Proceedings of International Conference on Education, Technology, and Innovation

Homepage: http://proceedings.upi.edu/index.php/ICETI/index

AI Application for States Security: A Literature Review

Rizky Hamdani Sakti[1], Alimudinsyah Alrasyid[2], Jenni Febiyola Sari[3], Diky Zakaria[4,*]

[1] *Department of Mechatronics and Artificial Intelligence, Universitas Pendidikan Indonesia, Purwakarta, Indonesia*
[2] *Department of Mechatronics and Artificial Intelligence, Universitas Pendidikan Indonesia, Purwakarta, indonesia*
[3] *Department of Mechatronics and Artificial Intelligence, Universitas Pendidikan Indonesia, Purwakarta, indonesia*
[4] *Department of Mechatronics and Artificial Intelligence, Universitas Pendidikan Indonesia, Purwakarta, indonesia*
**Correspondence author email: dikyzak@upi.edu*

ABSTRACT

Artificial intelligence is opening up new avenues for value generation in enterprises, industries, communities, and society as a whole. Technology has been researched to be relevant in many aspects of the world. This factor has made it to be included mainly in different businesses and industries. The applications of AI are endless to discuss. The research below examines the applications of artificial intelligence (AI) in state security. This article reviews articles from the Scopus database related to artificial intelligence for state security with research questions: what is AI?, why does security matter?, how long has the advancement of AI been today?, what is the future potential of AI?, and how can AI be implemented in state security. The method used is Systematic Literature Review (SLR). The result of this article can provide an overview of the research development related to AI application for state security. The majority of researchers using AI techniques for state security such as cybersecurity. Using Machine Learning methods on big data is the most significantly induced in recent technologies supporting state security. The research paper performs a literature review and examines the overall impacts of artificial intelligence on cybersecurity.

Keywords: *artificial intelligence, review, state security*

1. Introduction

Artificial Intelligence is a branch of computer science which focuses on developing theories, methods, technologies and application systems for simulating, extending and expanding human intelligence[1]–[8]. Artificial Intelligence is now a central part of the technology industry. Since it was first introduced to the world at the Dartmouth Conference in 1956, Artificial Intelligence has grown rapidly. From it just theoretically and don't know how to realize it, until it has expand to almost all of sector especially technology. Today, Artificial Intelligence has existed in various technology sectors such as

language translator, searching system, social media, even security system. Rapid development of artificial intelligence has come from high demand for artificial intelligence itself. The reason of rapid development of artificial intelligence comes from the human itself, artificial Intelligence can help people doing they job more easily. For a big company, they can cut costs of employee salaries and change it to artificial intelligence, because artificial intelligence is more effective and cheaper than should pay the employee salaries.

Experts predict with a 75% probability that by the year 2105 AI has learned how to learn beyond a point of human assistance. At that point, the concept of moral agency (or 'free will') of machines comes to play and fears are that humans might become an intelligently inferior species. The rapid of Artificial Intelligence can have a big threat of human, the effective and less costs of Artificial Intelligence makes human as useless things and make more unemployment people, that's only for beginning, psychologist and AI expert Geoffrey Hinton has warned that human race can extinct if artificial intelligence is out of control.

As a rapid development of Artificial Intelligence in this modern era, data security is very precious, almost 4 from 5 big companies in the world use data as their business such as business intelligence. Of course not surprisingly a lot of irresponsible people try to find a gap and collect the precious data for bad things and use it for criminal things. Artificial Intelligence has become essential to almost all areas including computer science, security, criminology, psychology and robotics. Especially deep learning that inspired by the structure and function of brain that has been the major breakthrough in the Artificial Intelligence field. Deep learning has been studied to process a huge amount of data [1]–[19].

As humans, security has become a basic need for us. Maslow has explained the Theory of Needs. Security itself is a part of safety needs in his theorem. Someone needs safety in terms of support to achieve more needs. Safety needs consist of protection, freedom of fear and away from threats. To conquer this issue, traffic regulations, work safety regulations, health protocol, social norms and rule of law exist to fulfil a sense of security needs. To address this issue, Artificial Intelligence has a solid role to solve security matters.

In security, AI can predict whether incoming data are potentially malicious or safe. One of the biggest potential security benefits of AI lies in detecting internal threats. Imagine an AI system that, day in and day out, watches the comings and goings of all employees within corporate headquarters via biometrics and login information.

Artificial Intelligence has a lot of potential that can be obtained to help people fulfil their security needs, such as cyber attack or physical attack as a part of a country's security. Artificial Intelligence is increasingly being integrated into the cyber attack and used in a variety of use cases to automate security tasks or support the work of human security teams. Artificial intelligence can detect which massage is spam to cheat the victim and which massage is now a spam. Securing computers from virus and malicious attack, searching criminal data from every access such as citizen data, recording camera and even tracking the criminal which can help police to find the perpetrator of a crime. Police can use computer vision and deep learning to tackle this issues by Surveillance AI.

Surveillance AI involves the "systematic collection and analysis of personal information in the population for purposes of influence, management, protection, or direction". Common applications include smart CCTV crowd surveillance, sound-of-movements monitoring, or the use of police robots. A primary benefit of surveillance technologies is to increase safety or public security . These societal benefits clash with personal freedoms though, because they tend to require privacy infringements, loss of autonomy, limited access to social systems, and threats of discrimination or bias [11]–[13], [20].

Artificial Intelligence developers have a unique responsibility to design systems that are robust and resilient against misuse. Techniques like differential privacy and federated learning can be used to protect data. As mentioned earlier, the cyber attack is a threat to the vital functions of society that targeting country's security. Artificial Intelligence is an exciting tool that can provide analytics and intelligence to protect country's security by providing more accurate and rapid analysis of information.

Based on the background, the author wishes to write a review paper discussing about artificial intelligence in state security with the following research questions (RQs):

- RQ1: What is artificial intelligence?
- RQ2: Why security is important?
- RQ3: How is artificial intelligence today?
- RQ4: How much potential of artificial intelligence in the future?
- RQ5: How is the implementation of artificial intelligence in state security?

The method used is systematic literature review (SLR) with the article that used SLR method. Based on the searching keyword, this article used SLR to gather information about RQs mentioned earlier. The results of this review are expected to provide an overview to researcher related to artificial intelligence in security to be able to find originality and novelty of their next research.

2. Methods

This article is a literature review with method described in detail as follows:

2.1. Article Selection

Using the Google Scholar database, relevant articles were selected. Google Scholar was chosen since it's one of the largest and most accessible databases in the world. The search keywords used were based on ("artificial intelligence" AND "state security"). The search was conducted on October 25, 2023 with the following details:

Table 1: Article Selection Process on Google Scholar database

No.	Process	Number of Article
1	Entering keywords ("artificial intelligence" AND "state security") in the Google Scholar search field.	5460 articles
2	Costum the range time to 2018 - 2023	3620 articles
3	Review articles type	128 articles
3	Closed access articles	95 articles
4	Filter articles is not relevant	20 articles
Final number of articles used		20 articles

Based on table 1, the total Google Scholar document based on the keyword are 5460 documents. After we applied the exclusion criteria, we only use 20 articles fot this literature review.

2.2. Article Review Process

After the article selection process is complete, then the author downloads the 20 articles and reviews the articles by answering the 5 predetermined RQs, providing discussion, and providing conclusions.

3. Results and Discussion

3.1. Article Metadata

The metadata of the 20 articles used in shown in The Table 2:

Table 2: Metadata of the Articles Used

No	Author (s)	Year	Paper Title	Conference / Journal Source
1	Bistron and Piotrowski	2021	Artificial Intelligence Application in Military System and Their Influence on Sense of Security of Citizens	Multidisciplinary Digital Publishing Institute
2	B.S. et al	2019	Providing Cyber Security using Artificial Intelligence - A survey	2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)
3	Briscoe and Fairbanks	2020	Artificial Intelligence and its Impact on National Security and Foreign Policy	ScienceDirect, Orbis, 64(4)
4	Dorotic et al	2023	AI on the Street: Context-Dependent Response to Artificial Intelligence	International Journal of Research in Marketing
5	Francisco	2023	Artificial Intelligence for Environmental Security: National, International, Human and Ecological Perspectives	ScienceDirect, Current Opinion in Environmental Sustainability, 61
6	Herrmann	2023	What's Next for Responsible Artificial Intelligence: A Way Forward Through Responsible Innovation	Heliyon, 9(3)
7	Jeong	2020	Artificial Intelligence Security Threat, Crime, and Forensics: Taxonomy an Open Issues	Institute of Electrical and Electronics Engineers
8	Jialiang Zhang	2018	Application of Artificial Intelligence Technology in Computer Network Security	International Journal of Network Security
9	Kaur et al	2023	Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions	ScienceDirect, Information Fusion, 97
10	Martin and Freeland	2021	The Advent of Artificial Intelligence in Space Activities: New Legal Challenges	ScienceDirect, Space Policy, 55
11	Mohammadi and Sohn	2023	AI Based Energy Harvesting Security Methods: A survey	ICT Express
12	Mohanta et al	2020	Survey in IoT Security: Challenges and Solution using Machine Learning, Artificial	Internet of Things, 11

			Intelligence and Blockchain Technology	
13	Nguyen et al	2020	Artificial Intelligence Based Data Processing Algorithm for Video Surveillance to Empower Industry 3.5	ScienceDirect, Computers & Industrial Engineering, 148
14	Noriega	2020	The Application of Artificial Intelligence in Police Interrogations: An Analysis Addressing the Proposed Effect AI has on Racial and Gender Bias, Cooperation, and False Confessions	ScienceDirect, Future, 117
15	Petri Vähäkainu and Martti Lehto	2019	Artificial Intelligence in the Cyber Security Environment	Proceedings of the 14th International Conference on Cyber Warfare and Security, ICC2S 2019
16	Radulov	2019	Artificial Intelligence and Security. Security 4.0	International Science Journal
17	Talwar and Koury	2017	Artificial Intelligence - The Next Frontier in IT Security	ScienceDirect, Network Security, 2017
18	Thuraisingham	2020	The Role of Artificial Intelligence and Cyber Security for Social Media	2020 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW)
19	Zeng	2022	AI Empowers Security Threats and Strategies for Cyber Attacks	7th International Conference on Intelligent, Interactive System and Application
20	Zhou et al	2014	A Heuristic Approach for Secure Service Composition Adaption	Proceedings of the 2012 International Conference on Cybernetics and Informatics

3.2. Answering RQs

Based on the article review result, RQ1 about "What is AI?" has answered. Artificial intelligence, a branch of computer science, is a new technical science which focuses on developing theories, methods, technologies and application systems for simulating, extending and expanding human intelligence. The technology enable computer to simulating the intelligence of multiple people to solve and analyze problems like humans.

In back reason of the title, to answer of the RQ2, how importance security is cause the data we use everydays was precious. Cause today, 4-5 big companies in the world use data as they sell profit. They change our data to something more valuable to give it to us. So for that reason, many irresponsible people need our data to manipulate it to make more profit for themselve. Another reason why security is important

comes not far from data, it comes from owner of data itself, human. Human mind was weak, everyone can't manipulate anyone to do what they can do, as long they have the ingredients which in this case the data, they can manipulate and cheating innocent people. So to avoid that, artificial intelegence come to help people protect they data and make system and data secure and safe.

To know how we can upgrade the AI what we want, we should know how AI today, by answering the RQ3 we can know that today AI has used almost every aspect in technology. Such as computer science, security engineering, criminology, psychology, and robotics. Not only a few aspect above, AI also has use in almost every big companies today, like in the RQ before, AI almost looks like selling market for they company. Together with AI in they system, it help many problem and many feature has introduce. Especially in security it helps protect customer data, help customer to find what they want, and specifically protect the our data from irresponsible people.

So after know the main reason of the title, and more familiar with AI with answering 3 RQ above, corresponding to answer RQ4 we can know that AI has a lot of potential in the future. From helping company to expand they potential, until protect our data from irresponsible people. AI can do all of that, starting from small things that human can do such as manage data to make it looks clean, until processing data like data scientist. In step with our topic, AI can secure data and protect human from cheating and fake massage that can make human fractious.

In relation to RQ5, The most prevalent problem in state security is cyber crime, the majority of researchers using AI techniques for cyber crime such as data leakage prevention, smart email protection, malicious domain blocking and reporting, and agent-based integrity monitoring to ensure data confidentiality, integrity, and availability. Application of Machine Learning methods on big data generated in the smart grid to extract useful information and to detect and protect the data for state security. There are also researchers using AI applications include smart CCTV crowd surveillance, motion sound monitoring, or the use of police robots. The primary benefit of surveillance technology is to improve public safety or security.

4. Conclusion

This article examines this article examines Scopus-indexed articles on AI application for state security. The search keywords used were based on ("artificial intelligence" AND "state security"). The search was conducted on October 25, 2023 and obtained 20 articles. After the review process is done, it can be concluded that AI has proven more beneficial to state security than limitations. Artificial intelligence

is still growing, and more research is being done on the technology. Based on the research above, the conclusion is that Artificial Intelligence has dramatically impacted state security.

Acknowledgement

We are thankful to our advisor Diky Zakaria, S.Pd., M.T. from the Universitas Pendidikan Indonesia, for all his support and guidance, especially for reviewing it before the submission in this journal.

References

[1] B.S., S., S., N., Kashyap, N., & D.N., S. (2019). "Providing Cyber Security using Artificial Intelligence – A survey," 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), 717–720. https://doi.org/10.1109/ICCMC.2019.8819719

[2] Bistron, M., & Piotrowski, Z. (2021). "Artificial Intelligence Applications in Military Systems and Their Influence on Sense of Security of Citizens," *Electronics*, 10(7), 871. https://doi.org/10.3390/electronics10070871

[3] Briscoe, E., & Fairbanks, J. (2020). "Artificial Scientific Intelligence and its Impact on National Security and Foreign Policy," Orbis, 64(4), 544–554. https://doi.org/10.1016/j.orbis.2020.08.004

[4] Dorotic, M., Stagno, E., & Warlop, L. (2023). AI on the street: Context-dependent responses to artificial intelligence. International Journal of Research in Marketing, S0167811623000642. https://doi.org/10.1016/j.ijresmar.2023.08.010

[5] Francisco, M. (2023). Artificial intelligence for environmental security: National, international, human and ecological perspectives. Current Opinion in Environmental Sustainability, 61, 101250. https://doi.org/10.1016/j.cosust.2022.101250

[6] Herrmann, H. (2023). What's next for responsible artificial intelligence: A way forward through responsible innovation. Heliyon, 9(3), e14379. https://doi.org/10.1016/j.heliyon.2023.e14379

[7] Jeong, D. (2020). Artificial Intelligence Security Threat, Crime, and Forensics: Taxonomy and Open Issues. IEEE Access, 8, 184560–184574. https://doi.org/10.1109/ACCESS.2020.3029280

[8] Jialiang Zhang. (2018). Application of Artificial Intelligence Technology in Computer Network Security. International Journal of Network Security, 20(6). https://doi.org/10.6633/IJNS.201811_20(6).02

[9] Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804. https://doi.org/10.1016/j.inffus.2023.101804

[10] Martin, A.-S., & Freeland, S. (2021). The Advent of Artificial Intelligence in Space Activities: New Legal Challenges. Space Policy, 55, 101408. https://doi.org/10.1016/j.spacepol.2020.101408

[11] Mohammadi, M., & Sohn, I. (2023). AI based energy harvesting security methods: A survey. ICT Express, S2405959523000644. https://doi.org/10.1016/j.icte.2023.06.002

[12] Mohanta, B. K., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet of Things, 11, 100227. https://doi.org/10.1016/j.iot.2020.100227

[13] Nguyen, M. T., Truong, L. H., Tran, T. T., & Chien, C.-F. (2020). Artificial intelligence based data processing algorithm for video surveillance to empower industry 3.5. Computers & Industrial Engineering, 148, 106671. https://doi.org/10.1016/j.cie.2020.106671

[14] Noriega, M. (2020). The application of artificial intelligence in police interrogations: An analysis addressing the proposed effect AI has on racial and gender bias, cooperation, and false confessions. Futures, 117, 102510. https://doi.org/10.1016/j.futures.2019.102510

[15] Petri Vähäkainu & Martti Lehto. (2019). Artificial intelligence in the cyber security environment. Proceedings of the 14th International Conference on Cyber Warfare and Security ICCWS2019, 431–440. https://jyx.jyu.fi/bitstream/handle/123456789/67298/vhkainulehtoartificialintelligenceinthecybersecurityenvironment.pdf?sequence=1&isAllowed=y

[16] Radulov, N. (2019). Artificial intelligence and security. Security 4.0. Security & Future, 3(1), 3–5.

[17] Talwar, R., & Koury, A. (2017). Artificial intelligence – the next frontier in IT security? Network Security, 2017(4), 14–17. https://doi.org/10.1016/S1353-4858(17)30039-9

[18] Thuraisingham, B. (2020). The Role of Artificial Intelligence and Cyber Security for Social Media. 2020 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW), 1–3. https://doi.org/10.1109/IPDPSW50202.2020.00184

[19] Zeng, Y. (2022). AI Empowers Security Threats and Strategies for Cyber Attacks. Procedia Computer Science, 208, 170–175. https://doi.org/10.1016/j.procs.2022.10.025

[20] Zhou, B., Llewellyn-Jones, D., Lamb, D., Asim, M., Shi, Q., & Merabti, M. (2014). A heuristic approach for secure service composition adaptation. Cyberpatterns: Unifying Design Patterns with Security and Attack Patterns, 97–105.