International Journal of Social Science Archives

ISSN: 2707-8892

Available at www.ijssa.com

International Journal of Social Science Archives, Jun, 2023, 6(1), 10-25.

Analyzing the Best Practices and Risks of Artificial Intelligence in Human Security

Naila Ahmed (MS-IR)

*Email: nailaahmed1992@gmail.com

Abstract: The Copenhagen School of thought on human security examines the need to protect individuals from physical, economic, social and environmental threats. Unlike traditional state-centric approaches, this school focuses on a human-centered perspective, considering the well-being of individuals as opposed to just the security of the state. It advocates a holistic approach to security, combining traditional measures like military protection with non-traditional ones such as economic assistance, social services, and environmental protection. The text also highlights the potential of Artificial Intelligence (AI) in enhancing human security. AI can detect and respond to threats more rapidly and accurately than humans, leading to more effective security solutions. It can analyze vast amounts of data to identify patterns and anticipate security threats, ultimately aiming to improve human security. However, it is essential to consider ethical issues and potential challenges associated with the use of AI in security, including data collection, privacy concerns, and the responsible use of AI to protect individual rights. Overall, the text emphasizes the need to utilize AI-based security solutions responsibly while understanding their potential benefits and implications for human security on a global level. Human security

Keywords: Protect individuals, Physical threats, Economic threats, Social threats, Environmental threats, Human-centered perspective, State-centric approach

Introduction

Artificial intelligence (AI) and human security are two interrelated concepts increasingly being discussed in the context of digital technology [1]. In addition to automating and optimizing tasks, AI is also being utilized to create intelligent systems that can interact with humans through data analysis and decision-making [2]. In addition to ensuring the safety and security of individuals and communities, human security also encompasses the protection of their rights and freedoms. This includes a variety of aspects, such as physical, economic, environmental, and psychological security. Artificial intelligence has become increasingly important in the security industry due to its ability to detect and prevent threats, improve response times, and improve accuracy [3]. It is possible to identify patterns and recognize trends in data using artificial intelligence to provide early warnings and alerts. Furthermore, it can detect suspicious behaviour, allowing authorities to respond promptly to prevent further harm from occurring. A

further application of AI is identifying potential threats, such as cyber-attacks, and tracking down malicious actors based on large data sets [4], [5]. Lastly, AI can provide personalized security solutions for individuals, such as facial recognition systems, to ensure citizens' safety. Finally, AI and Human Security are two concepts that are becoming increasingly intertwined, as AI is being utilized to improve the safety and security of individuals and communities [6], [7]. In addition to detecting and preventing threats more quickly, authorities can also provide personalized solutions to individuals by utilizing Artificial Intelligence (AI).

As AI technology advances and applications become more widespread, artificial intelligence and human security have become increasingly important topics. AI can revolutionize how we protect ourselves, our data, and our physical assets, as well as make our daily lives more secure [8]. Current security measures for AI-enabled systems differ greatly depending on the type of system and the level of security desired. This includes authentication, encryption, access control, and AI-based detection methods such as anomaly detection and machine learning citebenzaid2022ai. In addition, organizations should also consider the use of ethical AI systems to ensure that their AI-enabled systems are used responsibly and ethically [9]. Despite these measures, there are still areas in need of improvements, such as the development of better AI-enabled security systems, the implementation of more comprehensive security policies and procedures, and the need for greater public awareness and education regarding the risks associated with AI-enabled systems [10].

The ethical implications of AI-enabled security measures involve the use of highly advanced technology to protect data and ensure privacy. These types of security measures utilize artificial intelligence algorithms to detect potential threats and take preventative action [11]. The system can also be used to monitor user behaviour and access to sensitive information and control user access to certain areas or functions. Aside from analyzing data and generating insights that can be used to improve security, AI-enabled security measures may also have some ethical implications associated with them [12]. Using AI-enabled security measures, for example, can result in mass surveillance and profiling, which may violate individual privacy and civil liberties. Moreover, AI algorithms may be biased and discriminatory, resulting in unfair or inaccurate decisions [13].

Furthermore, AI-enabled security measures can be vulnerable to attack, potentially losing sensitive data and other information. The ethical implications of AI-enabled security measures should be carefully considered when implementing such measures. To protect user data and privacy, it is important to be aware of potential risks and to ensure the appropriate safeguards are in place [14].

Best practices should be based on principles that prioritize the protection of human security, such as privacy, autonomy, fairness, non-discrimination, and transparency [15]. These best practices should consider the ethical implications of the application of AI-enabled security measures, including the potential for misuse or abuse, the need to consider the impact on vulnerable populations, and the need to ensure appropriate oversight and accountability. Additionally, best practices should include measures to ensure the accuracy and reliability of the AI-enabled security measures and ensure that the data used for training and testing is of sufficient quality and quantity [16]. Finally, best

practices should address the need for ongoing monitoring and evaluation of the effectiveness of AI-enabled security measures in order to ensure that human security is adequately protected.

Theoretical framework of Research Paper:

For the topic under research the Copenhagen School of Security Studies says that the importance of human security is a primary focus of security studies. This school of thought argues that the focus of security should be on the people, not on states. This means that instead of focusing on the military power of states, security studies should focus on protecting people and their rights such as their right to life, health, safety, and access to resources. The Copenhagen School also puts emphasis on the importance of understanding the social and economic contexts of security issues, since these contexts often shape the nature and severity of security threats. Thus, the Copenhagen School emphasizes the importance of considering the social, economic, and cultural aspects of security in order to better address security threats. As a result of this research paper, we aim to explore the possibility of enhancing human security using artificial intelligence (AI). As well as providing more efficient and effective security solutions, artificial intelligence can be used to detect and respond to threats more efficiently and accurately than humans. Thereby, focusing on non-traditional aspect of security as per Barry Buzan. In this paper, we examine how artificial intelligence can be utilized to enhance security in a variety of contexts, including home and business security, border security, and public safety, among others. Moreover, the paper discusses the ethical implications of using AI for security purposes and possible risks associated with its use. Finally, the paper explores how AI can be used to promote human security over the long term. In particular, this work has the following contribution:

1) Exploring the potential of AI to enhance human security and reduce global risks.
2) Investigating the impact of AI-based security systems on the privacy of citizens.

Explanation:

The related work section of"Human Security through Artificial Intelligence" describes existing research on the use of AI for human security [17], [8], [1], [3], [5], [4]. It outlines the various applications of AI in the security space, such as facial recognition, biometric authentication, intrusion detection systems, and autonomous drones. It also discusses the challenges associated with using AI in security, such as privacy concerns, data security, and ethical issues [11], [10], [9]. The section also reviews existing research on the use of AI to enable human security, including its potential applications in developing countries and its implications for global security [16], [15], [14], [13], [12].

The paper examines the integration of digital technologies, specifically artificial intelligence technology, into a state's security system [18]. Digital technologies, including artificial intelligence, are described as part of the security systems of states and the changes that result. Using artificial intelligence technology is not linear but undulating, and it reflects both national characteristics of the conceptualization of national security and the internal characteristics of particular types of digital technologies. Research directions based on this study's theoretical and instrumental (methodological) developments may relate to both the topic of data-driven political science and comparative political science paradigms.

Technology has advanced rapidly, resulting in a gap between society's ability to keep up with artificial intelligence and the hidden risks associated with it [19]. As technology advances rapidly, humans are finding it increasingly difficult to stay abreast of the hidden complexities of artificial intelligence. This technology is based on neural activity and natural language processing, creating products that pose a threat to human security. Fake news and deep fakes on social media are among the most dangerous non-kinetic weapons in information warfare. In order to combat them, people must become media literate, think critically and keep up with machine learning and natural language processing.

As a result of the 4th Industrial Revolution (4IR), two significant threats to human security are discussed: the increase in inequality within and between countries resulting from digital transformation and the emergence of new threats to individual autonomy resulting from surveillance by the private sector [20]. As a result of applying the concept of human security to the 4IR, it is argued that self-serving perspectives can be overcome, and individuals' risks are fore-emphasized. This paper suggests decentralized advocacy as a way to reshape or contest technological insecurities, emphasizing private sector actors and their technological assemblages. In order to remain relevant, human security concepts and advocacy must continue to adapt to emerging challenges and new actors. This strategy is a compromise. A comprehensive synthesis of human security with the participatory design and implementation of cutting-edge technologies could increase the resilience of East Asia at this critical point in its history.

As a result of the combination of human and machine intelligence, hybrid intelligence systems are intended to overcome the limitations of conventional artificial intelligence (AI) systems. In this paper, we examine recent research efforts in hybrid systems development, emphasizing reasoning approaches to improve human intelligence and gain a deeper understanding of people as AI systems' assistants [2]. It concludes by discussing the potential short and long-term research directions related to hybrid intelligence systems. The work from Microsoft provides an overview of recent research related to hybrid intelligence systems, with a focus on enhancing the understanding of human intelligence and how it can be used in combination with AI systems.

The recent digital revolution has led to an increase in the use of robots in various domains, such as agricultural, medical, industrial, military, police (law enforcement), and logistics. Robots are designed to improve the quality of life for humans, but unfortunately, many incidents have occurred that have caused serious injuries and even deaths [3]. Malicious attacks on robots are a particularly challenging issue, as they can cause economic and financial losses. A review of security vulnerabilities, threats, risks, and their impacts, as well as security attacks in the robotics field, is presented in this paper. It also proposes various approaches and recommendations to enhance the security level of robotic systems, such as multi-factor device/user authentication schemes and multi-factor cryptographic algorithms. The paper concludes by reviewing recently proposed security solutions for robotic systems.

The Concept of a "borderless cyberspace as part of global commons" is an ideal that does not exist in reality [5]. As technology advances, so too make the threats of cyberattacks, cybercrimes, and malware attacks. This chapter discusses the need for cyber security and how it can be addressed with the use of Artificial Intelligence (AI) techniques. In addition to traditional approaches to cyber security, more intelligent methods are emerging, such as

deep learning, which can be used to develop models for malware classification, intrusion detection, and threat intelligence. As part of the chapter, artificial intelligence models can also be utilized to modify multilayered security mechanisms used by companies today. The chapter concludes by discussing the potential future of artificial intelligence and cyber security.

It is increasingly common for organizations to be under threat from malicious hackers, who can breach security parameters, disrupt infrastructure, steal confidential information and financial data, and violate consumer privacy. The use of Endpoint Detection and Response (EDR) systems can provide additional security by preventing an endpoint action from resulting in a security breach [4]. To identify and respond to advanced threats, EDR combines endpoint and network data to provide sophisticated detection and response tools. The system offers unparalleled security and operational efficiency by combining prevention, investigation, detection, and reaction on a single platform. As a result of its continuous monitoring and response to threats, it offers enterprise-wide protection and uninterrupted defense. This comprehensive analysis of existing EDRs covers various security layers, including detection, response, and management capabilities, allowing security teams to have unified end-to-end corporate access, powerful analytics, as well as additional capabilities such as web threat scanning, external device scanning, and automatic response across the entire technological towers.

The article examines the history of human security and environmental security within the context of the United Nations Human Development Report of 1994 [7]. It illustrates how the two concepts have intertwined and diverged over time. However, there has been little analytical depth in the UN's analysis of the impact of environmental degradation on people and communities. As a result, the Concept of environmental security has become increasingly detached from its roots in human security and has instead become focused on non-traditional threats to traditional referents, such as the government. As a result, the author suggests, human/environmental security has been narrowed, and human freedom and dignity have been foreclosed rather than protected.

Human security is presented as a unified concept and agenda that is adaptable, yet unified in its definition, which can be analyzed beginning with the Human Security Now report by the Ogata-Sen Commission [6]. In accordance with the report, human security is defined as a combination of freedom, basic needs, stability, and a certain level of essential human development characteristics. In addition, it identifies when human security discourse repeats the notion of human needs and where it contributes to and demonstrates the coherence of human rights, human security, and human needs. Also, it describes the sorts of intellectual "border work" the idea and discourse attempt, including mobilizing concern and attention, combining explanatory and normative agendas, and bringing together disparate intellectual and policy groups. Finally, the concept of human security, including the selected label, is evaluated and latent hazards and possibilities are identified.

The work discusses the potential risks and benefits of machines being used as teammates rather than tools [8]. An international initiative of 65 collaborative scientists was conducted to create a research agenda for exploring this Concept. The team generated 819 research questions, which were then narrowed down to three design areas and 17 dualities. This research agenda provides a structure and archetypal research questions to organize early thought and

research on this new topic. The three design areas are Machine Artifact, Collaboration, and Institution, and the 17 dualities are significant effects with the potential for benefit or harm. The paper concludes that the MaT research agenda provides a valuable resource for exploring the implications of using machines as teammates.

The paper introduces a novel autonomic and cognitive security management framework that aims to provide a secure and efficient way to manage 5G and beyond networks [17]. The proposed framework uses a zero-touch approach to enable fine-grained security management across different levels (i.e., network functions, sub-slice, and slice) and different administrative and technological domains. It complies with existing standards such as ZSM, 3GPP, and NFV. Its feasibility is demonstrated by suggesting potential open-source solutions for its implementation in a cloud-native service-based environment.

During the past several years, Financial Technology (FinTech) has been rapidly developed and spread across the globe. It is difficult to manage risk with peer-to-peer (P2P) lending, a FinTech financing. This procedure generates ethical challenges and concerns, but it may serve as a risk mitigation strategy for evaluating the creditworthiness of prospective consumers [9]. Artificial intelligence (AI) may be used as a risk mitigation strategy to evaluate the creditworthiness of prospective consumers.

The study employs consequentialism and deontology as decision-making aids to address these ethical concerns and challenges. Using artificial intelligence to automate the evaluation of potential P2P loan applications can minimize ethical lapses and adverse effects on the data of potential customers. A rapidly developing technology, Artificial Intelligence (AI) has the potential to significantly impact our lives in the near future. As a result, it has been utilized to develop novel teaching and learning solutions, which are being evaluated across a variety of settings [10]. Nevertheless, there is a debate over whether AI is a priority for poor nations, since it requires modern infrastructure and a vibrant innovation ecosystem. This article argues that AI should be emphasized in developing nations in order to lessen the digital and social divide, as it may provide a number of benefits, including greater access to education, healthcare, and other resources for those countries. AI may also eliminate inequality and poverty by creating employment opportunities and making access to new markets easier. AI should be a priority for poorer nations in order to develop a more equal and affluent society, according to the article.

In this study, ethical concerns are explored regarding the application of artificial intelligence (AI). The report presents a literature review on AI ethics as well as empirical insights derived from ten case studies. A cross-case analysis of organizational responses to these ethical challenges is presented in the report [11]. Although organizations are cognizant of the AI ethics debate and are proactive in resolving ethical challenges, they only employ a small fraction of the techniques presented in the literature when resolving ethical challenges. These findings are relevant for businesses that deploy or utilize artificial intelligence, for academic discussion on artificial intelligence ethics, and for politicians engaged in the present debate regarding the establishment of appropriate policies to address the ethical challenges posed by artificial intelligence.

This paper presents methods for detecting how applications obtain unauthorized access to sensitive data and system resources by utilizing side and covert channels [12]. An architecture for instrumenting hundreds of thousands of applications was established by the authors. As part of this environment, runtime behavior and network traffic were monitored in order to detect sensitive data communicated over the network without the consent of the app transmitting it. In order to measure the ubiquity of the technique, the authors reverse engineered the applications responsible for this behavior and used software fingerprinting techniques to determine their ubiquity. As a result of the investigation, hundreds of popular applications and third-party SDKs were found to use covert and side channels to obtain access to unique identifiers and geolocation information illegally. Google rewarded them for their effort after they communicated their results in a responsible manner. It examines the potential ramifications of introducing surveillance devices powered by artificial intelligence into our society. It focuses on the implementation of real-time face recognition (FRT) and public health monitoring technology, including contact tracking apps. Both of these methods can be used by public authorities to enforce the law by tracking individuals' movements and extrapolating the data for monitoring and forecasting society's behavior. An analysis of the potentials and risks associated with such tools is provided by the article in three dimensions: a function dimension examines the type, quality, and quantity of data the system needs to utilize to function effectively [13]. Consent dimension, which considers the user's right to be informed about surveillance and to reject it; and a societal dimension, which focuses on vulnerabilities and the effects of enhanced political power resulting from the use of such tools by established political regimes. Public authorities may benefit from the approach described in this article in determining how to establish and implement public surveillance systems that comply with the law, while highlighting the costs to individuals and society as a whole.

As discussed in the article, viral illnesses such as COVID-19 pose a threat to global health in an interconnected [14]. Several factors have contributed to the spread of these diseases, including global travel, urbanization, climate change, and environmental degradation. In this section, we discuss how artificial intelligence (AI) can be used to monitor disease and how a framework for ethical AI could be used to investigate its potential application to global health surveillance. According to the article's conclusion, there is a lack of literature that addresses the consideration of numerous and interrelated levels of disease surveillance and emergency health management from the perspective of a responsible AI framework.

A current controversy surrounds ethical AI, or artificial intelligence intended to be ethical [15]. Although several organizations have produced ethical AI guidelines and principles in the past five years, there remains a disagreement regarding the definition of ethical AI and the standards and best practices that should be employed in order to achieve it. The authors of this research analyzed the corpus of accessible ethical AI principles and standards and mapped the increasing worldwide consensus on five ethical principles: transparency, justice and fairness, nonmaleficence, responsibility, and privacy. Despite the fact that there is a consensus on these principles, they indicate significant differences in how they are perceived, why they are critical, which areas they apply to, and how they should be applied. According to the authors, guideline creation efforts should be combined with substantial ethical analyses and implementation methodologies in order to effectively implement ethical AI.

It examines the ethical concepts and norms that have been developed for artificial intelligence (AI) over the past five years [16]. A review of the present corpus of rules and principles revealed a global convergence around five ethical concepts (transparency, justice, fairness, no maleficence, accountability, and privacy). However, considerable disagreement remains regarding their interpretation and application despite this. Due to this, the authors emphasize the necessity of combining efforts to develop standards with ethical analyses and implementation methodologies.

Many systems used in our daily lives are increasingly incorporating Artificial Intelligence (AI), including autonomous automobiles, healthcare systems, and unmanned aircraft [18]. Machine Learning is a branch of artificial intelligence that allows computers to learn from data and make decisions based upon models to achieve specific objectives. There may be inherent biases in AI models, such as repeatability bias, selection bias, and reporting bias, which can be stochastic and contain inherent biases. As a result of their black-box nature, AI systems are difficult to audit and verify, as well as vulnerable to attacks. Several ideas have been presented by governments and organizations to resolve these concerns, but their practical implementation is limited. This article examines trust in the context of AI-based systems in order to comprehend what it means for an AI system to be trustworthy and to identify the steps that should be taken to ensure that AI systems are trustworthy. It examines potential ways for assuring the trustworthiness of AI systems and proposes a trust (resp. zero-trust) paradigm for AI. Furthermore, it proposes a set of conditions which must be met for AI systems to be credible. As security sectors have grown more prevalent and information and communication technologies have become increasingly digital, artificial intelligence is increasingly being used for national security. Most research has focused on the use of artificial intelligence in the security sector and the changes resulting from it. AI has the potential to change government approaches to the management of security. Artificial intelligence may be utilized to automate and expedite security procedures, such as monitoring and surveillance, and identify weaknesses and possible threats. In addition to boosting the precision and speed of decision-making, artificial intelligence can also be used to improve the efficacy of security operations. In addition, artificial intelligence is used to collect and analyze massive volumes of data in order to more efficiently identify and respond to security risks. As more nations understand its potential to increase the efficiency and efficacy of security operations, it is expected that the use of artificial intelligence in national security will continue to increase in the future.

A study examined the impact of technological advancement on human security by spreading unconventional weapons. Social media has enabled the spread of information and the development of fake news and deepfake as hybrid warfare tools as a consequence of the rapid rise of social media [19]. This tool has increased the level of hazard for individuals and society by manipulating words and images, AI algorithms, and social engineering tactics. A conceptual definition of social media security vulnerabilities is presented along with an overview of the vulnerabilities posed by social media to human security. Due to the world's 7,7 billion inhabitants, food, water, and energy supplies are under growing strain. This study examines the numerous difficulties and possibilities posed by these shifts. As the worldwide urban population is projected to reach 68% by 2050, food security will become a major concern for the future of cities as a result of rural-to-urban migration. Due to the Fourth Industrial Revolution

and the rise of Smart Cities, a variety of measures may be done to solve food security issues in urban settings. This document gives a comprehensive overview of the different possible actions.

METHODOLOGY

In this research, we analyze current Artificial Intelligence (AI) technology and identify potential uses to enhance human security. Artificial intelligence has experienced rapid advancements in recent years, addressing an array of issues. There are a number of ways to utilize artificial intelligence in human security, including facial recognition, automated detection systems, and predictive analytics to predict and prevent security threats. In addition, AI can be used to identify patterns in data that can be utilized to develop security improvement strategies. It is possible to use artificial intelligence to assist with resource allocation, such as determining where security personnel or resources should be assigned or to help identify potential security threats. In addition to helping with data analysis, AI can also assist with identifying ways to prevent similar incidents from occurring again in the future by analyzing past security incidents. In the end, artificial intelligence technology can enhance human security by providing more efficient and effective solutions to security challenges.

A. Concepts

Recent years have seen extensive research into the connection between artificial intelligence and human security. Artificial Intelligence is the ability of a machine or computer to learn and reason in a way similar to that of a human. Using AI in a variety of ways, from controlling robots to playing chess, is becoming increasingly important. Meanwhile, human security is a concept that emphasizes protecting individuals from violence and other threats. It is a broad concept that covers a range of topics, including economics, health, food, and environmental security, as mentioned in Figure 1. The relationship between AI and Human Security is complex and multifaceted. On the one hand, artificial intelligence can improve individuals' security by providing them with more sophisticated security measures and solutions. The use of facial recognition technology, detection of malicious software, and prevention of cyber-attacks are among the measures that are included in this process. Furthermore, artificial intelligence can be used in ways that threaten human security, such as through mass surveillance, automated weapons systems, and other technologies that threaten the privacy and autonomy of individuals. Human Security and AI are two topics which are closely intertwined and will continue to evolve as technology advances. It is important to understand the implications of AI in order to ensure that technology is used responsibly and in a way that respects and protects human rights.

A field of computer science known as Artificial Intelligence (AI) focuses on designing, developing, and implementing intelligent computer systems and applications. Through the development of algorithms that can learn and respond to their environment, artificial intelligence theory seeks to solve complex problems. In AI theory, algorithms and systems are developed that can think rationally in complex and uncertain environments. In addition to discussing the ethical implications of applying AI technology to solve problems, AI theory also addresses these issues. A human security-related area of computer science is concerned with ensuring the safety and security of individuals and organizations in the event of malicious cyber-attacks, data

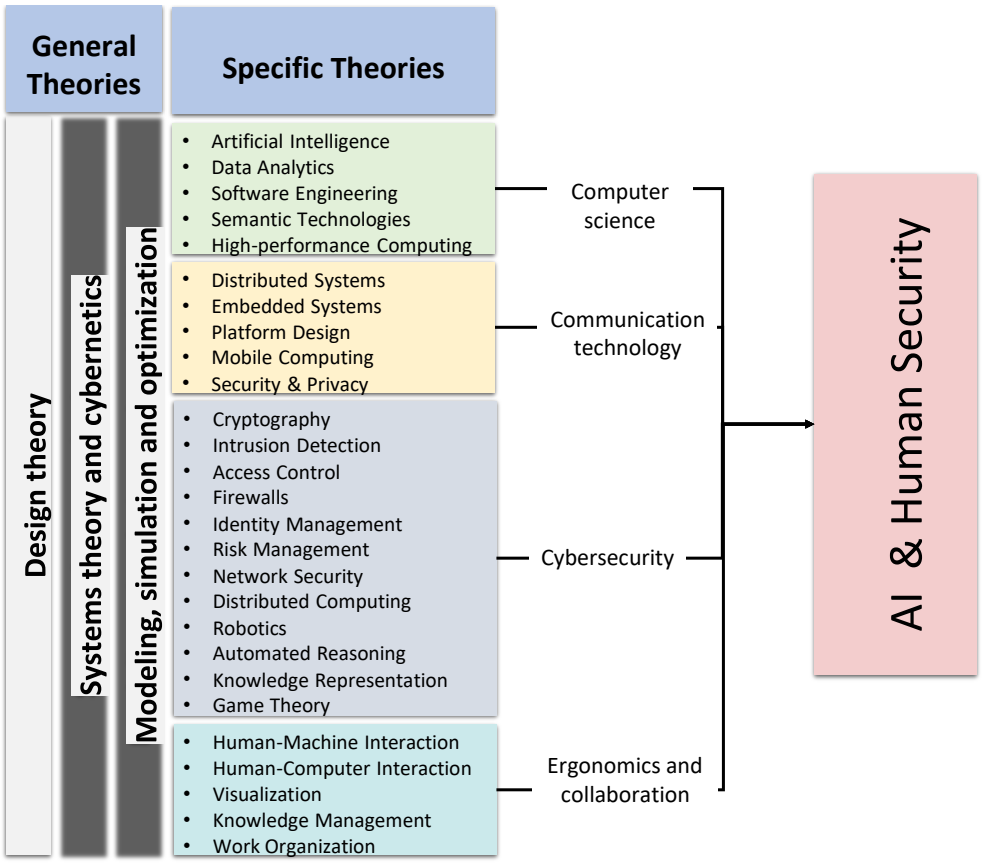

Fig. 1. Concept and theory related to AI and Human security.

breaches, or other cyber-related incidents. As a multidisciplinary field, it focuses on the use of computer technology to prevent cyber threats from individuals, businesses, and other organizations. This includes the development of secure systems, the use of encryption and other security technologies, and the development of policies and procedures to protect data. Human security related to Computer science also looks at how AI and machine learning technologies can be used to detect and respond to cyber threats.

Organizational security refers to the process of protecting an organization and its assets from external threats, as mentioned in Figure 2. This includes physical security, such as locks and access controls, as well as cyber security, such as firewalls and encryption. An individual's personal security refers to the protection of themselves against potential harm, such as identity theft, cybercrime, and physical violence. As part of physical security, physical premises and personnel are protected from potential threats, such as theft, vandalism, or terrorist attacks. Through encryption and other measures, communication security protects the privacy of information shared between two or more parties. Hardware security's responsibility is to prevent unauthorized access to, damage to, or theft of computer equipment. Software security protects applications, data, and systems from malicious code, vulnerabilities, and other threats. Integrity is the assurance that data is accurate and reliable. Confidentiality is the practice of protecting sensitive information from unauthorized access or disclosure. Availability is the assurance that information and

systems can be accessed whenever necessary. Information security aims to prevent unauthorized access to, modification of, and destruction of data and systems.

FINDINGS'S

An assessment of the effectiveness of artificial intelligence (AI) security measures in comparison with human security measures was conducted as part of the research project. Various papers were analyzed, and a summary of the findings was presented. According to the results of this study, artificial intelligence can be used to detect threats more rapidly and accurately than human-based security measures. Artificial intelligence has been found to be more cost-effective than human security solutions, not only because it is less prone to errors but also because it provides better protection against cyber threats. According to the study, although AI can provide a strong layer of security, combining AI with human security measures is important to ensure a comprehensive approach to preventing cyber threats. In order to develop an effective method for human security using AI, the followings are the potential ways.

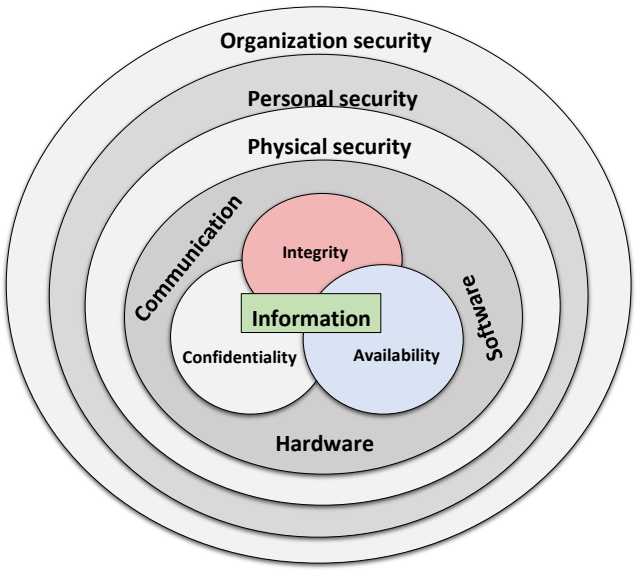

Fig. 2. Organization security.

Develop a framework for assessing the potential of AI-enabled security measures to improve human security: This is a step-by-step process for implementing an AI-enabled security solution. The process begins with identifying security needs and assessing the current security measures in place. The next step is to research and evaluate existing AI-enabled security solutions and determine which ones are suitable for the organization's security needs. After that, the AI-enabled security solution should be analyzed to assess its feasibility with the organization's technical capabilities and resources in mind. The cost/benefit of the AI-enabled security solution must then be assessed to determine if the investment is worth it. Any risks associated with the AI-enabled security solution must also be identified and assessed. The AI-enabled security solution should then be tested and evaluated in a secure test environment. Once it is implemented, the performance of the AI-enabled security solution should be monitored and

adjusted as needed. Lastly, the impact of the AI-enabled security solution on human security must be evaluated to determine if it is improving human security.

Explore the ethical implications of AI-enabled security measures: As part of the ethical implications of artificial intelligence-enabled security measures, artificial intelligence (AI) is used to enhance security measures and protect data and information. AI-enabled security measures are increasingly performing detection, prevention, and response to security threats and breaches. AI-based solutions can assist in identifying suspicious behaviour, detecting fraud, and monitoring and blocking malicious activity. However, there are ethical implications associated with the use of AI-enabled security measures, including potential privacy violations, the risk of false positives, the risk of unfair discrimination, and the possibility of misusing data. In addition, the use of AI-enabled security measures may result in an increased reliance on automation, resulting in a decrease in human oversight and accountability as a result. Prior to implementing AI-enabled security measures, organizations should consider the ethical implications and ensure that appropriate safeguards are in place to ensure data and information security.

Design and test AI-enabled security measures to ensure their efficacy in protecting human security: development and testing of Artificial Intelligence (AI) enabled security measures to ensure they are effective in protecting human security. This process typically involves designing, implementing, and testing AI-based technology to detect and prevent security threats. The security measures must be designed to be effective in preventing malicious actors from accessing confidential data, networks, and other sensitive information. Testing should also be conducted to ensure that security measures effectively detect and respond to potential threats. Additionally, measures should be taken to ensure the AI technology is secure from attack and does not have any security vulnerabilities. Finally, security measures should be regularly monitored and updated to keep up with the changing security environment.

Evaluate the impact of AI-enabled security measures on human security: The impact of AI-enabled security measures on human security is increasingly becoming a major concern for many people. AI-enabled security measures are designed to detect and respond to potential security threats in an automated and intelligent manner. These technologies can help to detect malicious activities, protect data, and respond to threats more quickly than traditional security systems. In addition, they can help to identify suspicious activity before it becomes a major problem and can even be used to detect and respond to cyber-attacks. However, there are also concerns that AI-enabled security measures may lead to an erosion of privacy and the potential for misuse of personal data. Ultimately, AI-enabled security measures can be a useful tool to help protect organizations, businesses, and individuals from malicious activity. However, it is important

to carefully evaluate the potential risks and benefits of these systems in order to ensure that the benefits outweigh the risks. Additionally, organizations should ensure that AI-enabled security systems are properly monitored and managed to ensure that any data collected is handled responsibly and securely.

A. Best practices for the use of AI and human security best practices should be based on principles that prioritize the protection of human rights when using artificial intelligence. This includes ensuring fairness, transparency, accountability, security, and privacy when designing and operating AI systems.

Transparency: AI systems should be designed and operated in a manner that is transparent and explainable. This will enable users to understand how decisions are made and enable responsible decision-making.

Fairness: AI systems should be designed and operated in a manner that is fair, equitable, and unbiased. This includes avoiding the use of data or algorithms that could lead to unfair discrimination and avoiding the misuse of data or algorithms that could lead to unfair outcomes.

Accountability: AI systems should be designed and operated in a manner that is accountable and traceable. This includes providing clear documentation of how decisions are made and enabling users to review and audit decisions.

Security: AI systems should be designed and operated in a manner that is secure and resilient. This includes protecting data, algorithms, and other components of the system from unauthorized access.

Privacy: AI systems should be designed and operated in a manner that respects and protects user privacy. This includes ensuring that data is collected and used in accordance with applicable laws and regulations and ensuring that data is not used for unintended purposes.

B. Potential issues AI and human security

AI and human security are growing concerns as artificial intelligence (AI) becomes increasingly prevalent in our society. AI has the potential to disrupt existing security systems, create new security threats, and even challenge the notion of what it means to be secure. Potential issues include the potential for AI to be used for malicious purposes, such as hacking, surveillance, and data manipulation; the potential for AI to be used to automate tasks that could lead to job displacement; and the potential for AI to be used to create autonomous weapons systems or other autonomous systems that could be used to cause harm. Additionally, there are ethical and legal implications to consider when using AI, such as how to ensure that AI systems are designed in a way that respects human rights and privacy. Finally, there is the potential for AI to be used to create powerful algorithms that can be used to manipulate public opinion or influence decision-making. All of these potential issues need to be addressed in order to ensure that AI is used responsibly and ethically. The following are the potential issues related to AI and human security.

Data privacy: Data privacy is a growing concern as artificial intelligence systems are increasingly being used to collect, store, and analyze large amounts of data. This data can include personal information about individuals, such as their name, address, or financial information. If this data is not properly protected, it could be vulnerable to unauthorized access or misuse. To protect this data, organizations should implement appropriate security measures, such as encryption, access control, and data anonymization. Additionally, organizations should ensure that they have clear and transparent policies in place to protect the data and inform individuals about how their data is being used.

Finally, organizations should ensure that their systems are regularly monitored to detect any unauthorized access or misuse of the data.

Unintended Bias: Unintended bias is an issue that has been brought to the forefront of discussions about artificial intelligence (AI). AI systems can be trained on data sets that contain inherent biases, which can lead to decisions that are unfair or discriminatory. This can be a result of the data sets being incomplete or having been collected in a biased manner. For example, if an AI system is trained on a data set that is predominantly male, it may lead to decisions that are biased against women. Unintended bias can have serious implications, as it can lead to decisions that are not only unfair but also illegal. To address this issue, it is important to ensure that the data sets used to train AI systems are unbiased and complete. Additionally, AI systems should be tested to ensure that they are not making decisions that are biased or discriminatory. By taking these steps, we can ensure that AI systems are making decisions that are fair and equitable.

Job Loss: The increasing capabilities of AI systems could lead to job losses and economic disruption. As AI systems become more capable, they could potentially replace human workers in certain roles, such as customer service, data entry, and other repetitive tasks. This could lead to a decrease in the number of jobs available, as well as a decrease in wages for those jobs that remain. Additionally, it could lead to a decrease in consumer spending, as people may not have the disposable income to purchase goods and services. This could lead to a decrease in economic growth and an increase in unemployment. It is important to consider the potential implications of AI systems on the labour market and to develop strategies to mitigate the potential negative impacts.

Autonomous weapons: Autonomous weapons, or weapons systems powered by artificial intelligence, have the potential to cause a great deal of harm if used without human intervention. Such weapons could be used to target and attack without any human control, leading to an increased risk of war and more civilian casualties. The lack of human oversight could also lead to unintended consequences, such as targeting the wrong people or using excessive force. Autonomous weapons could also be used to perpetrate war crimes, as there would be no one to hold accountable for the actions taken. It is important to consider the ethical implications of using such weapons and to ensure that adequate safeguards are in place to protect civilians and prevent misuse.

Cyber security: is an important issue when it comes to AI systems. AI systems are vulnerable to cyber-attacks, which can lead to the loss of sensitive data or the manipulation of AI systems. Cyber-attacks can come in many forms, such as malware, ransom ware, phishing, and data breaches. These attacks can be used to steal data, disrupt operations, or even manipulate AI systems. As AI systems become more prevalent, it is important to ensure that they are protected from these threats. Companies should invest in robust cyber security measures, such as firewalls, encryption, and authentication, to protect their AI systems from cyber-attacks. Additionally, organizations should educate their employees on Cyber security best practices to ensure that their AI systems remain secure.

Regulatory Compliance: is an important issue when it comes to AI systems, as they may not comply with existing laws and regulations, leading to potential legal issues. This could include issues such as data privacy, consumer

protection, and anti-discrimination laws. To ensure compliance, organizations should consider implementing policies and procedures that address the potential legal risks associated with AI systems. Additionally, organizations should ensure that their AI systems are regularly monitored and tested to ensure that they are compliant with applicable laws and regulations. Finally, organizations should consider engaging legal counsel to help them navigate the legal implications of their AI systems.

Ethical Considerations: AI systems have the potential to make decisions that are ethically questionable, which can lead to potential ethical issues. For example, AI algorithms can be used to make decisions about hiring, loan approvals, and other areas of decision-making that involve ethical considerations. AI algorithms can make decisions that are biased or that favour certain groups of people over others, leading to potential ethical issues. Additionally, AI systems can be used to make decisions that are not transparent, making it difficult to determine the ethical implications of the decisions made. Finally, AI systems can be used to make decisions that are not in the best interests of the people affected by them, leading to potential ethical issues. All of these potential ethical issues must be taken into consideration when using AI systems to make decisions.

CONCLUSION

We have examined the potential of artificial intelligence for improving human security and reducing global threats. AI can be used to enhance security in a wide variety of contexts, including home and business security, border security, and public safety, among others. In addition to discussing the ethical implications of using artificial intelligence for security purposes, we have also discussed possible risks associated with its application. In addition, we have explored how artificial intelligence can be employed in the long term to promote human security. Our research has shown that AI can be an effective tool for improving security and reducing global risks, but it is important to consider the ethical implication of using AI for security purposes. Using artificial intelligence can help to create a more secure world if it is carefully considered and implemented.

REFERENCES

[1] I. H. Sarker, "Ai-based modeling: Techniques, applications and research issues towards automation, intelligent and smart systems," *SN Computer Science*, vol. 3, no. 2, pp. 1–20, 2022.
[2] E. Kamar, "Directions in hybrid intelligence: Complementing ai systems with human intelligence." in *IJCAI*, 2016, pp. 4070–4073.
[3] J.-P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations," *International Journal of Information Security*, vol. 21, no. 1, pp. 115–158, 2022.
[4] A. Arfeen, S. Ahmed, M. A. Khan, and S. F. A. Jafri, "Endpoint detection & response: A malware identification solution," in *2021 International Conference on Cyber Warfare and Security (ICCWS)*. IEEE, 2021, pp. 1–8.
[5] I. Johns, "Role of ai in tackling cybercrime," *Jus Corpus LJ*, vol. 2, p. 1233, 2021.
[6] D. Gasper, "Securing humanity: situating 'human security'as concept and discourse," *Journal of Human Development*, vol. 6, no. 2, pp. 221–245, 2005. [7] L. Elliott, "Human security/environmental security," *Contemporary Politics*, vol. 21, no. 1, pp. 11–24, 2015.

[8] I. Seeber, E. Bittner, R. O. Briggs, T. De Vreede, G.-J. De Vreede, A. Elkins, R. Maier, A. B. Merz, S. Oeste-Reiß, N. Randrup *et al.*, "Machines as teammates: A research agenda on ai in team collaboration," *Information & management*, vol. 57, no. 2, p. 103174, 2020.

[9] M. Anshari, M. N. Almunawar, M. Masri, and M. Hrdy, "Financial technology with ai-enabled and ethical challenges," *Society*, vol. 58, no. 3, pp. 189–195, 2021.

[10] F. Pedro, M. Subosa, A. Rivas, and P. Valverde, "Artificial intelligence in education: Challenges and opportunities for sustainable development," 2019.

[11] B. C. Stahl, J. Antoniou, M. Ryan, K. Macnish, and T. Jiya, "Organisational responses to the ethical issues of artificial intelligence," *AI & SOCIETY*, vol. 37, no. 1, pp. 23–37, 2022.

[12] J. Reardon, A. Feal, P. Wijesekera, A. Elazari Bar On, N. Vallina-Rodriguez, and S. Egelman, "50 ways to leak your data: An exploration of apps' circumvention of the android permissions system," in *28th USENIX Security Symposium*, 2019.

[13] C. Fontes, E. Hohma, C. C. Corrigan, and C. Lutge, "Ai-powered public surveillance systems: why we (might) need them and how we want them,"" *Technology in Society*, vol. 71, p. 102137, 2022.

[14] A. Borda, A. Molnar, C. Neesham, and P. Kostkova, "Ethical issues in ai-enabled disease surveillance: Perspectives from global health," *Applied Sciences*, vol. 12, no. 8, p. 3890, 2022.

[15] A. Jobin, M. Ienca, and E. Vayena, "The global landscape of ai ethics guidelines," *Nature Machine Intelligence*, vol. 1, no. 9, pp. 389–399, 2019.

[16] L. N. Tidjon and F. Khomh, "Never trust, always verify: a roadmap for trustworthy ai?" *arXiv preprint arXiv:2206.11981*, 2022.

[17] C. Benzaid, T. Taleb, and J. Song, "Ai-based autonomic & scalable security management architecture for secure network slicing in b5g," *IEEE Network*, 2022.

[18] A. Turobov, "Artificial intelligence and security: Transformation and consistency," *Higher School of Economics Research Paper No. WP BRP*, vol. 88, 2022.

[19] F. REPEZ and M.-M. POPESCU, "Social media and the threats against human security deepfake and fake news." *Romanian Military Thinking*, no. 4, 2020.

[20] C. Soh and D. Connolly, "The human security implications of the fourth industrial revolution in east asia," *Asian Perspective*, vol. 44, no. 3, pp. 383–407, 2020.