Transactions on Engineering and Computing Sciences - Vol. 13, No. 02
Publication Date: April 25, 2025
DOI:10.14738/tmlai.1302.18411.
Arvin, S., Hendricks, N., & Ketel, M. (2025). Artificial Intelligence, Cybersecurity, and a Growing Ethical Dilemma. Transactions on Engineering and Computing Sciences, 13(02). 19-28.

Artificial Intelligence, Cybersecurity, and a Growing Ethical Dilemma

Steven Arvin
Applied Information Technology Department,
University of Baltimore, Baltimore, MD 21201, USA

Nigel Hendricks
Applied Information Technology Department
University of Baltimore, Baltimore, MD 21201, USA

Mohammed Ketel
Applied Information Technology Department
University of Baltimore, Baltimore, MD 21201, USA

ABSTRACT

Currently, cybersecurity threats, particularly cyber-attacks, are a growing concern. As time goes on, it becomes increasingly challenging to hinder these attacks. Nevertheless, a new participant has entered the arena, known as artificial intelligence (AI). AI offers a way for cybersecurity experts to counteract the ever-evolving attacks. By utilizing techniques such as identifying threats and automated responses to incidents, organizations can enhance their security measures and safeguard confidential data. Despite the numerous advantages of adopting AI, it is equally important to remain vigilant about potential risks. In recent years, the rapid growth in cybersecurity threats has necessitated the development of more effective measures to protect sensitive information and systems. This paper delves into the ethical concerns of AI in cybersecurity, stressing the crucial balance between technological innovation and maintaining ethical standards.

Keywords: Cybersecurity, Artificial Intelligence, Machine Learning, Deep Learning, IoT, Ethics.

INTRODUCTION

Artificial Intelligence may seem like an overused buzzword to many, but its utility and application are growing with each passing day. Whether the logic component of an artificial intelligence opponent in online chess or the extra set of eyes to see trends in a financial market that a human would miss, Artificial Intelligence is everywhere. With this ground-breaking field advancing at a breakneck pace, there are drawbacks as well. Often, technology advances significantly faster than regulations and laws permit. This can result in business and personal practices that are ethically questionable at best and dangerous at worst. Sometimes, the best of intentions can come with negative consequences. This can be seen in the world of cybersecurity. Artificial Intelligence is readily being applied to cybersecurity systems to provide active threat avoidance and defense. However, Artificial Intelligence is also being utilized by bad actors to attack vulnerable systems and victims. Like all things, it takes a

balancing act, accepting the good with the bad. But first, it helps to have a grasp on what Artificial Intelligence and cybersecurity are, along with how they can interact [2].

However, even with a firm grasp on the capabilities, pitfalls, and dangers of AI applications, there is only so much a person can be expected to prepare for. In addition, a private citizen is unlikely to have the knowledge, access, or resources to procure and implement hardware, software, and experience into a personal list of best practices. These private citizens are susceptible to an online attack now more than any other time in history between the ubiquitous implementation of Internet of Things devices and the decision by many industries to move services to an online platform. Also, history hasshown that businesses will not always implement practices that protect the consumer and can even be found to take advantage of vulnerable parties. For this reason, large governmental organizations, such as the European Union and the United States Federal Government have begun to layout guiding principles for how both public and private entities will be expected to utilize AI for the safety of all parties involved. This is a step in the right direction, but time will tell where more emphasis will need to be placed. [11, 12].

UNDERSTANDING ARTIFICIAL INTELLIGENCE

In order to understand how Artificial Intelligence (AI) and Machine Learning (ML) can be applied to cybersecurity safeguards and systems, it is first important to understand what AI is and how it operates. While in the not-too-distant past, AI was reserved for science fiction media and people with wild imaginations, it has now permeated many facets of society. It can be found in the malicious mail filters on email servers, online customer service chatbots, and the backbone of the logic component in computer games, as well as video games. While these applications of AI may seem trivial or marginally beneficial to many, they are just a small glimpse into its capabilities and a foundation for the vast possibilities in its future [8].

For many day-to-day activities and applications, traditional programming can be applied to satisfy a requirement. This can be covered by utilizing fuzzy sets, data structures, algorithms, and rules. Unfortunately, these traditional programming methods are not all-encompassing though. There will always be scenarios where a traditional program is presented with a problem that it is unable to solve via the resources available to it. This is where AI can bridge the disconnect or shortcoming. For example, since AI and ML are, in most cases, an extension of human intelligence, their learning capabilities and analysis of historical trends can be applied to financial models [8]. While data on users as a significant driver of revenue for large online conglomerates such as Meta, Google, and others is a relatively new phenomenon, the need to mine financial data is a long-held premise. The trends of markets, goods, and Gross Domestic Product (GDP) are arduously studied by analysts globally, looking for any competitive advantage that can be leveraged. However, they are limited to the models available to them and the inferences they can make from them based on what they are taught, their personal experiences, and what logical conclusions they can draw themselves. AI and ML offer an additional avenue of insight. They can draw conclusions that would seem illogical to a traditionally trained analyst, but historically, see a pattern or trend that could generate or save a bank significant sums of money [2].

LEVERAGING MACHINE LEARNING TO ENHANCE CYBERSECURITY

Machine Learning at Glance

As stated above, ML is a quintessential component of AI as a whole. ML is the term for a computer or machine's ability to "learn". While these devices do not have consciousness like humans, they are able to sort through vast amounts of data and draw conclusions, as well as see patterns. This is an incredibly simplistic description of how ML occurs. An example of ML at work would be a program that reads handwriting. The best way to "teach" the program would be to feed it as many handwriting samples as possible. This can be done manually via sample collection, or a simple web scraping program can be developed to feed the program millions of handwriting samples, readily available for free online. The ML program will then digest these samples and draw a long list of conclusions that it will utilize when reading future handwriting. Some of the conclusions or rules the ML program may develop are the differences between print and cursive, what characters are letters, numbers, or symbols and then it could even begin to realize when punctuation is missing or used incorrectly. Over time, the program will continue to digest more and more data, making it better equipped to analyze what it is reading. The goal is that the longer this program is operational and refined, the better it will be at its job [8].

An Overview of Cybersecurity

While the term Cybersecurity is used on a near daily basis, in regular conversation, and from the news media, many may not appreciate what it actually means and what it entails. At its core, cybersecurity is every policy, procedure, software, application, and hardware interface, that are utilized to protect the integrity of a network and all of the information that is contained and transmitted throughout the host network. This can be comprised of firewalls, network intrusion systems, policies that outline what type of web traffic is permitted behind a network firewall, along with the permitted variety ofoutgoing web traffic and a host of other products and standard operating procedures. It is also important to appreciate the reason for the ever-increasing emphasis on cybersecurity. As technology and the internet continue to bleed into every facet of daily life, so does the need for data and financial protection, which all fall under the umbrella of cybersecurity. Analysts estimate that the average data breach costs an entity just shy of 4 million dollars to recover from and when the data breach is specifically directed at a company based in the United States, it climbs to over 8 million dollars. While these numbers alone should be enough to give many corporate executives pause when assessing their cybersecurity budgets, it is arguably more important to consider the personal user data collected and stored by many companies. Private financial data, medical records and personally identifiable information (PII), such as social security numbers are frequently collected by companies and stored for tax and identification purposes. If a company is unable to show they made an earnest attempt to protect this user data, they will lose the trust of their clients and potentially find themselves at the receiving end of a civil or even criminal court case. Thankfully, AI solutions can be implemented to help combat these breaches [9].

ML at Work in Cybersecurity

As mentioned earlier referenced, ML plays an invaluable role in AI implementation in cybersecurity systems. ML programs are developed over time by parsing and digesting large amounts of data. This can be as simple as tracking which ports are most frequently used by an

internal device or which outside clients are regularly attempting to connect to the network. These trends are then stored and analyzed by the ML system to develop internal rules and policies to best mitigate security breaches. Some of the mechanisms implemented by ML include tasks such as clustering, classification, and regression. Clustering is beneficial because it helps an ML system identify trends or similarities in data or network requests, aiding it in viewing patterns. Classification, on the other hand, relies on data it is fed from a repository or administrator, showing it different types of data and requests it can encounter, and then classifies future requests and data based on what it was taught. Finally, regression, which heavily relies on algorithms, does its best to form relationships between different inputs, helping it to better identify outliers or threats [9].

For consumers and businesses alike, the benefits of AI and ML are often most appreciated, but not necessarily noticed at the firewall level of defense. Viruses, malware, and ransomware can be distributed in a variety of ways, whether it be a phishing email or a nefarious link embedded in an image. However, the power of AI and ML, is that this threat can be detected well in advance of any human intervention and then quickly dispatched before any damage can be done. As soon as the ML system detects the threat, it can sequester it from the system it intends to infect, then after a quick analysis, it can remove it from the system, preventing any damage done. These systems have also been implemented at the authentication level of systems, notifying users if their login credentials are weak, making them susceptible to compromise, along with producing more robust authentication systems and procedures, such as iPhone's Face ID.

With the introduction of iOS 10 on iPhone in 2016, Apple introduced Face ID. Prior to the introduction of this software, face identification programs had exponential memory requirements, taking up more processing power than was available on all commercial cellular phones. The only solution, prior to Apple's development, was to send any facial recognition requirement to a cloud-based server, which could easily expend the needed processing power for the facial recognition check and would then send back an approval or rejection. However, since Apple takes user privacy seriously, they did not deem this solution as acceptable because it would require the software to send PII, such as personal photos over the internet, to be verified and then returned. The only way this program could move forward is if the check was performed within the phone itself. This then led them to produce a Deep Learning (DL) solution. This DL system leaned heavily on both classification and regression methods. The classification was utilized to simply help the program identify if there was a face being displayed. If no facial features were noted, the program would reject the ID. Then regression would make use of its relationships by determining which, preferably one, face was being used for the ID. The program had more intricate nuances, but these ML and DL principles were at the heart of how it operated [3].

EXPLORING DEEP LEARNING AND THE INTERNET OF THINGS

The Internet of Things or IoT is a term to describe all of the connected devices we encounter in our day-to-day lives. This could be the smart thermostat that controls your house's air conditioning or your smartwatch that is warning you that you haven't taken a break and stood up from your desk in several hours. Although these devices have expanded into nearly every facet of daily life, the science behind how they operate amongst one another can be

cumbersome. This iswhere AI and DL come into play. While the technology on the surface making these devices run is strictly quantitative, the thinking behind how it interacts with humans can be covered by the term Cyber-physical systems or CPS theory. This theory, at its core, strives to integrate internet-connected devices, often found in the IoTs, as seamlessly as possible into everyday human life [5].

This integration requires extensive AI and DL to make it effective at what it does, as well as provide a continual benefit to its users. Luckily, since IoT devices are so ubiquitous in society today, there is ample data for DL programs to work off of. However, the benefits of this readily available data for DL enhancement also come with a plethora of security concerns. It is a fact that data is a business today. In order to introduce IoT devices into everyday life, there needs to be an acceptance of risk. All connected devices are continually collecting data and this data is then being relayed to the host network. It is the responsibility of the host to do everything in their power to keep this data secure and protected from attackers. This does not mean that the data cannot be utilized for DL device enhancement. One way that companies utilizing CPS theory attempt to keep their user data secure is to limit the number of employees that have access to the closed-source software that is the brains behind their devices. This level of security is a form of cybersecurity [5].

IOT SAFETY, PRIVACY AND ETHICS

The sale and distribution of personal data is a lucrative endeavor for many tech companies. This, however, is a direct contradiction to some of the core tenets of IoT distribution. Privacy by Design is a principle that supports the development of IoT devices and the software that operates them, with privacy in the front of the engineer's mind. If privacy is put at the forefront of development, it will not need to be incorporated at a later point via a patch method [13, 14]. In a similar vein, safety is another core tenet of IoT development. Today, IoT devices are used in everything from smart thermostats in residential homes, all the way up to monitoring sensitive government locations, as well as industrial manufacturing facilities. It is of the upmost importance that these devices are secure and protected from outside intrusions, but also that they operate as promised. For example, if an IoT-connected smoke alarm in a residential home goes offline, could it prevent it from relaying a warning message to the other IoT-connected smoke alarms in the home? If so, the results could be deadly. Similarly, if a nuclear power plant deployed IoT-connected devices to monitor and regulate the performance of the reactor, it would be of the utmost importance that the devices were accurate, had redundant backups and incredibly secure from outside intrusion. If any of these parameters were not met to the highest standards, it could result in catastrophic loss of life and untold destruction to the surrounding environment [13, 14].

With safety and privacy in the forefront of IoT developer's minds, the final tenet is ethics. While an expectation of privacy and safety seems like a rudimentary starting point, it takes an ethical company and team of engineers for it to be implemented in practice. While innovation is needed and should be celebrated, it should be met with thorough evaluation and regulation. If innovation goes unregulated, the best of inventions can be used for the worst of means [14].

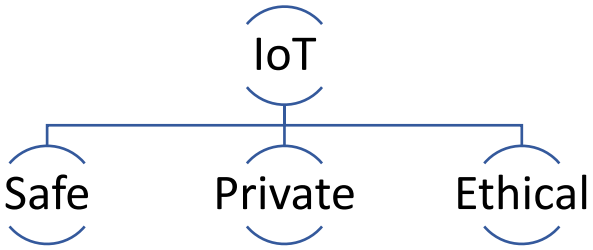

Figure 1: IoT and its core tenets

LEGALITY OF AI

Although the implementation of AI is exciting and scary for many, at an objective level, there are legal and ethical concerns with its expansion. While some describe it as an over exaggeration, or fear mongering, there is no question that in the coming years, some jobs, particularly in manufacturing and software development, will be replaced by AI. There is an ethical concern about what to do with the millions of workers in these fields that will be displaced from their jobs with no alternate sources of income. That is a socio-political conversation for another time. However, an immediateconversation will need to be had to address the ramifications of any illegal or even fatal consequences from the introduction of AI [6]. One example of this quandary can be found with the advent of self-driving vehicles. Once a pipe dream from a science-fiction movie, self-driving vehicles are quickly becoming a reality. While lobbying groups are quick to point out the benefits of self-driving vehicles, such as reduced congestion when adopted in masse, they are not quick to assign blame when the vehicle's miscalculation results in a fatality. Currently, if a person were to injure or kill someone else in a vehicular accident, they would be held accountable. If they were intoxicated or negligent, there is a possibility they could even serve time in jail. However, what happens if the person metaphorically behind the wheel of a self-driving vehicle, has no control over what it does? The "driver" would not have the means to avoid the crash because the vehicle and its AI-supported system would be telling the car what to do. But this would not bring solace or relief to the injured party. This is the conundrum faced by manufacturers and lawmakers alike. An argument could be made that the manufacturer of the vehicle and its AI-powered software would be responsible for the accident. Even worse, what if a Denial of Service (DoS) attack is unleashed on all self-driving cars during rush hour in a major city? Do you hold the manufacturer accountable because they didn't adequately secure their network or do you solely blame the attacker [1, 6]?

ETHICAL CONCERNS WITH AI

When discussing ethical concerns in the seemingly ubiquitous application of AI, the list can be endless. A recent paper published in the Proceedings of the 27th International Conference on Evaluation and Assessment in Software Engineering [10] takes a closer look at where ethical requirements in companies begin, along with their implementation. The paper, looking at the business and managerial practices of several Finnish software engineering departments, attempts to decipher how ethical concerns associated with AI are taken into account and then implemented into the code that makes AI work. It was quickly discovered that many of the decisions when it came to AI and business ethics were decided at the middle and executive

management level of companies. However, when the people holding these positions were interviewed, the researchers realized that ethical integrity in software engineering and specifically AI development is considered a very low priority because it has no direct correlation to profit and it is something that has little to no tangible effect on the end user [10]. Since managers place little emphasis on ethical design and application, these requirements then fall to the lower-level developers, who are responsible for crafting and deploying the code. Unfortunately, when the upper management does not place an emphasis on something, their subordinates will not value it either [10]. This methodology, however, is in direct disagreement with the standards set forth by the Institute of Electrical and Electronics Engineers (IEEE). Specifically, the IEEE STD 7000-2021 [7] recommends that all stakeholders, from executive level leadership, down to the lowest level of a team, all put an emphasis on ethical decision-making when producing anything with AI incorporated. Unfortunately, this is often not the case and is another reason why proactively incorporating ethics into AI development is important [10].

European Union Guidelines for Ethical and Trustworthy AI

Since AI has reached the mainstream level, numerous government entities have begun developing ethical and, slowly, legal requirements for AI-backed systems. One of these developments has been the European Union (EU) Ethics Guidelines for Trustworthy AI. These guidelines provide directions to member countries on how AI should be deployed and monitored, ensuring that its implementation is safe and equitable for all citizens. To summarize the items referenced in Table 1, the EU aimed to develop an AI policy that protects vulnerable users from malicious threats and corporate overreach, provides a level of privacy and accountability so users know whether their data is open to being compromised and most of all, holding people accountable that utilize AI in their business [11].

Table 1: Key Requirements and Descriptions of the EU Ethics Guidelines for Trustworthy AI

Key Requirements	Description
Human Agency and Oversight	AI-integrated systems should be implemented to aid and advance human development. While this action is occuring, efforts should be made to integrate humans into the decision-making process, via several different industry standard approaches, such as human-in-the-loop, human-on-the-loop and human-in-command.
Technical Robustness and Safety	AI systems have an obligation to be secure, accurate and reliable. There should be failsafes, double-checks and extensive security measures inherently built into AI systems, preventing catastrophic failures.
Privacy and Data Governance	Similarly to the previous requirement, secured data should be reliable and accessible only to those with the authority or need to access it.
Transparency	No one should ever encounter an AI-supported system that they are unaware of. It is the responsibility of the developers to make this abundantly clear to all users. In conjunction with this, the decision-making process of an AI-backed or generated system, should be explained in layman's terms to the user, so there is no confusion on what the system will generate or produce.

Key Requirements	Description
Diversity, Non-Discrimination and Fairness	Because of the risk of implicit bias, developers have a requirement to be proactive in their approach to ethical development of AI systems. An all-inclusive approach should be utilized when developing a new AI system, that does its best effort to include as many groups as possible, making a particular effort to include marginalized and often forgotten gorups.
Societal and Environmental Well-Being	The goal of AI should be to better society for everyone, past, present, and future. With this taken into account, any AI system should be sustainable and bring no harm to the environment.
Accountability	A clear responsible party should be known for any and all decision-making by an AI system.

United States Executive Order for AI Implementation

Although the United States is a single country compared to the many countries that make up the EU, they do not have a clear, delineated AI policy or set of laws that need to be followed in their country. The closest thing they have is an Executive Order, enacted by the President of the United States, providing guidance for how Federal government entities will utilize AI, as well as how it can be better managed and implemented in the future. [12]. Much like the EU policies, the Executive Order outlines the intent of ethical innovation that protects end users, especially those most vulnerable. These policies are outlined in eight policy and procedure points that spell out the expectations of government agencies as well as corporate entities when it comes to the development and implementation of AI. These points cover things such as the expectation of safety, security, and integrity in the systems being utilized. For example, a medical insurance company that has numerous databases full of Personally Identifiable Information (PII) from its users would need to take extra steps to ensure that any AI program with access to these databases would be secure. Failure to do so could be catastrophic to the citizens covered by the company. In addition to the safety and security of the systems deploying AI-backed programs, the civil rights of American citizens are of utmost importance as well. As technology advances, the rights of the most vulnerable still need to be upheld. Failure to do so would be unethical at best and could result in legal ramifications at worst. This is to make it clear that although AI is a new technology, civil rights laws and policies still apply [12]. Unfortunately, the executive order does not provide any insight into the potential ramifications if a corporation or entity were to overstep and utilize AI for exploitation or nefarious purposes. Without this key facet in the order, it is merely a list of requests with no possibility of punishment. For this executive order to carry more weight, a law enacted by the United States Congress will most likely need to be put in place [12]. The key requirements and descriptions of the United States Executive Order on AI deployment are summarized in Table 2.

Table 2: Key requirements and descriptions of the US Executive Order on AI deployment

Key Requirements	Description
Safety and Security	The goal of all AI is safety and security. In order for this to be implemented, the policies and procedures surrounding AI should be clear, all-encompassing and easily digestable. This will be achieved through extensive testing, review, critique, and adjustment.

Key Requirements	Description
Promote Innovation and Competition	While safety and security are paramount, the development and implementation of AI is critical for the US Government and the companies based there. For this reason, the US Government will make investments in industries moving AI forward, encouraging accessibility to those most in need.
Inclusion	The innovations and development of AI would not be possible without the hard work of the American people. For this reason, the US Government will invest in programs and resources to train a diverse group of citizens in this new and fast-paced industry.
Civil Rights	All industries that deploy AI have an expectation to increase diversity and show respect for all user's civil rights. Any indication of the contrary will draw the ire and legal repercussions of the US Government.
Corporate Obligation to Safety	As AI increasingly bleeds into daily life, corporate entities, as well as government agencies, have an obligation to protect their users when interacting with AI. This is of the utmost importance in industries interacting with vulnerable populations such as healthcare, transportation, education, housing, and many others.
Integrity and Security	With Personally Identifiable Information (PII) regularly being submitted and exchanged online, AI can be seen as another avenue to compromise citizen's personal data. It is critical that all entities utilizing AI guarantee they are exhausting all tools to secure and protect sensitive user data.
World Leader	The United States is seen as the leader of the free world and should act accordingly. All eyes will be on the nation as AI is developed and deployed. Because of this, it is essential that all of these principles are upheld.

CONCLUSION

The perils of new and evolving technologies are a tale as old as time. While the possibilities seem endless and arguably are, the dangers and vulnerabilities cannot be discounted. AI has already begun to bleed into many facets of daily life for most people, but the current implementation is arguably just a taste of what is to come. For these reasons, ethical companies and government regulation will be essential to the evolution and distribution of these systems. If ethical policies aren't at the forefront of policy maker's minds, the vulnerable will suffer as a result. This is why ethical innovation is essential to the ever-advancing world of technology. This paper provided a comprehensive overview of the ethical considerations that must be considered as AI becomes an integral part of cybersecurity practices. The ability tobalance technological progress with responsible ethical practices that prioritize human well-being and security was also discussed.

References

[1]. AI & Robotics. Tesla. (n.d.). https://www.tesla.com/AI

[2]. Al-Shabandar, R., Lightbody, G., Browne, F., Liu, J., Wang, H., and Zheng, H. (2019). The application of Artificial Intelligence in financial compliance management. Proceedings of the 2019 International Conference on Artificial Intelligence and Advanced Manufacturing. https://doi.org/10.1145/3358331.3358339

[3]. Apple. (2017, November). An on-device deep neural network for face detection. Apple Machine Learning Research. https://machinelearning.apple.com/research/face-detection

[4]. Ghelani, D. (2022). Cyber security, cyber threats, implications and future perspectives: A Review. American Journal of Science, Engineering and Technology. https://doi.org/10.22541/au.166385207.73483369/v1

[5]. Ghillani, D. (2022). Deep learning and artificial intelligence framework to improve the cyber security . American Journal of Artificial Intelligence. https://doi.org/10.22541/au.166379475.54266021/v1

[6]. Lin, H., Yu, Z., Peng, S., & Bian, B. (2021). Security issues in commercial application of Artificial Intelligence. 2021 3rd International Conference on Artificial Intelligence and Advanced Manufacture. https://doi.org/10.1145/3495018.3495359

[7]. JI Olszewska, Systems and Software Engineering Standards Committee (2021), IEEE Standard Model Process for Addressing Ethical Concerns During System Design: IEEE Standard 7000-2021. https://doi.org/10.1109/IEEESTD.2021.9536679

[8]. Rodríguez-García, J. D., Moreno-León, J., Román-González, M., & Robles, G. (2021). Introducing Artificial Intelligence Fundamentals with LearningML: Artificial Intelligence made easy. Eighth International Conference on Technological Ecosystems for Enhancing Multiculturality. https://doi.org/10.1145/3434780.3436705

[9]. Gautam Srivastava, Rutvij H Jhaveri, Sweta Bhattacharya, Sharnil Pandya, Rajeswari, Praveen Kumar Reddy Maddikunta, Gokul Yenduri, Jon G. Hall, Mamoun Alazab, Thippa Reddy Gadekallu (2022). XAI for Cybersecurity: State of the Art, Challenges, Open Issues and Future Directions. Association for Computing Machinery). https://doi.org/https://doi.org/10.1145/1122445.1122456

[10]. Agbese, M., Mohanani, R., Khan, A., & Abrahamsson, P. (2023). Implementing AI ethics: Making sense of the ethical requirements. Proceedings of the 27th International Conference on Evaluation and Assessment in Software Engineering. https://doi.org/10.1145/3593434.3593453

[11]. Ethics guidelines for Trustworthy AI. Shaping Europe's digital future. (n.d.). https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

[12]. The United States Government. (2023, October 30). Executive order on the safe, secure, and trustworthy development and use of artificial intelligence. The White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

[13]. Derek Johnson and Mohammed Ketel, (2019). IoT: Application Protocols and Security, International Journal of Computer Network and Information Security.

[14]. Atlam, H. F., & Wills, G. B. (2019). IoT Security, Privacy, Safety and Ethics. Internet of Things. https://doi.org/10.1007/978-3-030-18732-3_8