International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Designing Artificial Intelligence (AI) Based Secured Framework to Improvise the Data Security of Confidential Academic Records

[1]Dr. Mukesh Agarwal, [2]Dr. Manish Saraswat, [3]Dr. Promila Bahadur, 4Dr. Anju Asokan, [5]Dr. Varsha Bapat

Submitted: 21/01/2023 **Accepted:** 26/03/2023

Abstract: One of the difficulties associated with conducting analytics using artificial intelligence is trying to maximise utility while also safeguarding human rights and maintaining meaningful human control. In this situation, one of the most important things for policymakers and lawmakers to think about is how much they should let protection be done automatically in a society that is becoming more digital. Such Security-Preserving Technologies have the goal of implementing security-by-design into the back end and front end of digital services from the very beginning of the development process. They watch over the data architectures to make certain that they are safe and sound, as well as ensuring that any data-related dangers are neutralised during the design phase as well as during operation. In this paper, we talk about recent trends in the development of tools and technologies that help make AI security analytics safe and reliable. We also give recommendations based on the research's findings and insights. We also talk about recent trends in the creation of tools and technologies that make AI security analytics safe and reliable. This paper makes a contribution to the discussion by investigating the various technical solutions that have been developed by the projects of the AI-based secured framework. These solutions aim to protect academic records in terms of both their security and their confidentiality.

Keywords*: Artificial Intelligence (AI), Secured Framework, Data Security, Confidential Academic Records*

1. Introduction

Artificial intelligence, or AI, is the capacity of machines to carry out "smart" or "intelligent" tasks without the need for human direction or intervention. Artificial intelligence (AI) can be used for security by reducing the amount of human involvement required to detect and respond to cyber threats. For this purpose, we employ AI (AI).

The "good" and "bad" classifications made by AI safety equipment are typically determined by comparing the actions of entities in one environment to those in another environment that is similar to the first. Artificial intelligence is used to perform this comparison. This system allows the device to monitor for and report any changes automatically. This approach, known as unsupervised learning or "pattern of life" learning, generates many spurious positive and negative results. The concept represented by these two labels is identical.

1Assistant Professor, Department of Commerce (School of Studies in Management and Commerce, Guru Ghasidas Vishwavidyalaya (A Central University), Koni, Bilaspur (CG)
2 Associate professor, Faculty of Science & Technology, ICFAI University, Baddi, Himachal Pradesh
3 Associate Professor , Department of Computer Science and Engineering ,IET Lucknow, Uttar Pradesh
4Assistant Professor, Department of Computer and Communication Engineering , Sri Eshwar College of Engineering, Coimbatore, Tamil Nadu
5Associate Professor, Department of Electronic Science, PES'S Modern College of Arts, Science and Commerce, Pune, Maharashtra

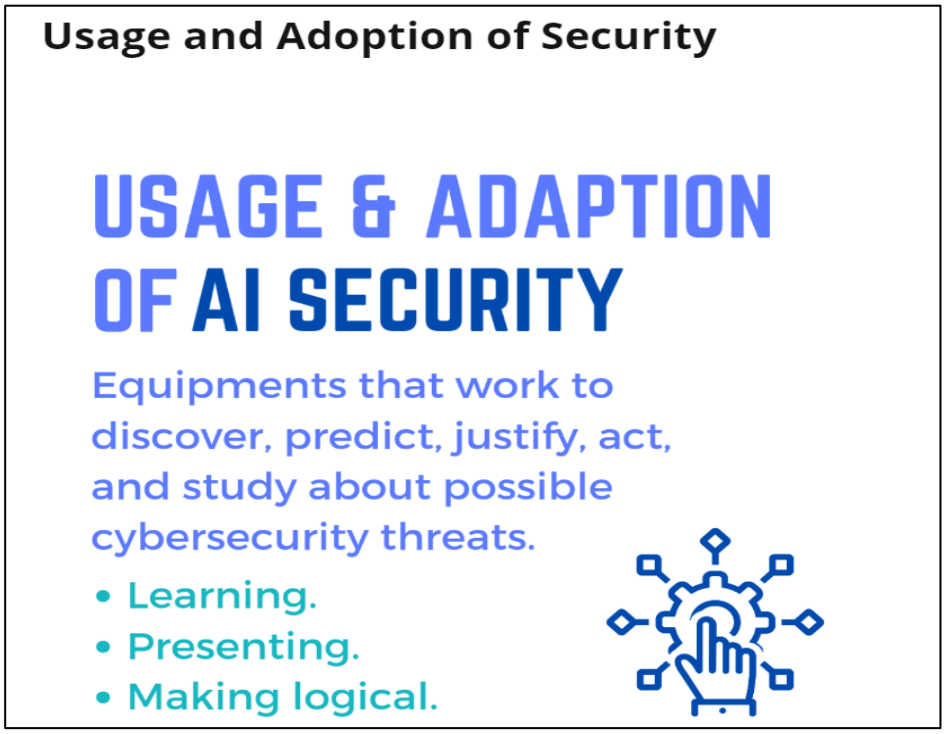
In more advanced applications, AI security can do more than just determine whether or not a user's actions are accurate or terrible by examining massive amounts of data and helping to piece together related activities that should point to suspicious behaviour. When used in this way, AI security functions in a manner similar to that of the most pleasant and successful human analyst.

Every day, new information equal to quintillions of bytes is added to the universe, and the total amount of data in the universe doubles about every two years. The information Big Bang is a term used to describe this event (Bernard Marr, 2018).

The three "Vs," volume, variety, and velocity, are frequently used to characterise the impact of big data. The more information is analysed, the more specific and useful the findings will be. Diversity aids in this strength and allows for the formation of novel and surprising inferences and interpretations. This real-time analysis and dissemination of information is made much simpler by the speed with which it can be transmitted. Information about every facet of our lives is being generated at an unprecedented rate thanks to the proliferation of data streams from mobile phones and other online devices, making privacy a pressing global public policy issue.

This development is likely to speed up thanks to AI. Many of today's most intrusive uses of data analysis rely on

machine learning and algorithmic decision making, including search algorithms, recommendation engines, and adtech networks. As AI improves, it will increase the speed and accuracy with which personal data can be analysed, which could compromise individuals' right to privacy.



Face recognition systems give us a hint of the privacy problems that will come up in the future. The availability of large collections of digital images makes this a reality. Facial recognition systems are being implemented at airports and other public locations across the United States at the present time. But (Paul Mozur,2019) has sparked opposition to this growth, leading to calls for a ban on the technology. Concerns about the accuracy and privacy of facial recognition technology have led to bans on its use in several cities, including Oakland, San Francisco in California, Somerville (Sara Merken, 2020). It is now against the law in California, New Hampshire, and Oregon for law enforcement to use body cameras equipped with facial recognition software (Matthias, 2017).

The use of AI and the ongoing controversy over the safety of student records are both topics explored in this policy brief. Congress is currently debating whether or not to pass a sweeping security and privacy bill to address the growing gaps between federal and state privacy and security regulations. Congress must decide if and how to regulate the collection, storage, and dissemination of individual data used by AI. In this paper, we explore some of the policy options currently under discussion and discuss some of the potential concerns related to AI security, including discrimination, ethical use as well as human control.

2. Review Literature

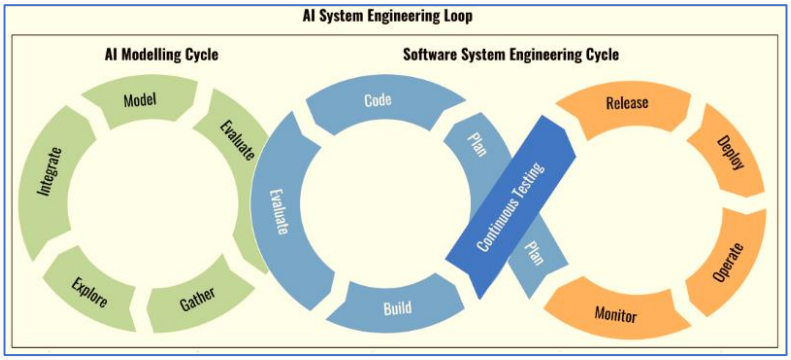
As recent news about data leaks, has shown, more people are becoming aware of misusing of academic data. This has made people less likely to trust these platforms and digital services (Newman et al. 2017). Many social media sites generate revenue either by charging users for access to their services or by keeping tabs on what their users are up to online. The shift from using a desktop or laptop computer and a web browser apps designed for those devices has made it possible to collect in near real time. People's physical and digital locations becoming more intertwined offers exciting new opportunities but also raises serious concerns about personal privacy. The dangers that this information poses, especially when mixed with other types of information, are not always obvious. Discussions on the specifics of what constitutes "personal data" (Purtova 2018) and how to implement safeguards for personal information in the context of large-scale data analytics have taken on an increased level of urgency in the current climate of data protection regulation.

Academic data protection challenges in the context of AI analytics centre on the use of large PHI for purposes like profiling and prediction. One unintended consequence of AI analytics is that it is possible to identify individuals or obtain other private data by combining seemingly innocuous pieces of information (Kerr 2012). Because of

this, many of the methods used to pseudonymize and anonymize data today are inadequate. The data protection premise that there must be a clear and well-articulated objective for any type of processing runs counter to the premise that data-driven innovation frequently relies on the exploration of data to establish an objective, creating a conundrum for the field of data science. This contrast is not new, but it has been exacerbated by the rapid development and increasing complexity of data analytics in recent years. If we want to protect research data without sacrificing the benefits of an AI framework, we'll have to try some new strategies.

3. Security Issues In AI

The difficulty lies in passing security legislation that safeguards individuals against any harm that may result from the use of personal information in AI without unduly restricting AI development or entangling security legislation in complex social and political quagmires (Jeffrey, 2018). Both are legitimate causes for concern, but privacy laws are already complex enough without factoring in the myriad of social and political issues that can arise from various uses of information. Neither of these is reassuring at all.

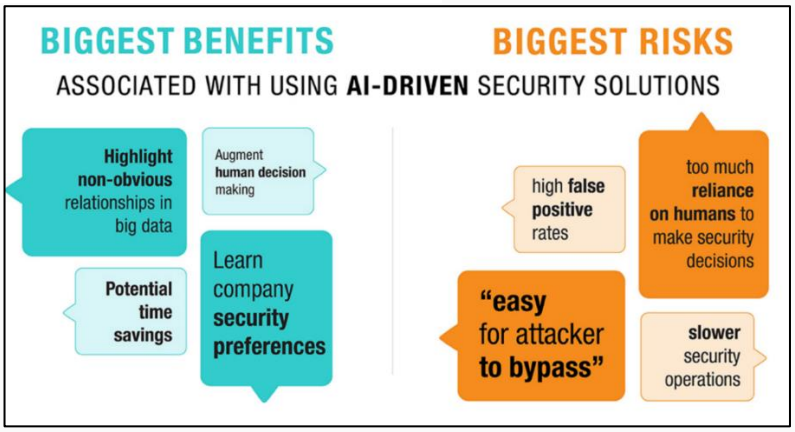


To figure out how AI affects security, it's important to separate the role of data problems that all AI has, like false positives and negatives or overfitting to patterns. Overfitting to patterns and the possibility of false positives and negatives are two examples of the problems that can arise due to imperfect data.

There is no direct mention of AI in any of the relevant legislative proposals addressing national security concerns. Instead, they use terms like "automated decisions" (a term borrowed from the European Union's data protection law) and "algorithmic decisions" (used in this discussion). The language used to describe AI's use of personal data and the potential effects of this use on individuals draws attention away from AI itself. The potential for algorithms to produce unlawful or unwelcome discrimination in decisions relating to algorithms, as well as algorithmic bias, are the primary topics of this discussion. Civil rights organisations and consumer advocacy groups, which represent people or communities that have been unfairly targeted, see these as major areas of focus.

4. AI Policy Options for Security Protection

When discussing AI in the context of security legislation, there are primarily two types of responses being discussed. The first strategy actively combats bias. Twenty-six civil rights and consumer organisations wrote an open letter calling for restrictions on or oversight of the sale or use of data that could be used to discriminate against "people of colour, women, religious minorities, members of the LGBTQ+ community, persons with disabilities, persons living in poverty, immigrants, and other vulnerable populations."



Law have incorporated this principle into model legislation. The goal of this proposed piece of legislation is to prohibit discrimination based on a person's personal information in the areas of employment, housing, and voting (Stanley, 2019). This law also contains a provision that prevents the use of personal information for the purpose of discrimination or classification based on legally protected characteristics like race, gender, and sexual orientation (Cameron, 2020).

5. Security & Privacy of Confidential Academic Records

When tackling the issue of algorithmic discrimination, important questions about the scope of security and privacy legislation are raised. When it comes to concerns of bias in algorithmic decision-making the only factor that brings discrimination into the realm of civil rights laws, however; it's just one piece of a much larger social problem. It is therefore not obvious that bias is a threat to individual safety and privacy. Furthermore, making these laws available for debate could be like opening the box of Pandora because they touch on emotionally charged political issues and multiple congressional committees have jurisdiction over a variety of these issues. Therefore, security and privacy interests in controlling how information is used are implicated when personally identifiable information about these characteristics is used, either directly through to the interests of the individual involved.

Second, the current model of how security and privacy laws are interpreted will need to be revised if these privacy interests are to be protected in the context of AI. The "notice-and-choice" (also known as "notice-and-consent") model of consumer choice is the basis for the vast majority of currently effective privacy laws as well as the enforcement efforts of the Federal Trade Commission (FTC) against unfair and deceptive business practises. The tactic consists of bombarding customers with notices and banners that lead to unwieldy and unclear privacy and terms and conditions documents. Such forms of paperwork have our "implied" approval, but we usually skip over them. The concept of "notice and choice" has been rendered meaningless as a result of this consent ruse. For many uses of artificial intelligence, such as the smart traffic lights and other sensors needed for autonomous vehicles, it will become impossible to do so.

6. Findings of the study

The following are just some of the ways in which data-driven research may one day affect artificial intelligence and algorithmic discrimination:

- Rules regarding the transparency or disclosure of data, along with the rights of individuals to access information that pertains to them, could shed light on the applications of algorithmic decision-making.
- Requirements for data stewardship, such as duties of fairness or loyalty, could act as a deterrent against the use of personal information in ways that are detrimental to or unfair to the individuals to whom the data relates.
- These overarching rules may have an indirect effect on algorithmic decisions, but there are also a few proposals that directly address the issue.

7. Conclusion

Potentially negative outcomes from using big data technologies in different contexts necessitate tailoring responses and developing different technological safeguards. Even though technical solutions that go with them, there is still more work to be done to identify, understand, and share the type of solution that is best for a given problem. Especially the data-driven, startup, and small and medium-sized business (SME) sectors stand to gain a lot from this. The work of ISO standardisation bodies and others who try to classify technologies helps a lot with understanding, forming, and ranking the order of importance for problems and solutions in the field of privacy engineering. Thanks to the work of the above projects to clean up data, a common privacy language and semantics between machine language and human language are getting better. This is a crucial stage in the process of preparing high-quality data for use by AI, which will allow for the automation of compliance processes. It is essential to keep pushing for a market that values technologies that protect privacy and security.

Furthermore, we need to keep pushing for improved technological standards surrounding privacy-protecting technologies. Despite the challenges and complications of implementing privacy regulations, the security measures taken by institutions can be viewed as a significant advance in the protection of students' academic records. This is so despite the many obstacles and complications that will arise during implementation. There is, however, still a lack of clarity regarding the operational ramifications of the security, especially when taken into account alongside other regulations concerning data.

References

[1] Archana, P., Divyabharathi, P., Balaji, S.R., Kumareshan, N., Veeramanikandan, P., Naitik, S.T., Rafi, S.M., Nandankar, P.V., Manikandan, G. Face recognition based vehicle starter using machine learning (2022) Measurement: Sensors, 24, art. no. 100575.

[2] Bernard Marr, “How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone

Should Read," Forbes, May 21, 2018. A quintillion is a 1 followed 30 zeroes.

[3] Cameron F. Kerry and Caitlin Chin, "Hitting refresh on privacy policies: Recommendations for notice and transparency," The Brookings Institution, January 6, 2020.

[4] De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. Computer Law & Security Review, 34(2), 193–203.

[5] Jeffrey Dastin, "Amazon scraps secret AI recruiting tool that showed bias against women," Reuters, October 9, 2018

[6] Kerr, O. S. (2012). The Mosaic Theory of the Fourth Amendment. Rev. 311.

[7] Matthias Spielkamp, "Inspecting Algorithms for Bias," MIT Technology Review, June 12, 2017.

[8] Mojjada, R. K., & Bhattacharyya, D. D. (2016). Data Security And Integrity in Adoption of Cloud Computing. Kaav International Journal of Science, Engineering & Technology, 3(1), 38-49. https://www.kaavpublications.org/abstracts/data-security-and-integrity-in-adoption-of-cloud-computing

[9] Newman, N. Fletcher, R. Kalogeropoulos, A., Levy, D., & Nielsen, R. K. (2017). Reuters Institute Digital News Report 2017.

[10] Nicol Turner Lee, Paul Resnick, and Genie Barton, "Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms," The Brookings Institution, May 22, 2019.

[11] Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority," New York Times, April 14, 2019.

[12] Patra, J. P., Sethia, N., & Gupta, P. (2018). Home Assistant Using Artificial Intelligence. Kaav International Journal of Economics, Commerce & Business Management, 5(2), 40-43.

[13] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. Law, Innovation and Technology, 10(1), 40–81.

[14] Patra, J. P., Sethia, N., & Gupta, P. (2018). Home Assistant Using Artificial Intelligence. Kaav International Journal of Economics, Commerce & Business Management, 5(2), 40-43.

[15] Shinde, S. N. (2016). Data Security Using Cryptic Steganography Approach. Kaav International Journal of Science, Engineering & Technology, 3(3), 16-22. https://www.kaavpublications.org/abstracts/data-security-using-cryptic-steganography-approach

[16] Sara Merken, "Berkeley Bans Government Face Recognition Use, Joining Other Cities," Bloomberg Law, October 16, 2019; Nikolas DeCosta-Klipa, "Brookline becomes 2nd Massachusetts community to ban facial recognition," Boston.com, December 12, 2019. Tori Bedford, "Cambridge Votes To Ban Face Surveillance Technology," WGBH, January 13, 2020.

[17] Stanley Augustin, "Lawyers' Committee for Civil Rights Under Law and Free Press Action Release Proposed 'Online Civil Rights and Privacy Act' to Combat Data Discrimination," Lawyers' Committee for Civil Rights Under Law, March 11, 2019.

[18] SR Ashokkumar, M Premkumar, P Dhilipkumar, P Manikandan, P Naveen, M Saravanan, "Application of Multi-Domain Feature for Automated Seizure Detection from EEG Signal", 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC), pp.280-285,2022

[19] https:/web.stanford.edu/class/aerchive/cs/cs106a.1188/lectures/lecture26.pdf