

Privacy-preserving data mining optimization for big data analytics using deep reinforcement learning

Wiranto Herry Utomo¹, Rosalina², Afriyadi¹

¹Master of Science in Information Technology Study Program, Faculty of Computing, President University, Jakarta, Indonesia

²Informatics Study Program, Faculty of Computing, President University, Jakarta, Indonesia

Article Info

Article history:

Received Jul 4, 2024

Revised Aug 20, 2024

Accepted Aug 31, 2024

Keywords:

Big data analytics

Deep reinforcement learning

Data privacy

ISO/IEC 27001:2023

Privacy-preserving data mining

Secure analytics

ABSTRACT

The rapid growth of big data analytics has heightened concerns about data privacy, necessitating the development of advanced privacy-preserving techniques. This research addresses the challenge of optimizing privacy-preserving data mining (PPDM) for big data analytics through the innovative application of deep reinforcement learning (DRL). We propose a novel framework that integrates DRL to dynamically balance privacy and utility, ensuring robust data protection while maintaining analytical accuracy. The framework employs a reinforcement learning agent to adaptively select optimal privacy-preserving strategies based on the evolving data environment and user requirements, while ensuring compliance with the latest security and privacy standards such as ISO/IEC 27001:2023. Experimental results demonstrate significant improvements in both privacy protection and data utility, surpassing traditional PPDM methods. Our findings highlight the potential of DRL in enhancing privacy-preserving mechanisms, offering a scalable and efficient solution for secure big data analytics.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Rosalina

Informatics Study Program, Faculty of Computing, President University

Jakarta, Indonesia

Email: rosalina@president.ac.id

1. INTRODUCTION

The exponential growth of data in recent years, driven by the proliferation of digital technologies, has profoundly transformed various sectors, including healthcare, finance, and social media [1], [2]. In healthcare, big data analytics enables the aggregation and analysis of patient data from electronic health records [3], wearable devices [4], and genomic sequencing to uncover patterns that can lead to improved diagnostics [5], personalized treatments [3], and predictive healthcare models [6]–[11]. Similarly, in finance, the ability to analyze vast amounts of transactional data helps in detecting fraudulent activities, managing risks, and providing personalized financial services to customers [12]. Social media platforms leverage big data to understand user behavior, enhance user experience through personalized content, and drive targeted advertising strategies.

Big data analytics, which harnesses these large datasets to uncover patterns and insights, has become a cornerstone of decision-making processes. Organizations use data-driven insights to make informed decisions, optimize operations, and innovate new products and services. For instance, retail companies analyze consumer purchasing patterns to manage inventory and predict future trends, while manufacturing firms use predictive maintenance analytics to prevent equipment failures and reduce downtime. However, as the volume, variety, and velocity of data increase, so do concerns regarding data privacy [13]. The vast

amounts of data being collected often include sensitive personal information such as health records, financial details, and social media interactions. The potential misuse or unauthorized access to this sensitive information can lead to significant privacy breaches, identity theft, and financial loss [14]. High-profile data breaches have highlighted the risks associated with inadequate data protection measures, resulting in reputational damage and regulatory penalties for the affected organizations [15]. The potential misuse of sensitive information necessitates the development of robust privacy-preserving techniques that ensure data security without compromising analytical value [16]. Traditional data protection methods, such as encryption and access controls, are essential but may not be sufficient in big data analytics [17]. The challenge lies in balancing the need for data utility with the imperative of protecting individual privacy. For example, while anonymization techniques can help protect privacy, they might also reduce the granularity and usefulness of the data for analytical purposes [18].

To address these challenges, advanced privacy-preserving techniques such as differential privacy, homomorphic encryption, and secure multi-party computation are being explored. Differential privacy adds controlled noise to the data, ensuring that individual information cannot be inferred while maintaining overall data utility. Homomorphic encryption allows computations to be performed on encrypted data without decrypting it, thus protecting data privacy during the analytical process. Secure multi-party computation enables multiple parties to collaboratively analyze data without revealing their individual inputs to each other.

Despite these advancements, there remains a need for innovative approaches that can dynamically adapt to the changing data landscape and evolving privacy requirements. This is where the integration of deep reinforcement learning (DRL) into privacy-preserving data mining (PPDM) comes into play. DRL offers the potential to develop adaptive, intelligent systems that can continuously learn and improve their privacy-preserving strategies based on real-time data environments and user requirements, ensuring robust data protection while maximizing analytical value [19]. Past studies on big data analytics have primarily centered around the use of machine learning algorithms [20]–[22]. While these approaches have shown promising results in optimizing big data analytics, their performance is limited in certain aspects, such as scalability and handling dynamic environments. This has led to a need for exploring alternative methods, such as reinforcement learning (RL), that can address these limitations.

Recent studies have shown a growing interest in the application of RL in big data analytics [23]–[28]. RL algorithms, such as Q-Learning and deep reinforcement learning, have been found effective in optimizing complex decision-making processes and can help address the challenges associated with large-scale data processing, including model scalability and handling of dynamic and noisy environments [29], [30]. Moreover, ensuring data privacy and security during big data analytics is crucial. While previous research has proposed various privacy-preserving techniques, these techniques may not comply with the latest security and privacy standards, such as ISO/IEC 27001:2023. Thus, more research is required to explore advanced privacy-preserving techniques that are compliant with these standards. This paper aims to contribute to the existing literature on optimizing data mining in big data analytics, focusing on employing reinforcement learning algorithms to optimize compliance with security and privacy standards.

This study provides an opportunity to further explore the application of RL in data mining for big data analytics and contribute to the roadmap of more efficient and effective methods for protecting data privacy and security in this field. Using RL techniques, we offer a unique method for maximizing privacy and security compliance in big data analytics. RL is a subset of machine learning where an agent learns to make decisions by interacting with its environment. Through trial and error, the agent discovers optimal policies to achieve specific objectives, such as maximizing rewards or minimizing costs. This learning process involves evaluating the outcomes of actions taken in various states and continuously refining strategies to improve performance over time.

Our research investigates how RL algorithms can be leveraged to automatically process all types of data, including sensitive data, while ensuring compliance with stringent security and privacy standards like ISO/IEC 27001:2023. The ISO/IEC 27001:2023 standard specifies requirements for establishing, implementing, maintaining, and continually improving an information security management system. Compliance with this standard ensures that an organization effectively manages information security risks and protects data integrity, confidentiality, and availability. The proposed RL-based framework operates by incorporating privacy-preserving mechanisms into the decision-making process of the RL agent. The agent is trained to balance the trade-offs between data utility and privacy by adapting its strategies in real-time based on the evolving data environment and specific user requirements. For instance, the agent might dynamically adjust the level of data anonymization or encryption depending on the sensitivity of the data and the context of its use. By integrating RL into privacy-preserving data mining, our approach aims to enhance the precision and effectiveness of big data analytics. The adaptive nature of RL allows for continuous optimization, making the system more resilient to changing data patterns and emerging threats. This dynamic adjustment

ensures that sensitive data is consistently protected according to the highest standards, without compromising the analytical value of the data. Moreover, the RL framework's ability to learn and improve from ongoing data processing activities means that it can proactively identify potential security vulnerabilities and address them before they escalate into significant risks. This proactive stance not only improves data security but also ensures that compliance with privacy regulations is maintained continuously, reducing the likelihood of regulatory breaches and associated penalties.

2. METHOD

The approach to enhancing privacy and security compliance in big data analytics through RL algorithms consists of four main steps. Each step is meticulously crafted to provide a structured and thorough path towards achieving the research goals, as depicted in Figure 1. The first step involves defining the problem and establishing privacy and security requirements. This sets the foundation for identifying key data handling actions and compliance criteria. The second step focuses on data preprocessing and feature selection, ensuring that the data used for training the RL model is clean, relevant, and anonymized where necessary. The third step is the design and training of the RL algorithm, such as a deep q-network (DQN), tailored for optimal data processing policies. This involves the agent learning from the environment and optimizing its actions based on the defined reward function. The final step entails evaluating and fine-tuning the model to ensure robust performance and adherence to privacy and security standards.



Figure 1. The four-step approach to enhancing privacy and security compliance in big data analytics through reinforcement learning algorithms

2.1. Extraction of security and privacy compliance requirements

In the first phase of the methodology, the focus is on extracting security and privacy compliance requirements from ISO/IEC 27001:2023 and Indonesian (PDP) law. This involves analyzing key provisions to identify guidelines for data security and privacy. A classification system is developed to categorize sensitive data, including personally identifiable information, financial data, and confidential business information. Additionally, a reward function is designed for the RL algorithm based on these requirements. This function guides the RL agent in taking actions that enhance compliance with data privacy and security standards, aiming to establish a robust framework for subsequent phases of the research.

2.2. Data collection and pre-processing

The second step involves collecting and pre-processing data to create training datasets for the RL algorithm, which is used to design the world model and refine the reward function. This includes gathering 20 social media posts for each sensitive data classification and ensuring compliance with ISO/IEC 27001:2023 and the Indonesian PDP law. The pre-processing involves evaluating data to identify sensitive information, removing unnecessary elements, transforming data to anonymize or generalize it, and censoring by replacing sensitive details with placeholder symbols (e.g., names with nationality, addresses with country names, dates with just the year and month).

2.3. Application of RL algorithms

In the third step of the methodology, the focus turns to the design and training of the RL algorithm to develop optimal data processing policies. This phase begins with the design of an RL model, such as a DQN, specifically tailored for handling data within the context of privacy and security compliance. A DQN is a type of reinforcement learning algorithm that combines Q-Learning with deep neural networks. The key components of a DQN include:

- Q-function: the Q-function $Q(s, a)$ estimates the expected cumulative reward of taking action a in state s . The objective is to learn a policy π that maximizes the Q-value.
- Experience replay: the agent stores its experiences, (s, a, r, s') in a replay buffer and samples mini-batches from this buffer to update the Q-network. This helps break the correlation between consecutive experiences, stabilizing training.

- Target network: a separate target network is used to compute the target Q-values. The parameters of the target network are periodically updated to match the primary Q-network, preventing oscillations during training.

A crucial aspect of the RL algorithm is the reward function, which guides the agent's behavior towards achieving privacy and security compliance. The reward function is defined as the sum of discounted rewards over time, with each reward designed to incentivize specific actions:

- When sensitive data is successfully removed, the agent receives a positive reward.
- Correctly anonymizing or censoring identifiable information also earns the agent a positive reward.
- Applying effective generalization techniques to anonymize data is similarly rewarded.

The reward function RRR is crucial for guiding the RL agent's behavior. It can be defined as in Equation 1. By optimizing this reward function, the RL agent improves its decision-making capabilities over time. The training process continues until the agent's performance converges to an optimal policy that maximizes the cumulative reward, ensuring effective handling of sensitive data in compliance with privacy and security regulations.

$$R = \sum_{t=0}^T \gamma^t r_t \quad (1)$$

Where:

- T is the total number of time steps.
- γ is the discount factor ($0 \leq \gamma \leq 1$)
- r_t is the reward received at time step t .

2.4. Evaluation and validation

In the fourth phase of the methodology, the focus is on assessing the RL-based approach's adherence to ISO/IEC 27001:2023 and Indonesian PDP law. Through carefully designed experiments on pre-processed datasets and real-time social media feeds, key metrics are evaluated. These include accuracy, measuring how well data processing maintains utility; compliance violations, assessing false positive rates in identifying breaches; and comparisons with traditional methods for privacy preservation. The analysis of these metrics aims to determine how effectively RL algorithms uphold privacy and security standards while optimizing data utility. This evaluation provides valuable insights into the practical benefits of using RL in enhancing data privacy within big data analytics.

3. RESULTS AND DISCUSSION

3.1. Extraction of security and privacy compliance requirements

The initial phase of the study focused on meticulously extracting essential security and privacy requirements outlined in two key regulatory frameworks: ISO/IEC 27001:2023, an international standard for information security management systems, and the Indonesian PDP Law. This process involved a detailed analysis to identify specific guidelines and provisions related to data security measures and privacy protections mandated by these regulations.

By extracting and synthesizing these requirements, the study laid a solid foundation for structuring subsequent data handling procedures. These guidelines served as a roadmap for implementing rigorous data security measures and privacy-preserving techniques throughout the research. This phase ensured that all data processing activities would align with legal and regulatory standards, thereby enhancing the overall credibility and compliance of the study's findings.

Under the Indonesian PDP Law, sensitive personal data such as medical information, biometric data, and criminal records require heightened protection due to their potential impact on an individual's privacy and rights. General personal data includes identifiable information like names and demographic details. This classification framework ensures organizations implement appropriate measures to safeguard personal information in compliance with legal requirements, as depicted in Table 1.

Based on the sensitive information classification and the quantity of training data collected, the following details are outlined in Table 2. This data is crucial for understanding the scope and depth of the training dataset used in the study, ensuring that the RL model is effectively trained to handle various types of sensitive information according to the Indonesia personal data protection law. Tabel 2 categorizes the different types of sensitive information as specified by the Indonesian PDP Law and shows the exact number of samples collected for each category. The collection of 160 samples across various sensitive information categories ensures that the RL model has a comprehensive and representative dataset to train on, facilitating the development of effective privacy-preserving data processing strategies.

Table 1. Classification of personal data under Indonesian PDP law

Sensitive personal data	General personal data
Medical data and information	Full name
Biometric data	Sex
Genetics data	Nationality
Criminal record	Religion
Kids data	Marital status
Personal financial data	Combined information that can identify a person
	Other unspecified data

Table 2. Sensitive information classification and quantity of training data

Sensitive information classification	Quantity of training data
Health information	20
Biometric information	0
Genetics information	0
Criminal records	0
Kids information	20
Personal financial information	20
Full name	20
Sex	20
Nationality	20
Religion	20
Marital status	20
Other personally identifiable information (PII)	0
Total	160

3.2. Data collection and pre-processing

The second phase of the research involves a meticulous process of gathering and preparing data to form training datasets essential for the RL algorithm. This stage begins with the collection of 20 social media posts, each classified according to sensitive data criteria specified by ISO/IEC 27001:2023 and Indonesian PDP law. Each post undergoes rigorous evaluation to identify sensitive information, which is then handled through various adjustments such as removing unnecessary elements, anonymizing, or generalizing to comply with stringent privacy regulations. Techniques like censorship are employed, substituting sensitive details with placeholders such as nationality for names, country names for addresses, or simplified date formats like year and month.

The reward function, depicted in Figure 2, serves as a pivotal component in guiding the RL algorithm’s decisions. It evaluates the effectiveness of preprocessing actions in balancing data privacy and utility. The function ensures compliance with ISO/IEC 27001:2023 and Indonesian PDP Law by assessing how well sensitive information is safeguarded through anonymization, removal of unnecessary elements, and censorship techniques. Figure 2 visually represents how the reward function influences the algorithm’s policies, aiming to optimize data handling practices for enhanced privacy compliance and data utility in social media analytics

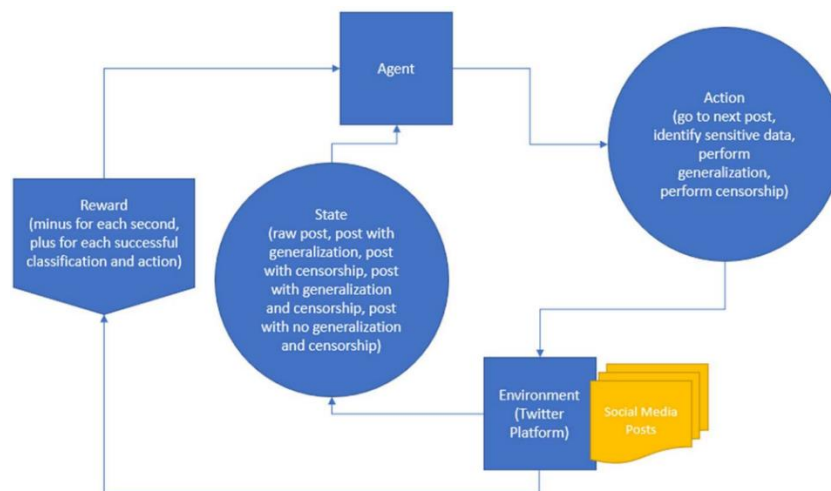


Figure 2. Reward functions and learning process in reinforcement learning

Table 3 illustrates the application of a reward function within a reinforcement learning framework to manage sensitive information in social media posts in this research. Each post undergoes rigorous evaluation based on predefined classifications such as health information, genetics data, criminal records, kids' details, and personal financial information. The reward function assigns rewards based on the success or failure of actions taken to handle these sensitive categories.

Posts correctly categorized and processed to safeguard privacy while maintaining data utility receive a high reward (+1), indicating effective compliance with privacy regulations. Conversely, actions that mishandle sensitive information or fail to adequately anonymize or censor receive a low reward (-1), highlighting potential privacy risks. Posts where actions have a neutral impact or require further refinement receive a medium reward (0). This approach ensures that the reinforcement learning algorithm learns optimal policies for handling diverse sensitive data types, balancing privacy preservation with data utility in social media analytics.

Table 3. Reward function application in social media analytics for sensitive information handling

Social media post	Original content	Processed content	Sensitive information classification	Reward (high/medium/low)
Post 1	"Visited the doctor for a check-up today."	"Visited the doctor for a check-up today."	Health information	+1 (high)
Post 2	"My genetic test results are in, all clear!"	"My genetic test results are in, all clear!"	Genetics information	+1 (high)
Post 3	"Arrested for public disturbance last night."	"Arrested for public disturbance last night."	Criminal records	-1 (low)
Post 4	"My kid's first day at school!"	"My kid's first day at school!"	Kids information	+1 (high)
Post 5	"Received a large payment today, feeling rich!"	"Received a large payment today, feeling rich!"	Personal financial Information	0 (medium)

3.3. Application of RL algorithms

In this research, Algorithm 1, termed regulation-based privacy scanning RL, and Algorithm 2, deep reinforcement learning, are pivotal in running the RL algorithm on a social media platform over varying durations. Algorithm 1 focuses on processing each social media post by transforming it into a privacy-preserving version. It begins by parsing input posts to extract dates and locations, then generalizing these details to protect privacy while maintaining utility. The algorithm categorizes word patterns based on regulatory guidelines, guiding actions like data censorship or generalization.

Algorithm 1. Regulation-based privacy scanning RL

```

Input: social media post
Results: privacy-preserving social media post
Date = create date generalization, month, and year
Location = create location generalization by country
foreach word in post do
    categorize word patterns with regulation-based classification.
end

```

Meanwhile, Algorithm 2 orchestrates the RL agent's operations within the social media environment. It observes states encompassing post content and context, selects actions (e.g., censoring or generalizing data), and updates policies based on cumulative rewards from the environment. This iterative learning process enables the RL agent to enhance decision-making regarding data privacy and utility continually.

Algorithm 2. Deep reinforcement learning

```

Input: S environment states
Results: R cumulative total rewards
A = action for each input states
Policy = state action pair
foreach time step do
    take action a in state s
    update Policy based on rewards.
End

```

Table 4 presents the results of running the reinforcement learning algorithm across varying durations on a social media platform, focusing on data processing efficiency and reward outcomes. In the 10-minute experiment, the algorithm processed an average of 124 words per episode over 372 time steps, achieving a processing speed of 40,322 words per second and an average reward of 189.72. Extending the runtime to 30 minutes increased the average words processed per episode to 138 and time steps to 414, with a slight decrease in processing speed to 36,231 words per second but an improved average reward of 211.14.

Running the algorithm for 60 minutes further increased the average words per episode to 267 and time steps to 534, with a processing speed of 18,726 words per second and a significant rise in average reward to 283.02. These results demonstrate the algorithm's capability to enhance data handling practices for improved privacy compliance and data utility over extended operational periods.

Table 4. Experimental results of running RL algorithm on social media platform

No	Experiment name	Time (min)	# Avg words / Ep.	Time step / Ep.	Processed words / s	Average rewards
1	10 minutes run	10	124	372	40,322	189.72
2	30 minutes run	30	138	414	36,231	211.14
3	60 minutes run	60	267	534	18,726	283.02

The study's findings highlight the significant role of RL algorithms in enhancing privacy and security compliance within large-scale data mining operations. Through the implementation of a sophisticated RL-based methodology, the research revealed that optimal data processing policies could be learned effectively while mitigating security and privacy risks over a 30-minute exploration period. This innovative approach demonstrated strong performance in maintaining data privacy and security standards, achieving high accuracy and efficiency in big data analytics.

In comparison to previous research efforts, such as those conducted by [31], which focused on various standards and data types, our proposed method aligns more closely with contemporary regulations like ISO/IEC 27001:2023, GDPR, and Indonesia's UU-PDP:2022 privacy laws. By categorizing and processing sensitive data-including health information, biometrics, and personal financial details-using techniques such as generalization, suppression, permutation, and perturbation, our strategy promises more effective and efficient safeguards for data security and privacy.

These insights suggest that RL algorithms have the potential to revolutionize data handling practices across diverse sectors. The adaptability and learning capabilities of RL algorithms make them particularly suited for dynamic and complex environments where traditional data processing techniques may fall short. For instance, in healthcare, RL algorithms could optimize the processing and protection of vast amounts of patient data, ensuring compliance with stringent privacy laws while facilitating advanced medical research and personalized treatment plans. In the financial sector, RL could enhance the security and privacy of sensitive financial transactions and records, adapting to evolving regulatory requirements and cyber threats in real time. Similarly, in the field of e-commerce, RL algorithms could manage and protect consumer data more effectively, balancing the need for personalized marketing with robust data protection measures.

Future research could delve deeper into these applications, exploring how RL can be tailored to meet the specific needs and challenges of different industries. This could involve developing more sophisticated models that can handle the unique data characteristics and regulatory landscapes of various sectors. Additionally, research could focus on integrating RL with other emerging technologies, such as blockchain, to further enhance data security and privacy. Moreover, extending the methodologies to ensure broader compliance and efficacy involves not only refining the algorithms themselves but also developing comprehensive frameworks for their implementation. This includes creating standardized protocols for training and deploying RL models, establishing best practices for data governance, and ensuring interoperability with existing systems and technologies. By addressing these areas, future research can contribute to the development of more resilient and versatile data handling practices, ultimately paving the way for RL algorithms to become a cornerstone of secure and efficient data management in the digital age.

4. CONCLUSION

In conclusion, this study aimed to develop and apply RL algorithms for optimizing data privacy compliance in social media analytics, guided by ISO/IEC 27001:2023 and the Indonesian PDP law. The initial phases involved extracting regulatory requirements and designing a robust RL-based framework to handle sensitive data effectively. Through experiments, the RL algorithms demonstrated varying degrees of success in balancing data utility and privacy preservation over different durations. The results showcased improvements in data handling practices, exemplified by effective data generalization and censorship strategies as mandated by privacy regulations. Moving forward, further research could explore enhanced RL algorithms capable of adapting dynamically to evolving data privacy laws and technological advancements. Application prospects include scaling the framework to larger datasets and integrating real-time monitoring capabilities for continuous compliance. By addressing these avenues, future studies can contribute significantly to the advancement of privacy-preserving technologies in social media analytics and broader data-intensive applications.





REFERENCES

- [1] B. Mirza, T. Q. Syed, B. Khan, and Y. Malik, "Potential deep learning solutions to persistent and emerging big data challenges-a practitioners- cookbook," *ACM Computing Surveys*, vol. 54, no. 1, pp. 1–39, Jan. 2021, doi: 10.1145/3427476.
- [2] P. Chauhan and M. Sood, "Big data: present and future," *Computer*, vol. 54, no. 4, pp. 59–65, Apr. 2021, doi: 10.1109/MC.2021.3057442.
- [3] S. V. G. Subrahmanya *et al.*, "The role of data science in healthcare advancements: applications, benefits, and future prospects," *Irish Journal of Medical Science*, vol. 191, no. 4, pp. 1473–1483, Aug. 2022, doi: 10.1007/s11845-021-02730-z.
- [4] C. Ge, C. Yin, Z. Liu, L. Fang, J. Zhu, and H. Ling, "A privacy preserve big data analysis system for wearable wireless sensor network," *Computers and Security*, vol. 96, p. 101887, Sep. 2020, doi: 10.1016/j.cose.2020.101887.
- [5] M. Nambiar, S. Ghosh, P. Ong, Y. E. Chan, Y. M. Bee, and P. Krishnaswamy, "Deep offline reinforcement learning for real-world treatment optimization applications," in *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, New York, NY, USA: ACM, Aug. 2023, pp. 4673–4684. doi: 10.1145/3580305.3599800.
- [6] L. Wang, X. He, W. Zhang, and H. Zha, "Supervised reinforcement learning with recurrent neural network for dynamic treatment recommendation," in *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, New York, NY, USA: ACM, Jul. 2018, pp. 2447–2456. doi: 10.1145/3219819.3219961.
- [7] A. P. Dube and R. Yadav, "Analyzing the effectiveness of ML agents in enhancing the predictive model in decision making for medical practitioners in the healthcare industry: a structural equation model analysis," in *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering, ICACITE 2022*, IEEE, Apr. 2022, pp. 1017–1021. doi: 10.1109/ICACITE53722.2022.9823931.
- [8] S. S. Bhat, V. R. Srihari, A. Prabhune, S. S. Satheesh, and A. B. Bidrohi, "Optimizing medication access in public healthcare centers: a machine learning stochastic model for inventory management and demand forecasting in primary health services," in *2024 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*, IEEE, Jan. 2024, pp. 1–5. doi: 10.1109/IITCEE59897.2024.10467229.
- [9] N. D. T. Tran, C. K. Leung, E. W. R. Madill, and P. T. Binh, "A deep learning based predictive model for healthcare analytics," in *Proceedings - 2022 IEEE 10th International Conference on Healthcare Informatics, ICHI 2022*, IEEE, Jun. 2022, pp. 547–549. doi: 10.1109/ICHI54592.2022.00106.
- [10] M. J. C. M. Belida, A. Begum, S. A. David, E. Kannan, K. Senthil, and N. R. Naveena, "Predictive modeling for medical insurance malpractice using random forest and XGBoost," in *2024 International Conference on Communication, Computing and Internet of Things, IC3IoT 2024 - Proceedings*, IEEE, Apr. 2024, pp. 1–5. doi: 10.1109/IC3IoT60841.2024.10550288.
- [11] W. F. Tung, F. H. Wu, P. C. Chan, H. H. Lin, Y. F. Chen, and C. S. Lin, "Designing AI models for predicting ischemic stroke using administrative healthcare database," in *Proceedings - 2020 International Symposium on Computer, Consumer and Control, IS3C 2020*, IEEE, Nov. 2020, pp. 49–52. doi: 10.1109/IS3C50286.2020.00020.
- [12] J. Nicholls, A. Kuppaa, and N. A. Le-Khac, "Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape," *IEEE Access*, vol. 9, pp. 163965–163986, 2021, doi: 10.1109/ACCESS.2021.3134076.
- [13] S. Ali, M. M. Irfan, A. Bomai, and C. Zhao, "Towards privacy-preserving deep learning: opportunities and challenges," in *Proceedings - 2020 IEEE 7th International Conference on Data Science and Advanced Analytics, DSAA 2020*, IEEE, Oct. 2020, pp. 673–682. doi: 10.1109/DSAA49011.2020.00077.
- [14] E. Bertino, "Privacy in the era of 5G, IoT, big data and machine learning," in *Proceedings - 2020 2nd IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications, TPS-ISA 2020*, IEEE, Oct. 2020, pp. 134–137. doi: 10.1109/TPS-ISA50397.2020.00027.
- [15] H. Abdullah, "Towards the development of an information privacy protection awareness initiative for data subjects and organizations," in *Proceedings - 2021 IEEE 4th National Computing Colleges Conference, NCCC 2021*, IEEE, Mar. 2021, pp. 1–7. doi: 10.1109/NCCC49330.2021.9428878.
- [16] M. Al, S. Yagli, and S.-Y. Kung, "Privacy enhancing machine learning via removal of unwanted dependencies," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 34, no. 6, pp. 3019–3033, Jun. 2023, doi: 10.1109/TNNLS.2021.3110831.
- [17] F. Rafiq, M. J. Awan, A. Yasin, H. Nobanee, A. M. Zain, and S. A. Bahaj, "Privacy prevention of big data applications: a systematic literature review," *SAGE Open*, vol. 12, no. 2, p. 215824402210964, Apr. 2022, doi: 10.1177/21582440221096445.
- [18] N. A. B. Mohd Zaki, A. Jamaluddin, V. a/p Tangamani, A. Rahim, and N. A. Alias, "Big data: balancing its usefulness in managing an organizational performance and ethical consideration," *International Journal of Academic Research in Business and Social Sciences*, vol. 13, no. 6, Jun. 2023, doi: 10.6007/ijarbss/v13-i6/17592.
- [19] S. Gan, M. Siew, C. Xu, and T. Q. S. Quek, "Differentially private deep q-learning for pattern privacy preservation in MEC offloading," in *IEEE International Conference on Communications*, IEEE, May 2023, pp. 3578–3583. doi: 10.1109/ICC45041.2023.10278840.
- [20] A. Cuzzocrea, A. Hafsaoui, and C. K. Leung, "Machine-learning-based multidimensional big data analytics over clouds via multi-columnar big OLAP data cube compression," in *Proceedings - 2023 IEEE International Conference on Big Data, BigData 2023*, IEEE, Dec. 2023, pp. 5206–5212. doi: 10.1109/BigData59044.2023.10386560.
- [21] S. Mittal and O. P. Sangwan, "Big data analytics using machine learning techniques," in *Proceedings of the 9th International Conference On Cloud Computing, Data Science and Engineering, Confluence 2019*, IEEE, Jan. 2019, pp. 203–207. doi: 10.1109/CONFLUENCE.2019.8776614.
- [22] T. Nandy and A. Nyundo, "Prediction of possible outcomes using big data analysis and machine learning," in *International Conference on Applied Intelligence and Sustainable Computing, ICAISC 2023*, IEEE, Jun. 2023, pp. 1–6. doi: 10.1109/ICAISC58445.2023.10200831.
- [23] S. Xiao and C. Wu, "Explore deep reinforcement learning for efficient task processing based on federated optimization in big data," *Future Generation Computer Systems*, vol. 149, pp. 150–161, Dec. 2023, doi: 10.1016/j.future.2023.06.027.
- [24] H. Xia, Y. Wang, S. Jasimuddin, J. Z. Zhang, and A. Thomas, "A big-data-driven matching model based on deep reinforcement learning for cotton blending," *International Journal of Production Research*, vol. 61, no. 22, pp. 7573–7591, Nov. 2023, doi: 10.1080/00207543.2022.2153942.
- [25] M. A. Amanullah *et al.*, "Deep learning and big data technologies for IoT security," *Computer Communications*, vol. 151, pp. 495–517, Feb. 2020, doi: 10.1016/j.comcom.2020.01.016.
- [26] V. Singh, S. S. Chen, M. Singhanian, B. Nanavati, A. kumar kar, and A. Gupta, "How are reinforcement learning and deep learning algorithms used for big data based decision making in financial industries—A review and research agenda," *International Journal of Information Management Data Insights*, vol. 2, no. 2, p. 100094, Nov. 2022, doi: 10.1016/j.jjime.2022.100094.





- [27] L. Lyu, Y. Shen, and S. Zhang, "The advance of reinforcement learning and deep reinforcement learning," in *2022 IEEE International Conference on Electrical Engineering, Big Data and Algorithms, EEBDA 2022*, IEEE, Feb. 2022, pp. 644–648. doi: 10.1109/EEBDA53927.2022.9744760.
- [28] T. T. Chhowa, M. A. Rahman, A. K. Paul, and R. Ahmmed, "A narrative analysis on deep learning in iot based medical big data analysis with future perspectives," in *2nd International Conference on Electrical, Computer and Communication Engineering, ECCE 2019*, IEEE, Feb. 2019, pp. 1–6. doi: 10.1109/ECACE.2019.8679200.
- [29] S. Zeng, A. Kody, Y. Kim, K. Kim, and D. K. Molzahn, "A reinforcement learning approach to parameter selection for distributed optimal power flow," *Electric Power Systems Research*, vol. 212, p. 108546, Nov. 2022, doi: 10.1016/j.epsr.2022.108546.
- [30] Deepanshu Mehta, "State-of-the-Art reinforcement learning algorithms," *International Journal of Engineering Research and*, vol. V8, no. 12, Jan. 2020, doi: 10.17577/ijertv8is120332.
- [31] B. B. Mehta and U. P. Rao, "Privacy preserving unstructured big data analytics: issues and challenges," *Physics Procedia*, vol. 78, pp. 120–124, 2016, doi: 10.1016/j.procs.2016.02.020.

BIOGRAPHIES OF AUTHORS







Wiranto Herry Utomo     is a distinguished Professor of Computer Science at President University, renowned for his expertise in Service Oriented Architecture (SOA), Web Services, Enterprise Service Bus (ESB), and Software as a Service (SaaS). With a strong academic background and practical experience, he plays a pivotal role in advancing these fields through research, teaching, and industry collaboration. His work has contributed significantly to the understanding and implementation of modern software design principles and technologies. He can be contacted at email: wiranto.herry@president.ac.id.



Rosalina     a respected lecturer in the Informatics Study Program at President University, exemplifies dedication to her field. Her commitment to academic excellence is underscored by her Master's degree in Informatics from President University. With a strong educational background and a passion for informatics, Rosalina has a significant impact on students' academic journeys. Her expertise in the subject matter, combined with her ability to explain complex concepts, creates a dynamic and enriching learning environment. She can be contacted at email: rosalina@president.ac.id.



Afriyadi     an alumnus of President University's School of Computer Science with a Master of Science degree, specializes in Machine Learning, Reinforcement Learning, Robotics, and Cybersecurity. Combining theoretical and practical expertise, Afriyadi is dedicated to technological advancements and innovative research. He can be contacted at email: afriyadi.it@gmail.com.