Balancing Usability and Protection in AI and Data Security: A Human-Centric Approach

Mohammed Jassim Al Ansari
School of Business
University of Central Lancashire
Preston, UK
mjmal-ansari@uclan.ac.uk

Yazan Al Ahmed
Faculty of Engineering
Al Ain University
Abu Dhabi, UAE
Yazan.alahmed@aau.ac.ae

Hadeel Hesham El Bahnaswi
Faculty of Engineering
Al Ain University
Abu Dhabi, U.A.E.
hadeelhesham246@gmail.com

Abstract*— As artificial intelligence (AI) systems become integral to our daily lives, the challenge lies in striking the delicate balance between usability and protection. This paper advocates for a human-centric approach—one that considers not only technical safeguards but also user experience. We explore behavioral insights, transparent communication, and collaborative efforts to enhance security while ensuring seamless interactions. By prioritizing both usability and protection, we pave the way for a secure and user-friendly AI landscape The increasing interplay between protection and usability results from the incorporation of artificial intelligence (AI) systems into our digital lifestyles. This research, which focuses on the Usability-Privacy Nexus, promotes a human-centric approach that goes beyond conventional security paradigms. We can design security procedures to fit users' mental models and decision-making processes by studying human behavior. Users must have open lines of communication and be trusted to understand the consequences of their actions. There are some methods for informing consumers about security measures without becoming too intrusive. Organizational culture, training initiatives, and user education are crucial factors that go beyond technical solutions. Awareness programs, nudges, and gamification can improve security literacy. Collaboration and user-centered design are also vital, incorporating people early in the process. Through the integration of behavioral information, entities can customize security protocols.

Keywords—artificial intelligence, usability, security, human-centric, security.

I. INTRODUCTION

In the last decade, we have witnessed an increased rate of development of artificial intelligence (AI), which has simplified our way of living. As this progress shows, several questions regarding data protection and security emerge. The increased usage of personal data by AI systems has, therefore, necessitated new approaches to AI and data protection. [1][2]

Usability may be more familiar as accessibility, that is the extent to which a product is easy to use and understand while protection is the security aspect, or how a system will keep its data safe from intruders. For both AI and data security, usability should not be an issue as complex systems such as machine learning could be very self-complicating, this would be counterproductive to the human-centered approach of AI.

However, cyber-attacks and data breaches have increased the demands for security and privacy enhancement. Data in general and particularly the personal type should be safeguarded from any wrong hands. It is alarming to detect what has happened and foresee further development of data breaches with the rising integration of various AI methods into our lives. Hence, protection is not always limited to and should not be left out in human-centric technologies of artificial intelligence and data security.[3]

In this respect, one provides a balance of usability and protection by applying privacy by design in the AI systems. This approach considers, data privacy and security capabilities from the early design of a system to allow for the storage or collection of user data with the necessary security features put into consideration.[4]

In a world that is connected, one must find a balance as to how useful information is and how it can be protected while living up to its actual potential in the enterprise through artificial intelligence (AI). This paper explores the tension between protection, putting in place robust security mechanisms and use, enabling efficient interaction. It emphasizes a human element since people are the focus of security. What security is today addresses people, processes, and things rather than simply technical challenges.

The research is a realism that security is about people: cognitive errors, decision processes, and the psychology of risk-based thought. An answer to these questions will allow us to build machines that provide power, not economic strength while protecting people. In today's connected world, enterprises need to find the middle ground between security and usability when it comes to AI. This research looks at the challenge of the balance between protection – strong security measures and usability – smooth interactions. It is a human-centric approach in which security design is based on end-user involvement as security is a shared responsibility among people, processes, and technology rather than just constituting of technical jumble.

The research is devoted to identifying what security is about: about people, and it looks at cognitive biases, decision-making procedures, and the psychology of risk perception. Providing answers to these questions allows us to create solutions that empower people without losing security. The paper calls for a holistic security perspective that goes beyond the technological fixes and the organization.

Another is, educating customers on data security and privacy. AI developers and companies that have access to the data of users around the world must take the responsibility to inform those users about the danger of sharing their data online. Users can then make more informed decisions about sharing their data begin to trust the AI system and understand why data protection is important.
(see Figure 1). [5]

Data security and AI were, and should be, human-centric approaches to AI and data security. The approaches focus on usability and try to simplify the process of security using more handy ways. For example, biometric authentication such as facial or fingerprint recognition means that passwords are no longer needed and a user burden is taken off, but it remains secure. As a result, personalized and personalized security measures can also be created by AI and machine learning, which will make the process of identifying others easy without compromising safety.[6]

In the world of AI and data security, there is a fine line of drawing between usable security and protection. Here, this paper dives into the main crucial question of maintaining the balance of this equilibrium through the human-centric approach, how we can make the user-centric design to improve the usability of security measures, how balancing usability with protection affects the trust and acceptance of user on the AI technology and how to implement security and ensure user-centric experience.

Apart from focusing on the requirements and experience of individuals, human-centric techniques also examine the ethical and social factors. Unseen by most people, the day brings with it an AI that can take in vast amounts of data and make decisions with little to no human oversight — a prospect that could lead to biased decision-making. By incorporating ethical principles and heterogeneous perspectives in the development and use of AI systems, human-centric approaches attempt to mitigate these risks.

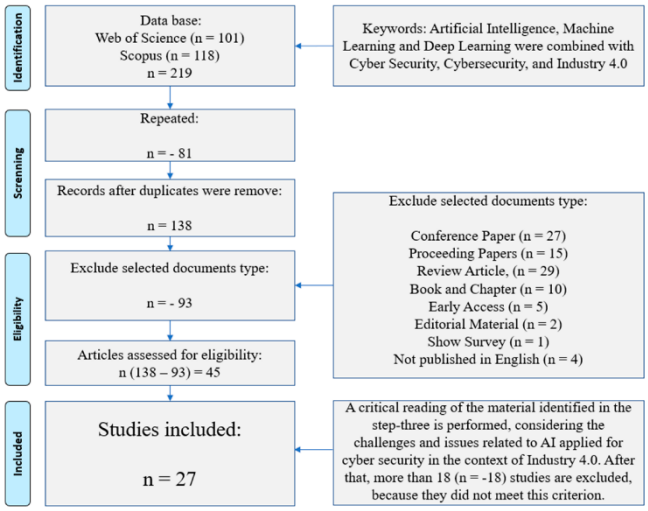

Fig.1, Prisma Flow, [38]

II. Literature Review

Today, AI and Data Security are very crucial, as advancements in AI create challenges in Data Privacy & Security. Hence, human-centric methods are offered as a solution to these problems. In this literature review, based on empirical and theoretical papers from the last 5 years on design choices regarding human-centric approaches to AI and data security, we study the trade-off between usability and protection.[8]

While many research studies concentrate on one or the other (i.e., usability in a nanny, protection in a kill switch), few acknowledge the significance of a complete, intermediate approach featuring human factors. A human-centric approach to this research is proposed which strives for a high level of security while ensuring a positive user experience. This research contributes to human needs and behaviors-oriented AI systems and data security protocols to a favorable human state and increases overall system performance and user satisfaction. [7]

Just in case: Usability and protection are the two essential parts of any system, but there is often a trade-off between the two. Protection means the prevention of unauthorized access to data or misuse of data to protect the data security and protection of data privacy and usability as ease of interaction between humans and the AI system. [9]

We want to achieve both usability and protection, but there is always tension between usability and protection. Depending upon the nature of the threat, robust security can make the system more productive and usable by trained professionals but less usable by the average user, whereas protecting users may impact the high level of usability in the system. Following a human-centered approach we can have a more comprehensive and efficient way of doing AI and data security practices that still allow for an optimal experience and at the same time cover important security.

The importance of a human-centric approach to both AI and data security in balancing what is usable with what is protected is the cornerstone of what we produce. The transparency and explainability of AI systems have critical effects on users' perception of usability by preserving high usability while protecting sensitive data. Other studies however have shown that a balance must be struck between usability and protection. As a result, users are willing to sacrifice their privacy to give sensitive data in return for convenience and ease of use; this indicates that the control of usability should be given over to protection. There's also trust involved in taking that balance between usability and protection.

A human-centered approach to AI and data security—putting the user's needs, concerns, and experiences first in decisions made regarding it. The downfall of this approach is it focuses on the ethical and responsible use of technology that that may play against the people and the society. It's meant to address concerns around AI and data security, like privacy, bias, and trust.

Usability is a term for how easy and efficient it is to use AI technology with users while protection is a term describing its measures to protect sensitive data from being unauthorized accessed. Usability and security seem

to be at odds with each other but balancing one can often feel like you're fighting against a losing cause; implementing strict security measures, although necessary, may prevent users from accessing and using data. This means that we must accommodate usability while safeguarding ourselves. In this domain of field, more work is still needed to develop more sophisticated and effective human-oriented approaches to AI and data security.

AI and data security is a prime aspect of what AI is and organizations around the globe must consider a few factors to make the workflow effective. User perspective, ethical use of AI, regulatory requirements, education and training, proactive security measures, and regular audits are among these.

However, decisions on usability and protection should consider the user's perspective, so that organizations know what they really need, what they prefer, and about what they are worried. Organizations should use AI in ethical ways — that means the ways that reflect their values and principles — tackling issues like bias and transparency in AI algorithms. It is necessary to comply with the requirements of regulation to implement the protection of sensitive data.

Increasing usability and protection requires education and training. Educating users about the risks of AI, and data security management, on the other hand, is another area of investment that should be made by organizations. Data encryption and multi-factor authentication can aid in addressing both the balance of usability and protection, as only the preferable users will have access to this sensitive data. [10]

With regular auditing and testing, you can identify vulnerabilities, and address them, before they become serious security risks. The successful and sustainable integration of AI and data security into our lives requires a human-centric approach. [11]

The design of AI and data security requires a human-centric approach to balancing usability and protection. Organizations strike a healthy balance between usability and protection by focusing on user needs and values, asking ethical questions, and proactive security measures. Maintaining regulatory requirements. Who knows if this will not change? Updating the technologies are also necessary to stay up to date. They would need to invest in education and training to use the technologies responsibly

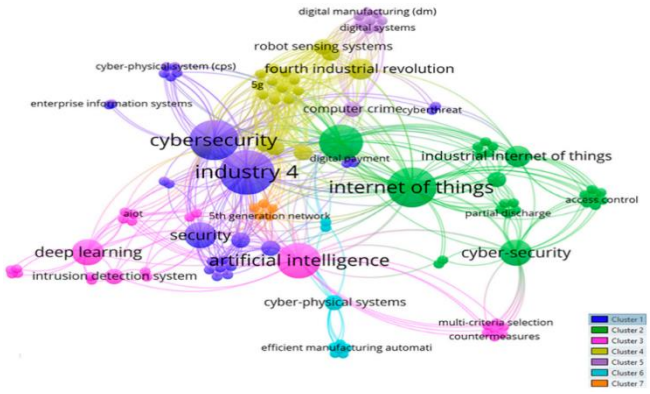

Fig.2, Diagram, [38]

and in the safe use of the technology. In conclusion, success and sustainability will not be long achieved by the effective and successful integration of AI and data security in our lives [12].

There are several factors that organizations must consider when balancing usability and protection in AI and data security:

1. User's Perspective: In the end, the final decisions of usability and protection should be guided by the user orientation. The key is to deeply know the user's needs, their preferences and their concerns. They do user research, and surveys and gather feedback to make appropriate use of their approach to what the user expects.
2. Ethical Use of AI: This means organizations must take on the ethical use of AI as a priority, making sure that it's aligned with everything your organization stands for. It covers concerns like eliminating bias and transparency on the part of the AI algorithms and making sure it doesn't exclude some from an

AI program. Increasing usability and protection requires education and training. Educating users about the risks of AI, and data security management, on the other hand, is another area of investment that should be made by organizations. Data encryption and multi-factor authentication can aid in addressing both the balance of usability and protection, as only the preferable users will have access to this sensitive data. [10]

With regular auditing and testing, you can identify vulnerabilities, and address them, before they become serious security risks. The successful and sustainable integration of AI and data security into our lives requires a human-centric approach. [11]

3. Regulatory Requirements: To protect sensitive data, the protection of the data follows regulatory requirements. To avoid legal consequences, the organizations must be updated on the changing laws and regulations regarding data security and privacy.
4. Education and Training: Education and training can improve usability and protection. Educating users on the risks of AI and data security, how to protect their data, and how to use AI technology in a productive manner is a responsibility that organizations must invest in.
5. Proactive Security Measures: Data encryption and multi-factor authentication are one way to balance usability with protection, but not the only one. That's to protect sensitive data, and, by only letting authorized users access it.
6. Regular Audits and Testing: Tests and regular audits can find vulnerabilities and rectify them before they turn into very large security risks. These measures may also help determine the effectiveness of current security measures and make needed improvements. .[12]

III. METHODOLOGY

AI and data security are progressing rapidly, causing an increase in concern about designing systems with a human-centric approach. In the security world, protection has traditionally trumped usability. But when it comes to

sensitive personal data and complex AI systems, it's all about balance between usable and protected.

A key method for achieving a human-centric approach to AI and data security is user-centered design (UCD). UCD comprises understanding end users' needs and preferences, adding them to the design process, and ensuring that the system is user-friendly yet secure and private. The result of this approach is continuous feedback from users to improve the balance between usability and protection.

Visual cues and simple language can make a system more usable by adding symbols such as icons and color making, helping prevent confusion. These cues also may convey to users' security measures so that complex security measures are easier to use and to understand and comply with.[13]

To strike the right balance between usability and protection in AI and data security, we need to tackle the problem from a human-centric perspective. This is an approach that combines qualitative and quantitative research methods (interviews, surveys, etc.) that gather and analyze data, as well as some usability testing. Using this method gives researchers insight into what users need or prefer, how effective security measures are in real life and a total picture of how users interact with technology. If companies place user needs and preferences out front during decision-making, then it enables the building of systems that are friendly to users as well as secure. Considering this, this approach accepts that ultimately, these systems will be used by people, and it is the people who must be at the Center of the design process.[14][15]

There are many ways that human-centric approaches to AI and data security exist. It's important to understand that the first step of user-centered design is done by understanding the user's needs, preferences, and behavior to create intuitive and easy-to-use AI systems. It also allows us to find potential usability issues early on and build user trust which in turn enables better adoption and usage.

Secondly, before you can implement any AI system, you need a thorough risk assessment and the means to mitigate that risk. It is the evaluation of potential threats and their impact and finding ways to mitigate them. However, because the threat agenda constantly changes, the system is being robustly tested, i.e. the system is regularly risk assessed to guarantee not only security but also adaptability to new threats.

Transparency and explainability are third things for the AI system. Users can have a hard time understanding complex algorithms and may mistrust and disagree. This has been overcome by human-centric approaches that call for transparent and explainable AI systems. That is, this means that users get to know how the system works as well as its decision-making process to be able to understand it and therefore trust it.

In the end, education and training are important methods of implementing human consciousness, which should be used in all data and AI. The use of these systems requires that properly trained individuals follow secure practices and use the system properly. It's important to continue to educate and train everyone who is involved because everyone is going to use the system and knowing how to do it safely is important.

Therefore, ethical considerations are essential to protect the rights and privacy of individuals. To achieve these human-centric approaches AI systems should be ethically responsible systems and should respect individual privacy, autonomy, and dignity. When designed accordingly, these elements enhance usability, while allowing for overall protection on different levels. AI can also be used to enhance the human-centric data security approach, such as with AI-based authentication systems alongside dropping complex passwords and regular logins. [17] [18]

By doing this, we can run them to balance usability and protection in AI and data security by analyzing user behaviors and detecting potential security breaches. Thanks to their system of continuously learning and updating their models, these algorithms can augment security while optimizing usability. Additionally, they can also automate some security processes to relieve the burden on the users and keep the sensitive data protected.

One other way of getting out of this conundrum is user-centric design principles for AI and data security. This technique places humans at the core of the design process, giving developers a better understanding of user needs and their preferences so that they can create interfaces that are more intuitive, more usable, and more secure, all the while keeping the user front and Center. This approach guarantees no extra effort with the inclusion of security features to the user experience, as well as minimizing the probability of user error and making available a more secure computing environment. [19]

For any AI-related decision-making, data analysis is important because data analysis identifies and finds patterns and trends in data and synthesizes the findings into meaningful conclusions. While the data can be interpreted using techniques such as thematic analysis or statistical analysis, to make recommendations for improvements to security measures, researchers may utilize such techniques. [20]

In this context, it is crucial to use the methodology in gathering and analyzing data used in the human-centered approach to achieve success. Both qualitative and quantitative research methods (interviews, surveys, and usability testing) can be combined with researchers to comprehend user's needs and wants and test the effectiveness of security measures in the real world. [21]

To end, balancing protection and usability needs to be human-centric, which applies to both AI and data security. Considering user interactions and potential consequences of security measures, companies can create systems that are both user-friendly and secure. [22] [23]

Fig. 3, AI Technology Landscape.[15]

The development of AI systems is strongly conditioned by data security and human aspects. Balancing usability and protection must be human centered to create a safe and efficient technological system. Creating user-friendly and secure AI systems is possible with user-centered design, risk assessment and transparency, education, and ethical considerations. However, these methods need to be continuously evaluated and improved to match the fast-evolving developments of the AI and data security landscape. By using UCD, visual cues, and AI technologies we can seek a balance between usability and protection. With prioritization of end-user needs and high levels of protection, a future of technology serving humanity safely and responsibly is possible [25].

IV. results

With the recent rapid growth of Artificial Intelligence (AI) and data security technologies comes concern about what they will do to human users. This has led to a trend of moving towards human-centric approaches to AI and data security built to balance usability and security. The human-centric approach is centered on the inclusion of human aspects in the design and development process to create technologies easy to use, understand, and trust. It is different than a technology-centered approach that puts technical functionality and security ahead of user experience.

In an increasingly digital life, AI and data security are tied together, and we must learn to design them with the end user in mind. Usability is prioritized; thus, creators can make sure that these technologies are accessible and user-friendly to the public. This research aimed to understand how organizations can find a balance between usability and protection when it comes to AI and data security, with research questions and objectives.

In the field of artificial intelligence, the fear of data security is very important, as the large amount of data being processed by artificial intelligence systems is often sensitive and confidential data. This research sought to investigate how to strike the balance between the usability and protection of AI and data security from a human-centric point of view. Using a human-centered approach can yield results that include users being able to trust and feel more confident that the AI systems they interact with or engage with are secure and also able to provide all them that they are usable and accessible, and as a result show increase in security because of adopting the AI systems. [15]

With the recent rapid growth of Artificial Intelligence (AI) and data security technologies comes concern about what they will do to human users. This has led to a trend of moving towards human-centric approaches to AI and data security built to balance usability and security. Human human-centric approach is centered on the inclusion of human aspects in the design and development process to create technologies easy to use, understand, and trust. It is different than a technology-centered approach that puts technical functionality and security ahead of user experience.

In an increasingly digital life, AI and data security are tied together, we must learn to design them with the end user in mind. Usability is prioritized; thus, creators can make sure that these technologies are accessible and user-friendly to the public. This research aimed to understand how organizations can find a balance between usability and protection when it comes to AI and data security, with research questions and objectives.

In the field of artificial intelligence, the fear of data security is very important, as the large amount of data being processed by artificial intelligence systems is often sensitive and confidential data. This research sought to investigate how to strike the balance between the usability and protection of AI and data security from a human-centric point of view. Using a human-centered approach can yield results that include users being able to trust and feel more confident that the AI systems they interact with or engage with are secure and is also able to provide all of them that they are usable and accessible, and as a result show increase in security because of adopting the AI systems. [15]

Therefore, an organization that wants to have AI systems trusted and confident must ensure better cybersecurity with a human-centered approach: balance usability and security in artificial intelligence and data security.

Data security is one of the big concerns in the modern digital era, which needs a human-centered methodology of approach, establishing trust between users and artificial intelligence, on one hand, and data security technologies on the other. A human-centered methodology focuses more on usability and transparency to make the process of trust establishment with security easier for sensitive information. It does come with one leak: the circle of security is compromised while focusing on the usability-for instance, the ease with which one logs into any device, or even with biometric security. Another important consideration involves the ethics of human-centric approaches toward AI and data security: the more advanced AI becomes, the more it will reach decisions or act in ways that, conventionally, have only been carried out by humans, and thus will begin to beg questions about responsibility and accountability where AI causes harm. In this respect, the human-centered approach places well-being and individual rights above functional feasibility.

Accessibility, trust, and ethical concerns make AI, with a focus on the user and security of data, so important.

It is important that artificial intelligence and the usage of data, from the developers, and designers to the policymakers, are underpinned with human-centered design principles, which not only make them secure but also more ethically responsible. Commitment to the guiding principles of human-centered design will be paramount by the actors as these technologies continue to develop in deploying AI and data securely and ethically.

At the same pace, AI and data technologies rapidly develop, revolutionizing not only business processes but also the level of engagement between people and technology. In turn, as AI and data are increasingly used, so do concerns about the security of data become widespread. Among those, human-centered AI and security of data were some of the approaches researchers suggested, trying to balance between usability and protection. These two approaches give center stage to the needs and competencies of individuals and are thus designed to come up with an effective and user-friendly framework for security.

Accordingly, some of the key human-centered approaches toward AI and data security are in applying usability engineering principles when designing security systems. Research by Tsitmidely and Mavromoustakis, 2020 shows that keeping the human factor in mind and applying principles of usability engineering in the design of security systems can increase user comprehension and observance and enhance general security. By making systems user-friendly and easy to operate, people will be much more likely to do what they need to do from a security aspect, making the capabilities of cyber-attacks a lot harder for them to take hold. [28] Other key elements include user-centric training and education programs. Zhang et al., in one of their studies, found that an education and training program focusing on user-centered design and usability significantly improves the compliance of users with security protocols and reduces the risk of data breaches.

Human-centric approaches to AI and data security have shown success in the usability of security systems while sustaining a high level of protection. .[29]

Fig.4, ENSURING DATA SECURITY IN AI SYSTEMS [30]

Human-centered design approaches to AI and data security have recently started to show some promising improvement in the usability and effectiveness of security. Designing intuitive systems and protocols minimizes users' burden and increases compliance to bring about effective ecosystems of security. User-oriented training and education programs make users aware of how best to protect their data from possible security threats. It would help, in the actual sense, to enable people to play an active role in data security and reduce human errors that often constitute one of the major factors in most cyberattacks. It is now time, in a world of rapidly changing technology, to focus on the human aspect of data security if a balance is to be struck between usability and protection. Further research and novelty in this domain would be required to meet the dynamic and ever-changing nature of data security threats. [30] [31] [32]

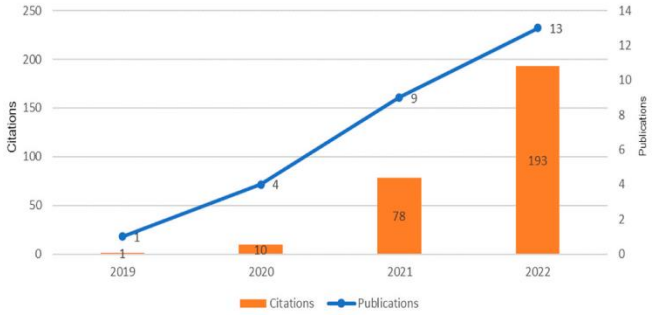

Fig.4, Times Cited and Publications Over Time.

V. DISCUSSION

The rapid development in AI and data science has broadly changed the face of the digital world. Also, with the changes, there are a lot of apprehensions related to privacy and safety concerning personal data. In this respect, an approach to AI and data security from a human-centric point of view is essential. There are two major streams concerning AI data security: usability and protection. [33] [34]

Usability is important in the design of systems that should be intuitive and thus easy to understand and navigate. This approach ensures that people using the technology can understand its features without frustration. A usability approach to data security puts the users in control and allows them to gain transparency over their data, hence making informed decisions about information disclosure. [35] [36]

Protection means keeping the data safe from potential perils and its misuse. Protection in AI includes encryption, controls over access, and other cybersecurity measures. In that respect, ensuring confidentiality, integrity, and availability protects privacy and user trust.

Usability and protection are two prime pillars of human-centered AI and data security, yet these two seem to be pulling in opposite directions more often. Loosening password complexity requirements or permissive data access can make the system more vulnerable to attacks. On the other hand, allowing an easier login increases the possibility of data breaches. A perfect balance between usability and protection needs to be met if one wants to get optimal data security and user experience in the virtual world. [8] The security of data is an integral part of the design process. To create something

user-friendly, one needs to make a very fine balance between usability and protection. While focusing on protection, a system becomes such that it is overly complicated and hard for a user, or simply that by paying too much attention to usability, frustration will set in and lead to non-adoption of the system. This is where the introduction of the principle of privacy by design in the creation of AI applications may provide a solution, embedding thus the notion of privacy and protection of personal data in the design and architecture. Accordingly, data security considerations will start right from the development stage and provide user-friendliness without any compromise to data security.[37][38][39] Moreover, human-centered design methodologies could be used in a very important way to adequately allow trade-offs between usability and protection. To be more precise, active users' involvement in design means understanding their needs and receiving feedback for the sake of catering systems toward intuitiveness and security preferences. The continuous growth of AI and data science use heightens the critical importance of human-centered approaches toward data security. A fine balance exists when developing technologies that are sensitive to user experience and data security. Fairly specifically, the research points out the human-centered approach to achieving a balance in usability and protection in AI and data security. It points out that the more complicated the security measure, the more frustrated users will be, which leads to non-compliance that affects security posture negatively. An organization will enhance security provided the design of technologies takes into consideration peoples' needs and genuine user feedback. It meets the ever-growing number of research recommendations that advocate for an approach that truly puts humans at the center of cybersecurity-one that incorporates understanding and addressing end-user needs and behaviors. Thus, AI takes security as the highest priority. Large volumes of data get processed through AI systems, which are often sensitive and of a highly confidential nature. A human-centered approach lets organizations create a balance in designing the AI systems for security, while at the same time making them more usable and accessible to engender user trust and confidence in the AI systems themselves. In this way, an organization should try to find new ways of ensuring data security, considering aspects of usability and protection. Of utmost importance, the design and application of AI need to be sensitive to the human factor. [40] [41]

VI. Conclusion

This is especially about the AI systems and the security of data. Human-centered approaches balance usability and protection to ensure that individuals and organizations can use AI and data security in ways that uphold their privacy and security. The approach, therefore, makes the interests of the individual and their rights the first consideration, insofar as data collection and use of AI could affect people's lives profoundly. A core dimension of a human-centered approach would therefore be that usability is foregrounded, in which security procedures in relation to data and AI systems are easy to understand and intuitive for users.

This, in turn, would incentivize users to interact even more with these systems and contribute data towards their development, which further refines and increases the accuracy of results coming out from AI.

Usability should not be at the expense of security, however; data security and AI should be robust and resilient enough to deflect any potential future cyberattacks to protect sensitive information. The human-centered approach can bring a lot of benefits both to organizations and individuals. This would give more control to people regarding their own data and its privacy, hence making them more confident in adopting AI systems.

It also allows transparency in the way it will enable the citizens to understand in what way their data is being collected, used, and protected.

The resulting trust and transparency can lead to more data being shared, which in turn will enable more accurate and diverse AI systems that will help society. Human-centered concepts let organizations create and implement AI and data security procedures that can ensure it serve people and society in general. Safety and usability in AI and data security cannot be balanced easily, and this is a major challenge; this aspect calls for a human-centered approach. Integration of users early in the design phase will enable intuitive solutions that are safe. More transparency is needed, and users do have a right to know how their data is processed and what security exists.

The behavioral insights can be used to keep security improved, suggesting password changes after certain periods of time or using two-factor authentication.

As the concept of security is somewhat dynamic, making a system secure involves constant reviews, improvements, and educating the users.

It is only by working in collaboration that true balance between security and usability can be achieved by the security experts, designers, and the end users themselves. Finally, the human-centric approach realizes that security is not a separate issue of technology, but a matter of cooperation. Data-driven and artificial intelligence without giving away to security must place usability first.

References

[1] K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, "A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities," IEEE Commun. Surv. Tutorials, vol. 22, no. 4, pp. 2489–2520, Oct. 2020, doi: 10.1109/COMST.2020.3011208.

[2] "ai privacy: AI and Privacy: The privacy concerns surrounding AI, its potential impact on personal data - The Economic Times." https://economictimes.indiatimes.com/news/how-to/ai-and-privacy-the-privacy-concerns-surrounding-ai-its-potential-impact-on-personal-data/articleshow/99738234.cms?from=mdr (accessed Mar. 11, 2024).

[3] "Risks of AI & Cybersecurity | Risks of Artificial Intelligence." https://www.malwarebytes.com/cybersecurity/basics/risks-of-ai-in-cyber-security (accessed Mar. 11, 2024).

[4] P. Mahesh et al., "A Survey of Cybersecurity of Digital Manufacturing," Proc. IEEE, vol. 109, no. 4, pp. 495–516, Apr. 2021, doi: 10.1109/JPROC.2020.3032074.

[5] A. Rajkomar et al., "Scalable and accurate deep learning with electronic health records," npj Digit. Med., vol. 1, no. 1, Dec.

2018, doi: 10.1038/S41746-018-0029-1.

[6] F. B. Saghezchi, G. Mantas, M. A. Violas, A. M. de Oliveira Duarte, and J. Rodriguez, “Machine Learning for DDoS Attack Detection in Industry 4.0 CPPSs,” Electron., vol. 11, no. 4, Feb. 2022, doi: 10.3390/ELECTRONICS11040602.

[7] P. Blanco-Medina, E. Fidalgo, E. Alegre, R. A. Vasco-Carofilis, F. Jañez-Martino, and V. F. Villar, “Detecting vulnerabilities in critical infrastructures by classifying exposed industrial control systems using deep learning,” Appl. Sci., vol. 11, no. 1, pp. 1–14, Jan. 2021, doi: 10.3390/APP11010367.

[8] M. Q. Tran, M. Elsisi, K. Mahmoud, M. K. Liu, M. Lehtonen, and M. M. F. Darwish, “Experimental Setup for Online Fault Diagnosis of Induction Machines via Promising IoT and Machine Learning: Towards Industry 4.0 Empowerment,” IEEE Access, vol. 9, pp. 115429–115441, 2021, doi: 10.1109/ACCESS.2021.3105297.

[9] S. Ali et al., “Explainable Artificial Intelligence (XAI): What we know and what is left to attain Trustworthy Artificial Intelligence,” Inf. Fusion, vol. 99, p. 101805, Nov. 2023, doi: 10.1016/J.INFFUS.2023.101805.

[10] T. H. Szymanski, “The ‘Cyber Security via Determinism’ Paradigm for a Quantum Safe Zero Trust Deterministic Internet of Things (IoT),” IEEE Access, vol. 10, pp. 45893–45930, 2022, doi: 10.1109/ACCESS.2022.3169137.

[11] S. M. McKinney et al., “International evaluation of an AI system for breast cancer screening,” Nature, vol. 577, no. 7788, pp. 89–94, Jan. 2020, doi: 10.1038/S41586-019-1799-6.

[12] T. Jadczyk, W. Wojakowski, M. Tendera, T. D. Henry, G. Egnaczyk, and S. Shreenivas, “Artificial intelligence can improve patient management at the time of a pandemic: The role of voice technology,” J. Med. Internet Res., vol. 23, no. 5, May 2021, doi: 10.2196/22959.

[13] P. Singh, “Systematic review of data-centric approaches in artificial intelligence and machine learning,” Data Sci. Manag., vol. 6, no. 3, pp. 144–157, Sep. 2023, doi: 10.1016/J.DSM.2023.06.001.

[14] “(PDF) Qualitative Exploration of AI’s Influence on E-commerce Satisfaction in C2C Platforms: A WEBQUAL Framework Perspective.” https://www.researchgate.net/publication/374372437_Qualitative_Exploration_of_AI’s_Influence_on_E-commerce_Satisfaction_in_C2C_Platforms_A_WEBQUAL_Framework_Perspective (accessed Aug. 12, 2024).

[15] A. Re-Thinking et al., “Re-Thinking Data Strategy and Integration for Artificial Intelligence: Concepts, Opportunities, and Challenges,” Appl. Sci. 2023, Vol. 13, Page 7082, vol. 13, no. 12, p. 7082, Jun. 2023, doi: 10.3390/APP13127082.

[16] D. S. Berman, A. L. Buczak, J. S. Chavis, and C. L. Corbett, “A survey of deep learning methods for cyber security,” Inf., vol. 10, no. 4, 2019, doi: 10.3390/INFO10040122.

[17] N. Tuptuk and S. Hailes, “Security of smart manufacturing systems,” J. Manuf. Syst., vol. 47, pp. 93–106, Apr. 2018, doi: 10.1016/J.JMSY.2018.04.007.

[18] T. Suleski, M. Ahmed, W. Yang, and E. Wang, “A review of multi-factor authentication in the Internet of HealthcareThings,” Digit. Heal., vol. 9, Jan. 2023, doi: 10.1177/20552076231177144.

[19] R. Kaur, D. Gabrijelčič, and T. Klobučar, “Artificial intelligence for cybersecurity: Literature review and future research directions,” Inf. Fusion, vol. 97, p. 101804, Sep. 2023, doi: 10.1016/J.INFFUS.2023.101804.

[20] “Balancing Security and Privacy in the Age of Artificial Intelligence: A Global Challenge.” https://www.linkedin.com/pulse/balancing-security-privacy-age-artificial-intelligence-santosh-g-1f1bc (accessed Aug. 12, 2024).

[21] “(PDF) AI and Predictive Analytics.” https://www.researchgate.net/publication/370074080_AI_and_Predictive_Analytics (accessed Aug. 12, 2024).

[22] R. Alfredo et al., “Human-centred learning analytics and AI in education: A systematic literature review,” Comput. Educ. Artif. Intell., vol. 6, p. 100215, Jun. 2024, doi: 10.1016/J.CAEAI.2024.100215.

[23] “What Is Human-Centered AI (HCAI)? — updated 2024 | IxDF.” https://www.interaction-design.org/literature/topics/human-centered-ai?srsltid=AfmBOoqzy-2c0rrCkCDrKyOA3b59BoEhs9h43tGkRvYfjwM8V2Ehd44f (accessed Aug. 12, 2024).

[24] J. H. Chen and S. M. Asch, “Machine Learning and Prediction in Medicine — Beyond the Peak of Inflated Expectations,” N. Engl. J. Med., vol. 376, no. 26, pp. 2507–2509, Jun. 2017, doi: 10.1056/NEJMP1702071.

[25] M. Barton, R. Budjac, P. Tanuska, G. Gaspar, and P. Schreiber, “Identification Overview of Industry 4.0 Essential Attributes and Resource-Limited Embedded Artificial-Intelligence-of-Things Devices for Small and Medium-Sized Enterprises,” Appl. Sci., vol. 12, no. 11, Jun. 2022, doi: 10.3390/APP12115672.

[26] “Artificial intelligence usage in multi-factor authentication | Blog - Future Processing.” https://www.future-processing.com/blog/artificial-intelligence-usage-in-multi-factor-authentication/ (accessed Aug. 12, 2024).

[27] “What Is Human-Centered AI (HCAI)? — updated 2024 | IxDF.” https://www.interaction-design.org/literature/topics/human-centered-ai?srsltid=AfmBOorgI3PsZSw2w53wH7fU0nxkhx7QpTSVcyju9Psub8X7bOgsVZRO (accessed Aug. 12, 2024).

[28] A. J. G. de Azambuja, C. Plesker, K. Schützer, R. Anderl, B. Schleich, and V. R. Almeida, “Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey,” Electron. 2023, Vol. 12, Page 1920, vol. 12, no. 8, p. 1920, Apr. 2023, doi: 10.3390/ELECTRONICS12081920.

[29] R. Y. Zhong, X. Xu, E. Klotz, and S. T. Newman, “Intelligent Manufacturing in the Context of Industry 4.0: A Review,” Engineering, vol. 3, no. 5, pp. 616–630, 2017, doi: 10.1016/J.ENG.2017.05.015.

[30] “Data security in AI systems.” https://www.leewayhertz.com/data-security-in-ai-systems/ (accessed Mar. 11, 2024).

[31] E. J. Topol, “High-performance medicine: the convergence of human and artificial intelligence,” Nat. Med., vol. 25, no. 1, pp. 44–56, Jan. 2019, doi: 10.1038/s41591-018-0300-7.

[32] N. Singh, V. Krishnaswamy, and J. Z. Zhang, “Intellectual structure of cybersecurity research in enterprise information systems,” Enterp. Inf. Syst., vol. 17, no. 6, 2023, doi: 10.1080/17517575.2022.2025545.

[33] H. Yang, K. Zhan, M. Kadoch, Y. Liang, and M. Cheriet, “BLCS: Brain-Like Distributed Control Security in Cyber Physical Systems,” IEEE Netw., vol. 34, no. 3, pp. 8–15, May 2020, doi: 10.1109/MNET.011.1900275.

[34] K. Saleem, G. M. Alabduljabbar, N. Alrowais, J. Al-Muhtadi, M. Imran, and J. J. P. C. Rodrigues, “Bio-Inspired Network Security for 5G-Enabled IoT Applications,” IEEE Access, vol. 8, pp. 229152–229160, 2020, doi: 10.1109/ACCESS.2020.3046325.

[35] N. D. Trung, D. T. N. Huy, L. T. T. Huong, T. Van Thanh, N. T. P. Thanh, and N. T. Dung, “Digital Transformation, AI Applications and IoTs in Blockchain Managing Commerce Secrets: And Cybersecurity Risk Solutions in the Era of Industry 4.0 and Further,” Webology, vol. 18, no. Special Issue, pp. 453–465, 2021, doi: 10.14704/WEB/V18SI04/WEB18140.

[36] A. S. Malik, S. Acharya, and S. Humane, “Exploring the Impact of Security Technologies on Mental Health: A Comprehensive Review,” Cureus, vol. 16, no. 2, Feb. 2024, doi: 10.7759/CUREUS.53664.

[37] Y. Alahmed, R. Abadla and M. J. A. Ansari, "Exploring the Potential Implications of AI-generated Content in Social Engineering Attacks," 2024 International Conference on Multimedia Computing, Networking and Applications (MCNA), Valencia, Spain, 2024, pp. 64-73, doi: 10.1109/MCNA63144.2024.10703950.

[38] Y. A. Ahmed and A. Sharo, "On the Education Effect of CHATGPT: Is AI CHATGPT to Dominate Education Career Profession?," 2023 International Conference on Intelligent Computing, Communication, Networking and Services (ICCNS), Valencia, Spain, 2023, pp. 79-84, doi: 10.1109/ICCNS58795.2023.10192993.

[39] Y. Alahmed, R. Abadla, A. A. Badri and N. Ameen, "“How Does ChatGPT Work” Examining Functionality To The Creative AI CHATGPT on X's (Twitter) Platform," 2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS), Abu Dhabi, United Arab Emirates, 2023, pp. 1-7, doi: 10.1109/SNAMS60348.2023.10375450.

[40] Yazan Alahmed, Reema Abadla, N. Ameen, and Abdulla Shteiwi, “Bridging the Gap Between Ethical AI Implementations,” International Journal of membrane science and technology, vol. 10, no. 3, pp. 3034–3046, Oct. 2023, doi: https://doi.org/10.15379/ijmst.v10i3.2953.

[41] H. Hesham, Y. Al Ahmed, B. Wael and M. Saleh, "Solar-Powered Smart Bin: Revolutionizing Waste Classification for a Sustainable Future," 2023 24th International Arab Conference on Information Technology (ACIT), Ajman, United Arab Emirates, 2023, pp. 1-8, doi: 10.1109/ACIT58888.2023.10453850.