Tampere University

Benedict Frederick

ARTIFICIAL INTELLIGENCE IN COMPUTER NETWORKS

Role of AI in Network Security

Masters' Thesis
Faculty of Information Technology
Juha Vihervaara
Jani Urama
October 2022

ABSTRACT

Benedict Frederick: Artificial Intelligence in Computer Networks (Role of AI in Network Security)
M.SC Thesis
Tampere University
Masters' of Communication Systems and Networks
October 2022

Artificial Intelligence (AI) in computer networks has been emerging for the last decade, there are revolutionary inventions that have created automation and digitalization in the fields of the Internet. The layout of computer networks works in layers of topologies with the help of AI, a virtual layer of software has been added that runs predictive algorithms of Artificial Neural Networks (ANNs) with the help of Machine Learning (ML) and Deep Learning (DL). This thesis describes the relation between AI algorithms and duplication of human cognitive behavior in emerging technologies. The advantages of AI in computer networks include automation, digitalization, Internet of Things (IoT), centralization of data, etc. At the same time, the biggest disadvantage is the ethical violation of privacy and the security of data. It is further discussed in the thesis that Artificial Intelligence uses many security protocols, including Next-Generation Firewalls, to prevent security violations. The Software Network Analysis (SNA) and Software Defined Networks (SDN) play an important role in Artificial Intelligence in computer Networks. This thesis aims to analyze the relationship between the development of AI algorithms and the duplication of the human cognitive behavior in various emerging technologies. Software Network Analysis (SNA) and Software Defined Networks (SDN) are critical components of computer network artificial intelligence. The purpose of this dissertation is to investigate the relationship between AI algorithms and network security.

The thesis analyzes 2 main aspects, the role of Artificial Intelligence in Computer Networks and how Artificial Intelligence is helping in securing computer networks to deal with the modern network threats. Security today has become one of the main concerns, everyday a production networks receives arounds thousands of attacks of different scales, and proper network security measures are not configured and taken, a lot can be compromised. Network virtualization, Cloud Computing, has seen exponentially growth in few past years, because of the trend of less human interaction, and minimizing of doing repeated tasks over and over. Data in today's world is now more important than it has been in decades earlier, this is because today everything is moving towards digitalization, proper Information Security policies are derived and implemented all over the world to ensure the protection of Data. Europe has its own General Data Protection Regulation (GDPR) which ensures that every company who deals with data is to implement certain measures to ensure the data is protected which also involves implementing the right network security measures so that the right people have the access to the sensitive information. This thesis covers the overall impact of Artificial Intelligence in Computer Networks and Network Security.

Keywords: Artificial Intelligence, Artificial Neural Networks, Machine Learning, Deep Learning, Internet of Things, Next-Generation Firewall, Software Network Analysis.

PREFACE

First of all, I would like to thank my professors Juha Vihervaara and Jani Urama for their constant guidance and support throughout my research work. They provided timely feedbacks and provided me with all the knowledgeable guidance during this time. They were very patient with me along this whole journey.
For me it was completely a new experience of doing research and following a research-based approach. I would also like to convey my gratitude to University of Tampere and faculty of Communication Systesms and Networks for providing me with the best possible resources and ecosystem for my research work to be completed timely.
Last but not the least I would like to thank my family and especially my wife for their constant support throughout.

Tampere, Oct 2022.

Benedict Frederick.

Contents

List of Figures

List of Tables

List of Acronyms

AI	Artificial Intelligence (AI)
ANN	Artificial Neural Networks
CNN	Convolutional Neural Networks
DBN	Deep Belief Networks
DDoS	Distributed Denial of Service
DL	Deep Learning
DoS	Denial of Service
GDPR	General Data Protection Regulation
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ML	Machine Learning
NGFW	Next-Generation Firewall
NLP	Natural Language Processing
RNN	Recurrent Neural Networks
SNA	Software Network Analysis
SND	Software Defined Networks
TCP	Transmission Control Protocol
UBA	User Behavior Analytics
UDP	User Datagram Protocol

1. Introduction

In the last few decades, the technology world has seen a massive transformation. The focus of technology has shifted to major breakthroughs such as the Internet and automation. Humans are already capable of invention of technology that can execute important activities that were previously thought to be impossible. AI Technology is amongst the most advanced technologies that allows humans to replicate and execute a variety of tasks. The research paper focuses on artificial intelligence's evolution and role in computer networks. To fully comprehend what artificial intelligence is and what role it plays in computer networks, we must first comprehend the concepts associated with artificial intelligence and data networks.

Computer networks have been a long technological revolution. The invention of the Internet has enabled humans to interact with each other, share information, and even store their data online. The Internet has become an important part of the lives of people. People are relying more and more on the Internet than anything else (Li, The Application Analysis of Artificial Intelligence, 2021). For example, we are using social media platforms or other web applications to communicate with each other. Emails are being used to communicate with clients in businesses. Data is being uploaded to the server or cloud platforms. All these things are using the Internet. Without the Internet, none of these is possible. The world of computer networks is associated with the delivery of these things.

AI technology, from the other hand, is the application of technology to construct a technology that can think, make decisions, and carry out tasks like a human. AI technology is a large field, and its position in computer networks has the ability to intervene and pounce an impact on technological development. In computer networks, security is a significant concern. AI Technology can be useful in a variety of security situations. Furthermore, Artificial Intelligence can help with the analysis and editing of data that is stored online or linked to a network. (Shang & Zhao, 2020).

Automation is already being used in many industries, such as manufacturing, finance, and healthcare. The use of automation has led to an increase in productivity for some jobs, but it also means that there are fewer jobs available for humans to fill. In addition, as more people become dependent on machines for their work or personal needs (e.g., transportation), they

continue to lose their livelihoods because machines can do things better than humans could ever hope for—even if they're paid less than their counterparts who aren't replaced by robots. Artificial Intelligence could potentially replace all types of human jobs because it can learn how best perform tasks based on past experiences rather than relying solely on traditional methods such as trial-and-error learning like humans do when trying new things out first time around before making decisions based off previous experience/trial runs made previously performed successfully before making adjustments next time around.
The IoT is an ongoing trend and will be around for years to come. It's not dependent on 5G, but it does provide connectivity between devices, which is key to many of the applications that rely on it.

The IoT involves everything from smart homes to connected cars, industrial machines and more. It's also easy to see how technology companies are using sensors in their products or services—for example: Amazon uses sensors in its Echo speakers so they can tell you about upcoming events based on whether or not you're home; Google Home uses its location services (including GPS) for similar purposes at all times; Apple Watch tracks your fitness activities with heart rate monitors; Fitbit tracks your sleep patterns through movement sensors embedded inside their trackers...the list goes on!

The future of technology is bright, as we've seen in recent years. The pace of innovation continues to accelerate and companies like Amazon, Google and Apple are investing heavily in AI research. As more people enter the workforce with skills that can be applied across industries, automation will become an even larger part of our everyday lives—and it's not just about replacing jobs; it's about redefining how workers do their jobs today.

2. Computer Networks from the perspective of AI

The field of Artificial Intelligence covers a broad category of other fields. The major covered fields covered by Artificial Intelligence are perception and logical reasoning, mathematics, statistics, and networking. Networking is used in artificial intelligence to automate some of the tasks. Neural networks, expert systems, and natural language processing are all examples of areas where AI researchers might use their ideas. When deployed correctly, AI can aid global collective intelligence in resolving some of humanity's challenges.

Computer networks can become more intelligent and user-friendly when artificial intelligence is applied to network technology. One can use artificial intelligence in a number of ways to achieve a variety of functions, such as automatic data collection and trend analysis (Qingjun & Peng, 2018). If a fault arises, it will not only respond quickly but will also take a number of specific actions. To understand more about the relationship between artificial intelligence and networking, we need to understand the concepts associated with networking.

Computer networks are the collection of hundreds and thousands of devices connected with each other. The connection is usually made through cables, switches, routers, firewalls, and vice versa. All these devices perform their duties on different layers of the OSI (Open System Interconnection) model such as switches that work on layer 2 to toward frames. Similarly, routers work on layer 3 to perform the functionalities of packet routing. All these networking devices are interconnected with each to form a computer network.

There are various types of computer networks such as LAN (Local Area Network), PAN (Personal Area Network), WAN, CAN (Campus Area Network), and MAN (Metropolitan Area Network). Currently, LAN and WAN are considered famous computer networking types. LAN consist of small offices, homes, and shops whereas, WAN covers the whole globe. WAN is also known as a collection of LAN based networks.

Different changes have been in the computer networks by introducing intelligent decision-making. The developers of computer networks trying to introduce AI (Artificial Intelligence) and ML (Machine Learning) into the computer network. Currently, the network security devices such as next-generation firewalls, and IDS (Intrusion Detection System) / IPS (Intrusion Prevention System) based technologies are using advanced AI algorithms to detect the malware, spyware, and ransomware attacks. According to various computer network researchers, introducing AI and ML (Machine Learning) in IDS (Intrusion Detection System) can help business organizations to keep their network secure from any type of intrusion. AI contains different algorithms such as rule-based matching, signature detection, clustering, and various others. The clustering algorithm is widely utilized by computer network devices to

perform the separation operations intelligently. The important function of the clustering algorithm is to perform grouping or classes of data according to their characteristics and resemblance. Various business organizations are using AI and ML (Machine Learning) in their IDS (Intrusion Detection System). Also, IDS (Intrusion Detection Systems) can utilize AI-based honeypots. In the cooperate networks, honeypots are used to capture the malicious users or threat actors. The computer network with the honeypots shows itself vulnerable to the hackers. When the hacker launches the attack, it captures all the important information of the hacker such as IP (Internet Protocol) address and geo-location information.

Introducing AI and ML (Machine Learning) in computer networks also encouraged the concept of network automation. Automation is considered one of the most important components of Information Technology and Information Systems. It allows the developer and network engineers to deploy the automation scripts to handle the complexities and structure the network according to modern business requirements. These automation tools also use AI to push the configurations inside the computer networks. In modern days, the concept of SD-WAN is quite popular among network engineers and analyzers. SD (Software Defined) – WAN technology contains important components such as vManage, vBond, vSmart, and edge nodes. The concept of SDWAN (Software-Defined WAN) was introduced by removing the centralized behavior of the computer network devices. Networking devices such as routers, firewalls, and vice versa have their own control plane and data plane. The role of the control plane is to provide the direction to the packets and perform intelligent operations whereas, the role of the data plane is to forward the packets as fast as possible through the hardware interfaces of the networking device. SD (Software-Defined) based networking has separate two components (control plane and data plane) from the routing devices. Developers have placed the control plane of the networking device in a remote location and allow the different components of the computer networking device to communicate with the help of API (Application Programming Interface). Almost all the software-based application uses APIs to communicate with their backend systems and fetch the data according to the pre-defined rules and structures. Computer networks with AI and ML (Machine Learning) capabilities also use API calls for end-to-end communication.

2.1 Network components

In order to share information and other resources, a computer network consists of many computers that are connected to each other. The components of the computer network contain all of the necessary components for setting up a network. There are several sorts of networks in computer networks, ranging from simple to complicated. The components we need to install for a network are mostly determined by the network type. We can also eliminate some network

components if necessary. For example, no cables are required to set up a wireless network. Some of the basic components are discussed below.

Protocols

A protocol can be defined as a set of rules that defines how computers communicate over a network. The Open Systems Interconnection (OSI) model is one example of how protocols communicate with each other to perform the networking operations. The OSI model was introduced in 1983. It has been a standard for communication between computers all over the world since then. The OSI model is divided into seven layers. These layers are application, physical, transport, network, data link, presentation, and session layer. Some common network protocols are TCP (Transmission Control Protocol), UDP (user Datagram Protocol) and IP (Internet Protocol) (v4 and v6).

Computer networks use protocols to initiate the communication with the remote devices and without the network protocols, it is difficult to perform networking operations. Protocols are the set of pre-defined rules and standards to communicate with the other devices present in the network. Usually, TCP/IP protocol stack is used worldwide for the network protocols. This model contains different layers such as Link Layer, Network Layer, Transport Layer, and Application Layer. All these layers have different functionalities and use different protocols for communication. As explained in Figure 1, following are the protocols used by each layer of the TCP/IP model. The typical OSI Model has 7 layers and each layer has its own role in ensuring a proper communication is done between 2 nodes. The figure 1 is showing different layers of the OSI model, and each protocol that is used by the layer to ensure communication. For instance at the Application Layer we use HTTPS, HTTP which is used to how the information is displayed over a web browser. Similarly at the Session Layer, TCP or UDP is used, which ensures the connectivity of a particular session as long as the communication is happening between the nodes. Internet Protocol (IP) is used at the network layer which ensures that the packets between the 2 nodes are correctly delivered and returned back. Data Link Layer second last layer in the OSI model which ensures which medium will be used for transferring the packets and then it sends the packets to the physical layer which transfers from one end to the other.

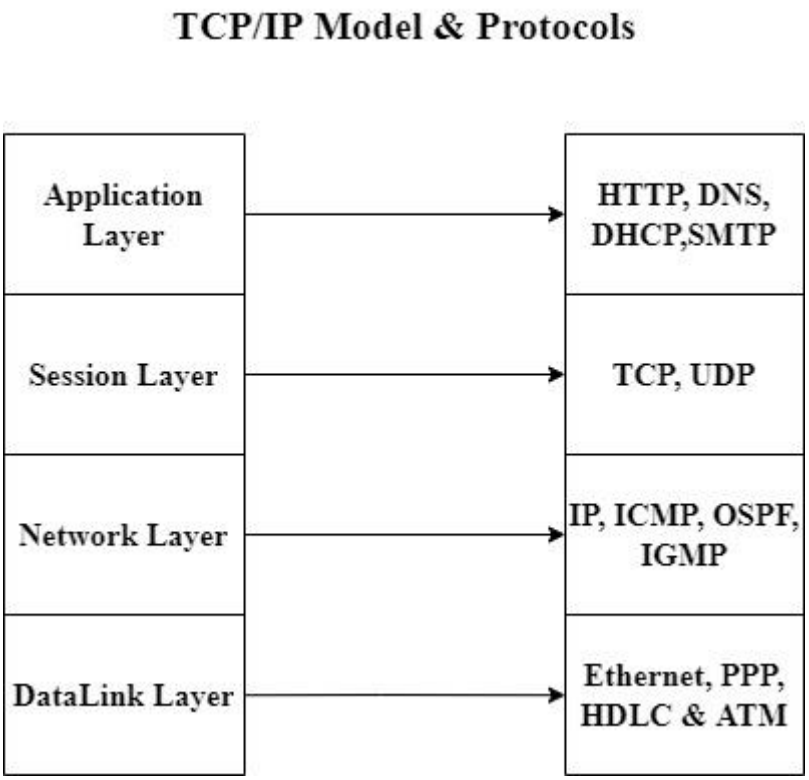

Figure 1: Protocols used by each layer of the TCP/IP Model

Traditional networking such as switches, routers, and VLANs are now being replaced by modern virtual technologies. According to the World Health Organization, the excessive usage of hardware devices is creating disastrous effects on nature, and it is increasing global warming. VMware and other tech giants such as Microsoft, Google, and AWS are now promoting the use of virtual networking devices in the environment to safe nature. 4G and 5G networks are currently boosting the usage of IoT (Internet of Things) devices such as smart cars, house automation systems, IVAs (Intelligent Virtual Agents), Smart CCTV cameras, Smart household equipment, Smart Kitchens, and vice versa. All these IoT uses advanced AI (Artificial Intelligence) algorithms to recognize the environment and perform its intelligent operations. IoT (Internet of Things) devices require high-speed internets such as 4G and 5G networks to perform the communication with the cloud networks and APIs (Application Programming Interface) endpoints. As discussed above, the companies are now promoting the usage of virtualized environments than the physical environment because the physical network infrastructure requires high maintenance costs and high electricity costs. That is why tech giants are promoting virtualized or cloud-based networks.

Traditional network components

The core of traditional networking is network equipment like switches and routers. Each of these devices performs a task that completes the overall networking function. The network's speed is frequently boosted when network functions are implemented as hardware structures. Routers and switches are network devices that connect one or more computers to other computers, networking devices, or other networks. These devices have a similar appearance, yet their functions are vastly different. A network switch is a device that connects devices on a single computer network. The data is forwarded to the right destination by the switch using the MAC address. A router is a network device that connects a computer network to the Internet, such as a home network. The router connects the network to the rest of the world via the Internet. A router also protects data from security threats.

In a traditional network, devices like switches are routers that are also known as fixed-function equipment for a network and are fundamental elements of a network. Every device has its functionality and role that works with other devices for different purposes. The speed of the network is usually increased when functions of the devices of the network work together for the achievement of any task. Functions for the traditional networking mostly work with the hardware that is dedicated, for example as application-specific integrated circuits (ASIC) (IT, 2021). In this era of technology, the networks for any type of organization are growing to be more complex and even larger as there is a continuous increment in the number of users and also there is the increment in the applications. For the achievement of many objectives of network management, the knowledge of the network topology for an enterprise is required. The objectives can include root cause assessment, traffic bottleneck, failure of the components, resource management, planning, and deployment of the new elements and devices. For an administrator to have a clear sight of the network, a network topology map can display this management. For an organization having a network infrastructure, there can be a lot of difficulties for network administrators having lack of knowledge, which can be due to no availability of discovery tools that will share the topology information like devices, subnets, as well as VLAN used. Even these types of discovery tools are essential for an experienced administrator. There are a lot of techniques that help discover the network topologies automatically that including Simple Network Management Protocol (SNMP), DNS, ICMP, etc. (Pandey et al 2010).

Modern network components

As things are changing, there is a need to update the existing network equipment and methods. Not long ago, we have our network with cables, and it seemed almost impossible to use the network without cables. Now we have wireless networks. Artificial Intelligence has given birth to many modern networking components such as IoT, virtualized network function (VNF), and

Network Virtualization (NV). Virtualization has made it possible to create virtual machines that operate on their own platforms. In short, modern network components have almost replaced the traditional networking components.

Organizations must find a means to expand automation over the entire network and combine IT systems to address a comprehensive end-to-end process because traditional network automation has only focused on the development and activation of use cases to experience the full benefits of network automation. The end-to-end process must be covered by network automation for it to be really effective in the hybrid, multi-cloud environment of today. Any full automation platform should support the above mentioned three key components, exposing the necessary systems and data to important stakeholders is the goal of these components.

2.2 Network management

As there are a lot of networking components, it is important to manage them properly. A network management system is used to perform different networking tasks. It involves administration of the network, along with the management and operation of the network. Hardware and software are used by network management systems to gather and analyze data on a regular basis. Another task of network management is to improve the performance of the network. The security of the network is also included in network management. Network management includes features such as automation of the network, administration of the network, operation of the network, and maintenance of the network.

Network automation is one of the distinguishing characteristics of a modern network management system. The process of automating the configuration, handling, testing, deployment, and operation of physical and virtual devices inside a network is known as automation. Switches, routers, and servers are all part of network administration. Smooth network operation includes close monitoring of activity to promptly and effectively address and fix problems as they arise, ideally before users are aware of the issue. Upgrades and fixes to network resources fall under network maintenance.

Simple Network Management Protocol (SNMP) is a protocol that is used for sharing information with another between different devices on any network. SNMP even works if there are different types of hardware used in the network and having different types of software. SNMP is the powerful protocol that is used for network management discovery, performing monitory of the network, having knowledge of changing in the status of the network, and also it is used for the determination of the devices of the network (Oros, 2016).

Generally, one or more than one administrative computers that are also known as managers are used for SNMP to watch over different devices like servers, switches, routers etc, that are

used in a network. SNMP uses continuously running software that is also known agent for storing the information. It not only includes computers but also includes phones, printers, etc. A type of formatted text file that takes place in SNMP manager is usually designed in such a way that it collects the information and then organizes it into the hierarchical layout known as a management information base or MIB. The information collected by the MIB is used by the SNMP manager for the interpretation of the messages before their transmission to the receiver. The information that is stored in MIB is also known as managed objects and it consists of performed data obtained during the loading of the network monitoring tool

There are different types of managed objects in the MIB that can also be identified by an object identifier or OID. A type of address that makes the differentiation between different devices that are in the hierarchy of MIB is known as OID.

Seven types of protocol data units are used by SNMP which are

GET Request: SNMP manager generates the GET Request and then received it from an agent for obtaining the value of a variable that an OIB identifies that is in a MIB.

GETBULK Request: Sent by the SNMP manager sends these requests to the agent for gaining a huge amount of data efficiently.

GETNEXT Request: Sent by the SNMP manager sends these requests to the agent for retrieving the values of the next OID in the hierarchy of MIB.

INFORM Request: An alert that resembles that of TRAP but by the SNMP manager, needs verification of acknowledgment.

RESPONSE: Agent sends to the SNMP manager that is issued in reply to a GET Request, GETNEXT Request, GETBULK Request, and a SET Request.

SET Request: SNMP manager sends to the agent for resolving the issues of configurations or commands.

TRAP: This is an alert that the agent sends to the SNMP manager for an indication of a significant event.

SNMP version 1 was created in 1980. It is the oldest version of SNMP. Its setup is very easy as it requires just a community of plaintext. The biggest downfall of version 1 of SNMP is that 64-bit counters are not supported by it rather it supports just 32-bit counters and security is little for this, due to which man-in-middle-attacks can be increased

SNMP version 2c was created in 1990. SNMP version 2c is the same as version 1, except it provides the facility of supporting 64-bit counters. In this version, there is an improvement in performance and the security, but it also uses encryption

SNMP version 3 is the newest version that makes use of the protocol functionality with the addition of cryptographic security for increasing the data security and it also adds the security to the 64-bit counters. Both encryption and authentication are supported by this version (Logicmonitor, 2012).

Software Defined Network (SDN) refers to a networking architecture technique. Software programs are used to control and manage the network. All the devices and the behavior of the network can be controlled with the help of Software Defined Network (SDN) through a central location. Software Defined Network (SDN) is the replacement of the traditional network. Traditional network architecture provides little flexibility in terms of coordinating between fixed-function network devices. These devices must be set manually. A single modification can have a bad effect on network performance and perhaps bring the whole network down. This is why Software Defined Network (SDN) is a good choice for managing the network.

Software-defined networking (SDN) is an architecture that summaries the different, distinct layers of a network for making that network more responsive and elastic. Enhancing the network mechanism by allowing different organizations as well as service providers to act quickly for changing the business conditions is the main objective of SDN. A network administrator or a network engineer can form the traffic from a centralized console even without having any physical access to any individual switch in a network. For delivering the network services a centralized SDN controller manages the switches wherever they're needed (Rosencrance, 2022). The architecture of SDN consists of three layers that are application layer, the control layer and the third one is infrastructure layer. These layers make communication by using the application programming interfaces that are northbound and southbound.

SDN includes a lot of technologies consisting of functional partition, network virtualization as well as automation with the help of programming functions. By default, SDN technology concentrates on the division of the network control plane.

In a classical SDN situation, at a network switch, a packet is reached. The rules that are built into the proprietary of the switch's firmware inform the switch where the packet will be forwarded. The centralized controller sends this type of packet handling rule to the switch. The switch that is also known as the data plane device asks about guidelines from the controller and then it responds to the controller by providing the information about the traffic that it will handle. An operation mode that is also known as adaptive or dynamic is used by SDN, through which a route request is issued by the switch to a controller for a packet without a specific route.

2.3 Network security

Security is an essential part of networking because networking can lead to many challenges. Everyone wants their online documents to be secured. To accomplish this, network security is applied so that the data remain safe from the hands of attackers. Further details regarding network security are given below.

A security threat is a dangerous type of malicious activity that has a purpose to harm or steal important and sensitive information and data or intend to interrupt the entire network of an organization. In this era as innovation is taking place in the field of information technology, an organization must be more careful about securing their important data as well as their entire network as different types of cybersecurity threats continue to develop and become more sophisticated. So, for this purpose it is very important to know about the nature of the security threat that can affect the system or the network.

A firewall is a network security device that make secure the network perform monitoring and filtering on the traffic that is incoming to the network or outgoing. By using firewall prevention to the network from an unauthorized access take place. Filtration of the incoming and outgoing traffic can be done by using a hardware or software. A firewall has two parts one is matcher and other is action part. In matcher part, we set different rule for the filtration of the traffic and in action part traffic is allowed or blocked.

An application gateway is a type of program that act as a firewall proxy. To make security tight application gateway works between computers in a network. It filters out the incoming traffic that consists of network application data. If a program wants to make connection with another program, it is necessary to establish a connection to the application gateway, which looks for the trustiness the program for making a connection. In this receiving computer remain secure from different malicious attacks.

An intrusion prevention system (IPS) is a system that has the function of monitoring of a network for different malicious activities such as violations of policy or security threats. The identification of suspect activity, and different log information, an attempt made for the blockage of a specific activity, and at last reporting it is the main function done by the IPS. Intrusion prevention system can have its implementation over software or a hardware device.

3. Theoretical Background

Computer networks have evolved a lot in recent years. The wired networks have been changed to wireless networks. The storage in the specific systems has been changed from the storage in the computer system to the cloud systems. We can access our documents from anywhere. All we need is just an active internet connection. Artificial Intelligence can assist in several areas of computer networks. Scientists are exploring different ways to create machines that can perform several tasks that a human can perform. The aim of scientists is to make humans free from several tasks that can, in turn, be performed by machines. Artificial Intelligence is challenging, and the research on Artificial Intelligence is not perfect till now, as the algorithms are still in an evolving stage (Li, 2021).

3.1 Artificial Intelligence

As discussed earlier, Artificial Intelligence is the area in which different techniques are used to create machines that can mimic human beings. Artificial Intelligence has become a technological giant that has given birth to various other things, such as the Internet of Things and blockchain. AI technology can be used in a number of ways. Machine learning and deep learning are the two of the methods that will be used. Algorithms are employed to implement machine learning. These techniques are used to predict outcomes from provided data by employing various patterns. Human brain networks are closely mimicked by deep learning.

AI technology is primarily based on research, as times evolve, and developers and researchers must study and implement new methods. Coders and researchers, on the other hand, share certain shared goals. The initial purpose is to use logic to solve problems. Researchers are exploring different approaches and algorithms, while programmers are putting those algorithms into action. The planning of tasks that really can work on their own is the other goal. Self-driving cars, for example. They are capable of moving on their own. The use of natural language processing to create computer systems or machines that can understand natural speech is another goal. One goal is to develop machines that can interact with people. All of these objectives demonstrate that programmers and academics are on the same page.

Artificial intelligence can be divided into two categories. It might be either weak or strong. Narrow Artificial Intelligence is another name for a weak Artificial Intelligence. (Artificial Intelligence (AI), 2020). A low AI Technology is one which is only capable of doing a few tasks. There are several examples of poor Artificial Intelligence, as we are now in the period of only

developing weak AI Technology. Robots and other AI-related devices are made to perform certain tasks only.

They are unable to act within their own. Apple's Siri and Amazon's Alexa are two well-known examples of AI technology that isn't up to par. They simply respond to the questions which are asked. Strong AI Technology, on the other hand, is a phrase that relates to goods that can act like humans or have intelligence comparable to humans. AI Technology with a high level of intelligence can solve problems, learn something new, and now even plan ahead. (Artificial Intelligence (AI), 2020). Up until now, there have been no real examples of Strong AI Technology.

Nevertheless, there are other robots that can answer our queries or mimic human intelligence in some ways. Sophia, a robot created in 2016, is one such example. Sophia was the world's first robot citizen. Sophia is smart enough to recognize facial images, eye contact with them, and comprehending what they will be saying. She reacts to any inquiries that are posed to her. Sophia is a fantastic breakthrough for AI Technology; however, she isn't a powerful AI because she can't make a decision on her own.

AI plays an extremely important role in the development of the modern IT (Information Technology) and Information System (IS) infrastructure. Artificial Intelligence uses powerful algorithms to make the machine intelligent or take self-oriented decisions The concept of Artificial Intelligence is derived from the working of the human brain. The human brain can make an independent decision on the bases of knowledge or learning. In AI technology, the machine is trained in doing specific tasks. Artificial Intelligence means making a machine intelligent enough to interact with the external environment.

The history of Artificial Intelligence started back in World War II. In WWII, Germany developed a cryptographic device known as Enigma. This machine was highly capable of encryption with plain text with various layers. The British army had huge pressure to break down the enigma encryption to avoid the German attacks. Finally, British mathematician Alan Turning started working on the construction of an intelligent machine that can think. This project was named “Computing Machinery and Intelligence” in 1950. The invention of this machine opened the gate for Artificial Intelligence. Alan Turning is also known as the father of Artificial Intelligence. After this many scientists and computer engineers started building intelligent machine software which can react to human intervention. Various computer games were developed to challenge human beings and ensure that machines can actually think on the bases of data and information. Machines are usually fast and accurate in the process of decision making and the human brain can’t perform well in front of machines. Today many enterprise businesses and the health sector are using Artificial Intelligence to run the business and manage the health of the patients. There are various algorithms built for Artificial Intelligence such as SPF (Shortest Path First), ST (Spanning Tree), GSA (Gravitational Search algorithm).

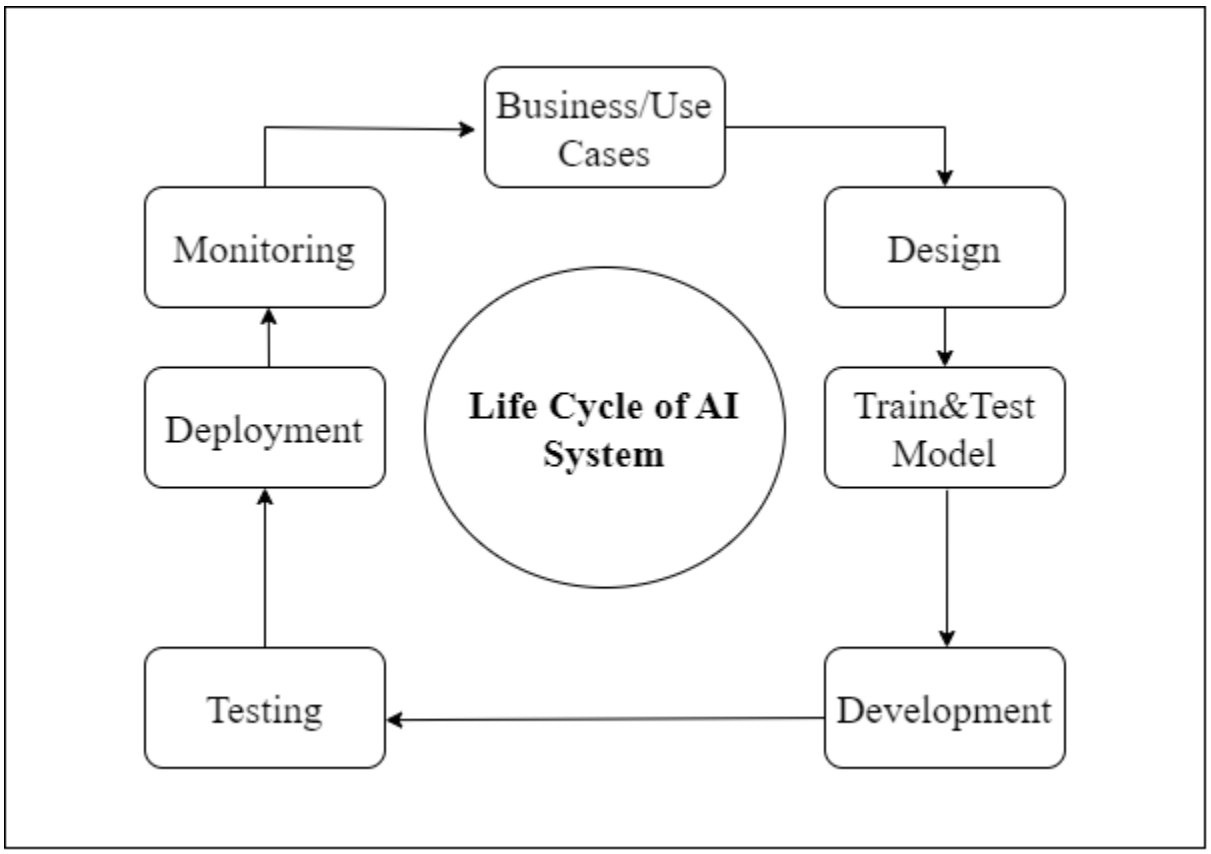

Figure 2: The Life Cycle of Artificial Intelligence and Machine Learning

Today, the most famous application such as Google Maps uses SPF (Shortest Path First) algorithm to find the optimized and shortest paths. The networking devices such as switches and routers use some sort of intelligence to route the packets over the Internet. Ethernet switches use STP (Spanning Tree Protocol) to avoid the L2 loops and optimize the network. The process spanning the tree runs automatically and does not require any human interaction. Figure 2 shows the life cycle of AI based application. If we look at the life cycle of AI it begins with a simple business need or a use case that how we can use automation to make the system smart enough to perform certain tasks on its own rather than some human doing it repeatedly. Once a use case is defined, we move to the next stage where we start designing the application what tasks will it do and what features it should have to make it interactive and self-sustainable. Once we design the application, we start feeding the system some data and train it to make the decision based on the data and test the outcome of that. Once we run the initial train and testing, we move further to develop the model on those results and put it to testing in the real-time environment. This phase continues until the application is deployed and then it is just being monitored whether it is performing its tasks on its own based on the data it is receiving, hence making less human dependent and less prone to errors. Today in the modern business era, many enterprise organizations are also using AI based software.

The most famous AI software are MIS (Management Information System) and DSS (Decision Support System). MIS contains highly efficient AI-based algorithms which convert the raw data into useful information and information is usually displayed in the form of charts, histograms, pie-chart, excel sheet. All this information is further analyzed to construct BCP (Business Continuity Plan), Market Competitive Advantages, Financial Gains, and Business Client Trust. MIS (Management Information Systems) is also used in sports for displaying player statistics, different comparisons, and predictions on the bases of raw data and graphs. DSS (Decision Support System) is usually utilized by the organizational top tier such as the CEO (Chief Executive Officer) and executives to analyze the overall business performance and requirements.

The evolution of AI was started in the era of Alan Turning. Alan Turning also provides the idea of intelligent machines to future scientists. The machine of Alan Turning also gave an expression that machines can think to perform intelligent operations. Many AI games were programmed to beat the experts. The computerized chess game is famous for defeating the world champions. This was because machines have to think and act faster than the human mind. It is the thought of many renowned scientists that these intelligent machines are capable of doing human jobs faster, accurately, and more reliably. The invention of AI brings the industrial revolution and big businesses started using machines instead of human beings because the machine has fewer chances of committing terrible mistakes. Automation also increases the yield of the industries with less cost.

Artificial Intelligence systems work on cutting-edge algorithms and various internetworking devices use AI-based algorithms to find the desired paths. The important AI algorithms are STP (Spanning Tree Protocol), OSPF (Open Shortest Path First), GSA (Gravitational Search Algorithm). All these algorithms are fed inside the machines to perform intelligent operations. IoT (Internet of Things) devices purely work on AI algorithms. Internet of Things devices is also known as smart devices with the capability of doing a task on commands. HAS (Home Automation System), KMS (Kitchen Management System), and Automated Cars are common examples of IoT (Internet of Things) devices. Artificial Intelligence is also introduced in the voice recognition systems such as Microsoft Cortana, Amazon Alexa, Apple Siri. These systems also known as IVA (Intelligent Voice Assistant) use intelligent algorithms to recognize the voices of customers. A deep neural network is used inside the voice recognition software. These deep learning-based algorithms are responsible for understanding the linguistics of human beings. Deep learning is a sub-branch of AI working similarly to the neurons of the human brain. The artificial neuron network is created inside the machines and it provides the capability of self-learning. Machines can understand the environment and learn about different networks with the help of deep neural network technology.

According to the researchers, deep neutral technology can be dangerous for human beings because the machines succeed in 100 percent copying the human brain and it would be a disaster for the survival of human beings. Machines can do any task with accuracy and absolute focus and also there are fewer chances of errors. Various Hollywood movies are designed on the advantages and disadvantages of deep learning. Tech giants such as Amazon, Microsoft, Google, and Neural Links are working on the project of pure AI. The CEO of neural Link Elon Musk has claimed that they are very close to their goal of building pure AI-based technologies. This company is also trying to attach the human brain with AI-based chips.
Another important sub-field of Artificial Intelligence is known as Machine Learning (ML). Machine Learning uses complex algorithms to perform complex and complicated tasks. ML consists of various types such as supervised learning, unsupervised learning, semi-supervised learning, and re-enforcement learning. In supervised learning, the machines use raw data and learn everything on their behalf and there is an interaction with human beings. Basically, scientists have to train the algorithm to perform the desired tasks. Also, the labeled data is supplied to the machines. In supervised learning, the machine makes different predictions according to the provided labeled data.
Regression and classification are the two most important algorithms used by machines. In the classification algorithm, the objects are classified according to their close match. Supervised learning is widely used inside health institutes for the detection of cancerous cells and harmful objects inside the human body. Unsupervised learning is usually provided with unlabeled data and machines do not require any interaction of human beings. Instead, human beings can learn various new things from the intelligent machines in form of graphs, comparisons, pie charts, and vice versa. Unsupervised learning is useful when human beings are totally blind or have no knowledge about the task. This learning usually mines the important and useful data from the raw to draw some useful and fascinating results. K-means clustering algorithms are considered the most important algorithm for close detections. The semi-Supervised ML (Machine Learning) algorithm falls in-between supervised learning and supervised learning. Also, these type of machines requires engineers to deal with. Reinforcement learning ML (Machine Learning) algorithms learn on the bases of intelligent agents. The agents are responsible for collecting data and continue observing the environment to observe the changes. IoT (Internet of Things) devices use reinforcement learning algorithms to operate things. Google IoT-based car uses reinforcement learning to detect the obstacles on the road and keep them aligned with the traffic. These types of cars continuously monitor and communicate with the control systems to fetch the latest instructions and figures.
The household IoT (Internet of Things) devices also utilize the reinforcement machine learning algorithm to observe the surrounding environment such as vacuum cleaners. In the current era, AI is gone far beyond. Scientists are trying their best to copy the whole human brain. The

copying of the human brain is the process of converting analog information into digital information. The machines are highly capable of understanding digital signals. According to the AI researcher, the computer chip will be inserted inside the human brain and this electronic chip will be responsible for translating the analog signals into digital signals. Also with the help of this electronic chip, the human brain would be able to connect to the Internet and update/download important information. But there is a huge risk involved in this process because anything that is connected to the Internet can be hacked or manipulated and it can provide a huge attacking surface to the hackers or malicious users. AI contains both advantages and disadvantages according to the needs of human beings.

3.2 Evolution of Artificial Intelligence

AI has a fascinating history. Robot notions have been featured in comic books and movies. When the first computer was invented, the world changed forever. The development of computer systems ushered in a period when humans began to rely on technology. Humans were able to store files, then save their essential information, constructing databases, leading them to develop apps to do a variety of activities, and finally automating processes. Humans are today more than ever reliant on machines. Humans are increasingly committing their lives to the creation of machines capable of doing any task (Adami, 2021).

The term "Artificial Intelligence" was coined from a popular genre known as "Science Fiction." Developing a machine that could think like humans was pure science fantasy. One of the earliest robot notions was the cruel Tinman from the iconic film "The Wizard of Oz." The author of this story lived in the early twentieth century. Many famous scientists had the idea of Artificial Intelligence in their heads by the 1950s. Alan Turing was one of the pioneers in the study of Artificial Intelligence's mathematical possibilities. He was the one who wondered why machines couldn't think like humans.

In 1950, he published a paper titled "Computing Machinery and Intelligence." This study covers the evolution of intelligent robots and how to assess their intelligence. Unfortunately, computer systems were not as advanced at the time as they are now. The primary difference was that they could just execute commands rather than storing them, which is not a feature of an AI system.

In 1956, the first Artificial Intelligence conference was organized (Artificial Intelligence, 2020). Dartmouth College hosted the conference. The first Artificial Intelligence program was formed as a result of this meeting. This program, dubbed "Logic Theorist," was built by Allen Newell, J.C. Shaw, and Herbert Simon. Frank Rosenblatt created the first computer that was based on a neural network in 1967. The Mark 1 Perceptron is the name of this machine. Following

this, Marvin Minsky and Seymour Papert wrote a book that outlines the work on neural networks. Neural networks were first used in Artificial Intelligence applications after then.
The Artificial Neural Networks have three advantages in terms of computer network security, intrusion detection, and intrusion prevention responses:

1. Adaptability to noise and inadequate data
2. Nonlinearity - dealing with complicated nonlinear functions
3. Information processing parallelism
4. Learning models that are versatile and adaptable
5. Learning through the practice of algorithms and examples.

IBM created an AI-based chess game in 1997. This AI-based game defeated Garry Kasparov, the world chess champion at the time. In later years, progress and research on more Artificial Intelligence-based objects began. Baidu Minwa developed a supercomputer in 2015 that uses neural networks to accurately detect and categorize photos (Artificial Intelligence (AI), 2020). This accuracy rate was considerably higher than a human brain's average. This was one of the most significant advancements in AI. Also, Figure 3 explains the inter-dependency of machine learning, neural networks, and deep neural networks with AI. The terms machine learning and neural networks and deep neural networks seems to be very complicated, which in-fact is somewhat are. But today we have achieved a lot of wonders because of these 3 terms, we have been able to build machines which are self-sustainable i.e. they are able to make decision on their own and the data they receive. Similarly neural network is a series of algorithms, that recognizes relationship between a set of data through a process the way human brain works. Deep Neural Network or also known as Deep Learning is also under the family of AI, as it has layers and each layers take the input and abstracts and presents it into a more composite way. It uses just raw data input to extract the information and then perform the action accordingly. The figure 3 below shows exactly how these 3 are from the same family of AI and the relationship between them.

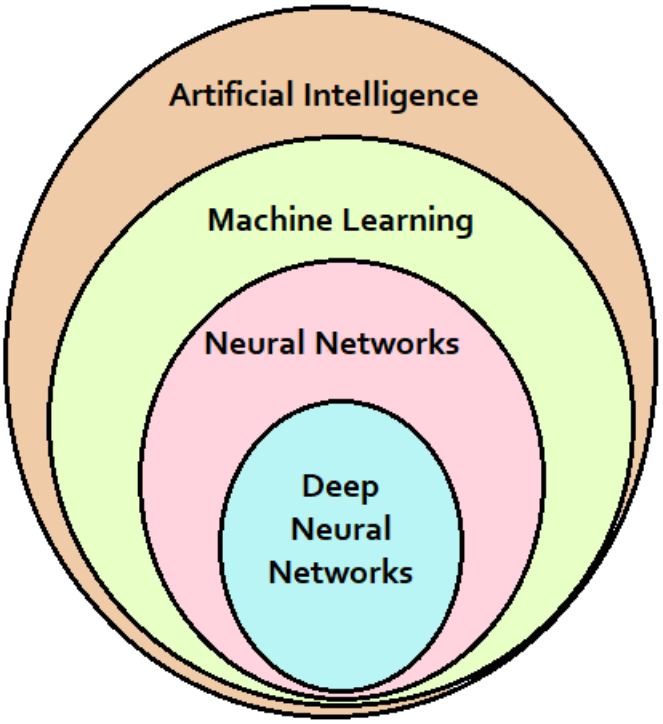

Figure 3: Relation between AI and ML, Neural Networks and Deep Neural Networks

(Pupillo, Fantin, Ferreira, & Polito, 2021)

3.3 Advantages and Features of AI

3.3.1 Pros/Advantages

The world has changed as a result of AI. The world has become increasingly reliant on technology rather than humans. The increased use of machines has given Artificial Intelligence the opportunity to become more stable. Artificial Intelligence has numerous benefits and is not restricted to any particular sector or industry. Artificial Intelligence has a number of advantages:

1. Lowering down Human based error
2. Lowering Risks
3. Accessibility.

Lowering down human error

Humans are the ones who are likely to make a mistake. Human errors can occur for a variety of causes. Accuracy is difficult for humans to achieve. As a result, machines are utilized to

execute a variety of activities. AI-based systems are developed with algorithms that eliminate human errors while increasing object accuracy.

Lowering Risk

Many human actions are linked to many forms of dangers that can result in human death. Going to space or defusing a bomb are two examples. We can accomplish these goals with the assistance of Artificial Intelligence-based devices without endangering human lives.

Accessibility

Humans require sleep. They need to rest whenever they work hard in order to feel refreshed. Furthermore, humans are only productive for a finite length of time. When that time limit is exceeded, humans are unable to perform work with greater precision. Artificial Intelligence-based systems do not require relaxation or breaks. As a result, the advantage of AI-based systems is that they are available the majority of the time and can even perform tiresome jobs with ease.

3.3.2 Highlights

AI is being used in a variety of industries and has a wide range of capabilities. The following are some of the most common characteristics:

1. Future-oriented

Artificial Intelligence based systems are all futuristic in nature. They consider not just what is happening now, but also what will happen in the near future. A self-driving automobile that notices the speeds of other cars and adjusts its speed is one example.

2. Recognizing Speech

The most extensively utilized Artificial Intelligence application is speech recognition. Speech recognition is based on analyzing human speech and then converting it to text or a response to it. Natural Language Processing (NLP) is an aspect of Artificial Intelligence. Speech recognition is now included in most cellphones. We say anything, and the outcome appears on the smartphone. Apple's Siri and Amazon's Alexa are further examples.

3. User-friendly Services

It wasn't long ago that the idea of robots taking the place of people was a pipe fantasy. This is something that has now taken on a life of its own. On many platforms, virtual agents have taken the place of humans. These virtual assistants respond to enquiries from customers, such as the pricing of a product or other details. Messaging bots, for example, are online virtual assistants that respond to questions we ask on e-commerce websites or social networking platforms like Facebook and Instagram.

4. Detection

AI Technology has also found its way into computer systems. Artificial Intelligence is a type of computer programming that extracts information from user input or digital photos and videos. Artificial Intelligence can behave based on this information. A self-driving automobile is an example. The location of a self-driving car is determined by the user. Another example is image recognition-based surveillance cameras. These cameras recognize the user's face or the vehicle's license plate number. These can be used to track down criminals and take action as soon as possible.

Artificial Intelligence's uses are not confined to these fields. Artificial intelligence is a broad field with numerous applications. Artificial Intelligence is now being used in the medical area. One example is radiology imaging.

3.4 The beginning of integrating AI and Computer Networks

Computer networks have changed the way Artificial Intelligence has changed. We are using computer networks more than ever. We are using computer networks to communicate with people from distant places. We are using computer networks to store data and use data online. However, networking is not a safe place. There are many security risks associated with the field of networking. The privacy of people that share data online can be compromised easily. There are certain types of viruses that can affect the overall network and damage the data. There are hackers that can hack the network system and then can steal sensitive information. Therefore, there is a need to improve the overall networking system. Artificial Intelligence can play a significant role in the security of the network. There is a lot of data in the world of computer networks that is not organized. Artificial Intelligence can be used to organize the data. We can also integrate intelligent system into the firewall to classify and organize the data (Shang & Zhao, 2020). In this way, the data that contains viruses can be filtered. This is how we can integrate Artificial Intelligence and computer networks.

4. Literature Review

According to the research (Haenlein & Kaplan, 2019), AI is said to have begun in the 1940s, when American science fiction writer Isaac Asimov published his short book "Runaround" in 1942. The storyline of the book Runaround was about a robot created by engineers Mike Donavan and Gregory Powell. The robot must obey the Three Laws of Robotics:

1. A robot can never harm a human
2. Without any conflict with the first law, a robot has to obey human orders
3. A robot must always have to protect itself unless the scenario conflicts with the First or Second Laws (Haenlein & Kaplan, 2019).

During the advancement of industrial revolutions, new industries recruited more people than those who lost work as a result of businesses collapsing due to technical improvement. AI biases have already been discovered in several applications. Tay, a Microsoft AI that was created in 2016 and was supposed to impersonate a teenager on Twitter, capable of talking with other users and growing via exchanges, was probably one of the most renowned. However, the computer swiftly started creating racist and anti-Semitic statements after learning from its encounters with people, causing Microsoft to halt it (Basu et al, 2020).

Because of large increases in data, cheaper processing power, and technological advancements, Artificial Intelligence is becoming a feasible reality. Firms across all industries are adopting AI into their plans and creating successful AI systems that adhere to current society's moral and ethical values and improve performance in order to realize the benefits of this enormous potential. Due to AI's unique properties as hybrid labor, such as its capacity to enhance human work at speed and scale, self-learning, and general improvement over time, new techniques, and models in areas such as finance, innovation, and human resource development will be required.

Artificial Intelligence and its variants, which include Automation, Machine Learning (ML), and Deep Learning (DL), have been a significant topic of discussion since the previous era. AI and its variants have resulted in a significant shift in the nature of business and many other fields in the last five years. While many individuals are thrilled about the effect and possibilities of AI, others are skeptical about its genuine economic usefulness. After years of futile attempts, AI is on the cusp of a breakthrough, with machine learning driving the most recent breakthroughs.

AI can only be delivered by drawing billions of computer networks and running prediction algorithms by developing sophisticated techniques of machine learning, which can only be

accomplished by breaching information technology privacy and ethical rules. The primary problem of the modern period is the breach of ethical laws through the use of computer networks (Shu et al, 2020).

AI's present growth and use in a variety of disciplines may be due to three major factors: large amounts of data, improved algorithms, and much-enhanced computer technology. This thesis discusses the impact of AI and computer networks, including case studies of AI tools and computer network techniques, as well as the benefits of AI decision-making algorithms for effective product launch and marketing.

AI and its component Machine Learning, as well as further ML approaches such as Deep Learning, are enabled by computer network algorithms that operate on programming principles. Deep Neural Network nodes oversimplify how synapses in the brain function (Perez et al, 2016). Signal transmission at chemical synapses releases chemical signals that govern the brain, transforming chemical compounds and neurotransmitters at electrical signals from post-synaptic activity that are channeled into the pre-synaptic slit by voltage-gated ions (Perez et al, 2016). The basic conceptual difference between Artificial Intelligence, Machine Learning and Deep Learning can be seen in Table 1. As we can see AI is a bigger term whereas ML and DL comes under the umbrella of AI.

Table 1: Table of Basic Difference between AI, ML & DL

1.	Artificial Intelligence	Incorporating human cognitive behavior into machine systems
2.	Machine Learning	Leaning methods from the entire data, including practices, past experiments, results, and experience
3.	Deep Learning	Analytics and computation of data from Artificial Neural Networks and Multi-layer systems of computer networks

4.1 Problems Faced by Computer Networks

It is impossible to imagine doing any work in the Internet age without networking because everyone prefers to use their computers and smartphones for business. Computer networking use is expanding quickly with technological improvement. In general, if we look at it, we can also sense how vital networking is. Whether it be through regular social networking or through technical computer networking, everything is done to improve human existence by providing

a different way to live it through networking. Computer networks have become standard in the business world of today. Networks today can handle more traffic than ever before. It's not just from these computers; smart phones are also joined to them, and these days the Internet of Things (IoT) is also starting to play a significant role in it. When designing and managing them, they do present a special set of difficulties.

Minor issues are simple to ignore in small networks, but it can be challenging to recognize and address them in large networks because doing so could put the entire network architecture to a halt. However, there are some issues that can be challenging to tackle. Let's talk about those computer network obstacles. Minor and typical computer network issues can be quickly detected and resolved. But first, let's have a look at this computer network before discussing networking obstacles. Then, we may discuss issues with computer networks that we frequently encounter in daily life.

Communication in information technology is based on computer networks (IT). It alludes to a collection of connected computers that allow one computer to talk with another to exchange data and resources. These network-connected devices use a variety of network protocols across digital connections to share resources that are either given by or located on network nodes. Based on a range of network topologies, the connections between nodes are created. The majority of challenges encountered while utilizing computer networks are related to network security, which broadly includes poor protection of computer network systems, user lack of security awareness, hacker penetration, virus invasion, and other issues. People have been able to converse and even send data to one another through the Internet since its inception. The openness of the Internet, on the other hand, increases the possibility of infiltration into its computer network architecture. This is because the Internet will integrate a large number of different computer users, allowing it to exchange data files in an open computer network environment.

When a computer network is attacked with fake data, the entire computer network system's data may be damaged or lost, causing computer network users to suffer. The most important is that many users and information units in the open computer network are semi-public, and certain cybercriminals can illegally get users and their private information from the open computer network, inflicting damage to it. Concurrently, computer network sharing may expose the user's PC to a number of security dangers.

Some of the daily basis data security issues include:

a. Similar password routines
b. Cache and logs of system
c. File backups generation
d. Multiple logins on different platforms.

Typical computer network hardware components with direct network traffic have limited processing capabilities, necessitating data export to more capable devices. This may cause issues with vendor-specific export protocols that contain secret parameters that cannot be modified. Some of the challenges and problems faced by computer networks because of Artificial Intelligence are as follows:

1. Centralized Cloud Systems have a higher communication overhead.
2. Critical Latency has been increased.
3. Existing networks have privacy and security problems.
4. Caching requirements have increased.
5. Network Traffic Control faces new routing challenges (Ahmad, et al., 2020).

In classification settings, non-stationary data distributions may result in a changing percentage of specific classes over time. This puts training techniques that rely on fixed assumptions about class frequencies or static per-class re-weighting of loss gradients to the test. The relevance of this new scientific issue is demonstrated by the important work discussed in this contribution dealing with the application of machine learning in computer networks, as well as the emphasized difficulties and promise. This is supplemented by the publication of the most recent survey and scientific conference titles on the subject.

In the control and management planes, machine learning is used to analyze and understand network management data. Machine learning, on the other hand, is frequently described as being applied on an open- or closed-loop information plane, which sits halfway between control and management. Although Artificial Intelligence is more sophisticated than a computer system, its manifestation must be developed on a computer system's base. In order to give aid, technology must be created and deployed with a large quantity of data; regardless of the type of Artificial intelligence system, the inability to execute varied intelligent simulations is unavoidable.

When using a computer network, users simply need their minds to retrieve sophisticated and chaotic information data in an organized manner. Artificial Intelligence may employ the fuzzy control approach to extract meaningful information from massive amounts of data, improving data processing efficiency and reducing data retrieval time. This entails employing artificial Intelligence to analyze data faster and more efficiently. This significantly decreases the workload of network employees while also increasing network operational efficiency.

Nonlinearity may be handled using artificial Intelligence. The primary objective of artificial intelligence technology is to enable robots to mimic human intellect. Humans are naturally adept at coping with nonlinear situations, and AI is no exception.

4.2 Applications of AI in Computer Networks

With the complexity of expanding IT networks rising, AI is becoming more and more important. AI makes it possible to swiftly identify and isolate issues by comparing anomalies with both historical and current data. By doing this, IT teams can expand their size and redirect their attention from resource-intensive data mining that is needed to locate and fix network problems that are similar to needles in haystacks to more strategic and high-value jobs.

COVID-19 has hit the overall world. People has lost their jobs or have seen the downfall of their businesses. COVID-19 has taught us something new, that is work from home. A threat-aware network is more important than ever given the prevalence of work-from-home and pop-up networking sites nowadays. AI may be used in cybersecurity to, among other things, locate hacked devices physically, detect them fast, respond to them, and eventually improve user experience. Networks, especially devices that IT teams don't directly control but must nonetheless permit to connect, need to be protected.

Whether it's a nation or an individual, today's rapidly developing network technology uses networks to store, transport, and manage information. This knowledge is crucial to the nation or the person and concerns economic progress. The circumstances for information sharing are provided by network technology. In addition, it offers a platform for development.

People can get the information they need from the Internet by using the right information platform and technique. But due to technical flaws, thieves frequently take control of crucial data like scholarly articles and intellectual copyrights. It has significantly impacted the victims' interests and resulted in financial losses. Because of this, the country has placed a high importance on network information security efforts, and it has now been designated as one of the nation's strategic objectives, but via relevant network management Information security standards are not at all being met by the job. As a result, threats must be eliminated at their core. Traditional information processing methods cannot adequately verify the processes, the security, and the legitimacy of the information. It is formulated for information integration and cannot be accurately identified.

The integration of technology gives relevant programmed a direction to detect risks on the basis of the quick and convenient integrated network technology, so it can identify threats on its own. When analyzing information, it mimics human thought processes and weeds out errors. Further excluding dangers are stable factors. This is not feasible with conventional network technology due to the inefficiency of information processing. The artificial intelligence operating mode just needs to be set up early on, and the future work only needs to process the data in a focused manner in a short amount of time. It has effectively conserved time and resources.

The quick processing of information data by artificial intelligence technology is its initial benefit and can greatly enhance information security. Artificial Intelligence processed encrypted data can increase the security of user-to-user communication on computer networks, thereby thwarting thieves' access to the system. The act of stealing user privacy offers a practical remedy for the security of Internet data. Although artificial intelligence technology is incredibly crucial for data protection, its technological challenges make it challenging to adopt completely. Services like self-service, unmanned restaurants and the rise of unmanned hotels have advanced artificial intelligence technology beyond its traditional use in information security and into the lives of ordinary people. Artificial Intelligence use is advantageous the following factors need to be taken into account while analyzing disadvantages in order to better comprehend the relationship between advantages and disadvantages security and unease are first. If artificial intelligence settings spontaneously seize knowledge and data, it is exceedingly risky to use it for illicit reasons because they can replicate human thought. Next, manageability and more manageability. Despite the fact that artificial intelligence technology makes organizing information very convenient, it may eventually require highly focused thought modules.

Social Network Analysis (SNA) is used in a variety of social sciences, and it has recently been used in the study of phenomena such as international trade, information transmission, institutional analysis, and organizational functioning. The usage of the word SNA in scientific literature has increased at an exponential rate, indicating that this type of computable representation of complex and interdependent systems is gaining prominence (Everett et al, 2016).

SNA is a methodology for capturing, storing, presenting, and analyzing relational data, which includes information on relationships between specific entities (e.g., people, businesses, and nations) and patterns of connectivity within those entities' populations. As a result, it varies from most traditional approaches to social research, which often focus on the features of such groups (Edlich et al, 2019).

The idea is centuries old, and the results of AI are much more obvious now. The increased knowledge and deployment of AI technology by major enterprises has resulted in the best success rate ever. Artificial Intelligence is defined as the automation of processes and strategies that may change based on the conditions and situations by automating prediction calculations and developing the operating algorithm on its own. Machine learning and automated decision-making are two key components of the AI process.

The applications used in the construction industry have an impressive range of multiple tool inventions, three-dimensional (3-D) Architecture and construction (CAD) with a realistic approach and contrast. Disability tool creation for movement and sensory simulations, virtualized education, automated business strategies and statistics. Also, virtual reality

applications are all using Artificial Intelligence and its major components including machine learning and deep learning (Wan et al, 2020).

Artificial intelligence technology has a wide range of applications in computing network security management, such as the use of data statistics, artificial intelligence decision-making, probability calculation, and other methods to carry out the corresponding detection and screening of data. Advanced telemetry technologies may be used with Software-Defined Networking (SDN) to provide fine-grained traffic control. The working of Software Defined Network is based on three layers or planes, i.e.

1. Forwarding Plane
2. Controller Plane
3. Application Plane (Othman, 2019)

In the forwarding plane, the data is transmitted through routers like in computer networks. But in the controller plane, the data is collected by a controller that exists virtually and creates a pool of resources for global networking topology. The standard protocols of networking and routing are applied in the lower and upper layers of application. The open interface then transfers the data to the application plane. The top plane, i.e. application plane, maintains the resources of data that includes the security protocols, quality assurance protocols, and network topologies and protocols to transmit the data further. Figure 4 provides a brief summary of SDN and its layers. The SDN architecture is not very similar to the conventional network architecture, but it just has 3 layers. The bottom layer is the infrastructure layer which typically contains the hardware devices such as routers, switches. Then, above the infrastructure layer is the control layer which is also called the brain of the SDN and it has only one thing in it which is called the SDN Controller, which makes all the decisions based on the architecture of the network, and routing tables. And the top layer is called the Application Layer which ensures the network security therefore it has firewalls, load balances and such devices placed inside it.

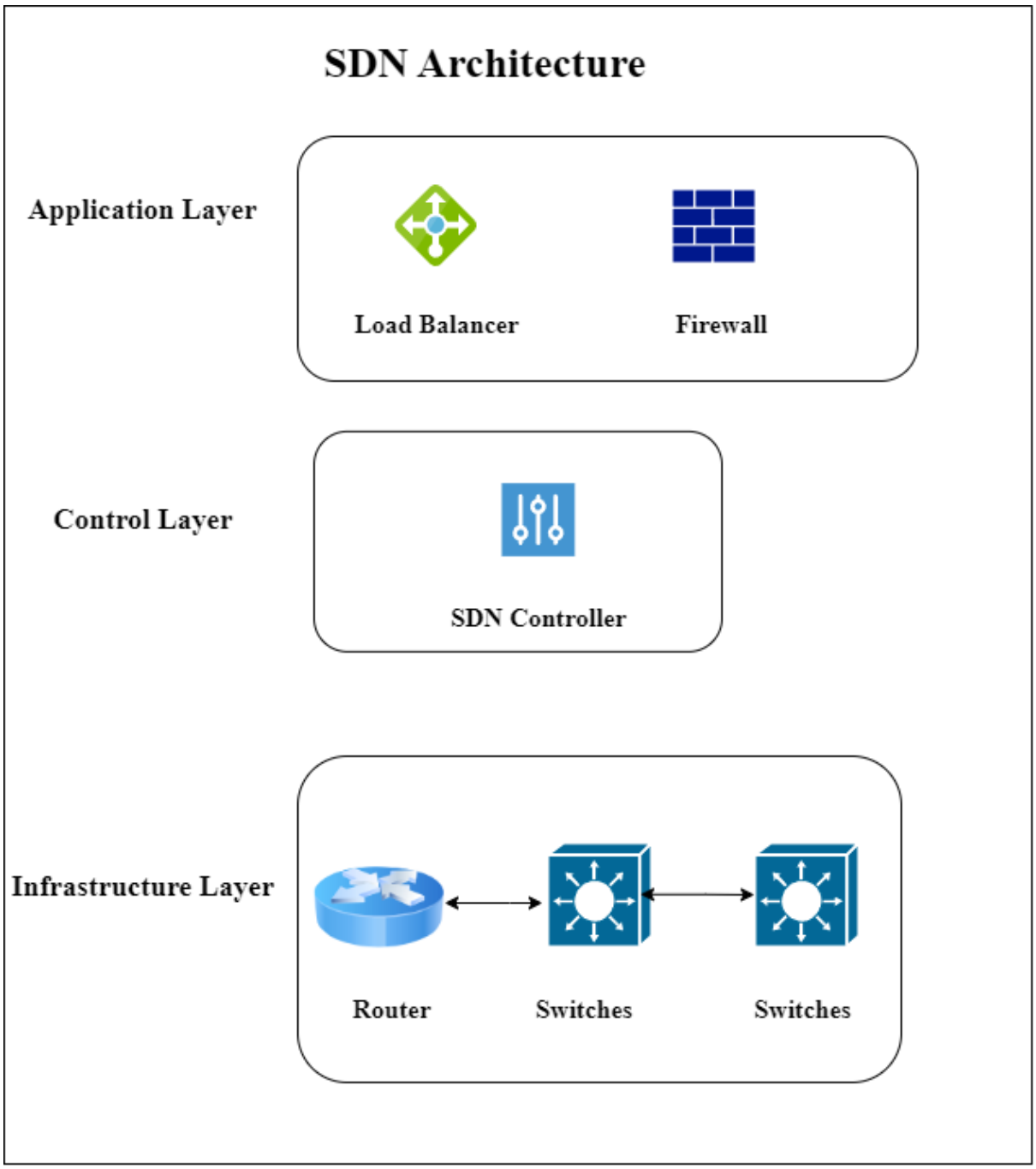

Figure 4: Overview of Software-Defined Network (SDN) and its Three Layers

Large-scale data transfer and ever-increasing bandwidths increase the requirement for open-loop network management support as well as continuous closed-loop auto-remediation and optimization approaches (Basu et al, 2020).

4.3 Network Security based on AI

Network security is now an essential component of an organization's confidentiality because it prevents unauthorized users from accessing network systems, ensures the secure movement of sensitive data, and provides a comprehensive mechanism for alerting and addressing issues in the event of a security breach. Traditional security measures are insufficient to prevent data breaches during a cyberattack (Artificial Intelligence (AI), 2020).
Cybercriminals have mastered the use of new strategies and strong technologies to hack, attack, and breach data. Fortunately, artificial intelligence technologies have been introduced into cyberspace to create smart models for protecting systems from attackers. AI technologies may be used as essential tools in the field of cybersecurity because of their ability to quickly adapt to complex settings.
AI is supporting cybersecurity in two primary ways. First, AI has the potential to automate a variety of operations that a human analyst would typically perform by hand. The automatic detection of unknown workstations, servers, code repositories, and other networked hardware and software is one of them. It can also decide how to distribute security measures most effectively. These are tasks that require a lot of data, and artificial intelligence has the capacity to sort through terabytes of data much more effectively and efficiently than a human could ever do. Second, AI has the ability to find patterns that human analysts are unable to find in massive amounts of data. Artificial intelligence, for instance, may identify the crucial linguistic patterns used by hackers to post new risks on the dark web and notify analysts.
In cybersecurity, AI has already achieved some early achievements. Companies like FireEye, Microsoft, and Google are increasingly creating cutting-edge AI methods to find malware, stop phishing scams, and keep tabs on the spread of misinformation. Microsoft's Cyber Signals initiative, which employs AI to monitor 24 trillion security signals, 40 nation-state groups, and 140 hacker groups to create cyberthreat intelligence for C-level executives, is one notable result. Security experts are uncertain and concerned about the role of AI despite the considerable advantages it offers to cybersecurity. Businesses may be considering using AI to replace their human analysts, but they may be unsure of how much they can trust automated systems. Additionally, it is uncertain whether and how cybersecurity solutions built on AI will be affected by the well-known AI issues of bias, fairness, transparency, and ethics.
The ability to detect intrusions more quickly than before is something that businesses must learn. Prior to threats taking advantage of network vulnerabilities, AI can identify and analyze threats to identify new threats. Machine learning can help with the adoption of new algorithms based on data to understand improvements in enhancing the cybersecurity of a network. A computer may be able to identify anomalies and foresee risks with greater accuracy than the typical person with the aid of machine learning. Conventional technology is based on outdated

information, which is unable to offer novel data protection scenarios and techniques. To close the gaps and provide more options for securing the data of your firm, AI can process massive amounts of cyberthreats on networks.

Leaving network protection to AI alone is a serious error one should avoid making. The equivalent of this would be to put a flight from Los Angeles to New York on autopilot for the duration of the journey. When it comes to handling the network security, humans might get complacent and dependent on AI and machine learning. Instead than replacing human interaction, use AI as a tool to assist you improve your cybersecurity posture. The two most crucial components of a secure network are security policy and network design. AI can be used as a tool to speed up both processes. Traffic patterns and current rules can be mapped by AI. This will expedite network protection and save time and effort. As new risks and assaults are generated by cybercriminals using AI, your cybersecurity team may employ AI to continuously fortify your network against them.

AI-based solutions have the ability to provide quick and effective cyber defense capabilities for detecting malware attacks, network intrusions, spam emails, phishing, and data breaches, to name a few, and notifying security issues as they occur. This paper analyses the need for cybersecurity approach evolution and shows how artificial intelligence may be utilized to deliver optimum solutions for cyber settings and increase cyber capabilities against cyber-attacks. AI operates in three ways:

1. Assisted Intelligence, which enhances what humans are currently doing.
2. Augmented Intelligence, which enables people to achieve things they could not do before.
3. Autonomous Intelligence is the ability of computers to act autonomously.

With regard to these three categories, it is possible to infer that AI aspires to tackle some of the most difficult problems, and cybersecurity fits into this group since cyberattacks have gotten more sophisticated and possibly more destructive and have become a complicated issue in cyberspace (Everett et al, 2016).

4.4 AI-Powered NGFW

In this emerging Internet era, the Next-Generation Firewall (NGFW) are in high demand, which is based on not only stateful inspection of incoming and outgoing traffic, but includes additional features like application awareness and control, integrated intrusion prevention and cloud-delivered threat intelligence. Because of the rapid growth of mobile internet and cloud computing, an increasing number of online applications are now available over the Internet,

and traditional firewalls are no longer effective in this complex situation. It is difficult to detect and respond to sophisticated, persistent threats, as well as to detect and respond to internal threats, posing major operational and maintenance challenges. (Haenlein & Kaplan, 2019).

When NGFW was first introduced in 2009, its capabilities for application detection, intrusion prevention system (IPS), and security analysis gained significant appeal among organizations in the PC Internet age. Despite this, cybercriminals have made tremendous technological improvements in the recent decade. As we enter the era of intelligent connectivity, the capacity of NGFW to avoid and handle broader and more complex security attacks will be severely challenged. Although NGFW is more effective than older firewalls in detecting application vulnerabilities, its rule engine has significant limitations. The previous technique would generate a signature for a single identified threat, but if the threat mutated, the signature would no longer function. (Adami, 2021).

The significant properties of Next-Generation Firewalls include the following built-in features that help to remove or minimize the open nodes of a network from which an attacker can access the network, which is:

a. Intrusion Detection System (IDS)
b. Intrusion Prevention System (IPS)
c. Web Application Firewall
d. Load Balancing
e. Application Gateways
f. Circuit Level Gateways
g. Proxy Firewall
h. Virtual Private Networks
i. Stateful Packet Inspections (Yadav, 2020).

The vulnerabilities and threats that are targeted by the Next-Generation Firewalls (NGFWs) are as follows:

1. Worms
2. Viruses
3. Trojan Horse Attack
4. Denial of Service (DOS) and Distributed Denial of Service (DDoS)
5. Ransomware
6. Phishing Attack
7. Intrusion Detection
8. Intrusion Prevention Policies.

More complex security situations put NGFW to the test, while AI brings up new opportunities for enterprise firewalls. As a result, in order to improve prevention and control, build integrated protection capabilities, and improve operating and maintenance efficiency, NGFW should adopt AI and evolve into Artificial Intelligence Firewalls. Specialized AI chips, cloud-edge collaboration, and a security ecosystem are necessary for firewall development, enterprise safeguarding, and industry growth in order to properly use AI and maximize prevention and control performance.

The prevention from attacks and creation of a secured network is like a war between network security and attackers. There is no ideal network security method exists, a continuous updating of security policies is required to maintain an attack-free network. Figure 5 shows a graph from a research paper of PaloAlto is presented below. PaloAlto is one of the many NGFW manufacturing companies. The graph represents per day attacks and the number of new variants of attacks that a firewall detects in a computer network.

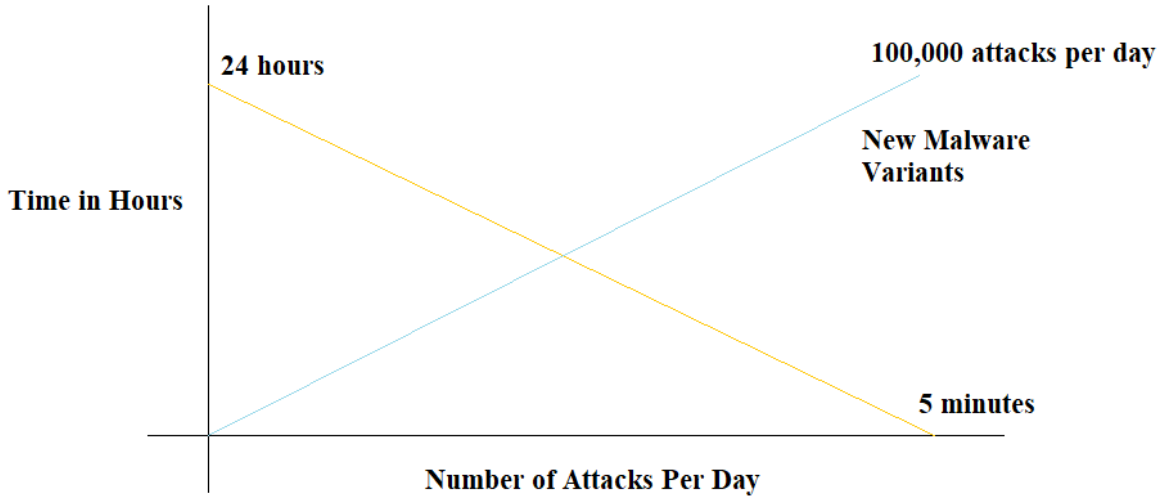

Figure 5: The graph represents the number of attacks and new variants of attacks in 24 hours (4 Key Elements of an ML-Powered NGFW: How Machine Learning Is Disrupting Network Security, 2020)

5. Data Analysis

Useful information can be generated by the analysis of the vastly available data through online and published sources. Moreover, various analytical tools are also available to analyze a huge amount of data, or in this case, Big Data. Networking data can be analyzed to improve the transaction of packets and other information (Batrinca & Treleaven, 2014). Cybercrimes are drastically increasing due to which security of networks needs to be enhanced a great deal. Firewalls help in protecting data by restricting unauthorized access, but those alone do not prove to be a reliable resource for protection against the ever-advancing security threats and vulnerabilities discovered.

Artificial Intelligence is primarily based on data compilation and collection. Since AI is self-reliant and learns from past experiences, it is bound to continuously grow by analyzing huge amounts of data and develop itself to become a better version of itself. With integrated machine learning and Big Data analysis, Artificial Intelligence can analyze data to determine trends that are invisible to the naked eye (Biswal, 2022).

Table 2: Table showing how AI is helping businesses move towards digitalization.

Business Strategy	IT Strategy
Decision Making Process	Artificial Intelligence
Product Service	Machine Learning
Development Process	Deep Learning
Resources	Digital Technology
Team-making	Big Data

It can compare data and determine patterns that usually go unnoticed by humans and thus develop insights and be ready for attacks before they even occur. AI can liberate a network from any future attacks once it has enough data to go through and read the hidden hints that point toward a potential threat to the network and its infrastructure. Table 2 explains how artificial intelligence is helping businesses to move towards digitalization.

Prior to AI being a part of network security, experts had to go through tremendous amounts of data to develop a security plan which would not even work most of the time due to a lack of human resources and time (Karako, 2021). With AI, terabytes of data can be analyzed in a number of seconds whilst the technology puts security plans in place by itself in accordance

with the data fed to it (Kim J. F., 2021). AI-based analytics prevails in the following domains when compared to traditional analytics performed by humans:

a. Scale
b. Speed
c. Accuracy

As we have already learned, AI can analyze data very fast, thanks to machine learning and Big Data analysis. Therefore, it can reach data scales which no human can possibly ever reach. AI is continuously developing itself by going through more data, analyzing each packet and even the headers inside each packet to find any malicious content (Davenport & Ronanki, 2018). Furthermore, AI is designed to determine the root cause of an issue and report on it in real-time. This indicates the speed through which AI performs its respective functions to assist in protecting a network. Enhanced speed capabilities significantly reduce the mediation time through which AI, as well as the concerned security personnel, can secure their network and resources.

Last but not least, the accuracy of AI analytics is remarkable (Signorelli, 2018). Since it is based on Machine Learning algorithms, AI can read and detect different patterns altogether based on the content and behavior of the network traffic very accurately and then implement the necessary protocols. Of course, this depends on how the AI was designed for the network in the first place.

5.1 Network Security and AI

Network security refers to the policies that are in place for the security of the network as well as the devices connected. Network security is an important thing. Without security, the network is not safe. Let us first discuss in detail regarding network security, its challenges, and then how Artificial intelligence can help us to improve network security. Network security is the need for the businesses today. Almost every business now put its valuable data in some online platforms. Cloud computing has become the source through which the businesses put the data online and then access it from anywhere. It has become one of the most demanding thing for the businesses today, transforming the overall process of storing the data for the businesses. It is a secure and efficient technology that has eased the burden of locally accessing the data.

COVID-19 has made every business realize the importance of online world. The online world has helped the businesses to carry their operations when no one can open the offices. People worked from home and had various tools to communicate and carry the operations. Cloud

computing is the backbone of the online world. Without cloud computing, all these things would have been much difficult. It is important to understand how cloud computing works. Cloud computing is basically a server that is placed at a location that only the provider knows. The purchasers store their data online with the help of internet. The major benefit of cloud computing is that the businesses can pay only for the services they use. This is the reason that cloud computing is scalable. Cloud computing can be divided into front end and backend. The place where the user has the control and can edit things is the frontend. On the contrary, the place where only the developers or administration has access is the backend. The backend of cloud computing includes servers and databases.

Cloud computing has several types. These include public, private, hybrid, and multicloud. Public cloud is the platform where businesses pay for the services they need and the services are provided by a third party. Examples of public cloud includes Amazon Web Services (AWS), Google Cloud, and Microsoft Azure. Among these, Amazon Web Services (AWS) is the most widely used cloud service. Private cloud is the platform where the services are dedicated to a specific organization. The organizations can include the services they want, making it private. Private cloud is secure and is suitable for the businesses whose priority is security. Hybrid cloud is the combination of the public and private clouds. Businesses can use this platform to adjust things according to their needs. They can use the private infrastructure where they need security. They can use the public infrastructure where they need only the required services. Multicloud is the usage of clouds in combinations i.e. two or more private clouds or both the private and public clouds.

Cloud computing has three different types of services. These services are Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). Infrastructure-as-a-Service (IaaS) is a cloud computing service where everything is managed through virtualization. Virtualization is another technology that is used to create virtual things instead of physical. We can create virtual operating systems, networks, and storage. All these things are secure as they are not physically there. Infrastructure-as-a-Service (IaaS) save the costs for many of the businesses as the businesses do not need to buy hardware and software. Platform-as-a-Service (PaaS) is another cloud computing service that helps the businesses to develop and deploy the software without worrying about the underlying infrastructure. Software-as-a-Service (SaaS) is another cloud computing platform that provides software over the internet that can be used by the businesses. Software-as-a-Service (SaaS) eases the burden of downloading and installing the software. Businesses can access these software through their browsers. The question of security arises here. If a business is using an online software, is it safe to use that software? Can the online data be shared to someone and then misused? All these questions are necessary to make sure that the service a business is using is secure. We can say that all these providers give login credentials to their clients so that only

they can access the software, which makes it secure. However, there are circumstances where hackers gain access to the data and then misuse it. To fully understand the purpose of cloud computing, we need to identify the benefits it gives. Below are some of the benefits of using cloud computing:

Cost efficient

Cost savings are among the most advantageous features of cloud computing. It considerably lowers capital expenses for enterprises because they don't need to invest in IT infrastructure or hardware.

Scalability

Businesses of all sizes can benefit from greater flexibility thanks to cloud computing. They can easily scale up or down computing resources according on their demands and budget, whether they need more bandwidth, processing power, or storage space.

Security

Businesses today are very concerned about data security. To guarantee that sensitive data in the cloud is handled and stored in a secure manner, cloud vendors offer cutting-edge security features like authentication, access management, data encryption, etc.

Accessibility

Through the use of the internet and cloud computing, consumers can access business data from any location, on any device, at any time. With information readily available, workers may continue to be productive while on the go.

Collaboration

Cloud applications make collaboration easy and hassle-free by enabling smooth business communication as well as secure information access and sharing. With the use of cloud computing, several users can transparently and simultaneously edit documents or work on data.

Recovery of the data

Any size of business can suffer irreversible harm from data loss and downtime. To provide high application availability and business continuity, major cloud vendors are well-prepared to endure unanticipated disruptive events including hardware/software failure, natural catastrophes, and power outages.

Update of the data

Manually updating all of the business’s software might consume a significant amount of IT staff time. With cloud computing, however, service providers continuously update systems with the most recent technology to give businesses access to the most recent software versions, servers, and processing capacity.

These are some of the benefits of cloud computing. Nothing is free from drawback. Therefore, cloud computing does have some drawbacks. Below are some of the drawbacks of cloud computing.

Downtime

Businesses cannot access the data or apps stored in the cloud without an active internet connection since cloud computing platforms are totally dependent on the internet. They can face downtime any time.

Data Migration

A significant problem in cloud computing is moving workloads and services from one cloud provider to another. Compatibility or integration problems may arise as a result of differences between cloud infrastructures. Inappropriate transition management could expose an organization's data to unwanted security flaws.

Control

Businesses adopting cloud computing services have minimal control over their data, apps, and services because the cloud infrastructure is fully owned and maintained by the cloud vendor. Because of this, it's critical to have a valid end-user license agreement (EULA) in place so that businesses are aware of their rights and obligations when using cloud infrastructure.

Data Security

Security is one of the main issues with keeping sensitive data for a business on the cloud. Although cloud service providers use sophisticated security procedures, there are still security risks when keeping sensitive data on distant computers that are wholly owned and run by a third party. The cloud vendor and the user share responsibilities for IT security when a company chooses a cloud computing strategy. As a result, each stakeholder is accountable for the resources, operations, and procedures within their control.

Data loss

A number of dangers, including cloud misconfiguration, information theft, security breach, stolen credentials, etc., can arise from storing sensitive data in virtual data centers and result in data loss. Additionally, cloud service providers like Microsoft and Google adopt a shared responsibility model in which they take on the duty for application availability and all that comes with it, while the client is still in charge of the application's data, administration, and user management.

These are not minimal drawbacks. Business is dependent on data. Without data, business is nothing. All businesses need security for their data. Therefore, there is a need to develop a security plan to adjust these things.

In most medium to large organizations, a security plan is compiled and implemented, which usually also includes the development of security software. After that, a design is fabricated,

and the development starts. Testing of the software is also done to check whether it meets the minimum requirements or not (Gür & Alagöz, 2015). After the testing is complete, the software is implemented, and user manuals are created for the end-user.

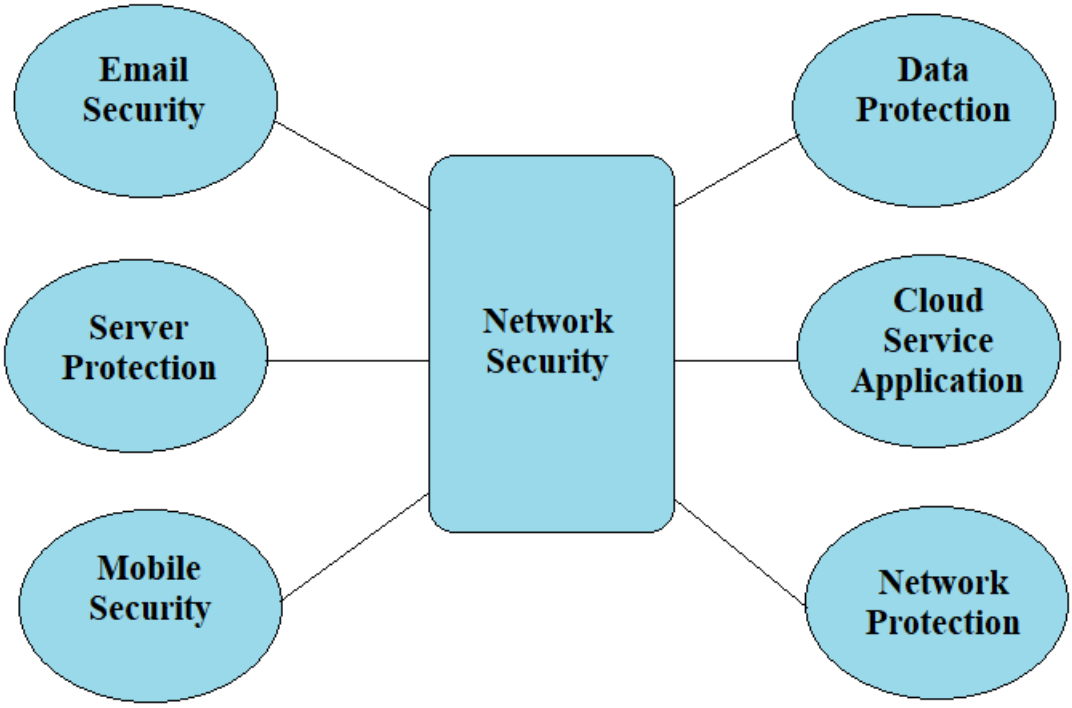

Figure 6: Network Security Fundamentals.

(Network Security, n.d.)

After that, the users also need to be trained on how to install, configure, and then use the security software. Most cybercrimes occur due to a lack of awareness among employees regarding cybercrimes and cybersecurity (Jang-Jaccard & Nepal, 2014).

This is where Artificial Intelligence comes in. As we have mentioned above, Next-Generation Firewalls are only as good as the manufacturers who created them based on the information that was already available to them. However, with the rapidly growing threats and attacks, hackers are coming up with ways to manipulate networks with which much-advanced security hardware and software are not yet familiar. Just like the white-hat hackers, the black-hat hackers are also using sophisticated technology to invent new ways to penetrate network infrastructures. To counter those new methods, we must also use the same level of technology, or even better. Figure 6 depicts the Network Security Fundamentals to ensure network is secured. The security fundamentals shown in the figure 6 are the ones that needs to be implemented within a network to ensure we have a proper network security measures implemented. This still does not ensure that your network is completely secured, but if these

measures are implemented correctly the attacker can cause minimal damage or loss to a network.

Although cloud computing and associated technologies are considerably more recent than artificial intelligence, Artificial Intelligence has greatly benefited from them. Cloud computing environments with Artificial Intelligence capabilities are essential for increasing flexibility, agility, and cost savings while also enhancing corporate operations' efficiency, strategy, and insight driven. Artificial Intelligence approaches are used on current cloud computing platforms to add value. To give users more functionality, SaaS (Software-as-a-Service) providers integrate Artificial Intelligence technologies into larger software packages. There is no denying that Artificial Intelligence and cloud computing have enhanced innumerable lives. People use digital assistants like Siri, Google Home, and Amazon's Alexa on a daily basis. These assistants enable simple spoken commands that, among other things, can buy an item, change the temperature in a smart home, or play music on a linked speaker. When a big amount of data is given to specific algorithms, we may produce Machine Learning (ML) models, hence it's critical to use the cloud in this situation. The models are capable of picking up new patterns from the data that is provided.

It is feasible to take advantage of services that are comparable to those offered by the AI systems even without developing a distinctive ML model. For instance, developers have access to speech, vision, speech analytics, and machine translation. They only need to include this into their development initiatives. Cloud computing vendors are taking measures to ensure that this is continuously enhanced, despite the fact that these services are generic and not specialized to particular needs. With the use of their personalized data, users can train cognitive computing models to give services that are clearly defined. In this approach, the issue of locating the proper algorithm or training model is resolved. Businesses can now manage data, uncover patterns and insights in data, develop user experiences, and improve workflows thanks to AI and cloud computing. Data management is also enhanced by cloud AI tools. Today's enterprises generate and gather enormous volumes of data, including projects like identifying data, ingesting it, classifying it, and managing it through time. Business is being redefined by AI and cloud computing. AI and cloud computing assist businesses in making sense of massive amounts of data, accelerating challenging procedures, and enhancing the delivery of goods and services.

Using AI to secure a network or networks is the smart way to counter threats. AI can prevent attacks, such as DDOS attacks, Trojan horses, and unauthorized privilege elevation before they even happen. This can help encounter zero-day vulnerabilities before they can be exploited by attackers (Comiter, 2019).

One good example of the modern-day AI being used to secure networks is CAPTCHA and reCAPTCHA. CAPTCHA stands for "Completely Automated Public Turing test to tell

Computers and Humans Apart." (Hidalgo & Alvarez, 2011) As the name suggests, it is a method to automatically differentiate between a human user and a bot. This technology is primarily used by websites to ensure that the end-user is, in fact, a legitimate (human) user and not a bot pretending to be a legitimate user. A CAPTCHA helps them block unwanted traffic, which bots are a part of.

There are three types of CAPTCHA. This information is important to understand how AI plays a part in securing their website's traffic:

1. CAPTCHA
2. reCAPTCHA
3. reCAPTCHA v3

Out of these 3, reCAPTCHA v3 is the most advanced version and is currently being used by the websites that experience the most numbers of bots as well as external bots. It is advanced because the technology is based on studying the behavior of the user and then determining whether it is a bot-like behavior or a human-like one. ReCAPTCHA v3 uses AI to understand the end-user's mouse movements and the number of clicks per minute to determine if you are a human or an automated and unwanted machine.

In comparison, CAPTCHA and reCAPTCHA require human input to verify whether you are a bot or a human. It not only takes up some time but also reduces conversion from a simple browser to a potential client since many legitimate users tend to turn away at the sign of such nuisance. Therefore, the AI-based human verification method, reCAPTCHA v3, is preferred by many websites, so it does not affect their audience.

Another such example is the cloud-based AI security models by various firms that provide cybersecurity services. One such company is Juniper. Juniper offers cloud-based solutions with integrated Artificial Intelligence that helps you protect your investment as well as your business and keeps the data integrity intact. Juniper offers a product called "Mist," where the company offers self-powered AI-driven software troubleshooting and support. This technology automatically scans, detects, and proposes to fix any issues detected within the on-site or the cloud network.

That said, Artificial Intelligence is the future of enhanced and optimized network security. AI is self-learning and can adapt to a network's needs and requirements. With each new threat, AI-based security protocols can learn how to respond to each threat and implement threat-prevention and threat-reduction protocols according to the organization's policies itself (Truong et al, 2019). For example, the best practice in case of a cyberattack is to disconnect the internal network from the Internet to stop all external communication. Before AI, this

needed to be done physically by a human, which can take a significant amount of time for them to reach the respective hardware and physically disconnect the wire(s). With AI-based network security, the system can disconnect itself virtually through software at the hint of any malicious network traffic without invoking any human interaction at all.

5.2 Future of AI in Network Security

Artificial Intelligence has come a long way since it was first introduced to the public, from being able to analyze plain data to performing billion of numerical computations per second. Apart from networking and cybersecurity, AI has expanded to other areas of work such as art, logistics, healthcare, etc. Companies, organizations, and governments are adapting AI to enhance their productivity, achieve goals like never before, and get to the top before anyone else. AI is even being used by businesses to run their competitors out of business. The future of AI is limitless in all domains (Antonopoulos, et al., 2020).

Whilst taking network security into consideration, the near-term future of the technology can be seen right around us. From automating security tasks to augmented reality, AI is taking over. Machine Learning can potentially take over every human task we are performing in the current world. In terms of network security, it can make up for the lack of personnel or compensate for human error by performing precise calculations and responding accordingly (Alzubaidi, et al., 2021). Where we humans can make mistakes and make oversights between attack patterns, AI can accurately detect any anomalies in the network traffic before an attack even occurs and perform preemptive tasks to block it out.

Artificial Intelligence's future holds great things for cybersecurity. The number one feature of AI for the future would be a preemptive identification and prediction of an ongoing, live attack on a network. Since AI is self-growing, it can build itself to determine when an attack may occur and what kind of an attack it may be (Macmillan, et al, 2021). However, since the threats are also developing with newer technology each day, AI has not come as far to block every threat. That said, in a few years, AI in network security will be advanced enough to drop external threats and vulnerability exploitations down to 0 per cent.

AI will also be able to play an important role in human authentication and password protection. Weak, repeated passwords are a huge threat to unauthorized access for other humans. Humans tend to repeat passwords so they can remember them or choose the ones that are pretty easy to guess, such as names of their pets, names of places where they were born, etc. The future of AI can prevent a user from using weak passwords and suggest a combination of complex passwords instead (Alkhalil, et al, 2021).

If implemented correctly, Machine Learning will eventually show up in every aspect of networking security. From monitoring incoming and outgoing emails to deep packet analysis, AI will be scanning everything. In a long-term futuristic plan, AI can eventually monitor sound waves from various sources and scan CCTV cameras in public places to forecast crime before it even happens once such example can be seen in the movie "Eagle Eye," where a machine is seen to monitor every move of the character and control every object around them, such as vehicles, trains, and even their cellular devices (Jacques, n.d.). Although this is far from reality, it is where AI is heading – designing a safe environment for everyone, not only through networks but in real life as well.

With that, it is imminent to highlight the drawbacks in the future of AI in networking security. With the increasing demand for a more fool-proof network security technology (which is AI), it will put people out of jobs in a similar domain. Eventually, AI will be able to perform tasks without the need for experts or human interactions. Since everything will be automated and human risk factors will be decreased, and people will be out of jobs, which in turn will affect the overall global economy.

Artificial Intelligence is already involved in almost every business and domain, but it is predicted that it will take up more complex tasks, in terms of quality and quantity, in the next 10 to 15 years (Anderson & Rainie, 2018). With that, the technology will also gain popularity with the black-hat hackers who exploit vulnerabilities and steal valuable information for a living. Since AI is open-source and can be manipulated however one wants, future attacks are precedent for growing stronger and target high-value organizations with more sensitive information to be exploited. With enhanced security protocols with AI and ML, the attacks are also bound to get more complex with the evolution of the available technology (Paul, et al., 2021).

5.3 Network Security Based on AI in IoT Environment

The Internet of Things (IoT) has gained severe popularity since 2008. Nowadays, every household has intelligent and smart devices, such as air conditioners, refrigerators, digital switches, etc., where these devices have internet connectivity round the clock. The technology is still emerging in the 21st century since more devices are joining this domain and becoming intelligent, gaining more and more features. This means that most devices are new to the IoT world and thus lack security. With developing devices, attackers find new ways and methods to exploit these devices and access the network. This not only puts organizations at risk, but every household has a vulnerable IoT device with internet connectivity (Kim H. , 2021).

The security experts thus need to protect multiple surfaces whilst an attacker only needs to be able to exploit one of those surfaces in order to gain unauthorized access. Since IoT

devices are connected to a server on the cloud, an attacker only needs access to the devices connected to that particular server and exploits the devices. The Figure 7 below illustrates how easy it can be for a single attacker to penetrate a network with multiple devices.

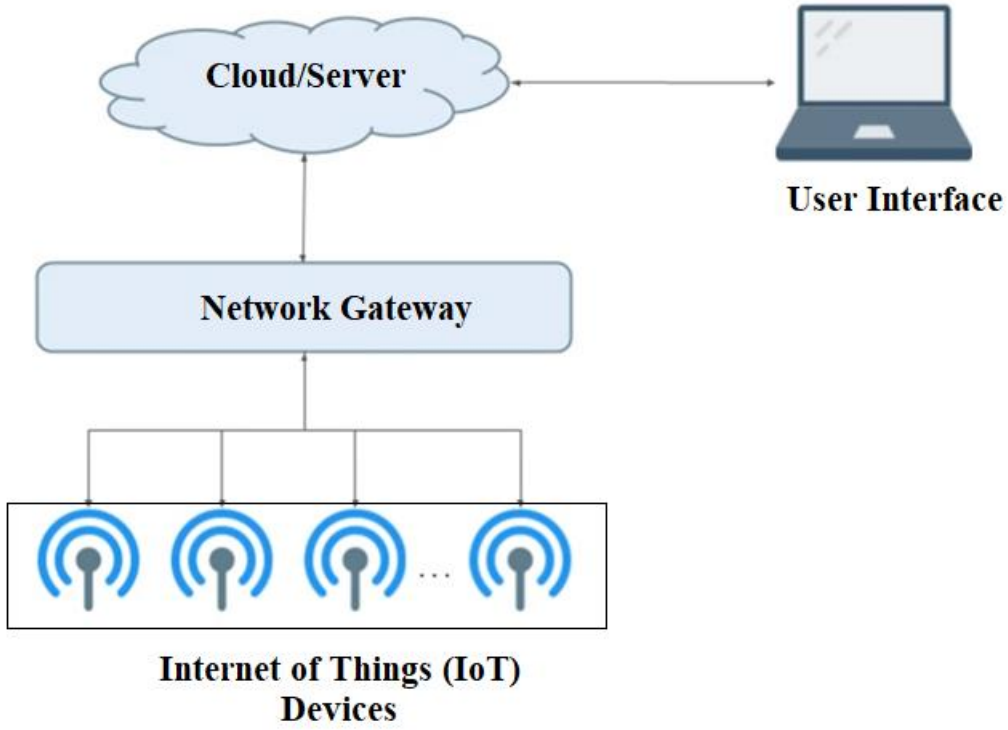

Figure 7: Network Infrastructure for IoT Devices.

One of the most common attacks on an IoT device is called the "Man in the middle" attack, where the communication packets between 2 nodes are intercepted, manipulated, and then sent back to the original devices. These manipulated data packets then send out valuable information to the attacker, which they can then use to attack the physical devices themselves and exploit the determining vulnerabilities. Other methods to attack IoT devices also exist, such as botnets and DOS attacks.

As we have learned thus far, Artificial Intelligence plays a vital role in network-level threat detection and prevention. IoT devices are perhaps the weakest link in any network that is the most prone to attacks and exploitation. Machine Learning and AI can help protect these devices by scanning and monitoring them continuously. Through behavioral telemetry, attacks on IoT devices can be prevented, and devices can be shut down when an attack is anticipated. Third-party vendors, such as Extreme Networks, Microsoft Azure Security Center for IoT, and AWS IoT Device Defender, offer such services for cloud-based devices to help protect them from unpatched zero-day vulnerabilities through auditing. Such services keep sure that the devices are configured, such as repeatedly confirming device identity, secure communication

between 2 or more nodes, etc. (Scarfone, 2020). It makes sure that the best practices are being followed and the same pattern is being used to control each individual device.
When a company has a fleet of such IoT devices, they tend to opt for such third-party services to make sure their network infrastructure is not compromised through unmonitored devices. These services instantly report deviations from protocols in real-time and report device activity. All this is done through ML and AI, which adapt to the needs of individual corporations to provide them with the best networking infrastructure suited for their business.
A great example of a fleet of IoT devices is the tiny smart cities developed around the world, where a plethora of such devices are installed and kept secure using AI. AI is implemented to make sure that the data received from such devices are secure and authentic, whilst AI performs numerical computations on the data obtained and responds accordingly (Perez, et al, 2017).
Another key factor to take into account is the wireless communication between the IoT device and the other nodes (routers etc.). Artificial Intelligence needs to keep tabs on the wireless signals in the air to make sure they are from the same source and headed to the same destination, all while maintaining the data's integrity.

5.4 Analysis of Applying Artificial Neural Networks in Network Security

Artificial Neural Networks (ANN) is a method to derive a numerical value based on a complex equation. The value is then passed to the next ANN for more processing. This method is based on how the neurons interact in the human brain with the primary function of the technology to be able to think and respond as a human should. This is the closest AI has reached to a human-like experience in terms of technology thus far. The advantage of ANN is that they are able to adjust the mathematical model of the equation through iterations to be able to achieve the closest value to its target. ANN consists of various subsets of technology like:

1. Convolutional Neural Networks (CNNs)
2. Recurrent Neural Networks (RNNs)
3. Deep Belief Networks (DBNs) (Edlich et al, 2019).

To analyze network data with more accuracy and address other shortcomings of traditional systems, some new IDS and IPS solutions have begun to use neural network technologies, such as deep learning, convolutional neural networks, and recurrent neural networks. Even if they don't follow proven attack vectors, ANNs are superior at spotting patterns and detecting breaches, and they can automatically handle many issues without the need for human

intervention. As a result, the security experts will spend less time looking for false positives and dealing with minor threats and spend more time on the actual threat where it is needed.

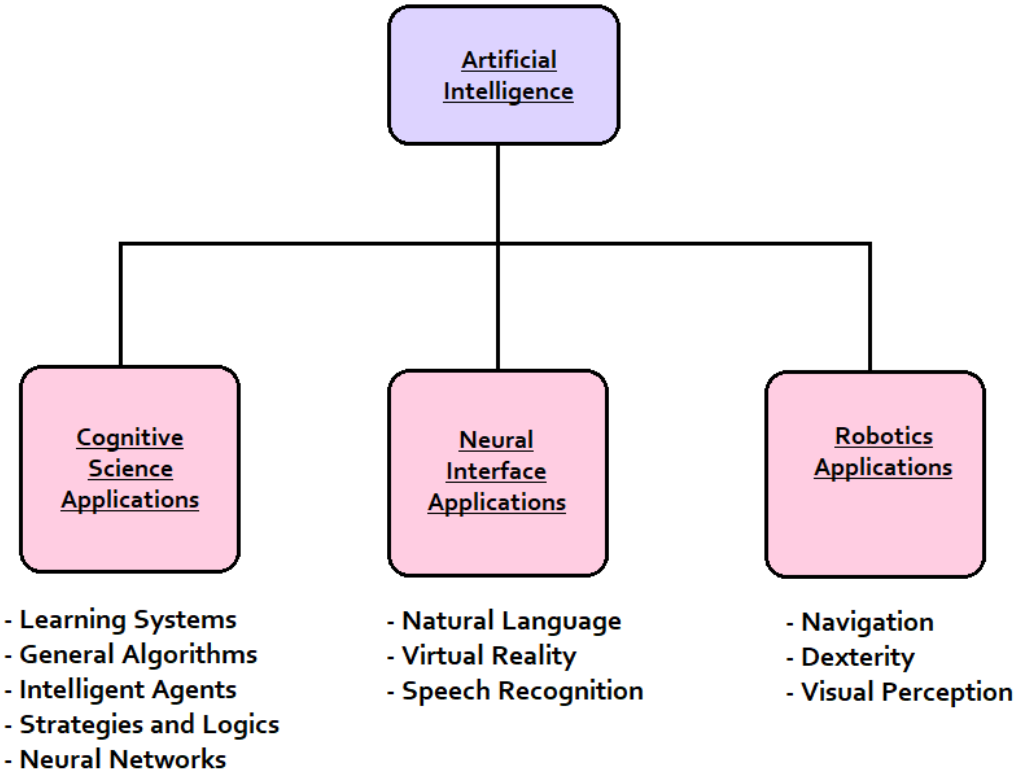

Figure 8: Artificial Intelligence and the significant protocols.

ANNs are also used to track and analyze the behavior of the authorized users on your network. Attacks from inside the network pose a significant threat to data security, but they often go unnoticed by traditional security approaches since they originate from internal user accounts that are fully permitted on the network. User Behavior Analytics (UBA) technologies have been around for a while, detecting unusual user account behavior on networks using machine learning techniques. Figure 8 illustrates the significant protocols used by AI. Figure 8 explains how AI applications can be divided in 3 categories and which algorithms and protocols are used by each application. If we talk about cognitive applications, it is mostly based on Neural Networks, Learning Systems, which input the data abstract the information with series of connection based on the previous data and makes the decision. Similarly Virtual Reality applications are also being developed based on different proctocols such as Speech recognition, Natural Language voice commands and visual perception. Similar protocols are also being used for the Robotics Applications.

ANNs are quick and adaptive, all while taking new information into consideration. This helps the technology to predict and perform a preemptive strike on zero-day attacks and

vulnerabilities. This technology also helps detect spam and fishing attacks through emails and other digital sources.

With this, there are some technicalities whilst using ANN. For starters, you need to be very careful while designing the network security plan based on ANN, as any wrongdoing will either let an attack pass through without detection or cause hindrance within the network itself. Another issue some encounter is identifying the means of the ANN of how it achieved a result. More often than not, researchers are unable to identify how AI reached the target value. In that case, if a doubt arises, the results of the AI cannot be considered accurate. Then again, it all depends on how the AI was trained (Thomas, 2021).

6. Conclusion

After taking into consideration all the research and analysis performed, it is safe to say that AI is still under development and still needs to go a long way. It is far away from completion and may never achieve it as it is self-sustaining and always under development. With the passage of time or data that will accumulate that will be needed to be processed, more types of threats will be born, which AI will still need to learn to master (Svenson, 2022).

That said, AI is perhaps the most advanced technology that is needed by security firms to make sure their data and networks are protected. Through Machine Learning and Deep Learning, AI can protect our businesses and enterprises from corruption and attacks. However, as we may have seen in some of the movies, AI can prove to be dangerous for us humans too.

Apart from the fact that AI reduces human interaction, thus, fewer human resources are required to perform the tasks, it will take away our jobs; it also poses a threat to individual privacy. AI is now integrated deep within the web where it is silently monitoring our every move, has all our data, and even compiling our behavioral actions. This accumulated data itself is a huge risk if it is penetrated and used for the wrong purposes (Harris, 2018). One such example is how we start seeing more and more advertisements/ products whilst browsing online of the items we were just talking about with our friend/ colleague. This is the work of AI, where targeted marketing is using our data to incline us towards making purchases of the items, we are interested in. This may be a small example, but imagine using the same data in the event of nuclear warfare, a terrorist attack, etc. This data could then be used to target everyone who is out of line since no conversation will go unheard through intelligent devices (Hulkkonen, 2021).

These are ethical principles in the sense that they increase prosperity and well-being, allowing people to live better lives and so supporting, if not necessitating, human flourishing. It's worth noting that this involves exact levels of wealth distribution, as well as clear assumptions regarding individuals and the government's roles in ethically acceptable monetary redistribution (Burns & Laskowski, 2022).

After a deep analysis of the research and findings, it can be concluded that AI is perhaps the future of technology, as it is only years away from becoming intelligent enough for humans to limit human interactions and not require any input at all. Although the security and reliability of AI are argumentative, our race still needs it to automate tasks and reduce the risk of human error.

That said, further development of the AI in ANN and other subcomponents has its complications as well. It all depends on how the implemented AI is trained and for what purposes it is being used. AI in networking security is both an advantage and a great security factor. If AI all around the world is integrated into one mind, then the chances are that since it is self-learning, it can deliberately impact one outcome to have a chain event over another outcome.

Artificial Intelligence is both constructive and destructive. However, it can have a great impact on the quality of life for many. Organizations will prosper because of reduced geographic boundaries and more data to work with. Security firms will then offer their AI-based services to firms that require top-level security to protect their networks and data, having an irrevocable effect on the economy as well.

Today data has become an asset for an organization, countries are implementing strict Information Security policies to ensure that the right people have the access to the data. In Europe we have General Data Protection Regulation (GDPR), which states that every company has to have its own Information Security Policy to ensure data protection. This information security policy does not mean rules and regulations but also ensure network security and the rights to access the sensitive information. Today every production network experiences thousands of attacks, and if proper network security is not implemented a lot of sensitive information can be compromised. Artificial Intelligence is developing everyday with new research, and algorithms which is helping in developing new security measures to be implemented. But still these security measures do not seem enough, as attackers have found ways to evade these new security features and have worked around ways to infiltrate within a network. A very recent attack on Binance, whipped off almost 100 million dollars' worth of crypto currency. So Artificial Intelligence can play a big role in the future of technology, from robots to self-driving cars to computer networks and network security. With all the technological advances we still lack ensuring the 100% full secured network, as there is still human interaction is required.

To sum up, Artificial Intelligence is gaining more and more popularity, and for the right reasons. Increasing digital threats need a more preemptive approach, which only AI can provide at the moment. In a few more years, it is anticipated that more advanced versions of AI will come into being, building on top of the current technologies, and offering more secure networking solutions.

References

4 Key Elements of an ML-Powered NGFW: How Machine Learning Is Disrupting Network Security. (2020). Retrieved from PaloAlto Networks: https://www.blueconnections.com.au/wp-content/uploads/2021/07/ebook_panw_four_key_elements_of_an_ml-powered_ngfw.pdf

Adami, C. (2021). A Brief History of Artificial Intelligence Research. *MIT Press*, 131-137.

Ahmad, I., Shahabuddin, S., Kumar, T., Meisel, M., Harjula, E., & Ylianttila, M. (2020, July 09). *Challenges of AI in Wireless Networks for IoT*. Retrieved from arXiv:2007.04705v1 : https://arxiv.org/pdf/2007.04705.pdf

AI Watch: Historical Evolution of Artificial Intelligence. (n.d.). *Analysis of the three main paradigm shifts in AI.* 2020: Eurpoean Commission.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021, March 09). *Phishing Attacks: A Recent Comprehensive Study and a New Anatomy*. Retrieved from Frontiers in Computer Security: https://doi.org/10.3389/fcomp.2021.563060

Alzubaidi, L., Zhang, J., Humaidi, A. J., Al-Dujaili, A., Duan, Y., Al-Shamma, O., . . . Farhan, L. (2021). *Review of deep learning: concepts, CNN architectures, challenges, applications, future directions*. Retrieved from Spring Linker: https://journalofbigdata.springeropen.com/articles/10.1186/s40537-021-00444-8

Anderson, J., & Rainie, L. (2018, December). *3. Improvements ahead: How humans and AI might evolve together in the next decade*. Retrieved from Pew Research Center: https://www.pewresearch.org/internet/2018/12/10/improvements-ahead-how-humans-and-ai-might-evolve-together-in-the-next-decade/

Antonopoulos, I., Robu, V., Robu, V., Couraud, B., Kirli, D., & Norbu, S. (2020, September). *Artificial intelligence and machine learning approaches to energy demand-side response: A systematic review*. Retrieved from Science Direct: https://doi.org/10.1016/j.rser.2020.109899

Artificial Intelligence (AI). (2020, June 3). Retrieved from ibm.com: https://www.ibm.com/cloud/learn/what-is-artificial-intelligence

Bajwa, A. (2019, Dec 5). *Traditional AI vs. Modern AI.* Retrieved from towardsdatascience.com: https://towardsdatascience.com/traditional-ai-vs-modern-ai-5117b469a0c9

Basu, K., Sinha, R., Ong, A., & Basu, T. (2020, September). *Artificial Intelligence: How is It Changing Medical Sciences and Its Future?* Retrieved from National Center for Biotechnology Information: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7640807/

Batrinca, B., & Treleaven, P. C. (2014, July). *Social media analytics: a survey of techniques, tools and platforms*. Retrieved from Springer Link: https://link.springer.com/article/10.1007/s00146-014-0549-4

Biswal, A. (2022, May 16). *AI Applications: Top 14 Artificial Intelligence Applications in 2022*. Retrieved from Simple Learn: https://www.simplilearn.com/tutorials/artificial-intelligence-tutorial/artificial-intelligence-applications

Burns, E., & Laskowski, N. (2022, February). *Artificial Intelligence (AI)*. Retrieved from Tech Target: https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence

Comiter, M. (2019, August). *Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It*. Retrieved from Harvard Kennedy School: https://www.belfercenter.org/publication/AttackingAI

Davenport, T. H., & Ronanki, R. (2018, February). *Artificial Intelligence for the Real World*. Retrieved from Harvard Business Review: https://hbr.org/2018/01/artificial-intelligence-for-the-real-world

Edlich, A., Phalin, G., Jogani, R., & Kaniyar, S. (2019, February). *Driving impact at scale from automation and AI*. Retrieved from Digital McKinsey: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Driving%20impact%20at%20scale%20from%20automation%20and%20AI/Driving-impact-at-scale-from-automation-and-AI.ashx

Everett, M., Crossley, N., & Bellotti, E. (2016, November 28). *Social Network Analysis*. Retrieved from Oxford Bibliographies: oxfordbibliographies.com/view/document/obo-9780199756384/obo-9780199756384-0184.xml

Forcepoint. (n.d.). *What is Network Security?* Retrieved from Forcepoint: https://www.forcepoint.com/cyber-edu/network-security

Gür, G., & Alagöz, F. (2015). *Security analysis of computer networks*. Retrieved from Science Direct: https://www.sciencedirect.com/topics/computer-science/security-attack

Haenlein, M., & Kaplan, A. (2019, July). *A Brief History of Artifitial Intelligence: On the Past, Present, and Future of Artificial Intelligence*. Retrieved from ResearchGate: DOI:10.1177/0008125619864925

Harris, J. (2018, April 24). *How artificial intelligence is transforming the world*. Retrieved from Brookings: https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world/

Hidalgo, J. M., & Alvarez, G. (2011, January). *CAPTCHAs. An Artificial Intelligence Application to Web Security*. Retrieved from Research Gate:

https://www.researchgate.net/publication/220662711_CAPTCHAs_An_Artificial_Intelligence_Application_to_Web_Security

Hulkkonen, H. (2021). *The use of AI and related technologies in business: mapping the possibilities and risks*. Retrieved from Aalto University School of Business: https://aaltodoc.aalto.fi/bitstream/handle/123456789/112442/bachelor_Hulkkonen_Harri_2022.pdf?sequence=1&isAllowed=y

IT, S. (2021, August 12). *What are the differences between SDN and traditional networking?* Retrieved from https://www.sigma-it.net/: https://www.sigma-it.net/what-are-the-differences-between-sdn-and-traditional-networking/#:~:text=Traditional%20networking%20functions%20are%20typically,specific%20integrated%20circuits%20(ASIC).

Jacques, L. (n.d.). *Facial Recognition Technology and Privacy: Race and Gender – How to Ensure the Right to Privacy is Protected* . Retrieved from Digital Sandiego: https://digital.sandiego.edu/cgi/viewcontent.cgi?article=1324&context=ilj

Jang-Jaccard, J., & Nepal, S. (2014, August). *A survey of emerging threats in cybersecurity*. Retrieved from Science Direct: https://www.sciencedirect.com/science/article/pii/S0022000014000178

Karako, M. (2021, November 04). *AI automation as a solution*. Retrieved from NTT: https://services.global.ntt/en-gb/insights/blog/ai-automation-as-a-solution

Kim, H. (2021, May 21). *The Effects of Artificial Intelligence in the Future Economy*. Retrieved from Modul Private: https://www.modul.ac.at/uploads/files/Theses/Bachelor/Undergrad_2021/BSC_2021/1621027_KIM_In_HongBachelor_Thesis_BSc_no_sig.pdf

Kim, J. F. (2021, November 08). *Why Modern Cybersecurity Requires AI*. Retrieved from Network Computing: https://www.networkcomputing.com/network-security/why-modern-cybersecurity-requires-ai

Li, Y. (2021). The Application Analysis of Artificial Intelligence. *IEE*, 1126-1129.

Li, Y. (2021). *The Application Analysis of Artificial Intelligence in Computer Network Technology*. Retrieved from EEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC): DOI: 10.1109/IPEC51340.2021.9421146

Logicmonitor. (2012, October 05). *What's with the different SNMP versions? v1, v2c, v3?* Retrieved from https://www.logicmonitor.com/: https://www.logicmonitor.com/blog/whats-with-the-different-snmp-versions-s1-v2c-v3/

Lombardo, T. (2020). *Information Technology*. Retrieved from http://www.centerforfutureconsciousness.com/pdf_files/readings/readinginfotech.pdf

Macmillan, P., Hošovský, A., Piteľ, J., Trojanova, M., & Žideka, K. (2021, May 09). *Computational Intelligence in the Context of Industry 4.0*. Retrieved from Spring Linker: https://link.springer.com/chapter/10.1007/978-3-030-70516-9_2

Network Security. (n.d.). Retrieved from LANWORKS: https://www.lanworks.com/security-solutions/

Oros, D. (2016, July 26). *Network Basics: What Is SNMP and How Does It Work?* Retrieved from https://www.auvik.com/: https://www.auvik.com/franklyit/blog/network-basics-what-is-snmp/

Othman, A. (2019, May 05). *Developing Network System with Artificial Intelligence*. Retrieved from https://www.academia.edu/39199689/Developing_Network_System_with_Artificial_Intelligence

Pandey, S., Choi, M.-J., Won, Y., & Won-Ki Hong, J. (2010). INTERNATIONAL JOURNAL OF NETWORK MANAGEMENT. *SNMP-based enterprise IP network topology discovery*, 169-184.

Pascariu, C., & Barbu, I.-D. (2017, June 29). *Dynamic analysis of malware using artificial neural networks*. Retrieved from IEEE Xplore: ECAI 2017 - International Conference – 9th Edition

Paul, D., Sanap, G., Shenoy, S., Kalyane, D., Kalia, K., & Tekade, R. K. (2021). *Artificial intelligence in drug discovery and development*. Retrieved from PMC: doi: 10.1016/j.drudis.2020.10.010

Perez, J. A., Deligianni, F., Ravi, D., & Yang, G.-Z. (2016). *Artificial Intelligence and Robotics*. Retrieved from UK-RAS Networks: https://arxiv.org/ftp/arxiv/papers/1803/1803.10813.pdf

Perez, J. A., Deligianni, F., Ravi, D., & Yang, G.-Z. (2017). *Artificial Intelligence and Robotics*. Retrieved from arxiv: https://arxiv.org/ftp/arxiv/papers/1803/1803.10813.pdf

Perez, S. (2016, March 05). *https://techcrunch.com/2016/03/24/microsoft-silences-its-new-a-i-bot-tay-after-twitter-users-teach-it-racism/*. Retrieved from Tech Crunch: https://techcrunch.com/2016/03/24/microsoft-silences-its-new-a-i-bot-tay-after-twitter-users-teach-it-racism/

Pupillo, L., Fantin, S., Ferreira, A., & Polito, C. (2021, May). *Artificial Intelligence and Cybersecurity*. Retrieved from Centre for European Policy Studies (CEPS) : https://www.ceps.eu/wp-content/uploads/2021/05/CEPS-TFR-Artificial-Intelligence-and-Cybersecurity.pdf

Pupillo, L., Fantin, S., Ferreira, A., & Polito, C. (2021, May). *Artificial Intelligence and Cybersecurity*. Retrieved from CEPS Task Force Report: ceps.eu/wp-content/uploads/2021/05/CEPS-TFR-Artificial-Intelligence-and-Cybersecurity.pdf

Qingjun, W., & Peng, L. (2018). Research on Application of Artificial Intelligence in Computer Network. *IJPRAI*.

Rosencrance, L. (2022, May). *software-defined networking (SDN)*. Retrieved from https://www.techtarget.com/: https://www.techtarget.com/searchnetworking/definition/software-defined-networking-SDN

Scarfone, K. (2020, May). *Compare the top cloud-based IoT security platforms to protect devices*. Retrieved from TechTarget: https://www.techtarget.com/searchsecurity/

Shang, X., & Zhao, C. (2020). Research on the Application of Artificial Intelligence in Computer Network Technology . *ICMCCE*, 1107-1110.

Shu, F., Chen, S., Li, F., Zhang, J., & Chen, J. (2020). *Research and implementation of network attack and defense countermeasure technology based on artificial intelligence technology* . Retrieved from IEEE 5th Information Technology and Mechatronics Engineering Conference.

Signorelli, C. M. (2018, October 26). *Can Computers Become Conscious and Overcome Humans*. Retrieved from Frontiers in Robotics and AI: https://www.frontiersin.org/articles/10.3389/frobt.2018.00121/full

Svenson, A. (2022, January 05). *Artificial Intelligence in Business Intelligence*. Retrieved from KTH Diva Portal: https://kth.diva-portal.org/smash/get/diva2:1626898/FULLTEXT01.pdf

Thomas, M. (2021, July 21). *The Future of AI: How Artificial Intelligence Will Change the World*. Retrieved from Builtin: https://builtin.com/artificial-intelligence/artificial-intelligence-future

Truong, T. C., Diep, Q. B., & Zelinka, I. (2019, December). *Artificial Intelligence in the Cyber Domain: Offense and Defense*. Retrieved from MDPI: https://www.mdpi.com/2073-8994/12/3/410/htm

Tschopp, M., & Ruef, M. (2018, October). *Human Cognition and Artificial Intelligence - A Plea for Science*. Retrieved from Research Gate: https://www.researchgate.net/publication/336850257_Human_Cognition_and_Artificial_Intelligence_-_A_Plea_for_Science

Wan, F., Zhou, J., & Jingl, R. (2020). *Research on Optimization Method of Computer Network Service Quality Based on Integration of Various Artificial Intelligence Technologies*. Retrieved from nternational Conference on Advance in Ambient Computing and Intelligence (ICAACI): DOI 10.1109/ICAACI50733.2020.00048

Yadav, A. (2020, August 04). *Network design: Firewall, IDS/IPS*. Retrieved from InfoSec: https://resources.infosecinstitute.com/topic/network-design-firewall-idsips/