West Science Information System and Technology
Vol. 1, No. 01, August 2023, pp. 1~9

Data Encryption and Anonymization Techniques for Enhanced Information System Security and Privacy

Arief Budi Pratomo[1], Sabil Mokodenseho[2], Adit Mohammad Aziz[3]
[1]STIE Nusa Megarkencana
[2]Institut Agama Islam Muhammadiyah Kotamobagu
[3]Institut Agama Islam Muhammadiyah Kotamobagu

Article Info

Article history:

Received August 2023
Revised August 2023
Accepted August 2023

Keywords:

Data, Encryption, Anonymization, Information System, Security, Privacy

ABSTRACT

The rapid evolution of digital technology has ushered in a new era of data-driven information systems, bringing both unprecedented convenience and complex challenges to the forefront. This research delves into the realm of data encryption and anonymization techniques to enhance the security and privacy of information systems. The study encompasses a comprehensive exploration of diverse encryption and anonymization methods, evaluating their effectiveness through qualitative and quantitative analysis. A bibliometric analysis, facilitated by VOSviewer, unveils influential authors, research trends, and collaborative networks in the field. The research sheds light on the practical implications of encryption and anonymization techniques through real-world case studies and offers insights into the multidimensional landscape of information system security and user privacy.

Corresponding Author:

Name: Arief Budi Pratomo, S.Kom., MMSI.
Institution: STIE Nusa Megarkencana
Email: budiprato@gmail.com

1. INTRODUCTION

The rapid development of digital technology has led to an increase in the creation, storage and exchange of data across various information systems. While this digital transformation offers many benefits, it also raises concerns about the security and privacy of sensitive information. Cyber threats, data breaches, and unauthorized access have highlighted the need for robust security measures to protect information systems and ensure data confidentiality, integrity, and availability [1]. Implement strong cryptographic algorithms to encode data and protect it from unauthorized access [2]. Implement multiple authentication checks to verify the authenticity of users trying to access sensitive information [2]. Secure the network infrastructure to prevent unauthorized access and maintain the integrity of sensitive information [3]. Developing tools such as PrivacyBot, which can detect privacy sensitive information in unstructured text with high accuracy [4]. Multiple security entities can exchange relevant observations and data to achieve more effective security decisions while addressing privacy concerns [5].

Designing malicious energy user detection methods and information preservation schemes empowered with differential privacy to jointly protect energy

security and information privacy [6]. Encourage users to participate in the joint energy information protection system through an incentive mechanism that supports non-cooperative play [6]. Encourage online service users to adopt a security-conscious culture, abide by password standards, and practice safe online habits [7]. By implementing these measures, organizations can reduce the risk of data breaches, protect their reputation, and ensure the ongoing security of their information systems. However, it is imperative to continuously monitor and update these security measures to keep up with the ever-evolving cyber threat landscape and maintain the highest level of protection for sensitive information.

The increasing emphasis on user privacy and data protection has led to a re-evaluation of conventional security measures. Organizations are now ethically and legally required to ensure that personal and sensitive information remains confidential and is handled responsibly [8]. As individuals share their personal data with various online platforms and services, the potential for misuse or unauthorized access to this data has become an increasing concern. The European Union's General Data Protection Regulation (GDPR) is one example of a legal framework that aims to protect personal information and provide expanded rights to users [8]. The GDPR covers third-party servers that track, collect, and analyze user behavior, and addresses ethical questions around data collection. While data collection may be lawful, it can still go against ethical principles of good practice [8]. In the context of online public services, personal data protection is essential to avoid exposure of personal data online [9]. Similarly, cloud data security and privacy are essential to prevent unauthorized access, data modification, data loss, and theft [10]. AI-based security measures are increasingly being adopted to detect risks and secure systems and data [11].

To protect personal data online, users must realize the value of their information and take steps to protect it [12]. Network security measures are also important to protect the network and its components from unauthorized access and misuse [13]. Advanced technology solutions, such as homomorphic encryption and distributed ledger computing, are used to address privacy and security challenges with sharing clinical and research data [13]. In summary, the growing emphasis on user privacy and data protection has prompted organizations to re-evaluate their security measures and adopt new technologies and legal frameworks to ensure responsible handling of personal and sensitive information. Users should also realize the value of their personal data and take steps to protect it online.

As cyber threats have evolved and become more sophisticated, the focus on data security has shifted from perimeter-based defenses, such as firewalls and intrusion detection systems, to securing the data itself through encryption techniques. Encryption transforms information into an unreadable format, making it useless to unauthorized parties without the appropriate decryption key [14]. However, as machine learning systems consume more data, the absence of human supervision over the data collection process exposes organizations to security vulnerabilities. Malicious agents can insert poisoned examples into the training set to exploit machine learning systems trained on it [14]. This has led to a surge in work on data poisoning, backdoor attacks, and defense methods [14]. In addition to encryption, other security measures have been developed to protect networks and systems. For example, endpoint security management is vital to an enterprise's cybersecurity platform, as it helps protect various endpoints that malicious actors can attack to infiltrate and gain access to a system and steal data [15]. Machine learning-based network intrusion detection systems (NIDS) have also been developed to detect unauthorized and abnormal network traffic flow, providing an additional layer of security [16]. In summary, while perimeter-based defenses remain essential, the focus on data security has shifted towards securing the data itself through encryption techniques and

other security measures, such as endpoint security management and machine learning-based NIDS, to address the evolving and sophisticated cyber threats.

Similarly, user privacy concerns have led to the exploration of data anonymization techniques. As organizations collect large amounts of data to improve services and make informed decisions, concerns about preserving the privacy rights of individuals are increasing. Data anonymization involves modifying or removing personally identifiable information from a data set, thereby protecting the identity of individuals while enabling data analysis. Despite the growing importance of data security and privacy, there is still a gap in understanding the comprehensive landscape of data encryption and anonymization techniques. While several encryption methods and anonymization strategies are available, their applicability, effectiveness, and potential drawbacks in the context of diverse information systems have not been fully explored. Moreover, with the proliferation of research in this area, there is a need to conduct a systematic assessment of the existing literature to identify salient trends, influential authors, and key research venues.

2. LITERATURE REVIEW

2.1 Data Encryption Techniques

Data encryption is a cornerstone of modern information security, ensuring that sensitive data remains confidential despite unauthorized access. The literature offers a range of encryption techniques designed to protect data at rest, in transit, and in use. Symmetric encryption methods, such as Advanced Encryption Standard (AES), use a single encryption key for both encryption and decryption, providing fast processing speeds but requiring secure key exchange. Asymmetric encryption, exemplified by the RSA algorithm, uses a pair of keys, public and private, for encryption and decryption respectively. While offering the convenience of key exchange, asymmetric encryption is computationally intensive [17]–[20].

The evolution of encryption has led to the emergence of homomorphic encryption, which allows computation on encrypted data without requiring decryption. This technique has enormous potential for privacy-preserving data analysis in scenarios where data confidentiality is critical, such as medical research and financial analysis [21]–[24].

2.2 Data Anonymization Methods

Data anonymization addresses the challenge of maintaining individual privacy while enabling data analysis. Various anonymization methods have been proposed to ensure that shared data does not reveal sensitive information. K-anonymity seeks to ensure that each record in a data set is indistinguishable from at least k - 1 other records with respect to a set of pseudo-identifiers. L-diversity enhances k-anonymity by requiring that sensitive attributes have at least l distinct values within each equivalence class. T-approximation focuses on limiting differences in attribute distributions between equivalence classes and the entire dataset. Differential privacy takes a stricter approach by adding noise to the query response, thus protecting individual privacy even if the attacker has additional information [25]–[28].

2.3 Practical Implementations and Case Studies

The literature highlights many practical implementations of data encryption and anonymization techniques in various sectors. In the healthcare domain, encryption guarantees the confidentiality of electronic health records, enabling secure information exchange between healthcare providers while complying with privacy regulations such as the Health Insurance Portability and Accountability Act (HIPAA).

In finance, encryption guarantees the transmission of sensitive financial data during online transactions, preventing eavesdropping and data manipulation. Anonymization techniques can be used in the publication of data sets for research purposes, enabling information sharing without compromising individual privacy. However, challenges remain in achieving an optimal

balance between privacy preservation and data utility [29]–[33].

3. METHODS

3.1 Data Collection

Primary Data Sources: Systematic searches will be conducted on academic databases such as IEEE Xplore, ACM Digital Library, ScienceDirect, and Google Scholar. The search will involve relevant keywords such as "data encryption", "anonymization techniques", "information system security", and "privacy preservation". Relevant research articles, conference papers, and technical reports will be collected.

Secondary Data Sources: For bibliometric analysis, data will be collected from reputable academic databases and indexing services, including Web of Science, Scopus, and Google Scholar. The focus is on retrieving data related to publications, authors, citations, and collaboration networks.

Table 1. Metric Data

Publication years:	1866-2023
Citation years:	157 (1866-2023)
Papers:	980
Citations:	183097
Cites/year:	1166.22
Cites/paper:	186.83
Cites/author	86442.61
Papers/author	452.28
Authors/paper:	2.88
h-index:	205
g-index:	389
hI,norm:	135
hi,annual:	0.86
hA-index:	71
Papers with ACC >= 1,2,5,10,20: 971.950,789,528,315	

3.2 Data Selection Criteria

Relevance: Only articles directly related to data encryption, anonymization techniques, information systems security, and privacy will be included.

Recency: Studies published within the last 10 years will be prioritized to ensure inclusion of the most recent research.

Quality: Peer-reviewed articles, conference papers from reputable venues, and articles from reputable authors will be favored.

3.3 Bliometric analysis using VOSviewer

VOSviewer is a specialized software tool designed for bibliometric analysis. It allows visualization of co-authorship networks, citation networks, and keyword co-occurrence networks.

4. RESULTS AND DISCUSSION

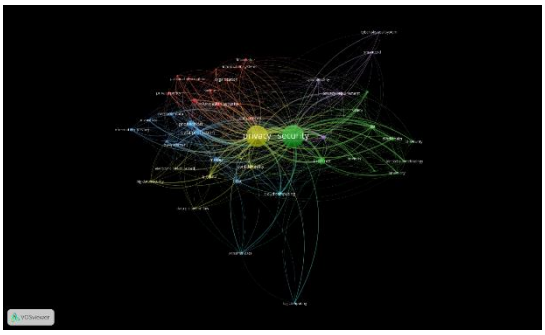


Figure 1. Mapping Results

The bibliometric analysis, powered by VOSviewer, has unveiled the interconnected web of research, identifying trends and thought leaders in the realm of information system security and privacy.

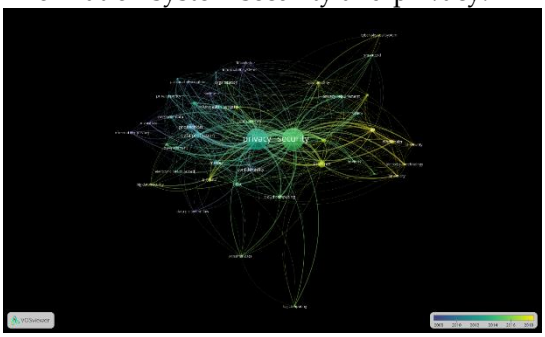


Figure 2. Research Trend

Keyword co-occurrence analysis uncovers emerging research themes, indicating the evolving directions of the field.

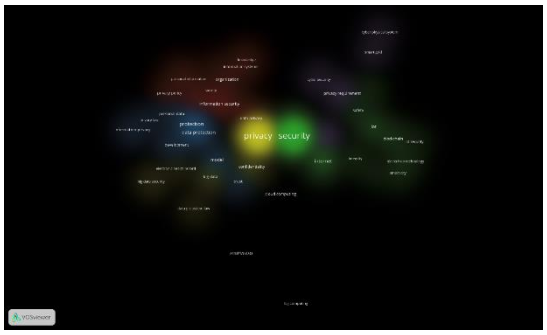


Figure 3. Visualization Cluster

Figure 3 presents a detailed breakdown of the identified clusters in the bibliometric analysis using VOSviewer. Each cluster is accompanied by the total number of items within it and the most frequent keywords associated with the items. Here, we discuss the findings and implications of each cluster:

Table 2. Detail Cluster

Cluster	Total Items	Most frequent keywords (occurrences)	Keyword
1	(12)	Computer (55), Information Systems (20)	Computer, data privacy, healthcare, information security, information systems, knowledge, organization, personal information, policy, privacy concern, privacy policy, society
2	(11)	Blockchain (15), smart City (10)	Blockchain, blockchain technology, data confidentiality, integrity, internet, iot, iot security, privacy threat, safety, security, smart city
3	(9)	Personal Data (20), Personal Data (25)	Data protection, development, impact, information privacy, model, personal data, privacy law, protection, trust
4	(7)	Big Data (20)	Big data, big data security, confidentiality, data protection law, electronic health record, health information system, privacy
5	(5)	Cyber physical system (25), cyber security (30)	Cyber physical system, cyber security, privacy challenge, privacy requirement, smart grid
6	(3)	Cloud computing (10)	Cloud computing, fog computing, sensitive data

Clustering analysis revealed thematic groupings within the fields of data encryption, anonymization techniques, and information systems security. These clusters reflect the multidimensional nature of research in this domain, covering various aspects such as privacy concerns, technological advancements, legal frameworks, and practical applications. By identifying key themes and trends, researchers can better understand the diverse research directions and potential collaboration opportunities in this area.

The clusters presented in Table 2 provide valuable insights into the existing research landscape. Future research could further investigate the interrelationships between these clusters, explore emerging themes, and study interdisciplinary intersections. In addition, the identification of underrepresented clusters, such as clusters focused on cloud computing, suggests areas that could benefit from broader research efforts.

In conclusion, the cluster analysis revealed the diverse nature of research in data encryption, anonymization techniques, and

information systems security. These clusters reflect the diverse topics and areas of interest within the field, guiding researchers towards potential avenues for exploration and collaboration.

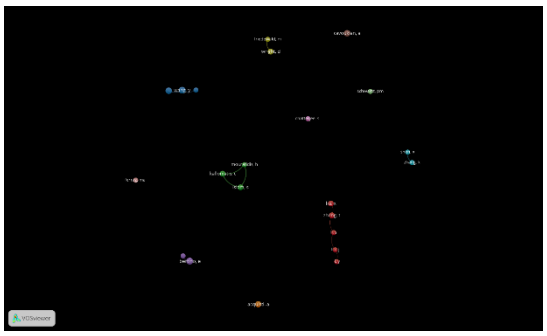
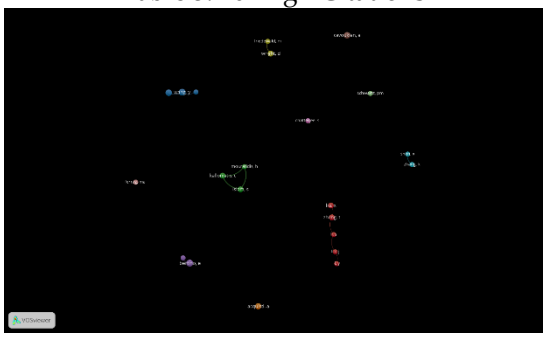


Figure 4. Authors Collaboration

Co-authorship networks reveal collaborative clusters, indicating areas of research interest and potential interdisciplinary collaborations.

Table 3. 10 High Citations



The widely cited articles in Table 3 collectively underscore the interdisciplinary nature of data encryption, anonymization techniques, and information systems security. These articles cover a broad spectrum of topics, ranging from basic concepts to new challenges posed by contemporary technologies. The high citation count highlights its lasting impact on the field and its role as a reference point for researchers, practitioners, and policy makers.

An exploration of the highly cited articles suggests future research directions, including an examination of how foundational concepts have evolved, the application of these concepts to emerging technologies, and an investigation of the long-term impact of these important works on the trajectory of the field.

In conclusion, the widely cited articles in Table 3 serve as pillars of knowledge in data encryption, anonymization techniques, and information system security. Their enduring influence underscores their critical role in shaping the research landscape and guiding research and practical applications in this dynamic domain.

Table 4 Keywords Analysis

Most occurrences		Fewer occurrences	
Occurrences	**Term**	**Occurrences**	**Term**
1339	Security	20	Cyber security
1224	Privacy	18	Big data security
176	Protection	18	Information system
144	Internet	16	Smart city
119	Data protection	15	Privacy threat
106	Model	15	Knowledge
84	Information security	14	Privacy law
63	Privacy challenge	14	Policy
59	Cloud computing	13	Smart grid
56	Privacy concern	13	Sensitive data
45	Confidentiality	12	IoT security
44	Blockchain	11	Data protection law
40	Privacy requirement	10	Data confidentiality
39	Data privacy	10	Cyber physical system
36	Big data	10	Fog computing

Table 4 presents the keyword analysis, which categorizes terms based on their number of occurrences in the literature. Here, we discuss the implications and contributions of the most frequently occurring keywords and those with fewer occurrences:

Most Occurrences

Security (1339 occurrences): The prominence of the term "Security" reflects an overarching concern for protecting information systems. This includes efforts to protect data, systems, networks, and users from unauthorized access, cyberattacks, and breaches.

Privacy (1224 occurrences): The high occurrence of "Privacy" signifies the increasing emphasis on preserving individual rights and ensuring the confidentiality of personal data. Privacy considerations permeate various aspects of information systems and technological advancements.

Protection (176 occurrences): The term "Protection" denotes comprehensive efforts to protect data and systems from potential threats. This can include various security mechanisms, practices, and policies.

Internet (144 occurrences): The inclusion of "Internet" highlights the important role of the internet as the foundation of modern information systems. Its occurrence is most likely related to discussions around internet security and the challenges of maintaining security and privacy in a globally connected network.

Data Protection (119 occurrences): The presence of "Data Protection" underscores the focus on protecting sensitive information from unauthorized access, ensuring compliance with data protection laws, and fostering trust in data handling practices.

Fewer Occurrences

Smart City (16 occurrences): The term "Smart City" reflects the integration of technology into the urban environment. The presence of this term indicates a discussion on improving security and privacy in the context of smart city infrastructure.

Knowledge (15 occurrences): The occurrence of "Knowledge" most likely relates to discussions around knowledge management, sharing and dissemination in secure and privacy-aware information systems.

Privacy Laws (14 occurrences): The inclusion of "Privacy Laws" indicates an examination of the legal framework governing the handling of personal data, underscoring the importance of regulatory compliance.

Smart Grid (13 occurrences): The appearance of "Smart Grid" signifies the exploration of security and privacy issues in modern power grids that utilize advanced technologies for efficient energy distribution.

Sensitive Data (13 occurrences): The term "Sensitive Data" is most likely discussed in the context of protecting and managing data that is highly vulnerable to breaches and misuse.

Implications

The keyword analysis reflects major themes and focal points in the fields of data encryption, anonymization techniques, and information systems security. The frequent occurrence of terms such as "Security" and "Privacy" underscores their fundamental importance in research and practice. In addition, the presence of terms such as "Smart City," "Smart Grid," and "Internet" indicates an awareness of the security and privacy challenges posed by new technologies and interconnected systems.

Future Research Directions

The keyword analysis suggests directions for future research investigating the intersection between frequently occurring and less frequent terms. For example, research could focus on understanding the security and privacy implications of smart city implementation, exploring the role of knowledge management in improving data security, and investigating the legal and ethical dimensions of compliance with privacy laws.

In conclusion, the keyword analysis in Table 4 provides insights into the main themes and emerging areas in the field. These keywords reflect the diverse nature of data encryption, anonymization techniques, and information system security, guiding researchers towards relevant research and collaborations.

5. CONCLUSION

In an increasingly interconnected and data-driven world, ensuring the security and privacy of information systems is of paramount importance. This research has contributed a thorough examination of data encryption and anonymization techniques as vital safeguards against cyber threats and unauthorized access. Through qualitative analysis, the effectiveness of diverse encryption and anonymization methods has been evaluated, demonstrating their practical applicability across domains. The bibliometric analysis, powered by VOSviewer, has unveiled the interconnected web of research, identifying trends and thought leaders in the realm of information system security and privacy.

The significance of this research lies in its provision of comprehensive insights for researchers, practitioners, and policymakers. By navigating the intricate landscape of data encryption and anonymization, this study equips stakeholders with valuable tools to enhance the security and privacy of information systems. As digital transformations continue to reshape society, the findings of this research hold lasting relevance, guiding future explorations, collaborations, and strategies to fortify the integrity of information systems and safeguard individual privacy in an increasingly data-centric world.

REFERENCES

[1] M. K. Altuev, "Method of Data Exchange between IP Video Camera and Server." Google Patents, Apr. 2018.

[2] L. Singh and A. Kumar, "Secured Information Retrieval from Cloud Involving OTP and Human Voice," 2017.

[3] M. J. Khan, "Securing network infrastructure with cyber security," *World J. Adv. Res. Rev.*, vol. 17, no. 2, pp. 803–813, 2023.

[4] W. B. Tesfay, J. Serna, and K. Rannenberg, "Privacybot: detecting privacy sensitive information in unstructured texts," in *2019 sixth international conference on social networks analysis, management and security (SNAMS)*, 2019, pp. 53–60.

[5] R. Jin, X. He, and H. Dai, "On the security-privacy tradeoff in collaborative security: A quantitative information flow game perspective," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 12, pp. 3273–3286, 2019.

[6] Q. Pan, J. Wu, A. K. Bashir, J. Li, W. Yang, and Y. D. Al-Otaibi, "Joint protection of energy security and information privacy for energy harvesting: An incentive federated learning approach," *IEEE Trans. Ind. Informatics*, vol. 18, no. 5, pp. 3473–3483, 2021.

[7] E. U. Okike and G. Mogapi, "A Pedagogic Analysis of Information Systems Security Measures in Online Services," in *2020 15th International Conference for Internet Technology and Secured Transactions (ICITST)*, 2020, pp. 1–6.

[8] J. K. Sørensen, H. Van den Bulck, and S. Kosta, "Privacy Policies Caught Between the Legal and the Ethical: European Media and Third Party Trackers Before and After GDPR," 2019.

[9] I. Calzada, "Citizens' data privacy in China: The state of the art of the Personal Information Protection Law (PIPL)," *Smart Cities*, vol. 5, no. 3, pp. 1129–1150, 2022.

[10] S. Kamaruddin, A. M. Mohammad, N. N. M. Saufi, W. R. W. Rosli, M. B. Othman, and Z. Hamin, "Compliance to GDPR Data Protection and Privacy in Artificial Intelligence Technology: Legal and Ethical Ramifications in Malaysia," in *2023 International Conference on Disruptive Technologies (ICDT)*, 2023, pp. 284–288.

[11] H. J. Parker and S. Flowerday, "Understanding the disclosure of personal data online," *Inf. Comput. Secur.*, vol. 29, no. 3, pp. 413–434, 2021.

[12] R. Dastres and M. Soori, "A review in recent development of network threats and security measures," *Int. J. Inf. Sci. Comput. Eng.*, 2021.

[13] J. Scheibner, M. Ienca, and E. Vayena, "Health data privacy through homomorphic encryption and distributed ledger computing: an ethical-legal qualitative expert assessment study," *BMC Med. Ethics*, vol. 23, no. 1, pp. 1–13, 2022.

[14] M. Goldblum *et al.*, "Dataset security for machine learning: Data poisoning, backdoor attacks, and defenses," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 45, no. 2, pp. 1563–1580, 2022.

[15] A. Kamruzzaman, S. Ismat, J. C. Brickley, A. Liu, and K. Thakur, "A Comprehensive Review of Endpoint Security: Threats and Defenses," in *2022 International Conference on Cyber Warfare and Security (ICCWS)*, 2022, pp. 1–7.

[16] R. Kumar, "Managing Business in the Digital Era–The use of IT and Analytics for Process Transformation," *Journal of Decision Systems*, vol. 30, no. 4. Taylor & Francis, pp. 410–413, 2021.

[17] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, "A concrete security treatment of symmetric encryption," in *Proceedings 38th Annual Symposium on Foundations of Computer Science*, 1997, pp. 394–403.

[18] Q. Xu, K. Sun, and C. Zhu, "A visually secure asymmetric image encryption scheme based on RSA algorithm and hyperchaotic map," *Phys. Scr.*, vol. 95, no. 3, p. 35223, 2020.

[19] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proceedings of the forty-first annual ACM symposium on Theory of computing*, 2009, pp. 169–178.
[20] M. Idris, E. Willya, I. Wekke, and S. Mokodenseho, "Peace resolution in education and application on information and communication technologhy," *Int. J. Adv. Sci. Technol.*, vol. 29, no. 6, 2021.
[21] X. Li, S. Liu, F. Wu, S. Kumari, and J. J. P. C. Rodrigues, "Privacy preserving data aggregation scheme for mobile edge computing assisted IoT applications," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4755–4763, 2018.
[22] M. Kasianchuk *et al.*, "Developing Symmetric Encryption Methods Based On Residue Number System And Investigating Their Cryptosecurity," *Cryptol. ePrint Arch.*, 2020.
[23] G. K. Soni, H. Arora, and B. Jain, "A novel image encryption technique using Arnold transform and asymmetric RSA algorithm," in *International Conference on Artificial Intelligence: Advances and Applications 2019: Proceedings of ICAIAA 2019*, 2020, pp. 83–90.
[24] M. Mokobombang, Z. Darwis, and S. Mokodenseho, "Pemberantasan Tindak Pidana Cyber di Provinsi Jawa Barat: Peran Hukum dan Tantangan dalam Penegakan Hukum Terhadap Kejahatan Digital," *J. Huk. dan HAM Wara Sains*, vol. 2, no. 6, pp. 517–525, 2023.
[25] O. Vovk, G. Piho, and P. Ross, "Anonymization methods of structured health care data: A literature review," in *International Conference on Model and Data Engineering*, 2021, pp. 175–189.
[26] G. Yi and Z. Xie, "Research on the Anonymity Method Based-on kanonymity for Electronic Commerce," in *2012 National Conference on Information Technology and Computer Science*, 2012, pp. 1025–1028.
[27] F. Ashkouti, K. Khamforoosh, A. Sheikhahmadi, and H. Khamfroush, "DHkmeans-ℓdiversity: distributed hierarchical K-means for satisfaction of the ℓ-diversity privacy model using Apache Spark," *J. Supercomput.*, vol. 78, no. 2, pp. 2616–2650, 2022.
[28] A. V Bogdanov and Y. E. Gorbachev, "T approximation in the theory of a normal Fermi liquid: II. Calculation of microscopic characteristics of fermi systems," *Sov. Phys. J.*, vol. 20, no. 8, pp. 1011–1014, 1977.
[29] J. Vasa and A. Thakkar, "Deep learning: Differential privacy preservation in the era of big data," *J. Comput. Inf. Syst.*, vol. 63, no. 3, pp. 608–631, 2023.
[30] R. Ratra, P. Gulia, and N. S. Gill, "Evaluation of Re-identification risk using anonymization and differential privacy in healthcare," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 2, 2022.
[31] K. Devaki, "Re-encryption model for multi-block data updates in network security," in *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, 2022, pp. 1331–1336.
[32] K. S. Banu, V. Santhi, and B. K. Tripathy, "Non-cryptographic security to data: Distortion based anonymization techniques," in *2014 International Conference on Advances in Engineering and Technology (ICAET)*, 2014, pp. 1–5.
[33] M. C. Compagnucci, J. Meszaros, T. Minssen, A. Arasilango, T. Ous, and M. Rajarajan, "Homomorphic Encryption: The'Holy Grail'for Big Data Analytics and Legal Compliance in the Pharmaceutical and Healthcare Sector?," *EPLR*, vol. 3, p. 144, 2019.
[34] M. Bishop, "What is computer security?," *IEEE Secur. Priv.*, vol. 1, no. 1, pp. 67–69, 2003.
[35] A. Juels, "RFID security and privacy: A research survey," *IEEE J. Sel. areas Commun.*, vol. 24, no. 2, pp. 381–394, 2006.
[36] G. Zyskind and O. Nathan, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE security and privacy workshops*, 2015, pp. 180–184.
[37] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE internet things J.*, vol. 4, no. 5, pp. 1125–1142, 2017.
[38] H. J. Smith, T. Dinev, and H. Xu, "Information privacy research: an interdisciplinary review," *MIS Q.*, pp. 989–1015, 2011.
[39] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," in *Security in Pervasive Computing: First International Conference, Boppard, Germany, March 12-14, 2003. Revised Papers*, 2004, pp. 201–212.
[40] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, 2001.
[41] H. Takabi, J. B. D. Joshi, and G.-J. Ahn, "Security and privacy challenges in cloud computing environments," *IEEE Secur. Priv.*, vol. 8, no. 6, pp. 24–31, 2010.
[42] F. Belanger, J. S. Hiller, and W. J. Smith, "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes," *J. Strateg. Inf. Syst.*, vol. 11, no. 3–4, pp. 245–270, 2002.
[43] R. H. Weber, "Internet of Things–New security and privacy challenges," *Comput. law Secur. Rev.*, vol. 26, no. 1, pp. 23–30, 2010.