or features in data. AI is a broad field of study that includes many technologies, methods, and philosophies (AIAA).

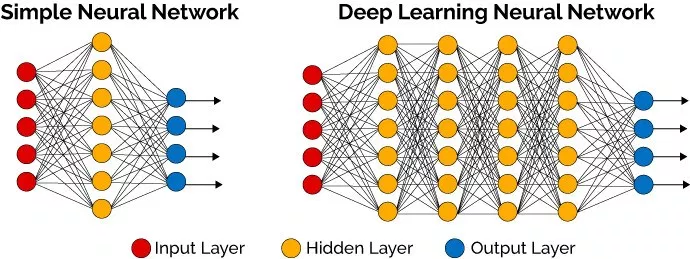
The next generation of cybersecurity products are increasingly incorporating AI and DL. By training AI software with enormous datasets from cybersecurity, network, and physical information, cybersecurity intends to distinguish and block anomalous behavior, even if it does not reveal a known pattern. Specialists expect that systems and software will integrate DL into every aspect of cybersecurity (Jeffcock). There are diverse tactics to using AI for cybersecurity, and it is imperative note which is suitable for a system of software. Some systems of software applications examine network data to spot any and all anomalies while others concentrate on behaviors to distinguish patterns that diverge from standard instructions. The level of effort needed, how they are collected, and the types of data streams by specialists completely contrast in tactic (AIAA). Cybersecurity solutions utilizing AI and DL can critically diminish the quantity of time needed for threat recognition and incident response to alert if there are any inconsistent behaviors in real time. These technologies also assist in reducing and prioritizing traditional security alerts. However, attackers are also using AI and DL to better understand their targets and launch attacks. AI and DL intensifies the ability of safeguards to recognize attacks but may also help attackers to acquire data and information about a target’s weaknesses.

**3.2 Deep Learning**

DL is a ML technique that teaches computers to do what comes naturally through learning and behavior. It is a key technology behind cybersecurity to enable it to recognize and prevent threats, which has been getting lots of attention lately (Jeffcock). DL has achieved impeccable results that were not possible before where computer models can learn to perform a classification of tasks directly from images, text, or sound. These models can achieve advanced state-of-the-art accuracy. It can sometimes exceed the performance of a human. Models are trained by using a large set of data and neural network architectures that contain many layers (MathWorks).

DL matters because of how it attains such impressive results through achieving recognition accuracy at higher levels than it has ever done before. This helps technology and electronics with systems and software to meet expectations that crucial for safety-critical applications within cybersecurity. Recent advances in DL have improved to the point where DL outperforms humans in some tasks like classifying objects in images. While DL was first theorized over 40 years ago, there are two main reasons it has only recently become useful: it requires large amounts of data and substantial computing power. DL requires substantial computing power because high-performance GPUs have parallel architecture that is efficient for DL. When combined with clusters or cloud computing, this enables development teams to reduce training time for a DL network to a meager few hours (MathWorks).

DL works by learning methods using neural network architectures. Therefore, DL models are often referred to as DL neural networks. The term “deep” usually refers to the number of hidden layers in the neural network. Simple neural networks only contain 2-3 hidden layers, while DL neural networks can have as many as 150. DL models are trained by using large sets of neural network architectures and data that learn structures directly from the data without the need for manual feature abstraction (Kampakis). Figure 2 below labeled Simple Neural Network vs. DL Neural Network demonstrates the number of hidden layers a DL neural network has compared to the number of layers a simple neural network has.



**Figure 2: Simple Neural Network vs. DL Neural Network**

One of the most prevalent types of deep neural networks is known as Convolutional Neural Networks (CNN). A CNN associates learned structures with inputted data and uses 2-D convolutional layers to make architecture well suited to processing 2-D data. CNNs remove the need for manual feature abstraction, so it does not need to classify structures used to categorize structures or patterns. CNN works by removing structures directly from patterns. The pertinent structures are learnt while the network studies an assortment of patterns. This mechanical feature abstraction makes DL models highly accurate for cybersecurity tasks such as cyberattack recognition and classification. CNNs learn to detect different features of a pattern using an assembly of concealed layers. Every concealed layer intensifies the intricacies of the learned pattern features (MathWorks).

**4. Results**

DL is not a solution to all cybersecurity problems because it needs extensive amounts of data. Unfortunately, not enough data is readily available, but there is several cybersecurity use cases where DL is making significant improvements to existing cybersecurity solutions. Malware detection and network intrusion detection are two such areas where DL has shown significant improvements over the instruction based and classic ML solutions. Network intrusion detection systems are typically instruction-based and signature-based which are deployed to detect any and all known threats. Attackers usually change malware signatures to easily evade the traditional network intrusion detection systems. DL using self-taught learning has shown to be promising in detecting unknown network intrusions. Traditional security use cases such as malware detection and spyware detection have been tackled with DL.

The primary goal of cybersecurity attacks is to steal any and all forms personal and business data ranging from sales data to intellectual property documents and source codes. Attackers withdraw stolen data to remote servers in encrypted traffic along with regular traffic. Most of the time attackers use an anonymous network that makes it difficult for cybersecurity methods to follow traffic. Moreover, the stolen data is typically encrypted, causing instruction-based network intrusion tools and firewalls to be ineffective. Recently, anonymous networks have been used for Command-and-Control (C&C) by specific variations of ransomware and malware. For example, Onion Ransomware uses The Onion Router (TOR) network to communicate with its own C&C (Singh and Balamurali).

Anonymous network/traffic can be accomplished through various means. They can be broadly classified into network based (TOR) and custom OS. Among them, TOR is one of the more popular choices. TOR is a free software that enables anonymous communication over the internet through a specialized routing protocol known as the Onion Routing Protocol. The protocol depends on redirecting internet traffic over various freely hosted relays across the world. Like layers of an onion, each HTTP (HyperText Transfer Protocol) packet is encrypted using a public key from the receiver during the relay. At each receiver point, the packet can be decrypted using a private key. After decrypting a layer, the next destination relay address is revealed. This continues until the departure node of the TOR network is met and a plain HTTP packet is sent to the original server terminal (Singh and Balamurali).

The intent of launching TOR was to safeguard the privacy of users. However, attackers have stolen data with the objective to use it for various immoral manners instead. As of 2016, around 20% of TOR traffic accounts for illegal activities. TOR traffic is curtained by not allowing the installation of the TOR client or blocking the Guard or Entry node IP address. However, there are numerous means through which attackers and malware can get access to the TOR network to steal and transfer data and information. Atackers can spawn different IP addresses to carry out communication. A bad bot landscape report by cleaned networks shows that 70% of automated attacks in 2015 used multiple IP addresses, and 20% of automated attacks used over 100 IP addresses. TOR traffic can be detected by analyzing traffic. This analysis can be on the TOR node, or in between the client and the access node. The analysis is done in a single flow package. Each flow institutes a tuple of source address, source port, destination address, and destination port. The method used follows a time-based approach over an extracted network flow to detect TOR traffic. However, the architecture uses an overabundance of other information that can be obtained to classify the traffic. This is inherently due to DL architectures that has been chosen to solve this problem (Singh and Balamurali).

The data obtained for this experiment consists of features extracted from the analysis of the internet traffic. Parameters, other than flow-based parameters, include sample instances of the data and architecture of the neural network. Source IP/port and destination IP/port and the protocol field have been removed from the instance as they exceed the model. The process of all other features using DL with N hidden layers which vary between 2 to 10, in which N=5 has been found to be optimal for the number of hidden layers. Neural networks were used in the beginning of this experiment for all the hidden layers where each hidden layer has the dimension 100 and is dense in nature (Singh and Balamurali). The output node is activated by a binary classification that is used as the output. Keras with TensorFlow are used to train the DL model. Keras is a “high-level neural networks API, written in Python” (Keras) and TensorFlow is an “open source machine learning library for research and production” (TensorFlow). These two models both implement AI and DL with their libraries and machine learning platforms. The model was trained in different times to show training simulations and to depict the increasing performance and decreasing loss value as the number of times increased (Singh and Balamurali).

The results of the DL were compared with various other estimations. DL was able to detect vulnerabilities in TOR with great success. However, it was Non-TOR that needs to be given more importance. DL can reduce the false positive cases of Non-TOR trials. Between the numerous classifiers, DL methods performed better than the rest. The results that are shown are based on 55,000 training test cases (Singh and Balamurali) . The data used in these experiments are relatively reduced compared to representative DL. As the data increased for training the test cases, performance increased further for DL. In large quantities of data, DL can outperform any and all classifiers and can be widespread for analogous categories of applications.

**5. Conclusion**

AI and DL have made boundless advancements in the field of computer science, specifically in the area of cybersecurity. With the existing and outdated methods adopted in cybersecurity such as using a firewall, using strong, safe passwords, enabling 2FA, updating systems and software, backing up data, and installing anti-malware software, DL has been able to solve the multitude of issues that have plagued these obsolete and archaic systems as deliberated in the Results section with identifying vulnerabilities with TOR software systems. DL has made electronic data and information more safe and secure against criminals and unauthorized users who do not have the express permission to access that data and information. DL was designed and developed to protect from these prohibited intrusions through taking extra precautionary measures to prevent it from occurring, compared to the approaches that are still in operation as deliberated in the Methodology of this research paper. The research and results of AI and DL have revealed that they are potential applications that will eventually and ultimately surpass the contemporary techniques practiced in cybersecurity. While AI and DL only found susceptibilities in Non-TOR software systems, it they were given the chance, they would also have been able to find susceptibilities is in TOR software systems as well. The determination and work that has been performed and attained from the research of AI and DL will have a prospective impact in cybersecurity, as well as the entire environment of computer science intrinsically in itself. The experiment done shows promise for future work and implantation, with the hopes of eventually preventing probable cybersecurity attacks in the future. There should be more contribution with AI and DL in cybersecurity since it will give the possibility and prospect of a more safe and secure future by preventing data breaches and cybersecurity attacks that could potentially harm many individuals.

# **References**

AIAA. "Artificial Intelligence for Cybersecu." *American Institute of Aeronautics and Astronautics* (2019). Article. <https://www.aiaa.org/protocolAI/>.

AUTHY. "What Is Two-Factor Authentication (2FA)?" *TWILIO, INC.* (2019). Article. <https://authy.com/what-is-2fa/>.

CISA. "Creating and Managing Strong Passwords." *CISA Cyber+Infrastructure* (2018). Article. <https://www.us-cert.gov/ncas/current-activity/2018/03/27/Creating-and-Managing-Strong-Passwords>.

CISCO. "What Is a Firewall?" *CISCO* (2018). Article. <https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html>.

Donovan, Kevin. "10 Cybersecurity Best Practices for IT, IS, Network & Data Security." *observeit* (2017). Article. <https://www.observeit.com/blog/10-best-practices-cyber-security-2017/>.

Ismail, Nick. "Securing the future: The evolution of cyber security in the wake of digitalisation." *InfromationAge* (2018). Article. <https://www.information-age.com/evolution-cyber-security-wake-digitalisation-123470747/>.

Jeffcock, Peter. "What's the Difference Between AI, Machine Learning, and Deep Learning?" *ORACLE* (2018). Article. <https://blogs.oracle.com/bigdata/difference-ai-machine-learning-deep-learning>.

Kampakis, Stylianos. "WHAT DEEP LEARNING IS AND ISN’T." *The Data Scientist* (2015). Article. <https://thedatascientist.com/what-deep-learning-is-and-isnt/>.

Keras. "Keras: The Python Deep Learning library." *Keras* (2019). Article. <https://keras.io/>.

MathWorks. "What Is Deep Learning? 3 things you need to know." *MathWorks* (n.d.). Article. <https://www.mathworks.com/discovery/deep-learning.html#withmatlab>.

Rouse, Margaret. "antimalware (anti-malware)." *TechTarget* (2019). Article. <https://searchsecurity.techtarget.com/definition/antimalware>.

Singh, Satnam and A R Balamurali. "Using the Power of Deep Learning for Cyber Security." *Analytics Vidhya* (2018). Article. <https://www.analyticsvidhya.com/blog/2018/07/using-power-deep-learning-cyber-security/>.

Solomon, John. "Understanding different types of cloud computing and their benefits." *Chargebee* (2018). Article. <https://www.chargebee.com/blog/understanding-types-cloud-computing/>.

TensorFlow. "An end-to-end open source machine learning platform." *TensorFlow* (2019). Article. <https://www.tensorflow.org/>.