World Journal of Advanced Engineering Technology and Sciences

eISSN: 2582-8266

Cross Ref DOI: 10.30574/wjaets

Journal homepage: https://wjaets.com/

WJAETS
World Journal of Advanced Engineering Technology and Sciences

(Review Article)

Reviewing advancements in privacy-enhancing technologies for big data analytics in an era of increased surveillance

Olakunle Abayomi Ajala [1], Chuka Anthony Arinze [2], Onyeka Chrisanctus Ofodile [3], Chinwe Chinazo Okoye [4], and Obinna Donald Daraojimba [5, *]

[1] *Indiana Wesleyan University, USA.*
[2] *Independent Researcher, Port Harcourt, Rivers State, Nigeria.*
[3] *Sanctus Maris Concepts, Nigeria Ltd.*
[4] *Access Bank Plc, Nigeria.*
[5] *Department of Information Management, Ahmadu Bello University, Zaria, Nigeria.*

World Journal of Advanced Engineering Technology and Sciences, 2024, 11(01), 294–300

Publication history: Received on 08 January 2024; revised on 15 February 2024; accepted on 17 February 2024

Article DOI: https://doi.org/10.30574/wjaets.2024.11.1.0060

Abstract

In the contemporary landscape of big data analytics, privacy concerns loom large, exacerbated by escalating surveillance measures. This review delves into the advancements of privacy-enhancing technologies (PETs) amidst this era of heightened scrutiny. The review explores the evolving landscape of PETs, highlighting their pivotal role in safeguarding individual privacy while enabling meaningful data analysis. Firstly, the review elucidates the escalating surveillance environment, characterized by ubiquitous data collection practices and the proliferation of sophisticated monitoring mechanisms. Against this backdrop, the imperative for robust privacy solutions becomes evident. Subsequently, the review navigates through the array of PETs, encompassing differential privacy, homomorphic encryption, secure multi-party computation, and federated learning, among others. Each technology is scrutinized for its efficacy in mitigating privacy risks without compromising analytical utility. Furthermore, the review delineates notable applications of PETs across diverse domains, including healthcare, finance, and social media. Case studies exemplify how PETs facilitate data sharing and collaborative analysis while preserving confidentiality and compliance with regulatory frameworks. Moreover, the review examines the challenges hindering the widespread adoption of PETs, such as computational overhead, interoperability issues, and regulatory ambiguities. Strategies for overcoming these hurdles are elucidated, encompassing advancements in algorithmic efficiency, standardization efforts, and policy advocacy. The review underscores the pivotal role of PETs in reconciling the imperatives of data analytics with the imperatives of privacy protection amidst escalating surveillance. It emphasizes the necessity for interdisciplinary collaboration among researchers, policymakers, and industry stakeholders to foster the development and deployment of effective PET solutions, thereby ensuring a harmonious balance between data utility and individual privacy rights in the digital age.

Keywords: Big Data; Analytics; Surveillance; Technology; Privacy-Enhanced; Review

1. Introduction

In recent years, big data analytics has emerged as a powerful tool for extracting valuable insights from vast and diverse datasets (Grover, and Kar, 2017). Leveraging advanced computational algorithms and technologies, organizations can analyze large volumes of data to inform decision-making, enhance operations, and drive innovation across various sectors (Vassakis, et al., 2018).

[*] Corresponding author: Obinna Donald Daraojimba.

However, the proliferation of surveillance practices, both by governments and private entities, has raised significant concerns regarding individual privacy rights (Slobogin, 2008). From ubiquitous data collection through digital platforms to the deployment of sophisticated monitoring systems, individuals are increasingly vulnerable to intrusive surveillance measures. This heightened surveillance poses a threat to personal privacy, autonomy, and civil liberties, particularly in the context of big data analytics where massive amounts of sensitive information are processed and analyzed (Banisar, and Davies, 1999; Aho, and Duffield, 2020).

In response to the escalating surveillance landscape and growing privacy concerns, the development and deployment of Privacy-Enhancing Technologies (PETs) have become imperative (Hasani, et al., 2023; Ifeji, and Adeniji,2023; Messinis, et al., 2024). PETs encompass a range of cryptographic, statistical, and computational techniques designed to protect individuals' privacy while enabling effective data analysis. By integrating privacy-preserving mechanisms into data processing and analytics workflows, PETs aim to mitigate the risks associated with data breaches, unauthorized access, and indiscriminate surveillance (Fitwi, 2021). In essence, PETs play a crucial role in safeguarding individual privacy rights, fostering trust in data-driven systems, and promoting ethical and responsible data practices in the era of increased surveillance.

2. Escalating Surveillance Landscape

Governments and intelligence agencies employ mass surveillance programs to monitor communications, collect metadata, and analyze vast amounts of data from various sources, including telecommunications, internet activities, and financial transactions (Andrejevic,. and Gates, 2014; Crampton, 2015). These programs often operate under the pretext of national security or counterterrorism efforts, raising concerns about privacy infringement and civil liberties violations. Technology companies gather extensive data on individuals' online activities, preferences, and behaviors through websites, social media platforms, mobile apps, and IoT devices (Lyon, 2014). This data includes browsing history, search queries, location information, and personal preferences, which are used for targeted advertising, user profiling, and data monetization purposes. Some governments utilize internet monitoring and censorship techniques to control online content, restrict access to certain websites, and surveil citizens' online activities (Zittrain, and Palfrey, 2008; Deibert, 2008). This includes the deployment of content filtering systems, surveillance tools, and censorship mechanisms to monitor and regulate online communication channels, social media platforms, and news outlets. Biometric surveillance technologies, such as facial recognition, fingerprint scanning, and iris recognition, are increasingly used for identification and tracking purposes in public spaces, airports, transportation hubs, and commercial establishments. These technologies raise significant privacy concerns regarding the collection, storage, and use of biometric data, as well as the potential for misuse, abuse, and discriminatory practices (Al-Saqaf, 2016; Deibert, et al., 2010).

The extensive collection and aggregation of personal data increase the risk of data breaches, cyberattacks, and unauthorized access, leading to the exposure of sensitive information, identity theft, and privacy violations. Big data analytics platforms and repositories become lucrative targets for malicious actors seeking to exploit vulnerabilities and gain unauthorized access to valuable data assets. (Romanosky, and Acquisti, 2009; Mills, et al., 2017) Surveillance data may contain biases, prejudices, and discriminatory patterns that are inadvertently incorporated into analytics algorithms, resulting in unfair or discriminatory outcomes for certain individuals or groups. Biased algorithms may perpetuate existing inequalities, reinforce stereotypes, and exacerbate social disparities, leading to unjust or discriminatory treatment in decision-making processes. With the proliferation of surveillance technologies and data collection practices, maintaining anonymity and pseudonymity becomes increasingly challenging, as individuals' activities, behaviors, and interactions are continuously monitored, tracked, and analyzed. The erosion of anonymity undermines individuals' ability to control their personal information, protect their privacy, and maintain autonomy over their digital identities (Rafiq, et al., 2022).

Implementing encryption and anonymization techniques can help protect sensitive data and preserve privacy by encrypting data at rest and in transit, and anonymizing personally identifiable information (PII) to prevent unauthorized access and disclosure (Gholami, 2016; Beleuta, V., 2017.). Differential privacy techniques add noise to query responses or datasets to protect individuals' privacy while allowing for accurate statistical analysis and data sharing, ensuring that individual privacy is preserved even when analyzing sensitive or personal data (Naranjo Rico, 2018) Privacy-preserving data mining techniques enable organizations to extract valuable insights from data without compromising individual privacy by utilizing techniques such as secure multi-party computation (SMPC), homomorphic encryption, and federated learning to perform analytics tasks while preserving data confidentiality and privacy.

In conclusion, addressing the challenges posed by the escalating surveillance landscape requires a comprehensive approach that integrates technological innovations, regulatory frameworks, and ethical considerations. By adopting robust privacy solutions and safeguards, organizations can mitigate privacy risks, uphold individual rights, and foster trust in data-driven systems and analytics platforms.

3. Privacy-Enhancing Technologies (PETs): A Review

Privacy-Enhancing Technologies (PETs) encompass a diverse set of cryptographic, statistical, and computational techniques designed to protect individuals' privacy while enabling effective data analysis (Jordan, ET AL., 2022; Cha, et al., 2018). In this review, we delve into several key PETs, examining their principles, mechanisms, practical implementations, applications, and challenges. Differential privacy ensures that the output of a computation or analysis does not reveal sensitive information about any individual in the dataset. It introduces noise or randomness to the data to provide plausible deniability while still allowing accurate aggregate results (Fantaye, 2022; Coopamootoo, 2020). Differential privacy can be achieved through various mechanisms such as adding noise to queries, randomizing data inputs, and implementing privacy-preserving algorithms like the Laplace mechanism or exponential mechanism. Differential privacy finds applications in various domains including data analysis, machine learning, and statistics. Case studies demonstrate its effectiveness in protecting privacy while enabling valuable insights, such as Google's use of differential privacy in Chrome's usage statistics and Apple's implementation in its iOS analytics.

Homomorphic encryption enables computations to be performed on encrypted data without decrypting it first, preserving privacy throughout the computation process (Hamza, et al., 2022; Alharbi, et al., 2020). It allows for operations such as addition and multiplication to be performed on ciphertexts, producing encrypted results. While homomorphic encryption offers strong privacy guarantees, its practical implementations often suffer from high computational overhead and performance limitations, making it less suitable for real-time or resource-constrained environments. Homomorphic encryption has been applied in scenarios where data confidentiality is paramount, such as secure cloud computing and privacy-preserving data sharing. Success stories include Microsoft's implementation of homomorphic encryption in Azure for secure data processing and collaboration (Parmar, et al., 2014).

Secure Multi-Party Computation (SMPC) allows multiple parties to jointly compute a function over their inputs while keeping those inputs private (Lindell, 2020). It ensures that no individual party learns more than what is revealed by the output of the computation. MPC protocols involve cryptographic primitives such as secret sharing, oblivious transfer, and garbled circuits. Practical implementations require careful protocol design and consideration of communication and computation overheads. Challenges in adopting SMPC include complexity, scalability, and interoperability issues. Solutions involve the development of efficient protocols, standardization efforts, and advancements in secure computation techniques (Zhao, et al., 2019; Jarin, and Eshete, 2021).

Federated Learning enables model training across decentralized devices or data sources while keeping data localized and private (AbdulRahman, et al., 2020; Yin,, et al., 2020). It involves aggregating model updates from multiple devices without centralizing data on a single server. Federated Learning operates through iterative rounds of model training and aggregation of local updates. Its advantages include privacy preservation, reduced data transfer, and improved scalability. Federated Learning has been applied in scenarios such as mobile device training and healthcare research. However, challenges such as communication overhead, data heterogeneity, and security vulnerabilities need to be addressed for broader adoption (Nguyen, et al., 2021; Beltrán,, et al., 2023).

Other PETs encompass a range of techniques including Privacy-Preserving Data Mining (PPDM) and Trusted Execution Environments (TEEs) (Danezis, et al., 2015). PPDM techniques enable data mining tasks while preserving privacy, while TEEs provide secure execution environments for sensitive computations (Almutairi, 2020). PETs differ in their approaches, strengths, and limitations. Comparative analysis helps identify the most suitable PETs for specific use cases based on factors such as privacy requirements, computational efficiency, and scalability. Emerging trends in PETs include advancements in PPDM algorithms, novel applications of TEEs in blockchain technology, and integration of PETs with AI/ML models for enhanced privacy and security.

In conclusion, PETs offer promising solutions for preserving privacy in the era of increased surveillance. Understanding their principles, mechanisms, and applications is essential for effectively implementing privacy-preserving measures while enabling valuable data analysis and collaboration (Oliveira, 2005).

4. Applications of PETs Across Domains

Privacy-Enhancing Technologies (PETs) find application across various domains, offering solutions to protect sensitive information while allowing for data utilization (Cha, et al., 2018). Here are some domains where PETs are making a significant impact; In healthcare, PETs play a crucial role in preserving patient confidentiality while enabling data sharing for research and treatment purposes. Techniques like differential privacy ensure that medical data can be analyzed without revealing individual identities, thereby safeguarding patient privacy. In the finance sector, PETs are utilized to secure financial transactions, protect sensitive customer data, and prevent fraud. Technologies like homomorphic encryption allow for secure computation on encrypted financial data, enabling analysis without exposing the underlying information. PETs are increasingly employed in social media platforms to enhance user privacy by providing features like end-to-end encryption, anonymous authentication, and secure data sharing (Yadav, and Tiwari, 2023; Kaaniche, et al., 2022). These technologies empower users to maintain control over their personal information and communications.

Governments and public sector organizations utilize PETs to protect citizen data, secure critical infrastructure, and ensure privacy compliance in public services. Techniques such as secure multi-party computation enable collaborative data analysis while preserving confidentiality (Sahinbas and Catak, 2012). PETs assist organizations in complying with data protection regulations such as GDPR, HIPAA, and CCPA by providing tools for anonymization, pseudonymization, and privacy impact assessments (Csomor, 2023; Lyons, and Fitzgerald, 2023). These technologies help mitigate legal risks associated with data processing activities. PETs contribute to addressing ethical concerns related to data privacy, surveillance, and discrimination. By implementing privacy-preserving mechanisms, organizations demonstrate a commitment to respecting individual rights and fostering trust with stakeholders (Lyons, and Fitzgerald, 2023).

5. Challenges and Barriers to PET Adoption

Many PETs incur significant computational overhead, impacting performance and scalability. Addressing this challenge requires optimizing algorithms and developing efficient implementations suitable for real-world applications.

Lack of interoperability among different PET solutions hinders their integration into existing systems and platforms. Standardization efforts are needed to ensure compatibility and seamless operation across diverse environments. Complex regulatory frameworks and evolving privacy laws pose challenges for PET adoption, as organizations must navigate legal requirements while implementing privacy-preserving measures. Clear guidelines and support from regulatory authorities are essential to facilitate compliance. The absence of standardized protocols and methodologies for PETs complicates their adoption and interoperability. Establishing industry standards and best practices can promote consistency and facilitate widespread implementation. Limited awareness among the general public about PETs and their benefits contributes to skepticism and mistrust. Educating users about privacy risks and the importance of PETs in safeguarding their data is crucial for fostering acceptance and adoption. Efforts to address these challenges are essential to realizing the full potential of PETs in protecting privacy and promoting responsible data stewardship across various domains (Namara, et al., 2020; Coopamootoo, 2020,).

6. Strategies for Overcoming Adoption Hurdles

Continued research and development efforts should focus on improving the efficiency of PET algorithms to minimize computational overhead. Optimizing algorithms for performance and scalability will make PETs more practical and attractive for real-world applications. Collaborative initiatives to establish industry standards and interoperability frameworks are crucial for promoting the seamless integration of PET solutions into existing systems (Hasani, et al., 2023). Standardized protocols will facilitate compatibility and enable organizations to leverage PETs more effectively. Engagement with policymakers and regulatory authorities is essential to advocate for supportive policies and provide guidance on privacy-enhancing measures. Clear regulatory frameworks that incentivize PET adoption and compliance will encourage organizations to prioritize privacy protection (Borking, 2009). Encouraging collaboration among industry stakeholders, including technology providers, businesses, and research institutions, can accelerate PET adoption. Partnerships enable the sharing of resources, expertise, and best practices, fostering innovation and driving the development of effective PET solutions.

Investing in education and training programs to raise awareness and enhance skills in PET implementation is critical. Educating both professionals and the general public about the benefits and importance of privacy protection will foster a culture of privacy-consciousness and promote widespread adoption of PETs.

7. Recommendation and Conclusion

Privacy-Enhancing Technologies have advanced significantly, offering solutions across various domains such as healthcare, finance, and social media. These technologies enable organizations to protect sensitive data while facilitating its secure utilization for research, transactions, and communication. It is crucial to strike a balance between data utility and privacy protection to ensure that PETs effectively safeguard individuals' rights while enabling beneficial data-driven innovations. Organizations must prioritize privacy considerations in their data handling practices to build trust and maintain compliance with regulations.

Addressing the challenges in PET adoption requires interdisciplinary collaboration among researchers, policymakers, industry stakeholders, and advocacy groups. By working together, we can develop holistic solutions that address technical, regulatory, and societal concerns, advancing the responsible use of data and technology. Looking ahead, continued research and innovation in PETs are essential to keep pace with evolving privacy threats and technological advancements. Future efforts should focus on enhancing the usability, efficiency, and scalability of PETs, as well as addressing emerging challenges in areas such as AI ethics, data governance, and digital rights.

8. Conclusion

In conclusion, Privacy-Enhancing Technologies offer promising solutions to protect privacy in an increasingly data-driven world. By overcoming adoption hurdles through collaborative efforts and strategic initiatives, we can harness the full potential of PETs to promote privacy, trust, and innovation.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] AbdulRahman, S., Tout, H., Ould-Slimane, H., Mourad, A., Talhi, C. and Guizani, M., 2020. A survey on federated learning: The journey from centralized to distributed on-site learning and beyond. *IEEE Internet of Things Journal*, *8*(7), pp.5476-5497.

[2] Aho, B. and Duffield, R., 2020. Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China. *Economy and Society*, *49*(2), pp.187-212.

[3] Alharbi, A., Zamzami, H. and Samkri, E., 2020. Survey on homomorphic encryption and address of new trend. *International Journal of Advanced Computer Science and Applications*, *11*(7).

[4] Almutairi, N.M., 2020. *Privacy Preserving Third Party Data Mining Using Cryptography*. The University of Liverpool (United Kingdom).

[5] Al-Saqaf, W., 2016. Internet censorship circumvention tools: Escaping the control of the Syrian regime. *Media and Communication*, *4*(1), pp.39-50.

[6] Andrejevic, M. and Gates, K., 2014. Big data surveillance: Introduction. *Surveillance & Society*, *12*(2), pp.185-196.

[7] Banisar, D. and Davies, S., 1999. Global trends in privacy protection: An international survey of privacy, data protection, and surveillance laws and developments. *J. Marshall J. Computer & Info. L.*, *18*, p.1.

[8] Beleuta, V., 2017. *Data privacy and security in Business Intelligence and Analytics* (Master's thesis, Universitat Politècnica de Catalunya).

[9] Beltrán, E.T.M., Pérez, M.Q., Sánchez, P.M.S., Bernal, S.L., Bovet, G., Pérez, M.G., Pérez, G.M. and Celdrán, A.H., 2023. Decentralized federated learning: Fundamentals, state of the art, frameworks, trends, and challenges. *IEEE Communications Surveys & Tutorials*.

[10] Borking, J., 2009. Organizational motives for adopting privacy enhancing technologies (PETs). In *D 7.3 PRISE Conference Proceedings:"Towards privacy enhancing security technologies–the next steps" Vienna, April 28th and 29th 2008* (p. 43).

[11] Cha, S.C., Hsu, T.Y., Xiang, Y. and Yeh, K.H., 2018. Privacy enhancing technologies in the Internet of Things: Perspectives and challenges. *IEEE Internet of Things Journal*, *6*(2), pp.2159-2187.

[12] Coopamootoo, K.P., 2020, October. Usage patterns of privacy-enhancing technologies. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1371-1390).

[13] Crampton, J.W., 2015. Collect it all: National security, big data and governance. *GeoJournal*, *80*, pp.519-531.

[14] Csomor, L.K., 2023. *Bridging the Gap between Privacy Incidents and PETs* (Master's thesis).

[15] Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.H., Metayer, D.L., Tirtea, R. and Schiffner, S., 2015. Privacy and data protection by design-from policy to engineering. *arXiv preprint arXiv:1501.03726*.

[16] Deibert, R., Palfrey, J., Rohozinski, R. and Zittrain, J., 2010. *Access controlled: The shaping of power, rights, and rule in cyberspace* (p. 634). the MIT Press.

[17] Deibert, .J., 2008. The geopolitics of internet control: Censorship, sovereignty, and cyberspace. In *Routledge handbook of Internet politics* (pp. 323-336). Routledge.

[18] Fantaye, J., 2022 An Introduction and Overview of Privacy-Enhancing Technologies for Data Processing and Analysis.

[19] Fitwi, A.H., 2021. *Privacy-Preserving Surveillance as an Edge Service* (Doctoral dissertation, State University of New York at Binghamton).

[20] Gholami, A., 2016. *Security and privacy of sensitive data in cloud computing* (Doctoral dissertation, KTH Royal Institute of Technology).

[21] Grover, P. and Kar, A.K., 2017. Big data analytics: A review on theoretical contributions and tools used in literature. *Global Journal of Flexible Systems Management*, *18*, pp.203-229.

[22] Hamza, R., Hassan, A., Ali, A., Bashir, M.B., Alqhtani, S.M., Tawfeeg, T.M. and Yousif, A., 2022. Towards secure big data analysis via fully homomorphic encryption algorithms. *Entropy*, *24*(4), p.519.

[23] Hasani, T., Rezania, D., Levallet, N., O'Reilly, N. and Mohammadi, M., 2023. Privacy enhancing technology adoption and its impact on SMEs' performance. *International Journal of Engineering Business Management*, *15*, p.18479790231172874.

[24] Ifeji, C.V. and Adeniji, O., 2023. Privacy Implications of IoT: Data Protection and Consent in a Connected World.

[25] Jarin, I. and Eshete, B., 2021, April. Pricure: privacy-preserving collaborative inference in a multi-party setting. In *Proceedings of the 2021 ACM Workshop on Security and Privacy Analytics* (pp. 25-35).

[26] Jordan, S., Fontaine, C. and Hendricks-Sturrup, R., 2022. Selecting privacy-enhancing technologies for managing health data use. *Frontiers in Public Health*, *10*, p.814163.

[27] Kaaniche, N., Laurent, M. and Belguith, S., 2022 Privacy Enhancing Technologies for solving the privacy-personalization. *title Journal of Network and Computer Applications*.

[28] Lindell, Y., 2020. Secure multiparty computation (MPC). *Cryptology ePrint Archive*.

[29] Lyon, D., 2014. Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big data & society*, *1*(2), p.2053951714541861.

[30] Lyons, V. and Fitzgerald, T., 2023. *The Privacy Leader Compass: A Comprehensive Business-Oriented Roadmap for Building and Leading Practical Privacy Programs*. CRC Press.

[31] Messinis, S., Temenos, N., Protonotarios, N.E., Rallis, I., Kalogeras, D. and Doulamis, N., 2024. Enhancing Internet of Medical Things security with artificial intelligence: A comprehensive review. *Computers in Biology and Medicine*, p.108036.

[32] Mills, J.L. and Harclerode, K., 2017. Privacy, mass intrusion, and the modern data breach. *Fla. L. Rev.*, *69*, p.771.

[33] Namara, M., Wilkinson, D., Caine, K. and Knijnenburg, B.P., 2020. Emotional and practical considerations towards the adoption and abandonment of vpns as a privacy-enhancing technology.

[34] Naranjo Rico, J.L., 2018. Holistic business approach for the protection of sensitive data: study of legal requirements and regulatory compliance at international level to define and implement data protection measures using encryption techniques.

[35] Nguyen, D.C., Ding, M., Pathirana, P.N., Seneviratne, A., Li, J. and Poor, H.V., 2021. Federated learning for internet of things: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, *23*(3), pp.1622-1658.

[36] Oliveira, S.R.D.M., 2005. Data transformation for privacy-preserving data mining.

[37] Parmar, P.V., Padhar, S.B., Patel, S.N., Bhatt, N.I. and Jhaveri, R.H., 2014. Survey of various homomorphic encryption algorithms and schemes. *International Journal of Computer Applications*, *91*(8)

[38] Rafiq, F., Awan, M.J., Yasin, A., Nobanee, H., Zain, A.M. and Bahaj, S.A., 2022. Privacy prevention of big data applications: A systematic literature review. *SAGE Open*, *12*(2), p.21582440221096445.

[39] Romanosky, S. and Acquisti, A., 2009. Privacy costs and personal data protection: Economic and legal perspectives. *Berkeley Tech. LJ*, *24*, p.1061.

[40] Sahinbas, K. and Catak, F.O., 2012. Secure Multi-party Computation-Based Privacy-Preserving Data Analysis in Healthcare IoT Systems. In *Interpretable Cognitive Internet of Things for Healthcare* (pp. 57-72). Cham: Springer International Publishing.

[41] Slobogin, C., 2008. *Privacy at risk: The new government surveillance and the Fourth Amendment*. University of Chicago Press.

[42] Vassakis, K., Petrakis, E. and Kopanakis, I., 2018. Big data analytics: Applications, prospects and challenges. *Mobile big data: A roadmap from models to technologies*, pp.3-20.

[43] Yadav, S. and Tiwari, N., 2023. Privacy preserving data sharing method for social media platforms. *PloS one*, *18*(1), p.e0280182.

[44] Yin, F., Lin, Z., Kong, Q., Xu, Y., Li, D., Theodoridis, S. and Cui, S.R., 2020. FedLoc: Federated learning framework for data-driven cooperative localization and location data processing. *IEEE Open Journal of Signal Processing*, *1*, pp.187-215.

[45] Zhao, C., Zhao, S., Zhao, M., Chen, Z., Gao, C.Z., Li, H. and Tan, Y.A., 2019. Secure multi-party computation: theory, practice and applications. *Information Sciences*, *476*, pp.357-372.

[46] Zittrain, J. and Palfrey, J., 2008. Internet filtering: The politics and mechanisms of control. *Access denied: The practice and policy of global Internet filtering*, *41*.