EAI Endorsed Transactions
on Creative Technologies
Research Article EAI.EU

The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey

Feng Tao[1,*], Muhammad Shoaib Akhtar[1] and Zhang Jiayuan[1]

[1]School of Computer and Communications, Lanzhou University of Technology, Gansu, China

Abstract

AI in Cybersecurity Market scheme helps organizations in observance, detecting, reporting, and countering cyber threats to keep up information confidentiality. The increasing awareness among folks, advancements in info technology, up-gradation of intelligence and police work solutions, and increasing volume of knowledge gathered from numerous sources have demanded the utilization of reliable and improved cybersecurity solutions all told industries. The increase in the incidence and quality of cyber-attacks is driving AI-enabled cyber systems. Increasing incidents of huge cyber-attacks globally have created awareness among organizations for securing their information. The motive behind these cyber-criminals are political competition, competitors move for gain and harming the name of others, international information theft, and radical non-secular cluster interest. Most cyber-attacks are for gain. In this review we have presented some previous studies related to Cybersecurity which involves AI.

Keywords: AI, Cybersecurity, ML, DL

Received on 06 May 2021, accepted on 05 July 2021, published on 07 July 2021

doi: 10.4108/_____

1. Introduction

Cybersecurity characterized as a collection of processes that help protect electronic data, human activity, and systems. Analogous to the rule of Moore that predicts the doubling of every two years, components on an integrated circuit (along with declining costs linked to the development of chips), cybercriminals are extremely doubling the efficacy of their targeted attacks for half the cost every several months [1], [2]. Worldwide spending on cybersecurity is estimated to cross $1 trillion from 2016 to 2021. Expenditure on cybersecurity from 2013 to $66, has already risen by over 40 percent. Artificial Intelligence or AI is the development of complex computer systems with the aid of human mentality and able to perform its function like a normal human being, for example, it can recognize the voice and processes it into different languages as a human being. AI is the comprehensive scientific system with varying branches in math, computer science, and philosophy that purpose to develop another intelligent system that shows intelligence properties usually, the word artificial intelligence mostly utilized to describe the machinery that emulates "perception" functions, which humans relate to their mind, i.e. problem- solving and swotting [3], [4].

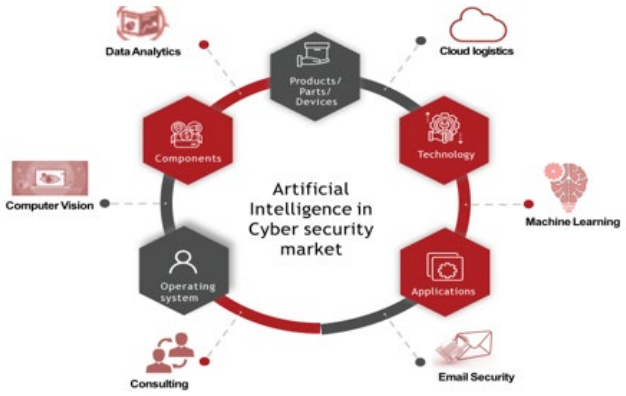

Figure 1. Usages of Artificial Intelligence

*Corresponding author. Email: Fengt@lut.cn

Machine learning is an essential factor in modern research and business. Algorithms are used and network-neutral models to oblige the systems of computers to improve the successfully Development. Machine learning algorithms automatically build a mathematical model by using sample data which is called training data to make decisions without being specifically arranged. Machine learning is based on a model that is the interaction of the brain cell. Donald Hebb introduced this model in 1949 [5]–[8].

Supervised learning

This type of learning is responsible for a pattern to implement a machine learning algorithm. As supervised learning is the easiest way to understand the solutions, it has been used over the years in working of many tools. It is relatively easy to understand this, such as teaching a child by the use of flashcards.

Spam Classification: a person, who is using a new email system, there will be more probability that you have got some filters of spam. These spam filters are supervised learning system. After getting emails and labels, these systems taught how to wipe out spam these spam emails can de track the user by giving them innovative tags.

Unsupervised learning

This type of learning is contradictory to supervised learning. In this, no labels are featured. As a substitute of this algorithm, it requires a considerable extent of data along with the tools that are certain to comprehend the data and its characteristics. Unsupervised learning learns to identify the data utilizing pattern recognition and data sortation.

Reinforcement Learning

This type of learning is totally distinctive from supervised learning and also dissimilar from unsupervised learning. In this way, authors can quickly analyse or see the relationship between the presence and absence of labels Industrial simulations are used for several types of robotic applications; it can finish tasks without owning to hardcode their processes

Deep learning, a technique of ML enables algorithms for using automatic feature learning which shows that algorithms to study further education by combining various features of input data into an abstract set of features. There are four types of machine learning algorithms: supervised, semi-supervised, and unsupervised and reinforcement. This allows the system to make complex predictions when treated with the massive datasets. In past years, the rapid increase in Cyber security, scientist using these algorithms in machine learning systems [9]–[11].

Two of the most popular computation method based on the principle of survival of the MI algorithm fitness for cyber security is- GA and GP. These algorithms functions on the population of the chromosomes that evolve based on certain operators. The three basic operator used is selection, crossover and mutation. The algorithm is started with a randomly generated population; a fitness value is computed for each individual. This signifies the ability of each individual to solve the current problem and individuals with higher probability have higher chance of being chosen in the mating pool. Two capable individual will perform the next step called crossover and finally each will undergo mutation. Among the two mutated individual the highest fit chromosome will be rallied over to the next generation [12]–[15].

The main aim of this algorithm based evaluation is to test the applicability of certain ML algorithms to detect cyber-attacks on MODBUS data. Tenfold cross validation was used to develop the ML models. In cross validation, authors can produce 10 different models for the data set provided. Then the weighted average of these models are calculated which is showed as the final result. The data set used was labelled telemetry data from gas pipeline developed by the Critical Infrastructure Protection Centre.

2. Cloud Computing based Machine Learning Systems for Cybersecurity

Deval Bhamare et al. [16] examined closely the transition of ICS from autonomous systems to cloud-based environments. Then researchers discussed the main works from industry and academia to the creation of safe ICSs, particularly the applicability of ICS cyber security machine learning techniques. The work can help address the challenges of securing industrial processes, particularly as they are migrated into the cloud. Murad A. Rassam et al. [17] Consequently cyber criminals create advanced techniques for exploiting individual devices, networks and states' vulnerabilities. Enterprises collect high-level security data annually for potential forensic tests, such as human log incidents, networks and software applications. There is not a good working experience with large data scales and high fake alarms, particularly when businesses are moved to the cloud architecture and gather more information. In addition it is necessary to track and analyses huge security data accurately and quickly to identify more recent and sumptuous attacks, such as advanced persistent menaces (APTs). Big data processing has been used actively in a number of areas, such as financial transactions, healthcare and industrial applications. The public recently caught attention on account of its promised ability to compare safety data and effectively draw insights on an unrivalled scale. This document analyses traditional technologies/systems and the SIEM tools to deal with massive data scales and sophisticated threats and demonstrates their vulnerabilities. Authors then explore criteria for high-level data analytics and sophisticated threats in cyber-threat intelligence and cyber-security. Finally, authors illustrate the challenges of this adoption and provide some ideas for future research to address the challenges of adoption. In another paper [18] author has shown that the Cloud-based applications have greatly extended multi-value business models. The financial sector is a major beneficiaries, such as big data and cloud computing, of emerging new technology. This shifting pattern has also contributed to significant concerns

about cyber security. Cyber security insurance is a growing domain in the financial industry in this context. However, cyber protection insurance also has some cyber issues by using web-based approaches. This article discusses a variety of the materials needed to understand cyber security risk taxonomy in depth with machine learning techniques. This paper focuses on this subject. The aim of this finding is to avoid maximum risk and develop potential risk solutions. Roberto et al. [19] Current social change is created by IoT, cloud computing, smartphones and social networks. This technological transformation however results in new threats and security attacks that create new and complex cyber security scenarios with large amounts of data and vectors of attack overcoming cognitive capabilities of security analysts. In that sense, cognitive science will support cognitive processes to increase the time and effectiveness of security analysts in implementing cyber security operations. This study provides a comprehensive, machine learning, and decision-making system-supporting cognitive process of security analysts that provide information, understanding, and security response actions. This model offers facts. Information. The model explores automation alternatives for implementing cognitive tasks found in cyber operations. It involves the analyst, with the use of MAPE-K, OODA, and Human Loops, as his key focus in the validation and decision-making phase.

Artificial intelligence finds wide-ranging applications for an intelligent, reliable, high-quality, mass-customized and service focused 3D printing production process. A comprehensive 3D artificial intelligence survey is available in this article [14]. The press learning is possible before a printing task starts through the printability checker to evaluate the printability of the provided 3D items. Parallel slicing algorithms accelerate the slice prefabrication, and smartly optimize the path planning. Smart demand matching algorithms and resource algorithms for service and security provide customers with on-demand services and access to a range of shared resources through the cloud service platform and assessment model. Authors also have three machine-learning algorithms in the case of cyber-attacks to identify product defects. The analysis of various applications provides good opportunities for further study, especially during the period of industry 4.0, for multiple indicator printing, reducing complexity thresholds, prefabrication accelerations, and controls on real time, enhancing safety and detecting defects for individual designs.

Stephan et al. [9] worked on future technological development. The financial sector will be transformed by an AI that allows services to be improved and customized, costs reduced and new business models developed. AI has recently released roadmaps for AI's further development in Germany and Hessen, both by the Federal Government and the Hessian Government. Over the next 5 years, the Federation will invest EUR 3 billion in a range of scientific and industrial fields while the State of Hesse will establish a new AI Centre, which will spend EUR 1 trillion on the growth of digitalization over the next 5 years. AI Hubs continues to provide extremely nuanced public solutions. The emphasis is on improved use of research results in corporate activities, the expansion of networks and ecosystems, and the development of existing centers. These programmes will benefit particularly in the Main Region of the Rhineland of Frankfurt, which already is a powerful hub for Fintech, Cyber Safety and AI. In addition to the unparalleled European university and computer infrastructure, Frankfurt Financial Center has a vibrant and rapidly increasing technology and start-up community: the largest data and cloud service hub in Europe, the biggest in the world, universities and foreign research institutions with a quality AI research, AI specialists and consultancies as well as surrounding fields. AI has the objective of producing highly personalized goods with higher quality and lower costs through integration into the production plants of industrial internet, big data analysis, and cloud computing and advanced robots [4]. Digital production systems are becoming more open than ever, as manufacturing machinery is increasingly retrofitted with sensors and linked via wireless networks or wired Ethernet. Although advances in sensing, artificial intelligence, and wireless technology make possible a paradigm shift in production, cyber-attacks pose major threats to manufacturing. This paper examines cyber protection in digital manufacturing systems, identifying, monitoring and risk determining aspects of device characterization, danger and vulnerability and identifying challenges and potential work.

Anqi Re et al. [12] discussed about the intelligent manufacturing by integrating the Industrial Web of Things, Big Data Analytics, Cloud Computing and advanced robots into factory floors. With more and more manufacturing equipment and devices equipped with sensors, as well as wireless networks and wired Ethernet connections, intelligent manufacturing systems are becoming more accessible than ever via the Internet. While progress in sensing, artificial intelligence and wireless technology allows for a manufacturing paradigm shift, cyber-attacks pose a major threat to the production sector. This paper is intended to review and discuss cutting-edge technologies that can address cyber security issues in intelligent production. In particular, an assessment of vulnerability and cyber-attacks (e.g., man-in-the-middle and denial-of service) are presented. There are also existing strategies to mitigate targeted cyber intrusions. Furthermore, research gaps and challenges in critical manufacturing industries are identified to improve cyber security. İsmail et al. [20] said that the industry 4.0 revolution was brought about by increasing technology and use of the Internet. Internet of things, intelligent computers, intelligent objects, knowledge and data is a technological development in many systems. Some of the problems lie in the major elements of Industry 4.0 such as cyber physical systems, the Internet of things, big data and cloud computing. One is cyber security. This study addressed the technology framework of Industry 4.0 and analyses of cyber security requirements for those technologies. These innovations are intended to be used safely in Industry 4.0 with these

guidelines. Finally, the requisite precautions against cyber-attacks and threats have been addressed with regard to the development of technology and the use of security systems.

3. Organizational Risk Assessment of Cybersecurity using AI

Rohit Nishant et al. [21] argued that the AI should foster creation of organizational processes and practice that are culturally appropriate to minimize the natural and energy intensity resources of human activities in order to facilitate creative sciences and practical environmental sustainability solutions for AI. The main advantages of AI may not be how it allows society to minimize the intensities of electricity, water and land use, but how it facilitates and encourages higher levels of environmental governance. A thorough literature review has shown that (1) over-reliance on historical data in models of machine learning, (2) unpredictable human behavioural responses to AI-oriented interventions, (3) an increase in cyber risk, (4) adverse AI implementations and (5) difficulties in measuring the impacts of intervention policies were threatened by sustainable AI research. This research shows that future sustainable AI studies should incorporate (1) multi-level perspectives, (2) dynamic system approaches, (3) design thinking, (4) economic benefit considerations in order to show how AI can provide immediate solutions without introducing long-term risks to the sustainable environment. Neha Soni et al. [22] examined the wide spectrum of impacts on Governments, counties, companies and persons from Artificial Intelligence (AI), and examined both positive and negative consequences. This paper discusses the overall impact of IA – from research and development before implementation. The paper looks at the major academic successes and progress made by AI and its influence on business practice and thus on the global market. Factors responsible for the development of AI are also examined in this article. In order to analyses entrepreneurial activities against AI there were two lists of the top 100 AI start-ups Research findings will improve technological understanding and the effect of AI on enterprises and society as a whole. It will also gain more knowledge of how business and the global economy are changing from AI.

Ziaul Haque et al. [23] shown a bibliometric research on large data and Artificial Intelligence (AI) technologies was examined for 279 studies in maritime industry performed by 842 scholars in 214 university outlets. The bibliographic information was obtained from the science web by researchers and analysed via the R software Bibliometric process. The most influential magazines, journals, writers and organizations were revealed by researchers on the basis of quotations. With the bibliographic coupling method, authors have developed four research clusters. (2) AI big data applications, (3) energy effectiveness, and (4) predictive analysis. (2) Digital Transformation in the maritime industry. These clusters were thoroughly analysed and potential questions of study were discussed. Further, researchers present research partnership institutional and authors' networks.

Tagarev et al. [24] continued digital transformation requires substantial investment and innovation in order to ensure cyber safety, a variety of critical infrastructures and essential services which rely more and more on digital infrastructure, as well as to increase resilience in malicious use of cyberspace by organizations, societies, sectors, nations and Alliances. This volume includes 28 papers that will be presented at the DIGILIENCE 2019 conference, covering the cyber information sharing and situational awareness, the advantages and challenges of emerging technologies such as artificial intelligence, the human factor, cyber security education and training and cyber resilience, and the need to include cyber safety efforts in the search for DIGILIENCE Conference series would encourage the exchange of information and expertise in IT management, cyber security and resilience, facilitating the dissemination of good practice.

4. Block Chain Technology using AI

Block Chain Technology has investigated the existing and future business applications of particular accounting and cyber security [25]. For existing cyber and accounting problems, authors apply to block chain uses. Researchers [25] are reviewing literature that includes topics such as large-scale data in the accounts, use of the financial security and cyber security chain and use of ledger technology in financial accounts, and financial malfeasance tracking. In order to understand the plans of the U.S. government with regard to cybersecurity, researchers also consider the Home Security Department's cyber security policy in the coming years. Researchers show that the block chain has different auditing consequences that will change the profession drastically. Researchers also believe it necessary to effectively implement the block chain in a number of fields, such as auditing and accounting, of cyber security and accounting.

5. IoT Based Cyberattacks Prevention Systems

Ioanni et al. [26] examined IoT-enabled cyber-attacks that have been found since 2010 in every application domain. The latest Iota attacks, world-renowned events and proof of concept attacks released for each sector are underlined. Authors methodologically analyse representative attacks and show paths through which critical targets are addressed directly and indirectly. Our aim is threefold: I to demonstrate a landscape for the risk-like assessment of iota-enabled cyber-attacks; (ii) to determine overwhelmed and iota-enabled subliminal paths of attack against critical infrastructure and services; and (iii) to address mitigation strategies across areas of application.

Internet of Things (IOT) is a network of different internet-connected devices capable of collecting and

exchanging data, and these IOT devices produce a great deal of information to be gathered and stored for use in artificial intelligence (AI) to handle enormous data flows and storage through the IOT network. In article [27], Researchers discussed briefly what IOT is, what AI is, AI algorithms, AI challenges, and IOT artificial intelligence systems? The self-optimizing network and the software-defined network form part of the major IoT system parameters.

The paradigm shift towards the Internet of Things (IoT) has created a huge capacity for different future IoT scenes such as smart home, intelligent transport, smart health and smart energy, and the advance of the edge measurement concept. There are also a host of emerging cyber-security threats. Authors of [28] intend to develop a number of new opportunities for research and innovation along with "Cyber Security + Edge Computing + IoT + AI." In this article, [28] authors have talk about the big new threats to cyber security and the relevant opportunities in this vision. The aim of, [29] is to define and analyse the technical issues involved and to review recent developments, identify potential solutions and propose new directions for study. First, authors have a survey of mMTC features and QoS problems with major enablers for mMTC in mobile networks. In addition to the highlights on random access inefficiency (RA) within the MMTC scenario, authors present the key characteristics and channel access mechanisms of the emerging IoT cells, LTE-M and IoT narrowband (NB-IoT). Authors then present a framework for performance analyses of transmission scheduling with support for QoS along with problems related to the transmission of short packets. Next, authors offer an exhaustive review of existing and new technologies to solve the problems of RAN congestion in the cellular network and address possible advantages, threats and use cases of evolving Machine Learning (ML) techniques. Authors, [29] focused on the use of the low-complexity Q-learning method in the MMTC scenario with recent advances in improving learning performance and integration from many ML technologies. Finally, authors are exploring open science barriers and exciting future research directions.

Monika et al. [30] discussed about profound learning models in IoT (Internet of Things) networks for cyber security. IoT network is a promising technology that links living and non-living worldwide. IoT deployment is increasing rapidly, but cyber security is a breakdown, so many cyber-attacks are likely and the network's success is mostly stable, so people would otherwise be unwilling to use this technology. In the recent past, the DDoS (Distributed Denial of Service) attack affected a large number of IoT networks, leading to significant losses. Authors have proposed and tested profound learning models using the new CICIDS2017 DDoS Attack Detection Databases which have been extremely accurate as 97.16% of the models already proposed are compared to machine learning algorithms. This paper also addresses open research issues for the use of an IoT cyber security deep learning algorithm.

Centre on a case study of a security operations framework that combines traditional data processing layers with a modern analytical data base engine. The engine enables security experts to query large log event data sets in a typical relationship format. The query results are larger than current database solutions, which work with comparable resources, and are also sufficiently reliable to correctly determine suspicious corner cases. The internal motor is powered by data granulation and overview procedures. These include data quantification principles, estimated calculations, harsh sets of data and probability propagation. In the paper [31] authors analyse the effect of motor parameters in the given environment on their efficiency. In addition, authors explore some of our high-level design decisions such as choosing an estimated measure of the accuracy of the query results that reflects the details of the risk monitoring operations.

In paper [32] authors described an approach to cyber security science powered by data (SOS). It argues that science is motivated by evidence. The following three aspects are then defined as questions and approaches: I Attack evidence-based science, ii) confidence and policy-based bases for sharing and (iii) risk-based security approaches. Authors assume that the three topics discussed in this paper form the basis for the study of the science of cyber security.

In order to evaluate the effect of unintended attacks on device security by the use of two parameters - user vulnerability and user interactions - in different times, authors provide a models for discrete event simulation. In addition, the recommended solution evaluates the potential effect of such activity on the overall health of the system. Authors in [33] demonstrate how simple authors can use the proposed simulation model to examine many analyses for a company system example and the next application. I'm more complete than user interactions, ii) user vulnerability effects rely on the topology of the system; and ii) user interacts increase the total system vulnerability, since the number of paths to be addressed increase as a result of credential leakage.

6. Involvement of AI in Intrusion Detection System (IDS)

Xavier A et al. [34] proposed algorithms for leaning the system which is concentrated in IDS scenarios. In order to do that, a categorization is taken into consideration for cyber security data sets grouping their data into many groups. This work will decide the models in the neural network (multilayer or recurrent), activation functions and learning algorithms, depending on the database, to achieve higher accuracy. Finally, the results were used to determine which data category of cyber safety data set was more important for intrusion detection and the most adequate configuration of the machine learning algorithm to minimize calculation burden. There are also significant safety risks in interconnections necessary to enable certain of the more advantageous features of cars. In order to co-

cyber security are no longer reliable, as their databases which no longer follow current developments in computer technology. Consequently, a new cyber security benchmark ADFA Linux data set (ADFA-LD) in 2013 was proposed to meet current global computer technology advances in order to analyse data mining machine learning and intrusion detection systems. Included in the ADFA-LD are better definitions of their attributes. The research community will use this study to abandon the current cyber security benchmarking datasets and to begin to use the newly implemented benchmarking data set for an effective and systematic evaluation of the computer and data mining intrusion detection system [46].

Social and internet traffic analysis is important for the identification and defence of cyber threats. Increased automated machine learning approaches replace traditional approaches which return to manually-defined rules. This revolution is accelerated via massive data sets that provide machine learning models with higher efficiency. The article [47] analyses a recent analytical study of cyber traffic through social networking and the Internet, using a set of common similarity, relation and collective indications principles in the context of a data-led model. This is not an isolated desire, but a general usage of various networks and social movements is attributable to this. Flows also show a number of features, including a fixed size and many messages between source and destination. The article introduces the current research methodology and application in social and Internet traffic data-driven Internet security (DDCS). The approach to DDCS involves three elements: data collection for cyber security, cyber security engineering and cyber security modelling. There is also a discussion of challenges and future paths.

Cyber-attacks provide the United States with significant national security threats. Today, a growing array of malicious instruments carries out many cyber-attacks. The knowledge and tools to deter and mitigate attacks was planned for cyber-threat intelligence (CTI) and the portal analysing malware. Current CTI portals and malware analyses have however been accused of being too reactive because they depend on previous cyber-attacks to collect data. Online hacker forums are providing the proactive CTI and malware portal with a new source of information. The research [48] shows the AZ Safe Hacker Assets Portal. This website gathers and analyses malicious goods from mostly untapped and rich data sources of on-line hacker groups, using state of the art techniques of machine learning. This paper discusses the creation and development of the AZ Safe Hacker Assets Portal. Authors also offer main portal features including asset search, navigation and download, source code view and code comparison analytics, as well as an interactive CTI dashboard.

In recent decades, cyber security threats have increased. Experts believe that existing security measures would soon be insufficient to avoid more advanced and dangerous cyber-attacks spreading. Recently, the complexity of cyber security has been more and more dominated by approaches borrowed from Artificial Intelligence (AI) to promote automation. In this paper [49] Researchers provide a short survey and hints on Bayesian cyber security applications to allow quantitative threat assessment for higher risk analysis and situational awareness.

Dipankar et al. [50] included a comprehensive survey of works on cyber security ML (2013 to 2018), the bases and corresponding protection of cyber-attacks, the basics of the most popular ML algorithms and proposed ML and cyber security data mining schemes for features, dimension reduction and classification and detection. This article also offers a summary of adversary ML, including safety features of deep learning methods. Finally, transparent problems and concerns are highlighted in cyber security and possible future avenues for study are addressed.

9. Business based Cyber-Security and AI involvements

Narcisa Roxana et al. [13] focused at highlighting the advantages of using Artificial Intelligence to increase business competitiveness while at the same time raising awareness in order to resolve fear in exploring emerging technologies due to cyber-attacks. How insecure are computerization companies? 100%. 100%. The Internet was a shared place for everyone. Store data on any computer connected to the internet in any given second may become vulnerable. This article shows how Researchers can use cyber protection to secure our company by simultaneously presenting cases of Malta risk management. The current AI status in cyber security was discussed, and numerous AI case studies and applications identified to support the community to better understand the problems and unresolved issues that AI has in cyber security, including the Engineering's and Leaders, Academics, Pedagogues, Innovators, Entrepreneurs and Students. Business and government management implications and policy recommendations are presented [51].

Cyber security is subject to great technical and organizational changes in a computing world in recent days, and data science is driving progress. In order to automate and intelligently construct a security architecture, extract patterns or insights from cybersecurity data and create the corresponding data-driven model. In order to understand and explain actual phenomena using data, various research methods, machine learning techniques, processes and systems, commonly called data studies, are used. The paper [52] focuses on and explores the cyber security data research briefly, which collects data from relevant cyber safety sources and complements analytics with the latest data-driven models to improve safety solutions. The cyber-security data science theory enables cyber-security computing to be more operational and intelligent than traditional processes. A number of relevant research problems and recommendations are then addressed and summarized. Authors also have a multi-layered cyber security modelling machine learning

framework. In summary, our goal is to focus on the application of smart data-enabled decision-making to cyber-assistance systems as well as on cyber safety science as well as relevant techniques.

The structure of the supply chain processes has also changed with digital developments. In this paper, authors synthesize the impact of disruptive technologies on supply chains and related cyber hazards through systematic literature. A taxonomy/cladistics approach is used to evaluate progress with a particular focus on cyber risk mitigation on incorporating the supply chain into Industrial Internet of Things and Industry 4.0. The questions about the evolving cyber risk types and the integration of new technology supply chains in an analytical sense are key assessed. The paper [53] describes an autonomous AI/ML and Real Time Intelligence supporting supply chain infrastructure for predictive cyber risk analysis. This unit is built into a cognition engine that provides real-time predictive cyber risk analysis using the IoT network. This enhances capability and helps to provide a detailed understanding of the opportunities and dangers associated with deploying the edge computing nodes and the migration to the periphery of IoT systems of AI/ML technologies.

10. Medical Image processing and Cyber Attacks

Miles et al. [54] Machine learning and artificial intelligence have been growing unprecedented. These technology has many useful applications, from machine translation to medical image processing. Countless more such innovations are being developed and can long-term be planned. The manner in which artificial intelligence can be misused has historically been paid less attention. The report explores the landscape of potential safety dangers from the misuse of artificial intelligence technologies and proposes ways to help predict, avoid and alleviate them. Authors analyse the long-term balance between aggressors and defenders, but authors do not address the issue. Instead, researchers focus on what types of attacks authors are soon to see if enough protection has not been developed.

11. Advances to the techniques of cryptographic and artificial intelligence

Cyber security is an ever-changing discipline that has been in the news for the past decade, as the number of threats is on the increase and cyber criminals actively try to keep the law enforcement ahead. While the initial reasons for cyber-attacks remain relatively unchanged over the years, cyber criminals are becoming increasingly sophisticated in their techniques. The detection and mitigation of new cyber threats are becoming ineffective in traditional cyber security solutions. Advances to the techniques of cryptographic and artificial intelligence (AI) (particularly machine learning and deep learning) are promising to allow cyber security experts to address the constantly growing threat posed by opponents. Here, authors [55] discuss the ability of AI to improve cyber security solutions, both by recognizing its strengths and its limitations. Authors talk about potential research opportunities in the field of cyber security related to the advancement of AI techniques across a variety of application domains. Faezeh et al. [56] proposed an intelligent-classic hybrid re-establishment and compensation solution for cyber-attacks to CPS and industrial IoT inputs via shared communications networks. A class of n linear non-linear structures in this study is understood to be a CPS model when cyber-attacks are only carried out on the front channel. In order to compensate for cyber-attacks, a smart classical control system is built. Neural Networks (NN), a traditional nonlinear control system based on the variable checking framework, was designed to compensate for attacks and to control the outcome of device in monitoring applications. In the proposed methodology, nonlinear control theory is used to ensure device stability when attacks happen. In this technique, NN is an online evaluation and rebuilding of the cyber-attacks started on the networked Gaussian radial infrastructure. The law on adaptation of the intelligent estimator comes from a feature of Lyapunov. The simulation results indicated that the proposed technique is reliable and feasible as a testbed for car cruise control applications.

Cybercrimes have become a constant threat to the unparalleled advances in IT (IT). Every day, cyber infrastructure is exposed to significant cybercrimes and assaults. The surveillance and security of these infrastructures have not been entirely effective with physical devices and human intervention; therefore highly efficient defence systems are required, which have to be scalable, adaptable and resilient, to defend IT infrastructure from countless and highly possible cyber-attacks. Modern artificial intelligence tools have played a vital role in the identification and prevention of cybercrime. The study [10] aims to show progress in the battle against multiple cybercrimes in artificial intelligence and to show the efficiency of various AI techniques in detecting and preventing cyber-attacks and also to provide scope for future work. During the last decade, cyber-attacks have increased extensively. Cyber-criminals became more advanced. Current security checks are not enough to protect networks from highly qualified cybercriminals. Cybercriminals have learned how to evade the most advanced techniques such as IDPS, and botnets are almost invisible to the latest instruments. Fortunately, the use of Artificial Intelligence (AI) can improve the IDPS device detection rates, and machine learning (ML) techniques can mine botnet source data. The application of AI can, however, entail other risks and cyber security experts must strike a balance between risk and profit [57].

11. Wireless communication based Cyberattacks and prevention from AI

New trends are expected with the advent of wireless communications networks, such as self-driving automobiles, unmanned air systems, autonomous robots, the internet of things, and virtual realities. With the 5th generation of wireless networks, these technology requires very high data speeds, incredibly low latencies and great reliability (5G). A large number of research organizations have claimed that 5G cannot fulfil its needs without artificial intelligence integration (A.I.), since 5G wireless networks would generate incomparable traffic and enable wireless scientists to access big data to help predict the demands and cell designs to meet user's requirements. Many researchers subsequently used AI in many aspects of 5G Wireless Networking Architecture, including radio resource allocation, network management, and Internet security. Authors in [58] provide a detailed analysis of A.I. for 5G wireless networks in this paper. The aim of this paper is to examine A.I. in wireless communications, analyse various case studies, tackle issues and clarify future testing recommendations for the use of A.I. in 5G wireless communications.

For all aspects of the modern world, cyberspace has become an indispensable element. The planet is increasingly reliant on the internet for daily life. The growing internet dependence has also increased the risk of malicious threats. Due to increasing cyber security dangers, cyber security has become a key element in the cyber world to combat all cyber threats, attacks and fraud. The growing cyberspace is highly exposed to the likelihood of endless cyber threats. The purpose of this survey is to provide a brief overview of various machine learning techniques (ML) to learn all innovations related to detection methods for possible cyber safety risks. These cyber security techniques are primarily used to detect fraud, to detect intrusion, to spam and to detect malware. In this study, authors draw on the literature currently available on ML models of cyber security applications and include an in-depth review of ML cyber security techniques. To the best of our understanding, authors tried first to compare the time complexity of widely used cyber security ML models. In [59], authors have comprehensively compared the output of each classifier based on often used data sets and cyber threat sub-domains. This work also briefly introduces machine learning models in addition to widely used safety datasets. Despite its primary precedent, cyber protection has compromises and problems with its constraints. This thesis also explains the immense obstacles and constraints facing the implementation of computer security machine learning techniques.

Creation of a cyber-security testing system testbed using the control and data acquisition monitor Presented (SCADA). The test bed consists of a water storage tank control device that is a level of water treatment and distribution. Comprehensive cyber-attacks have been carried out against the testbed [60]. The attacks collected the network traffic and collected traffic characteristics to generate a dataset for training and test different machine learning algorithms. Five standard machine learning algorithms were used as training for the attacks, such as random forest, decision trees, logistic recovery, Naïve Bays and KNN. Trained machine learning models were then built and put into the network to perform new tests using online network traffic. The resulting achievements have been contrasted with the results obtained through online use of these model in the network during training and testing of machine learning models. The results show the effectiveness of master learning models in the detection of attacks in real time. The test bed provides a direct insight into the influence and effects of attacks on real SCADA settings.

The paper focuses [61] in a particular way on artificial intelligence and the cognitive dynamic system. If the switches are new and extremely important, authors discuss standard switches and then implement task-switch control, then IS and CDS to outline their particular structures. Authors then use the special switch Conclusion the paper ends.

The modes of cyber assault are complex and diverse and it is often difficult to identify and predict dynamic types of attacks. In many fields research on information graphs is becoming more and more mature. It is currently very important for many researchers to merge the idea of the knowledge graph and cyber security to build a cyber-security knowledge base. The article [62] offers a knowledge base focused on a five-fold paradigm for cyber security and deduction laws. Authors eliminate organizations and draw on ontology by using computer training to gather an insight into cyber security. The path ranking algorithm calculates formulas and then deduces new rules. Stanford is also the object recognizer (NER) used to train an extractor to obtain useful information. The experimental results show that Stanford NER has many features and is able to train cybersecurity identifiers using the Gazettes parameter to prepare for future work.

Recent artificial intelligence advances (AIs) suggest that this new technology will have a more generally deterministic and potentially revolutionary impact on military power, geopolitical competition and global politics. After the initial surge of wide-ranging speculation in the AI literature, this paper gives the debate a necessary specificity. It argues that unchecks of the uncertainties and vulnerabilities posed by the rapid growth and spread of AI could become a major source of potential instability and high power strategic rivalry. The article [63] identifies many AI-innovations and technical advancements that are likely to have a real impact from a tactical to a strategic level on military applications.

12. Deep Learning based Cybersecurity Systems

V. Kanimozhi et al. [64] proposed framework of artificial neural networks has an excellent accuracy score of 99.97 percent and a ROC (Receiver Operator Characteristic) region of an average area of 0.999 and a False Positive average of just 0.001. The proposed system using artificial botnet attack detection intelligence is efficient, precise and precise. The new framework proposed for standard network transport analysis, cyber-physical system traffic data and real-time network traffic analysis can be implemented on the n devices.

Recent attacks demonstrate that cyber threats are not only increasing in scale, they are also increasingly refined. The attacks can involve several measures difficult to discern from friendly activities. High fake positive rates must therefore be addressed by standard detection techniques. Due to a failure to conduct automated detection techniques, the responses to such attacks highly rely on decision-making processes guided by people. Although game theory is used on many issues involving reasonable choice, authors restrict the use of such a procedure in security games if the defenders have minimal knowledge on the opposing player's strategies and benefits. The work [65] proposes that Learning respond automatically to the actions of an unfavourable user in order to protect the system. This work compares Q-learning with a typical stochastic game. Although there are minimal knowledge about rivals, the results of simulations suggest Naive Q-Learning possibilities.

Artificial intelligence advances (AI) attracted the attention of scientists and practitioners and opened up a wide variety of useful opportunities in the public sector for AI use. Against this context, a comprehensive understanding of the range and effects of AI-based applications and related challenges is emerging. However, previous research only looks in isolation and fragmentation at AI applications and challenges. Given the absence of a comprehensive overview of AI-based application and public sector challenges, our conceptual approach analyses and compiles applicable scientific literature insights to provide a comprehensive overview of AI applications and related challenges. Findings in [66] suggest 10 fields for AI applications outlining their development and operation of values as well as particular cases of public usage. In addition, four main dimensions of AI problems are established. Finally, authors analyse our conclusions, draw on the theory and practice implications, and provide recommendations for future study.

ML and DL network analysis literature surveys identified and provides a brief description of each ML and DL process. ML and DL analysis process are discussed. Time or thermal correlation was indexed, read and synthesized in documents representing each process. Due to the relevance of the data in ML/DL methods, authors clarify some popular network datasets in ML/DL, deal with cyber security problems with ML/DL, and provide recommendations for analysis [67].

This [68] research offers a solution for intelligent identification of disappointing identities created on social media sites by human beings (SMPs). First, this study measures computer model learning with attributes like the 'profile frame' in SMPs. Previous psychological findings like that human beings lie about their sex are used to improve the results of these models. Newly developed features such as the "gender profile image" are evaluated for the precise identification of disappointments with these features. In order to improve initial performance, research findings from non-human accounts (also known as bot) are also used to boost. Finally, these results are applied to a suggested SMP intelligently-identified model. The paper shows [68] that if the insecurity of the existing way to set up SMP user accounts in the future can theoretically be reduced by the cyber security threat of ID deception.

Samaneh et al. [69] concentrated on recent DL approaches in the field of cyber security, such as intrusion detection, malware detection, phishing / spam detection and detection of website default. The first is to explain preliminary descriptions of common DL models and algorithms. Then a general DL architecture is suggested and clarified on the basis of the four main modules of cyber security applications. The corresponding papers are subsequently summarized and analysed in the areas of concentration, methodology, application of the model, and granularity. The final comments and potential work, including possible research topics to improve various cyber security applications using DL models, will be addressed.
Yang Lu et al. [70] constructed a comprehensive survey of AI and deep learning between 1961 and 2018. The study gives researchers and practitioners a valuable guide through the systematic multi-angle analysis of AIs, from underlying mechanisms to functional implementations, from fundamental algorithms to industrial accomplishments, from current status to potential developments. AI is an innovative and breakthrough assistant with several different applications and sectors, despite a great deal of difficulty.

Benoit et al. [71] argue that cyber protection calls for new and special AI techniques which have been developed for this type of use. In reality, this paper is focused on a broad overview of various approaches that can alter cyber-security games. This paper focuses on the security of web applications and promotes the use of KNS, probabilistic reasoning and Bayesian upgrades to monitor the likelihood of fake positive and negative elements.

Owing to increased cyber threats and cyber hacking, cyber safety has emerged rapidly in recent years. Emerging research on technology highlights the risks and sometimes neglects the potential positive contribution to cyber security. The report aims to conduct a reasonably balanced long-term survey to identify key threat drivers and new technologies that could have a direct effect on cyber security protection and attack capabilities. The main instruments used in this research were horizon scanning and online expert surveys on emerging threats and the potential impact of several new technologies on cyber defence and cyber-attack capabilities. An expert study [7] has shown that cyber-strength, homomorphic encryption and the block chain are mainly security technology. The Internet of Things, organic hacking, the HMI and

independent technology mainly increase strike capability. There are independent technology, quantum computing and artificial intelligence in the centre that both help to defend and attack capacities and have about the same impact on each other. This research offers a balanced, long-term perspective and expert assessment of negative and positive effects, including maturity and consensus, of emerging technologies. Two new Likert scales were used to classify results into 4 groups to evaluate the potential effects of developing technologies on cyber security (net positive, net negative, positive-positive and negative-negative).

Artificial Intelligence (AI) interest and knowledge rise so fast that academia and higher education struggle to meet industry's increasing demand. Seventy-five percent of business software were forecast to use AI, machine learning, or deep learning technologies by 2021, but university programmes are also burdened by students with elective training through several divisions to receive their data science training. The data science calls for specific preparation of mathematics particularly for cyber security students whose programmes have minimized the advance mathematics requirements. To promote the curriculum planning and hands-on use of AI technologies, the first step in introducing computer science and cyber security students to AI concepts and capabilities was a notebook ("A Trellis for Novice AI Practitioners") prepared in the R programming language. The research [72] focuses on intrusion detection data to mitigate nine common cyber vulnerabilities. Trellis fills the theoretical and realistic gap for students by creating a predictive model of intrusion from scratch for the ANN network. It acts as a template but also promotes serious environmental changes and can be relied on for a number of data sets in all areas of the discipline in the initial stages of cyber-safety practitioner's data science activities.

13. AI-Driven Cybersecurity

Jiageng et al. [73] offered a detailed perspective on "AI-driven cyber security," which can play an important role in intelligent cyber security services and management. Threat intelligence modelling using such AI approaches will simplify and render the cyber security computing process smart over traditional security systems. Within the framework of our report, authors also highlight several directions for research to help researchers do future research in the field. The overall purpose of this paper is to serve as a point of reference and guidance for cyber security researchers and practitioners in the industry, in particular from a smart computer or technological point of view from an AI basis.

Noemi et al. [74] described the ontology of the reachability matrix (RMO). RMO is designed to define the networks and cyber security domain to calculate information on accessibility (reachability matrix). Reachability Matrix decides whether a node can reach another node (via the protocol on ISO/OSI layers). RMO defines the elements of a network, the network accessibility details and the access control policies to achieve this goal. RMO also includes some SWRL rules for calculating the matrix of accessibility. In addition to the RMO and SWRL laws, a number of SPARQL queries are also available to refine the calculation of the Reachability Matrix. RMO reflects a ground-breaking approach to calculating the reachability matrix, to the best of our understanding. Then authors define our approach on the basis of a strategy using a combination of OWL, definition logic rules and SPARQL queries.

The production of IT will make a machine behave and think like people. AI is an exceptional aspect of IT which requires the development of a computer that reacts and functions as a human mind. The core aspects of artificial intelligence include the comparison of the human senses. The system is able to recognize touch and speech as features placed within the system for operating the possible activities of a normal life situation without human assistance. However, artificial intelligence is the intelligence agent research, which takes the state of the world and successfully achieves its target. The majority of computer structures in the world are constructed to serve the purposes according to the essence of the situation with the special application of the human elements. Artificial intelligence is usually a human being who uses troubleshooting methods and learning to understand the high levels of activities in the operation of elements inspired by man, decision making and the emotional cycle. Artificial intelligence is machine-based intelligence as opposed to human intelligence. The research paper [75] aims to assess the emerging issues relating to artificial cyber security intelligence in the United States. The research paper proposes the ground-breaking Artificial Intelligence Cyber Security approach in the United States. Artificial intelligence methods have quickly advanced in recent years and their uses in many fields can be seen from face recognition to picture processing. AI technology will improve cyber security tools and allow opposes to evolve attack methods in the cyber security market. But malicious players are aware of the new prospects and are likely to try to hurt them. The paper [5] provides an overview of how artificial intelligence can be used in the sense of cyber security in both crime and defence [12]–[15].

14. Conclusion

Since cybercrimes are becoming increasingly complex, cyber security approaches are needed to be more robust and intelligent. This will allow defence mechanisms to make real-time decisions that can react effectively to sophisticated attacks. To help this, researchers and practitioners need to know existing cyber-security methods. The use of artificial intelligence in particular in the fight against cybercrimes. However, artificial intelligent approaches to combat cybercrimes are not summarised. The papers were reviewed using quantitative and qualitative approaches using a systematic mapping in

the fields of IoT, Blockchain, Cybercrimes, Business, IDS, Software defined networks and cyber forensics. It was found that artificial smart methods contributed remarkably to cybercrimes by significantly improving intrusion detection systems. It was also found that computer complexity, model training times and false alarms have been reduced. However, the domain is significantly skewed. Most research centred on intrusion detection and prevention systems and support vector machines were the most dominant technique used.

References

[1] X. Chen *et al.*, "Artificial intelligence-empowered path selection: A survey of ant colony optimization for static and mobile sensor networks," *IEEE Access*, vol. 8, pp. 71497–71511, 2020, doi: 10.1109/ACCESS.2020.2984329.

[2] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, "Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT Scenarios," *IEEE Access*, vol. 8, pp. 23022–23040, 2020, doi: 10.1109/ACCESS.2020.2970118.

[3] AI Forum of New Zealand and AsureQuality, "Artificial Intelligence for Agriculture in New Zealand," p. 40, 2019.

[4] D. Wu *et al.*, "Cybersecurity for digital manufacturing," *J. Manuf. Syst.*, vol. 48, pp. 3–12, 2018, doi: 10.1016/j.jmsy.2018.03.006.

[5] T. C. Truong, Q. B. Diep, and I. Zelinka, "Artificial intelligence in the cyber domain: Offense and defense," *Symmetry (Basel).*, vol. 12, no. 3, pp. 1–24, 2020, doi: 10.3390/sym12030410.

[6] I. H. Sarker, Y. B. Abushark, F. Alsolami, and A. I. Khan, "IntruDTree: A machine learning based cyber security intrusion detection model," *Symmetry (Basel).*, vol. 12, no. 5, pp. 1–15, 2020, doi: 10.3390/SYM12050754.

[7] Y. Raban and A. Hauptman, "Foresight of cyber security threat drivers and affecting technologies," *Foresight*, vol. 20, no. 4, pp. 353–363, 2018, doi: 10.1108/FS-02-2018-0020.

[8] A. S. Wilner, "Cybersecurity and its discontents: Artificial intelligence, the internet of things, and digital misinformation," *Int. J.*, vol. 73, no. 2, pp. 308–316, 2018, doi: 10.1177/0020702018782496.

[9] S. Bredt, "Artificial Intelligence (AI) in the Financial Sector—Potential and Public Strategies," *Front. Artif. Intell.*, vol. 2, no. October, pp. 1–5, 2019, doi: 10.3389/frai.2019.00016.

[10] Z. Siddiqui, M. S. Husain, and S. Yadav, "Application of Artificial Intelligence in Fighting Against Cyber Crimes: a Review," *Int. J. Adv. Res. Comput. Sci.*, vol. 9, no. 2, pp. 118–122, 2018.

[11] G. Petrica, S. D. Axinte, I. C. Bacivarov, M. Firoiu, and I. C. Mihai, "Studying cyber security threats to web platforms using attack tree diagrams," *Proc. 9th Int. Conf. Electron. Comput. Artif. Intell. ECAI 2017*, vol. 2017-Janua, pp. 1–6, 2017, doi: 10.1109/ECAI.2017.8166456.

[12] A. Ren, D. Wu, W. Zhang, J. Terpenny, and P. Liu, "Cyber security in smart manufacturing: Survey and challenges," *67th Annu. Conf. Expo Inst. Ind. Eng. 2017*, pp. 716–721, 2017.

[13] M. N. O. Sadiku, O. I. Fagbohungbe, and S. M. Musa, "Artificial Intelligence in Cyber Security," *Int. J. Eng. Res. Adv. Technol.*, vol. 06, no. 05, pp. 01–07, 2020, doi: 10.31695/ijerat.2020.3612.

[14] J. Yang, Y. Chen, W. Huang, and Y. Li, "Survey on artificial intelligence for additive manufacturing," *ICAC 2017 - 2017 23rd IEEE Int. Conf. Autom. Comput. Addressing Glob. Challenges through Autom. Comput.*, no. September, pp. 7–8, 2017, doi: 10.23919/IConAC.2017.8082053.

[15] B. S. Sagar, S. Niranjan, N. Kashyap, and D. N. Sachin, "Providing cyber security using artificial intelligence - A survey," *Proc. 3rd Int. Conf. Comput. Methodol. Commun. ICCMC 2019*, no. Iccmc, pp. 717–720, 2019, doi: 10.1109/ICCMC.2019.8819719.

[16] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, "Cybersecurity for industrial control systems: A survey," *Comput. Secur.*, vol. 89, p. 101677, 2020, doi: 10.1016/j.cose.2019.101677.

[17] M. A. Rassam, M. A. Maarof, and A. Zainal, "Big Data Analytics Adoption for Cyber-security: A Review of Current Solutions, Requirements, Challenges and Trends," *J. Inf. Assur. Secur.*, vol. 11, pp. 124–145, 2017.

[18] S. A. Elnagdy, M. Qiu, and K. Gai, "Understanding Taxonomy of Cyber Risks for Cybersecurity Insurance of Financial Industry in Cloud Computing," *Proc. - 3rd IEEE Int. Conf. Cyber Secur. Cloud Comput. CSCloud 2016 2nd IEEE Int. Conf. Scalable Smart Cloud, SSC 2016*, pp. 295–300, 2016, doi: 10.1109/CSCloud.2016.46.

[19] R. O. Andrade and S. G. Yoo, "Cognitive security: A comprehensive study of cognitive science in cybersecurity," *J. Inf. Secur. Appl.*, vol. 48, 2019, doi: 10.1016/j.jisa.2019.06.008.

[20] İ. İlhan, "Requirement Analysis for Cybersecurity Solutions in Organisations," 2015.

[21] R. Nishant, M. Kennedy, and J. Corbett, "Artificial intelligence for sustainability: Challenges, opportunities, and a research agenda," *Int. J. Inf. Manage.*, vol. 53, no. January, p. 102104, 2020, doi: 10.1016/j.ijinfomgt.2020.102104.

[22] N. Soni, E. K. Sharma, N. Singh, and A. Kapoor, "Artificial Intelligence in Business: From Research and Innovation to Market Deployment," *Procedia Comput. Sci.*, vol. 167, no. 2019, pp. 2200–2210, 2020, doi: 10.1016/j.procs.2020.03.272.

[23] Z. H. Munim, M. Dushenko, V. J. Jimenez, M. H. Shakil, and M. Imset, "Big data and artificial intelligence in the maritime industry: a bibliometric review and future research directions," *Marit. Policy Manag.*, vol. 00, no. 00, pp. 1–21, 2020, doi: 10.1080/03088839.2020.1788731.

[24] T. Tagarev, "DIGILIENCE - A Platform for Digital Transformation, Cyber Security and Resilience," *Inf. Secur. An Int. J.*, vol. 43, no. 1, pp. 7–10, 2019, doi: 10.11610/isij.4300.

[25] S. Demirkan, I. Demirkan, and A. McKee, "Blockchain technology in the future of business cyber security and accounting," *J. Manag. Anal.*, vol. 7, no. 2, pp. 189–208, 2020, doi: 10.1080/23270012.2020.1731721.

[26] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and

services," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 4, pp. 3453–3495, 2018, doi: 10.1109/COMST.2018.2855563.

[27] S. Mahalakshmi and R. Latha, "Artificial intelligence with the internet of things on healthcare systems: A survey," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, no. 6, pp. 2847–2854, 2019, doi: 10.30534/ijatcse/2019/27862019.

[28] J. Pan and Z. Yang, "Cybersecurity challenges and opportunities in the new 'edge computing + iot' world," *SDN-NFVSec 2018 - Proc. 2018 ACM Int. Work. Secur. Softw. Defin. Networks Netw. Funct. Virtualization, Co-located with CODASPY 2018*, vol. 2018-Janua, pp. 29–32, 2018, doi: 10.1145/3180465.3180470.

[29] S. K. Sharma and X. Wang, "Toward Massive Machine Type Communications in Ultra-Dense Cellular IoT Networks: Current Issues and Machine Learning-Assisted Solutions," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 1, pp. 426–471, 2020, doi: 10.1109/COMST.2019.2916177.

[30] M. Roopak, G. Yun Tian, and J. Chambers, "Deep learning models for cyber security in IoT networks," *2019 IEEE 9th Annu. Comput. Commun. Work. Conf. CCWC 2019*, pp. 452–457, 2019, doi: 10.1109/CCWC.2019.8666588.

[31] D. Ślęzak, A. Chadzyńska-Krasowska, J. Holland, P. Synak, R. Glick, and M. Perkowski, "Scalable cyber-security analytics with a new summary-based approximate query engine," *Proc. - 2017 IEEE Int. Conf. Big Data, Big Data 2017*, vol. 2018-Janua, pp. 1840–1849, 2017, doi: 10.1109/BigData.2017.8258128.

[32] B. Thuraisingham *et al.*, "A data driven approach for the science of cyber security: Challenges and directions," *Proc. - 2016 IEEE 17th Int. Conf. Inf. Reuse Integr. IRI 2016*, pp. 1–10, 2016, doi: 10.1109/IRI.2016.10.

[33] T. Baluta, L. Ramapantulu, Y. M. Teo, and E. C. Chang, "Modeling the effects of insider threats on cybersecurity of complex systems," *Proc. - Winter Simul. Conf.*, pp. 4360–4371, 2017, doi: 10.1109/WSC.2017.8248141.

[34] X. A. Larriva-Novo, M. Vega-Barbas, V. A. Villagra, and M. Sanz Rodrigo, "Evaluation of Cybersecurity Data Set Characteristics for Their Applicability to Neural Networks Algorithms Detecting Cybersecurity Anomalies," *IEEE Access*, vol. 8, pp. 9005–9014, 2020, doi: 10.1109/ACCESS.2019.2963407.

[35] J. Straub *et al.*, "CyberSecurity considerations for an interconnected self-driving car system of systems," *2017 12th Syst. Syst. Eng. Conf. SoSE 2017*, 2017, doi: 10.1109/SYSOSE.2017.7994973.

[36] M. Z. Alom and T. M. Taha, "Network intrusion detection for cyber security on neuromorphic computing system," *Proc. Int. Jt. Conf. Neural Networks*, vol. 2017-May, pp. 3830–3837, 2017, doi: 10.1109/IJCNN.2017.7966339.

[37] K. Shaukat *et al.*, "Performance comparison and current challenges of using machine learning techniques in cybersecurity," *Energies*, vol. 13, no. 10, 2020, doi: 10.3390/en13102509.

[38] S. Pissanetzky, "On the Future of Information: Reunification, Computability, Adaptation, Cybersecurity, Semantics," *IEEE Access*, vol. 4, no. 0, pp. 1117–1140, 2016, doi: 10.1109/ACCESS.2016.2524403.

[39] C. Sayan, S. Hariri, and G. Ball, "Cyber Security Assistant: Design Overview," *Proc. - 2017 IEEE 2nd Int. Work. Found. Appl. Self* Syst. FAS*W 2017*, pp. 313–317, 2017, doi: 10.1109/FAS-W.2017.165.

[40] T. M. GEORGESCU and I. SMEUREANU, "Using Ontologies in Cybersecurity Field," *Inform. Econ.*, vol. 21, no. 3/2017, pp. 5–15, 2017, doi: 10.12948/issn14531305/21.3.2017.01.

[41] C. Glantz, S. Somasundaram, M. Mylrea, and R. Underhill, "Evaluating the Maturity of Cybersecurity Programs for Building Control Systems," pp. 1–12, 2016.

[42] M. S. A. Humr, "Autonomous outcomes: Shaping the future data environment to build trust in artificial intelligence and machine learning applications," *AAAI Fall Symp. - Tech. Rep.*, vol. FS-17-01-, no. November 2017, pp. 210–211, 2017.

[43] L. Caviglione, M. Gaggero, E. Cambiaso, and M. Aiello, "Measuring the energy consumption of cyber security," *IEEE Commun. Mag.*, vol. 55, no. 7, pp. 58–63, 2017, doi: 10.1109/MCOM.2017.1600955.

[44] C. J. Cornel, D. C. Rowe, and C. M. Cornel, "Starships and cybersecurity: Teaching security concepts through immersive gaming experiences," *SIGITE 2017 - Proc. 18th Annu. Conf. Inf. Technol. Educ.*, pp. 27–32, 2017, doi: 10.1145/3125659.3125696.

[45] N. Y. Conteh and P. J. Schmick, "Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks," *Int. J. Adv. Comput. Res.*, vol. 6, no. 23, pp. 31–38, 2016, doi: 10.19101/ijacr.2016.623006.

[46] A. I. Abubakar, H. Chiroma, S. A. Muaz, and L. B. Ila, "A review of the advances in cyber security benchmark datasets for evaluating data-driven based intrusion detection systems," *Procedia Comput. Sci.*, vol. 62, no. Scse, pp. 221–227, 2015, doi: 10.1016/j.procs.2015.08.443.

[47] R. Coulter, Q. L. Han, L. Pan, J. Zhang, and Y. Xiang, "Data-Driven Cyber Security in Perspective - Intelligent Traffic Analysis," *IEEE Trans. Cybern.*, vol. 50, no. 7, pp. 3081–3093, 2020, doi: 10.1109/TCYB.2019.2940940.

[48] S. Samtani, K. Chinn, C. Larson, and H. Chen, "AZSecure Hacker Assets Portal: Cyber threat intelligence and malware analysis," *IEEE Int. Conf. Intell. Secur. Informatics Cybersecurity Big Data, ISI 2016*, pp. 19–24, 2016, doi: 10.1109/ISI.2016.7745437.

[49] M. J. Pappaterra and F. Flammini, "A review of intelligent cybersecurity with bayesian networks," *Conf. Proc. - IEEE Int. Conf. Syst. Man Cybern.*, vol. 2019-Octob, no. 1763, pp. 445–452, 2019, doi: 10.1109/SMC.2019.8913864.

[50] D. Dasgupta, Z. Akhtar, and S. Sen, "Machine learning in cybersecurity: a comprehensive survey," *J. Def. Model. Simul.*, 2020, doi: 10.1177/1548512920951275.

[51] L. Chan *et al.*, "Survey of AI in cybersecurity for information technology management," *2019 IEEE Technol. Eng. Manag. Conf. TEMSCON 2019*, pp. 1–8, 2019, doi: 10.1109/TEMSCON.2019.8813605.

[52] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," *J. Big Data*, vol. 7, no. 1, 2020, doi: 10.1186/s40537-020-00318-5.

[53] P. Radanliev *et al.*, "Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains," *Cybersecurity*, vol. 3, no. 1, 2020, doi: 10.1186/s42400-020-00052-8.

[54] S. Bhatnagar *et al.*, "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation Authors are listed in order of contribution Design Direction," *arXiv Prepr. arXiv1802.07228*, no. February 2018, p. 101, 2018.

[55] S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, "Harnessing artificial intelligence capabilities to improve cybersecurity," *IEEE Access*, vol. 8, pp. 23817–23837, 2020, doi: 10.1109/ACCESS.2020.2968045.

[56] F. Farivar, M. S. Haghighi, A. Jolfaei, and M. Alazab, "Artificial Intelligence for Detection, Estimation, and Compensation of Malicious Attacks in Nonlinear Cyber-Physical Systems and Industrial IoT," *IEEE Trans. Ind. Informatics*, vol. 16, no. 4, pp. 2716–2725, 2020, doi: 10.1109/TII.2019.2956474.

[57] R. Calderon, "The Benefits of Artificial Intelligence in Cybersecurity," *Econ. Crime Forensics Capstones. 36.*, 2019.

[58] Y. Arjoune and S. Faruque, "Artificial Intelligence for 5G Wireless Systems: Opportunities, Challenges, and Future Research Direction," *2020 10th Annu. Comput. Commun. Work. Conf. CCWC 2020*, pp. 1023–1028, 2020, doi: 10.1109/CCWC47524.2020.9031117.

[59] "样本量估算-Machine Learning.Pdf." .

[60] M. A. Teixeira, T. Salman, M. Zolanvari, R. Jain, N. Meskin, and M. Samaka, "SCADA system testbed for cybersecurity research using machine learning approach," *Futur. Internet*, vol. 10, no. 8, 2018, doi: 10.3390/fi10080076.

[61] S. Haykin, "Artificial Intelligence Communicates With Cognitive Dynamic System for Cybersecurity," *IEEE Trans. Cogn. Commun. Netw.*, vol. 5, no. 3, pp. 463–475, 2019, doi: 10.1109/tccn.2019.2930253.

[62] Y. Jia, Y. Qi, H. Shang, R. Jiang, and A. Li, "A Practical Approach to Constructing a Knowledge Graph for Cybersecurity," *Engineering*, vol. 4, no. 1, pp. 53–60, 2018, doi: 10.1016/j.eng.2018.01.004.

[63] J. Johnson, "Artificial intelligence & future warfare: Implications for international security," *Def. Secur. Anal.*, vol. 35, no. 2, pp. 147–169, 2019, doi: 10.1080/14751798.2019.1600800.

[64] V. Kanimozhi and T. Prem Jacob, "Artificial intelligence based network intrusion detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing," *Proc. 2019 IEEE Int. Conf. Commun. Signal Process. ICCSP 2019*, pp. 33–36, 2019, doi: 10.1109/ICCSP.2019.8698029.

[65] K. Chung, C. A. Kamhoua, K. A. Kwiat, Z. T. Kalbarczyk, and R. K. Iyer, "Game Theory with Learning for Cyber Security Monitoring," *Proc. IEEE Int. Symp. High Assur. Syst. Eng.*, vol. 2016-March, pp. 1–8, 2016, doi: 10.1109/HASE.2016.48.

[66] B. W. Wirtz, J. C. Weyerer, and C. Geyer, "Artificial Intelligence and the Public Sector—Applications and Challenges," *Int. J. Public Adm.*, vol. 42, no. 7, pp. 596–615, 2019, doi: 10.1080/01900692.2018.1498103.

[67] Y. Xin *et al.*, "Machine Learning and Deep Learning Methods for Cybersecurity," *IEEE Access*, vol. 6, no. c, pp. 35365–35381, 2018, doi: 10.1109/ACCESS.2018.2836950.

[68] E. van der Walt, J. H. P. Eloff, and J. Grobler, "Cyber-security: Identity deception detection on social media platforms," *Comput. Secur.*, vol. 78, pp. 76–89, 2018, doi: 10.1016/j.cose.2018.05.015.

[69] S. Mahdavifar and A. A. Ghorbani, "Application of deep learning to cybersecurity: A survey," *Neurocomputing*, vol. 347, pp. 149–176, 2019, doi: 10.1016/j.neucom.2019.02.056.

[70] Y. Lu, "Artificial intelligence: a survey on evolution, models, applications and future trends," *J. Manag. Anal.*, vol. 6, no. 1, pp. 1–29, 2019, doi: 10.1080/23270012.2019.1570365.

[71] B. Morel, "Artificial intelligence and key to the future of cybersecurity," *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 93–97, 2011, doi: 10.1145/2046684.2046699.

[72] G. W. Romney, J. Guymon, M. D. Romney, and D. A. Carlson, "Curriculum for hands-on artificial intelligence cybersecurity," *2019 18th Int. Conf. Inf. Technol. Based High. Educ. Training, ITHET 2019*, pp. 1–8, 2019, doi: 10.1109/ITHET46829.2019.8937373.

[73] "深度学习（Deep learning）那些事儿.pdf." .

[74] N. Scarpato, N. D. Cilia, and M. Romano, "Reachability Matrix Ontology: A Cybersecurity Ontology," *Appl. Artif. Intell.*, vol. 33, no. 7, pp. 643–655, 2019, doi: 10.1080/08839514.2019.1592344.

[75] V. D. Soni, "Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA," *SSRN Electron. J.*, pp. 1–17, 2020, doi: 10.2139/ssrn.3624487.