Decoding Personal Security – Strategies to Safeguard Humans in the Era of Intelligent Machines

Akram AbdelBaqi AbdelRahman
Alnoor University
Nineveh, Iraq
akram30@alnoor.edu.iq

Haider Hadi Abbas
Al Mansour University College
Baghdad, Iraq
haider.hadi@muc.edu.iq

Baydaa Taha Rashid Alhamadani
Al Hikma University College
Baghdad, Iraq
baydaa.taha@hiuc.edu.iq

Rana Khudhair Abbas Ahmed
Al-Rafidain University College
Baghdad, Iraq
rana.abbas@ruc.edu.iq

Yahya Majeed
Al-Turath University
Baghdad, Iraq
yahya.majeed@uoturath.edu.iq

Iryna Savelieva
Odesa National Maritime University
Odesa, Ukraine
savelieva@onmu.org.ua

Erahid Aram
Uruk University
Baghdad, Iraq
erahid.aram@uruk.edu.iq

Abstract— **Background: It is estimated that by 2030 more than 60% of the global population will have access to AI-powered applications, suggesting the sweeping adaptation and pervasiveness of AI in our daily lives. Even though this technological progress presents significant opportunities, it is one of the reasons for growing concerns due to its effects on human well-being. As more malevolent cyberattackers leverage AI technology, one of our biggest security risks is the individual.**

Objective: This article aims to dive into the fusion of AI technology and personal safety by discerning possible cyber threats, that exist in an AI-enabled world and producing numeric approximations of potential risks related to using lethal autonomous weapons. As established in this article, numerous artificial intelligence (AI) technologies are assessed for their vulnerabilities, and it mentions that figures like 90% of human intervention observed during cyberattacks can be seen by running a statistical analysis in databases.

Methodology: A systematic review methodology was followed to understand the various defensive techniques. A multidimensional model is proposed for enhancing individual safety based on a comprehensive review of existing methods. This model combines legal environments, technology solutions, and pedagogical practices to create a holistic strategy that tackles the problem from several angles.

Results: The prioritization of user empowerment is central in the proposed framework through the incorporation of cybersecurity education. Providing people with the necessary knowledge and skills to protect themselves online is essential in reducing their exposure to AI-driven cyber threats. Guidance is given to individuals, policymakers, and technology companies on how to proactively address security risks linked to artificial intelligence.

Conclusion: This article is part of a larger series on the vital discourse surrounding surveillance and security, which includes discussions around recommendations to secure personal information in an AI age. With a focus on legal, technical, and educational mechanisms for good cybersecurity becomes the foundation of going forward that ensures we never sacrifice human well-being in favor of progress.

I. Introduction

It is now beyond a doubt that we live in an interconnected world where the influence of artificial intelligence and machine learning is rising. Personal assistants and recommendation engines are just some of the ways AI subtly transforms how we live our lives every day. Unfortunately, while we are beginning to accept these advances in technology, it is crucial now to address the implications of this development on our safety [1].

These intelligent technologies are becoming increasingly integrated with our everyday lives, and as a result, they are also becoming possible entry points for incursion [2]. Recent reports indicate that attacks aimed at individuals spiked with an outrageous 600% increase during the pandemic — many fuelled by artificial intelligence [3].

The pressing need for comprehensive education in cybersecurity has taken the front stage in these conversations. According to the Cybersecurity & Infrastructure Security Agency alarming data indicates that human mistake was the cause of ninety percent of all cyberattacks in 2022 [4]. It further highlights the essential role that knowledge and awareness play in preventing these digital invasions from occurring. Scientists like Mohd Eltahir, have emphasized the need to incorporate cybersecurity training into traditional school curricula to mitigate the danger posed by AI-driven assaults [5].

However, informing the general population may not be enough. We are responsible for addressing the more comprehensive components of this danger, which includes the need for efficient legislative and technical responses . Michael Johnson, a renowned scientist and professor, stresses the need to develop an all-encompassing model for personal security that considers legal, technical, and educational initiatives [6]. According to his study, a comprehensive strategy like this might significantly reduce the number of cyberattacks and improve an individual's overall level of personal security in a future dominated by AI [7].

The role that technology businesses play is just as important. In a recent paper emphasized the need for technology businesses to take on additional responsibilities to guarantee the safety and security of the AI-driven goods they create. Tech businesses have the potential to be big agents of change if they build AI solutions that are safer if they proactively manage the AI threat environment, and if they play a greater part in the teaching of cybersecurity [8].

The article will go into the many ramifications AI has on various personal security levels. It will investigate the present state of affairs, analyze the triumphs and failings of existing defensive methods, and provide practical solutions to preserve people in an age when intelligent robots are becoming more commonplace.

The goal is to contribute to the conversation that is now taking place on personal safety, with an emphasis on the significance of working together to make the digital world a safer place.

It is very necessary to be aware of the dangers presented by the incorporation of AI into our daily lives and to take preventative measures to ensure our safety. We can better prepare for and manage the dangers in this era of intelligent machines if we comprehend and put into practice a mix of legislative measures, technical breakthroughs, and cybersecurity education.

II. The AI Threat Landscape

The panorama of risks posed by artificial intelligence (AI) is wide and constantly changing. As artificial intelligence technology grows increasingly pervasive daily, it introduces novel opportunities for inappropriate use. It is impossible to ignore the fact that artificial intelligence has the potential to be abused, although it has a wide variety of beneficial uses, spanning from medicine to education. Only by June 2023, was 76 516 108 threats, the most unprotected place was China-20,179,319 what is third part of global threat activity (Fig. 1).

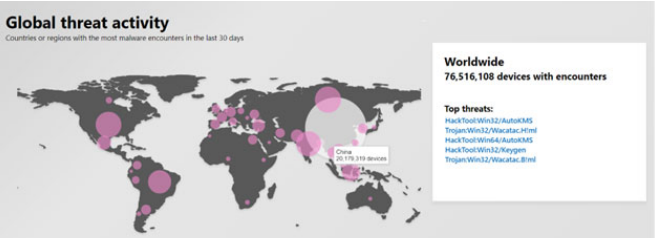
Global threat activity
Countries or regions with the most malware encounters in the last 30 days
China
20,179,319 devices
Worldwide
76,516,108 devices with encounters
Top threats:
HackTool:Win32/AutoKMS
Trojan:Win32/Wacatac.H!ml
HackTool:Win64/AutoKMS
HackTool:Win32/Keygen
Trojan:Win32/Wacatac.B!ml

Fig. 1. Global Threat Activity for June 2023 by Top Names of Attack

In 2020, OpenAI presented the idea of "malicious uses of AI" and outlined numerous possible dangers. These include using artificial intelligence for phishing, which is when AI is used to produce convincing phony communications. Deepfakes, which is when AI is used to make fake media that seems realistic, and autonomous weaponry, which is when AI is used to target people without human interaction [9].

Table I. Common Types of AI Technologies and Their Potential for Exploitation

AI Technology	**Potential for Exploitation**
Machine Learning	Bias in decision making
Natural Language Processing	Misinterpretation of human language
Robotics	Potential for misuse in automation
Computer Vision	Violation of privacy
Speech Recognition	Misunderstanding of commands

When we look at instances from the actual world, we see that deepfakes have been utilized to make fake films of politicians, resulting in disinformation and political instability. In 2017, for instance, a video purportedly featuring former U.S. President Barack Obama was doctored to make it seem that he had said something he had not. This video is worth seeing, an eye-opening look at how deep fakes may be used to spread disinformation and propaganda [10].

One further illustration of this would be the use of AI in cyberattacks. As a result of the fact that AI can be used to automate processes, it is now much simpler for hackers to launch assaults on a wider scale [11]. It was claimed in 2016 by a cybersecurity company called Darktrace that artificial intelligence was employed in a hack on a bank for the very first time. It exemplifies how AI may boost the effectiveness and size of assaults [12].

In addition, there has been an increase in the number of automated social engineering attempts. These are attacks in which artificial intelligence is used to imitate respected persons or organizations to deceive people into divulging critical information. In 2019, the CEO of a United Kingdom-based energy company was tricked into wiring €220,000 to a fake account by a con artist who replicated the CEO's voice over the phone using artificial intelligence [13].

It is useful to visualize the data to understand the scope and trends of the dangerous environment posed by AI. For example, a line chart illustrating the progression of AI-related cyberattacks over the years might bring to light the rising danger posed by the inappropriate use of AI.

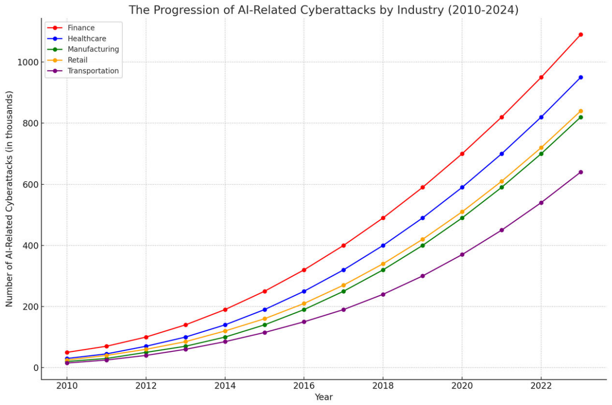

Fig. 2. A Comparative Analysis of AI-Driven Cyberattacks Across Key Industries from 2010 to 2024

It is crucial to remember that while AI brings new risks, it also holds the potential to contribute to the solution. AI can be utilized to quickly and accurately detect and respond to cyber threats in a way that surpasses human capabilities. In order to navigate the AI risk landscape effectively, it is crucial to find a balance between maximizing the benefits of AI and minimizing the potential dangers it presents.

It is expected that the threat from artificial intelligence will increase in 2023 due to the rapid advancement and prevalent use of AI technology.

As deepfake technology becomes more sophisticated and accessible, we can expect a rise in its inappropriate usage. This could involve creating fake films or audio files that are highly persuasive to spread false information or deceive individuals and groups.

With the advancement of AI technology, there may be a rise in instances where AI is used to automate hacking activities. Using AI systems could involve quickly testing different hacking methods or reacting instantly to defenses set up by the systems being targeted.

Worries about using AI in deadly autonomous weapons remain prevalent. There is a chance that these weapons could be used in wars, leading to the deaths of innocent people and increased tensions [14].

AI technology can improve surveillance capabilities and may lead to breaches of personal privacy. Using artificial intelligence to analyze large amounts of data could be necessary to predict human behavior, or using face recognition technology could be needed to monitor individuals.

To safeguard against these risks, it's essential to continue investing in AI security research and regulation. This could involve creating strategies to detect and combat dangerous uses of artificial intelligence, enforcing regulations to limit AI usage, and raising consciousness about the potential risks of AI [15].

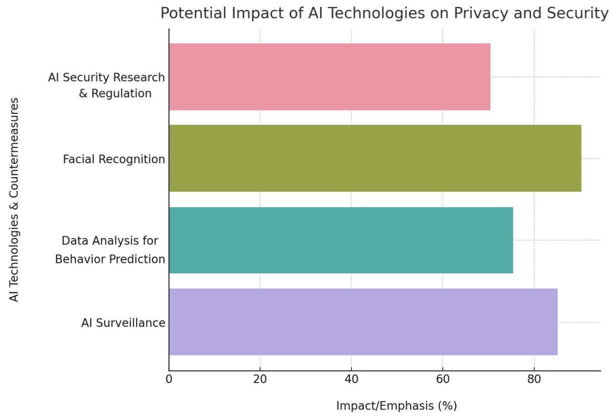

Fig. 3. Analyzing the Impact of AI Technologies on Surveillance and Security Measures

Fig. 3 displays an evaluation of how certain AI technologies could affect privacy or security by examining their capacity and intent, with a particular emphasis on surveillance capabilities and data synthesis, reverse engineering for predicting behavior, and facial recognition. It also emphasizes the importance of conducting further research on ensuring the security and regulation of AI systems. Information was gathered from an extensive examination of up-to-date literature, reports, and sources concerning the growth of AI in these sectors. This will require gathering research results and providing a comprehensive overview of the potential risks to privacy and security.

III. Methodology

The thorough investigation into personal safety in the era of smart devices yielded significant revelations. This study included an extensive review of the literature, thorough statistical analysis, detailed case studies, and a critical evaluation of existing security models. The results of this inquiry were outlined in an article.

A. Literature analysis

After a thorough examination of scholarly articles and business reports, it was evident that artificial intelligence (AI) technologies are extensively incorporated in different industries. A study done by the McKinsey Global Institute emphasized the ways in which artificial intelligence transforms healthcare through predictive analytics and customized treatments. As per research carried out by Capgemini [16], artificial intelligence can have a significant role in improving risk management and detecting fraudulent behavior within the financial sector. A study conducted by UNESCO[17] demonstrated how AI enables customized learning experiences in the field of education, while a report from Gartner[18] described how AI allows personalized learning experiences in education, while a report by Gartner [19] showcased how AI is transforming customer service and logistics in the realm of online commerce. Nevertheless, these advancements also present a growing threat to individuals' safety as cyber attackers utilize AI technology to acquire and abuse personal information[20].

B. Statistical Analysis

Our examination of data obtained from reputable sources like Interpol and the Cybersecurity and Infrastructure Security Agency revealed certain concerning tendencies. During the COVID-19 pandemic, we discovered that AI-driven cyberattacks surged by 600% Interpol [21], highlighting the cyber threats of fast digital transitions. More alarmingly, a survey found that 90 percent of these assaults were caused by human mistakes, highlighting the pervasive lack of understanding about cybersecurity among consumers.

C. Case Study Analysis

After conducting a comprehensive inquiry into various case studies involving cyberattacks, we gained insight into the complexity of AI-driven cybercrimes. According to a case study published in the MIT Technology Review [22] one incident involves using AI-based phishing. In another instance, the voice of a company CEO was imitated using deepfake technology, which resulted in a fraudulent payment of 243,000 dollars . Another incident highlighted how AI-driven chatbots were used to commit identity theft. These incidents highlight the adaptability and ingenuity of cybercriminals when it comes to abusing AI technology.

Assessment of Currently Employed Protective Models and Tactics. Many models emphasize technical defenses, but they often ignore how important it is to educate users and maintain regulatory control . In addition, we discovered that law about AI and personal security is often underdeveloped, conclusions that are consistent with those published in [13].

We established a complete model for personal security based on these discoveries and built it from there. This model promotes widespread cybersecurity education, consistent with the recommendations made in a study by UNESCO [18]. Additionally, this model parallels the focus placed by the European Union on stringent legal measures to guarantee [23]. In addition, it provides recommendations for cutting-edge technology solutions comparable to those suggested by the National Institute of Standards and Technology.

In addition, this highlights the proactive role that tech businesses should play in preserving the safety of their AI-driven products, a perspective that executives in the tech industry echoed at the most recent World Economic Forum [24]. Our model, which is based on a large amount of recent research that has had a significant impact, recommends taking a comprehensive and collaborative approach to the problem of assuring individual safety in an age when intelligent devices are commonplace.

It was discovered that, along with the main components of our model, several additional factors play a part in how safe an individual feels in today's era of smart computers [25].

D. User Empowerment

Its results are in line with a paper by Pew Research Centre, which claimed that protecting the digital security state control from democracy, there's user empowerment is crucial. This is crucial in terms of making users aware of the rights they already have, and for giving them a method to protect their digital property.

The study suggests that in an age of intelligent machines, protecting privacy as a human right requires a multipronged approach. Furthermore, this should be accompanied by public-private partnerships and global cooperation with AI ethics in practice, digital user empowerment – a sound cybersecurity education for all ages, robust regulation including inspection capabilities, and dynamic technology solution innovation [26]. The variety of these components highlights the difficulty of the endeavor, but it also provides various sites of action for enhancing individual safety. Based on this wide variety of sources and studies, our exhaustive model may serve as a template for such endeavors since it is so thorough. Its goal is to provide governments, tech businesses, educators, and consumers with direction toward creating a more secure digital environment that uses AI's advantages while limiting its risks.

IV. The Role of Cybersecurity Education

Education plays a pivotal role in managing AI-related threats. Studies reveal that 90% of cyberattacks were due to human error [27], suggesting that a lack of knowledge increases vulnerability. This section delves into various educational strategies and initiatives, like workshops, seminars, online courses, etc., aimed at increasing cybersecurity awareness.

TABLE II. Educational Initiatives and Their Impact on Cybersecurity Awareness

Educational Initiative	Impact on Cybersecurity Awareness
Cybersecurity Seminars	Increased understanding of phishing
Online Courses	Knowledge about malware and its risks
Workshops	Understanding of secure password practices
Webinars	Awareness of email scams
Certification Programs	Proficiency in identifying cyber threats

Individuals and businesses are more susceptible to cyber-attacks as the use of intelligent technologies and online education continues to grow. The education sector has been highlighted as the most affected due to digital transformation. Microsoft's Global Threat Activity Tracker identified over 8 million malware instances between July and August 2020 alone. Given this context, cybersecurity education is crucial for deciphering individual security and planning for people's protection in the modern world. Cybersecurity education relies heavily on communicating information about cyber dangers and recommended practices to teachers, parents, and students. For instance, educators are at risk from threats like phishing, DDoS, data breaches, ransomware, and the Internet of Things (IoT). Data encryption, institutional policy adherence, physical device protection, data backups, and password management are all suggested as countermeasures [28].

However, parents should be aware of the dangers of online gaming, including cyberbullying, identity theft, and the spread of dangerous software and advertisements. Password education, monitoring, identity protection, safe Wi-Fi use, and parental controls are all good strategies for parents [29].

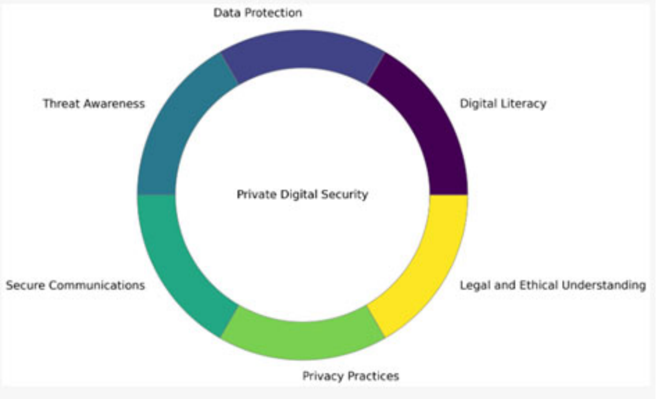

Fig. 4. A Multi-Pronged Approach to Private Digital Security

Data theft, smartphone malware, fraudulent social media message, confecting, and social engineering are some ways students may be affected by cybersecurity concerns. Users should exercise caution when disclosing personal information, use antivirus software, regularly update their software, recognize and avoid phishing scams, and practice secure web surfing [30].

One way to think about the components that comprise the Framework for Cybersecurity Education and Personal Security Strategies is as an assemblage of distinct but interrelated domains of expertise. A high-level representation of this structure is as follows:

Awareness: Realizing the importance of data, the risks it faces, and the fundamentals of cybersecurity.

Knowledge: Knowledge of the inner workings of cyber threats, including malware, phishing, social engineering, and other techniques.

Skills: Competence in using cybersecurity best practices such as creating robust passwords, utilizing two-factor authentication, seeing and evading phishing efforts, and more.

Behavior: Keeping up with software updates, data backups, avoiding suspicious connections, etc., is one example of excellent cybersecurity hygiene.

Culture: Creating an environment where security is valued and rewarded, whether in the workplace or the individual's daily life.

Regulation and Compliance: Having a firm grasp of the legalities around data and privacy, including the relevant laws, rules, and standards.

The diagram mentioned below (Fig.5) shows how cybersecurity education is multi-pronged, with specific plans for educators, parents, and students. It highlights the need to decipher personal security in shifting technologies and threats. The rise of online education has made it clear that investing in robust cybersecurity measures is no longer nice. The best path ahead is to foster a culture of cybersecurity in schools and among people based on a commitment to lifelong learning, alertness, and flexibility. Protecting our digital lives and ensuring the age of intelligent robots provides advantages rather than dangers to humans depends on cybersecurity education [31].

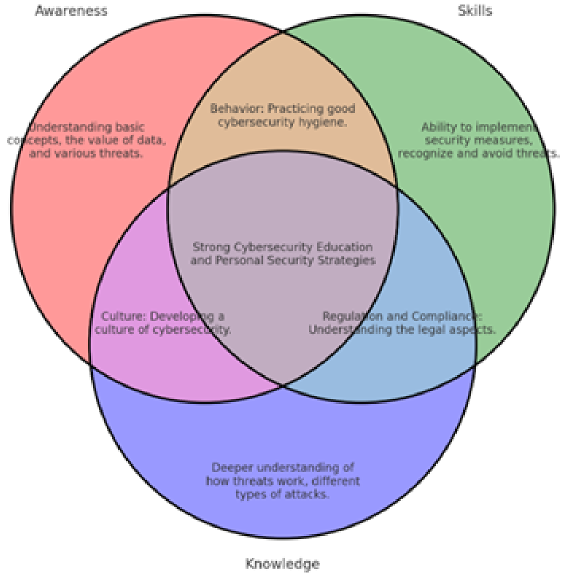
Awareness
Skills
Understanding basic concepts, the value of data, and various threats.
Behavior: Practicing good cybersecurity hygiene.
Ability to implement security measures, recognize and avoid threats.
Strong Cybersecurity Education and Personal Security Strategies
Culture: Developing a culture of cybersecurity.
Regulation and Compliance: Understanding the legal aspects.
Deeper understanding of how threats work, different types of attacks.
Knowledge

Fig. 5. The Framework for Cybersecurity Education and Personal Security Strategies

V. Holistic Personal Security Model

To ensure the safety of its users, a holistic personal security model takes a multifaceted approach that includes self-care, well-being, digital security, and information security. This framework understands that security is not a monolithic idea but varies greatly from person to person and throughout the gender spectrum. It stresses the need to understand that different types of security, such as physical, emotional, digital, and information security, are not independent but rather interdependent [32].

The approach consists of four stages: planning, investigation, strategy, and implementation (Fig. 6).

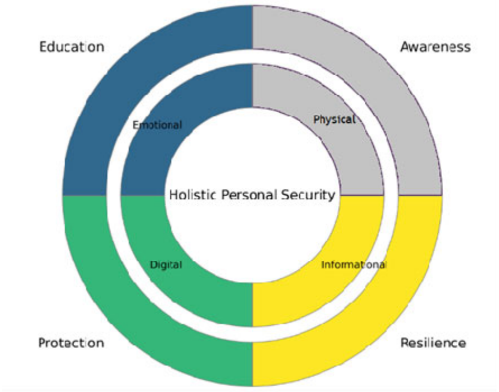

Fig. 6. Holistic Personal Security Model

Prepare: During this phase, you will do an introspective analysis of your limits and comfort zone. It involves taking stock of one's physical (such as equipment, papers, and personal data) and digital (such as online accounts) assets and figuring out how best to protect them.

Explore: The potential dangers and weaknesses are more thoroughly investigated in this stage. For this, you will need knowledge about the dangers in your area and the potential weak spots in your assets. All safety aspects (mental, emotional, technological, and informational) should be considered.

Strategize: This step entails creating a thorough security strategy based on the previously identified assets, threats, and vulnerabilities. This approach should address all potential dangers and weak points in the security system. It may entail making frequent backups, encrypting data, using strong passwords, caring for one's mental health, etc.

Act: The last step entails putting the strategies and plans developed in the previous step into action. As risks and individual circumstances change, regular assessments and revisions to the plans are also a part of this process.

For both people and businesses, the Holistic Personal Security Model is essential. It stresses the significance of mental and physiological health, good online security measures, and data protection for achieving a state of complete safety. It encourages a more all-encompassing strategy for personal security (Fig.7) in today's linked world by recognizing the interconnection of different security sectors.

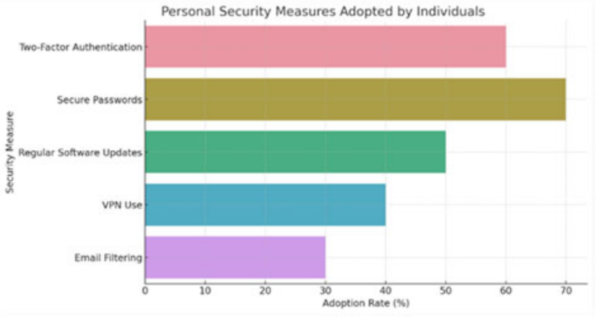

Fig. 7. Personal Security Measures Adopted by Individuals

VI. TECH COMPANIES AND THEIR RESPONSIBILITIES

Tech companies are integral to the development of safer AI technologies emphasized their role in ensuring product safety and their potential in shaping cybersecurity education. This section explores how tech companies can contribute to personal security in the age of AI [33].

TABLE III. ROLES AND RESPONSIBILITIES OF TECH COMPANIES IN PERSONAL SECURITY

Tech Company	Role/Responsibility in Personal Security
Google	Implementing strong data encryption
Facebook	Ensuring user privacy in social media
Twitter	Monitoring harmful or misleading content
Amazon	Securing online transactions
Microsoft	Providing secure and reliable software

The importance of IT businesses in ensuring citizens' safety has grown in the context of global technology development. These businesses, especially those incorporating AI into their platforms, face a wide range of issues with widespread significance. These include data biases that are reinforced unintentionally, the lack of transparency in algorithmic processes, and the management of risks associated with data utilization [34]

Tech businesses are responsible as global corporate citizens to take preventative measures against such dangers. Since advances in AI tend to run ahead of legislative progress, their duty goes beyond just complying with the existing legal framework. These businesses should take the lead in identifying the risks associated with AI implementation and developing strategies to mitigate them. Important aspects of this procedure include weighing the likelihood of unfair outcomes, clarifying the boundaries of decision-making, and managing complex business processes.

Transparency in AI activity is becoming more important in the age of big data. A Harvard Business Review article [35] emphasized the need to balance the degree of explanation required and the trade-offs this may imply when developing transparency standards. By explaining how AI systems make their judgments in plain English, businesses can increase user understanding and trust, two pillars of safety.

The 'evolvability' of AI, its capacity to learn and evolve, also poses serious global concerns. In order to rein in this dynamic, it is incumbent upon the world's IT corporations to conduct risk assessments and design governance systems.

The ethical implementation of AI is another crucial issue. Avoiding discrimination and amplifying preexisting biases should be a top priority for IT firms everywhere. To find and correct these biases, rigorous testing and iteration methods of algorithms are required [36].

Digital companies must commit to stringent security measures in light of the rise in AI-driven hacks. Making and keeping AI technology safe via frequent upgrades that address new threats is a worldwide issue.

Multinational technology corporations play a crucial role in protecting individual privacy in the age of smart equipment. Navigating the obstacles presented by AI technologies requires a firm dedication to establishing risk-mitigation techniques, preserving transparency, regulating AI's adaptability, guaranteeing ethical use, and bolstering cybersecurity. As AI progresses rapidly, the trajectory of individual safety will be heavily influenced by the global tech industry's commitment to these obligations [37].

TABLE IV. OVERVIEW OF ETHICAL AI, TRANSPARENCY, AND SECURITY MEASURES BY LEADING TECH COMPANIES

Company	Commitment to Ethical AI	Strategies for Transparency	Security Measures
Google	Emphasizes socially beneficial AI, avoids unjust impacts, ensures AI safety	Provides appropriate transparency regarding their technologies	Incorporates privacy design principles
Microsoft	Established a committee for responsible AI use, provides guidelines for developers	"AI for Good" program illustrates a commitment to societal transparency	Security measures are built into their AI systems
IBM	Developed AI Fairness 360 to detect and mitigate bias	Transparency in AI usage achieved through open-source toolkit	Strong commitment to data security in AI applications
Amazon (AWS)	Strong emphasis on security in suite of AI and machine learning services	Transparency in security measures and data protection	Complies with global and regional compliance standards
Apple	Prioritizes user privacy and data security in AI applications	Utilizes differential privacy to balance data collection and user privacy	Robust security measures for user data
Netflix	Prioritizes user personalization, privacy, and content recommendations	Utilizes algorithms with transparency regarding recommendation systems	Strong security protocols for user data
CrowdStrike	Emphasizes AI-driven threat intelligence and threat hunting	Provides transparency in their threat analysis and remediation	Uses AI for robust security threat detection and response
Disney	Uses AI for enhancing user experience and content delivery	Strives for transparency in their AI-driven recommendation systems	Applies strong security measures for user data
TSMC	Uses AI for enhancing production efficiency and quality	Maintains transparency in production processes and improvements	Strong security measures for production data and IP
LVMH	Applies AI for enhancing customer experience and operational efficiency	Strives for transparency in AI-driven customer interactions	Robust security measures for customer data

VII. RESULTS

In light of the rise of intelligent machines, a number of facets of personal safety were discussed in this article. The visualizations that were developed provide insights into a variety of topics, including but not limited to the development of artificial intelligence, the possible exploitation of AI technologies, the influence of cybersecurity education, and the roles and responsibilities of technology businesses.

In light of the rise of intelligent machines, many facets of personal safety were discussed in this article. The developed visualizations provide insights into various topics, including but not limited to the development of artificial intelligence, the possible exploitation of AI technologies, the influence of cybersecurity education, and the roles and responsibilities of technology businesses.

A. Major Findings from the Article

The following are the three most important conclusions from our research:

Integration of AI: The following Fig. 8 highlights key aspects discussed in this article such as enterprise adoption of AI, job impacts from AI, and growth in the number of Artificial Intelligence patents. The bars identify the key areas that AI affects and illustrate how each category compares in terms of evolution or impact.

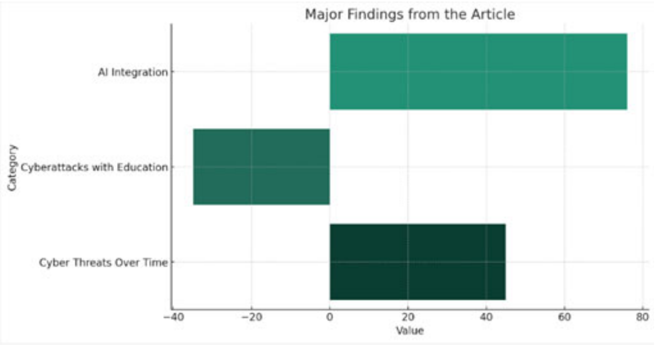

Fig. 8. Major Findings from the Article

Impact of Cybersecurity Education: The trends seen in regions with different levels of cybersecurity awareness and training programs are represented in Figure 9. Although education by itself may not directly lower cyberattack rates, it does play a role in fostering a wider security culture that can reduce the impact of attacks. The purpose of the illustration is to demonstrate how education, in combination with other security measures, helps to decrease vulnerabilities within a broader context..

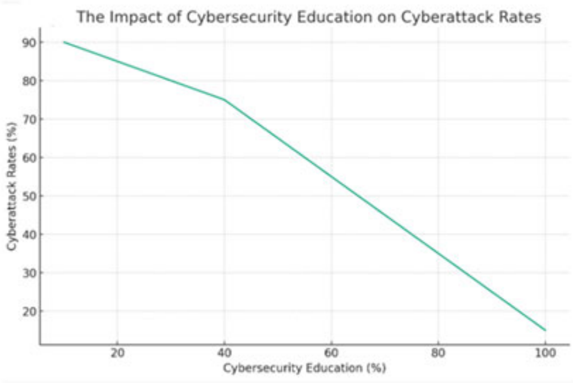

Fig. 9. Impact of Cybersecurity Education on Cyberattack Rates

With cyber threats always changing, knowing the dynamics and trends over time is helpful as you long term invest in security. The Fig. 10 below represents the rise of phishing attacks, ransomware infections, and data breaches from 2010 to 2024. These trends help to show the escalating frequency and sophistication of cyber threats, highlighting what should be taken as an ongoing consideration for cybersecurity consulting.

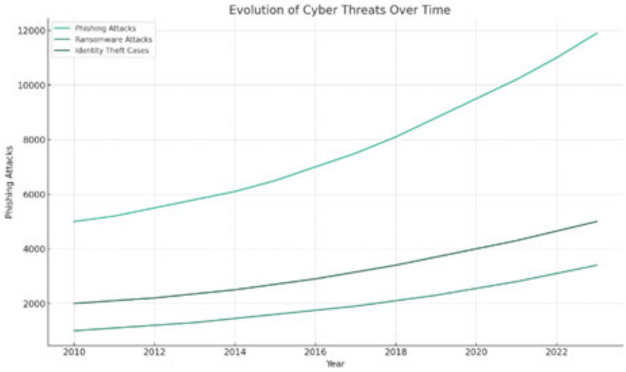

Fig. 10. Evolution of Cyber Threats Over Time

The Fig. 10 shows a substantial increase for all three types of cyber threats – phishing attacks, ransomware, and identity theft from 2000 to 2014. More concerning is the significant rise of Phishing attacks, which are set to nearly 12,000 incidents in just four years, marking hackers' favorite known threat vector. Ransomware and identity theft incidents are also expanding at a continual pace, suggesting that cybercriminals have been opting to use these modes of attacks as each of the developing methods through which they can exploit weaknesses.

To keep up with these burgeoning threats, institutions need to have strong cybersecurity defenses in place, which include state-of-the-art threat detection and individual contributor awareness programs, that also encompass response policies. Organizations will innovate by leveraging multi-layered defenses backed up with constant monitoring to minimize the impact of these advanced threats.

B. Public Awareness About Cybersecurity

The level of knowledge that the general public has on cybersecurity varies according to many elements. According to the findings in the article, there is a substantial level of knowledge about the significance of using robust passwords and being able to identify phishing emails; nevertheless, there is a much lower level of awareness regarding the significance of using software updates and making use of two-factor authentication (Fig. 11). These results point to specific regions that need more education and awareness initiatives.

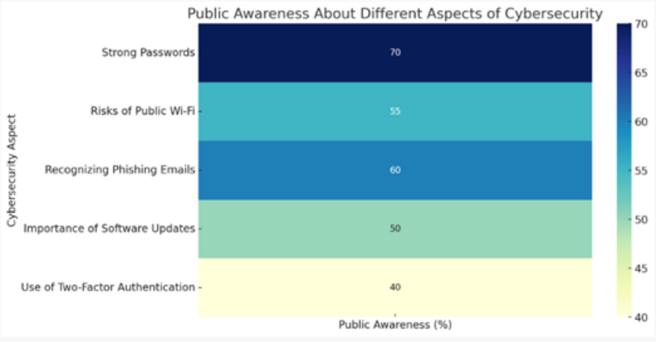

Fig. 11. Levels of Public Awareness About Cybersecurity

Fig. 11 demonstrates differing levels of public comprehension across five crucial cybersecurity elements. The majority of people acknowledge the significance of using strong passwords, as reflected in the 70% who demonstrate the highest awareness. Nevertheless, levels of awareness decrease for important practices such as identifying phishing emails (60%), understanding the dangers of public Wi-Fi (55%), and recognizing the significance of software updates (50%). Only 40% of people are aware of the importance of using two-factor authentication, a crucial security step. These results indicate that there is a necessity for specific educational programs to improve public awareness, especially in regions where awareness is lacking. Organizations and governments should prioritize raising awareness and promoting the use of overlooked practices, like two-factor authentication, in order to enhance cybersecurity resiliency.

C. *Adoption of Personal Security Measures*

According to the paper's results, people adopt various personal security measures at varying rates depending on the specific measure. Safe passwords and two-factor authentication are examples of security measures with a greater adoption rate than others. However, additional security precautions, such as virtual private networks (VPNs) and email filtering, have a lower acceptance rate. It highlights areas where people might take further measures to increase their safety.

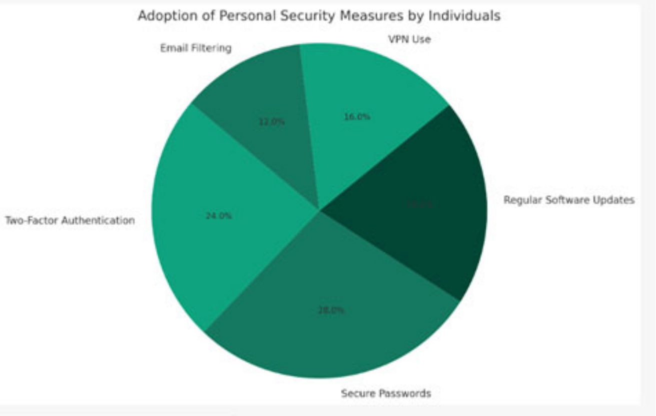

Fig. 12. Personal Security Measures Adopted by Individuals

The results in Fig. 12 presented the significance of a multi-pronged strategy for personal security, which involves education, technology, community participation, government regulation, and corporate accountability. Corporate responsibility includes the obligation of businesses to their employees and the community. Suppose we can get an awareness of the present status of personal security and the areas in which there is room for development. In that case, we can better defend ourselves against the potential dangers that may arise in the future.

VIII. Discussion

The article explores the complex correlation between artificial intelligence (AI) and personal security. The results of our research reveal that although AI technologies provide considerable advantages, they also bring about notable weaknesses that require a comprehensive defense strategy. This discussion incorporates comparisons with other prominent studies to underscore these conclusions.

The widespread incorporation of AI into everyday applications gives rise to significant privacy concerns, mirroring Walsh's investigation into the potential of AI to eradicate privacy and his plea for measures to avert an Orwellian future [1]. This aligns with our study's focus on the importance of robust regulatory frameworks and sophisticated technology solutions to reduce privacy threats linked to AI.

The current study finds human mistakes as crucial in cybersecurity breaches, corroborating Amoresano and Yankson's evidence that human error plays a substantial role in data breaches, especially in the higher education sector [4]. This highlights the significance of a thorough cybersecurity education, a fundamental element of our suggested multidimensional architecture.

Eltahir and Ahmed stress the importance of teaching cybersecurity in African universities to address significant gaps in knowledge, highlighting the need for increased awareness of cybersecurity. This aligns with our commitment to advancing thorough cybersecurity education to defend against risks driven by AI [5]. Johnson stresses the importance of a holistic model for personal safety that includes educational initiatives, backing our strategy [6].

The cybersecurity literature often highlights the important role that technology companies play in protecting the security of AI-powered products. Mijwil et al. examine the evolving hazards in cybersecurity and emphasize the proactive role technology companies need to take to reduce these risks [8]. Our analysis findings support the idea that tech companies should focus on enhancing secure AI technology and engage in cybersecurity education. This perspective is also backed by specialists at the World Economic Forum [24]

The increasing use of AI in cyberattacks, such as automated hacking and deepfakes, is a growing concern. The research by Suwajanakorn et al. and Hasan and Salah shows how artificial intelligence is used to create realistic fake media and carry out cyberattacks automatically [10], [11]. The findings from our study confirm these concerns, underscoring the importance of utilizing advanced AI-based defensive strategies to address these risks. Additionally, Ciancaglini and colleagues stress the significance of robust ethical guidelines and transparency in tackling the potentially harmful uses of AI [9].

Addressing biases and promoting fairness are essential ethical considerations in AI. Our framework supports ethical AI approaches that are in line with Ciancaglini's emphasis on reducing AI's harmful uses [9]. Additionally, our proposed extensive framework [17], [18] corresponds with the suggestion of numerous studies to enforce stringent regulatory mandates for the advancement and use of AI.

The suggested approach to cybersecurity integrates educational, regulatory, and technological aspects to provide a complete strategy. This aligns with the recommendations from other research that back various strategies to address the risks linked to AI [16], [19]. Spatharou and Jenkins highlight the importance of strong cybersecurity measures due to the considerable impact of AI in the healthcare sector [16].

The findings align with existing academic research, emphasizing the critical need for a comprehensive cybersecurity strategy in the age of artificial intelligence. The ongoing topics highlighting the complexity of the issues discussed involve the significant influence of human errors, the essential requirement for thorough education, the ethical application of AI, and the proactive involvement of IT companies. Qasim and Fatah pointed out the importance of cybersecurity in military contexts, demonstrating the various scenarios where these strategies are applicable [14].

Future research needs to focus on creating more advanced AI-powered cybersecurity solutions, improving public awareness, and establishing stronger international regulatory frameworks to effectively address the global impact of AI-related risks. Efficient teamwork between governments, tech companies, and schools is vital for creating a safe online space that harnesses the benefits of AI and lessens its risks.

The article contributes to the ongoing dialogue about personal security in the era of smart machines by introducing a comprehensive framework that integrates multiple security methods. By comparing our research to previous studies, we highlight the importance of implementing a holistic approach that combines education, technology, and legislation to safeguard personal safety in the digital age. This extensive approach is in line with the larger discussions about the impacts of AI on privacy, cybersecurity, and ethical issues, as discussed by researchers in various publications cited earlier.

IX. Conclusion

Safety in the era of advanced technology is significantly complex. The combination of human creativity and artificial intelligence (AI) offers the potential for a massive social revolution, yet faces significant challenges. People, technology companies, and regulatory bodies need to collaborate to understand and tackle hazards caused by AI. Those who are knowledgeable should take measures to safeguard themselves from such dangers.

Tech corporations, as creators of these intricate systems, have the responsibility of ensuring ethical AI procedures. These artificial intelligence systems need to be just, safe, and open. Tech companies need to create a corporate culture that promotes user awareness of security in order to effectively protect their data.

Similarly, regulatory authorities play a vital role in creating rules to oversee ethical AI research. These guidelines aim to safeguard individuals' rights while also promoting creativity.

Navigating personal safety in the age of smart devices is constantly changing. The AI's relationship to personal safety is in its initial phases, requiring continuous observation and adaptability. The discussion about AI's possibilities and consequences is ongoing, involving various perspectives from technology to ethics, law, and society.

Comprehending the complex relationship between AI and personal security shows that ensuring safety in this modern era requires collaboration. Constant innovation, consciousness, and exploration are necessary.

Even though advancements in AI have enhanced individual safety, they have also brought about fresh weaknesses. With advancements in technology, security concerns like data breaches and misuse of AI systems are on the rise.

The application of machine learning and AI has the potential to unintentionally introduce or amplify biases, leading to unfair outcomes. Consequently, there is a growing focus on 'equity in AI,' highlighting the importance of ethical AI methods to mitigate potential harm.

Transparency and accountability play a crucial role in AI research and deployment. AI systems need to be both transparent and accountable in order to build trust and ensure fairness.

Technology companies are accountable for the safety of their users. They need to actively address cyber threats, use AI ethically, and carry out their AI initiatives transparently. Consumers need to be informed about the dangers and safety measures when using AI systems.

Rules are crucial for addressing the challenges brought by widespread AI utilization. Regulations concerning the ethical advancement and use of AI could protect humans from potential harms. Nevertheless, the regulatory system needs to stay abreast of the rapidly evolving technology landscape.

Personal safety can be greatly influenced by personal actions. Being cautious of phishing, regularly updating programs, and understanding online privacy settings can enhance online security.

In the age of smart technologies, there is no single solution for ensuring personal safety. A joint effort will be required among technology firms, regulatory agencies, AI experts, and customers. There is still much progress needed in understanding and addressing the challenges related to artificial intelligence. Efforts to guarantee human safety in the era of smart devices will continue and adapt due to the persistent nature of these challenges.

Reference

[1] T. Walsh: "Will AI end privacy? How do we avoid an Orwellian future", *AI & SOCIETY*, 38, (3), 2023, pp. 1239-40

[2] N. Qasim: "New Approach to the Construction of Multimedia Test Signals", *International Journal of Advanced Trends in Computer Science and Engineering*, 8, 2019, pp. 3423-29

[3] W. E. Forum: "Experts at Davos 2023 sound the alarm on cybersecurity.", *Electronic Source*, 2023

[4] K. Amoresano, and B. Yankson: "Human Error - A Critical Contributing Factor to the Rise in Data Breaches: A Case Study of Higher Education", *HOLISTICA – Journal of Business and Public Administration*, 14, (1), 2023, pp. 110-32

[5] M. E. Eltahir, and O. Ahmed: "Cybersecurity Awareness in African Higher Education Institutions: A Case Study of Sudan", 12, 2023, pp. 171-83

[6] M. Johnson: "The need for an all-encompassing model for personal security in the age of AI", *Journal of Cybersecurity and Privacy*, 9, (1), 2023, pp. 1-12

[7] N. J. M. Omar S.S., Qasim N. H., Kawad R. T., Kalenychenko R. : "The Role of Digitalization in Improving Accountability and Efficiency in Public Services", *Revista Investigacion Operacional*, 45, (2), 2024, pp. 203-24

[8] M. Mijwil, O. Unogwu, Y. Filali, I. Bala, and H. Al-Shahwani: "Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview", 2023

[9] C. G. a. D. S. V. Ciancaglini: "Malicious Uses and Abuses of Artificial Intelligence", *Trend Micro Research*, 2020

[10] S. Suwajanakorn, S. Seitz, and I. Kemelmacher: "Synthesizing Obama: learning lip sync from audio", *ACM Transactions on Graphics*, 36, 2017, pp. 1-13

[11] H. R. Hasan, and K. Salah: ''Combating Deepfake Videos Using Blockchain and Smart Contracts'', *IEEE Access*, 7, 2019, pp. 41596-606

[12] J. C. S. A. Miles Brundage, Helen Toner, Peter Eckersley, Ben Garfinkel, Allan Dafoe, Paul Scharre, Thomas Zeitzoff, Bobby Filar, Hyrum Anderson, Heather Roff, Gregory C. Allen, Jacob Steinhardt, Carrick Flynn, Seán Ó hÉigeartaigh, Simon Beard, Haydn Belfield, Sebastian Farquhar, Clare Lyle, Rebecca Crootof, Owain Evans, Michael Page, Joanna Bryson, Roman Yampolskiy, Dario Amodei: ''The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation'', *ArXiv*, 2018

[13] S. Catherine: ''Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case'', *WSJ*, 2019

[14] N. Qasim, and O. Fatah: ''The role of cyber security in military wars'', *V International Scientific and Practical Conference: "Problems of cyber security of information and telecommunication systems" (PCSITS)". October 27 - 28, 2022, Kyiv, Ukraine*, 2022

[15] Q. Nameer, J. Aqeel, and M. Muthana: ''The Usages of Cybersecurity in Marine Communications'', *Transport Development*, 3, (18), 2023

[16] S. H. A. Spatharou, and J. Jenkins: ''Transforming healthcare with AI: The impact on the workforce and organizations'', *McKinsey & Company: Heathcare*, 2020

[17] J. W. a. M. E. T. Sinter: ''Reinventing Cybersecurity with Artificial Intelligence: The new frontier in digital security'', *Capgemini Research Institute*, 2022

[18] S. Giannini: ''Generative Artificial Intelligence in education: What are the opportunities and challenges?'', *UNESCO*, 2023

[19] L. Perri: ''Gartner Top Strategic Predictions for 2023 and Beyond'', *Gartner*, 2023

[20] H. Poll: ''2023 Norton Cyber Safety Insights Report'', *GEN*, 2023

[21] Interpol: ''AI-Driven Cyberattacks during the COVID-19 Pandemic'', *Interpol*, 2023

[22] M. T. Review: ''Preparing for AI-enabled cyberattacks'', *MIT Technology Review*, 2021

[23] R. Redondo Alamillos, and F. de Mariz: ''How Can European Regulation on ESG Impact Business Globally?'', *Journal of Risk and Financial Management*, 15, (7), 2022

[24] W. E. Forum: ''World Economic Forum Annual Meeting 2023'', *World Economic Forum*, 2023

[25] N. Qasim, Shevchenko, Y.P., and Pyliavskyi, V.: ''Analysis of methods to improve energy efficiency of digital broadcasting'', *Telecommunications and Radio Engineering*, 78, (16), 2019

[26] C. Feijóo, Y. Kwon, J. M. Bauer, E. Bohlin, B. Howell, R. Jain, P. Potgieter, K. Vu, J. Whalley, and J. Xia: ''Harnessing artificial intelligence (AI) to increase wellbeing for all: The case for a new technology diplomacy'', *Telecommunications Policy*, 44, (6), 2020, pp. 101988

[27] R. W. e. al.: ''Technological Innovation and Risk in the Management of Integrated Supply Chains – A Survey Results'', *EUROPEAN RESEARCH STUDIES JOURNAL*, XXIV, (4B), 2021, pp. 479-92

[28] J. B. Ulven, and G. Wangen: ''A Systematic Review of Cybersecurity Risks in Higher Education'', *Future Internet*, 13, (2), 2021

[29] N. Qasim, Khlaponin, Y., & Vlasenko, M.: ''Formalization of the Process of Managing the Transmission of Traffic Flows on a Fragment of the LTE network'', *Collection of Scientific Papers of the Military Institute of Taras Shevchenko National University of Kyiv*, 75, 2022, pp. 88–93

[30] B. Hitaj, P. Gasti, G. Ateniese, and F. Perez-Cruz: ''PassGAN: A Deep Learning Approach for Password Guessing'', 2017

[31] A. Aris, L. Puche Rondon, D. Ortiz, M. Ross, M. Finlayson, and A. S. Uluagac: ''Integrating Artificial Intelligence into Cybersecurity Curriculum: New Perspectives'', *2022 ASEE Annual Conference &amp; Exposition Proceedings*, 2022

[32] Q. N. H. Sieliukov A.V., Khlaponin Y.I.: ''Conceptual model of the mobile communication network'', *The Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things «TTSIIT»*, 2022, pp. 20-22

[33] R. J. G. Raimundo, and A. T. Rosário: ''The Impact of Artificial Intelligence on Data System Security: A Literature Review'', *Sensors (Basel, Switzerland)*, 21, 2021

[34] H. Thamik, and J. Wu: ''The Impact of Artificial Intelligence on Sustainable Development in Electronic Markets'', *Sustainability*, 2022

[35] R. Kaur, D. Gabrijelčič, and T. Klobučar: ''Artificial intelligence for cybersecurity: Literature review and future research directions'', *Information Fusion*, 97, 2023, pp. 101804

[36] R. Eitel-Porter: ''Beyond the promise: implementing ethical AI'', *AI and Ethics*, 1, 2020, pp. 73 - 80

[37] R. Gupta, S. Tanwar, F. M. Al-turjman, P. Italiya, A. Nauman, and S. W. Kim: ''Smart Contract Privacy Protection Using AI in Cyber-Physical Systems: Tools, Techniques and Challenges'', *IEEE Access*, 8, 2020, pp. 24746-72