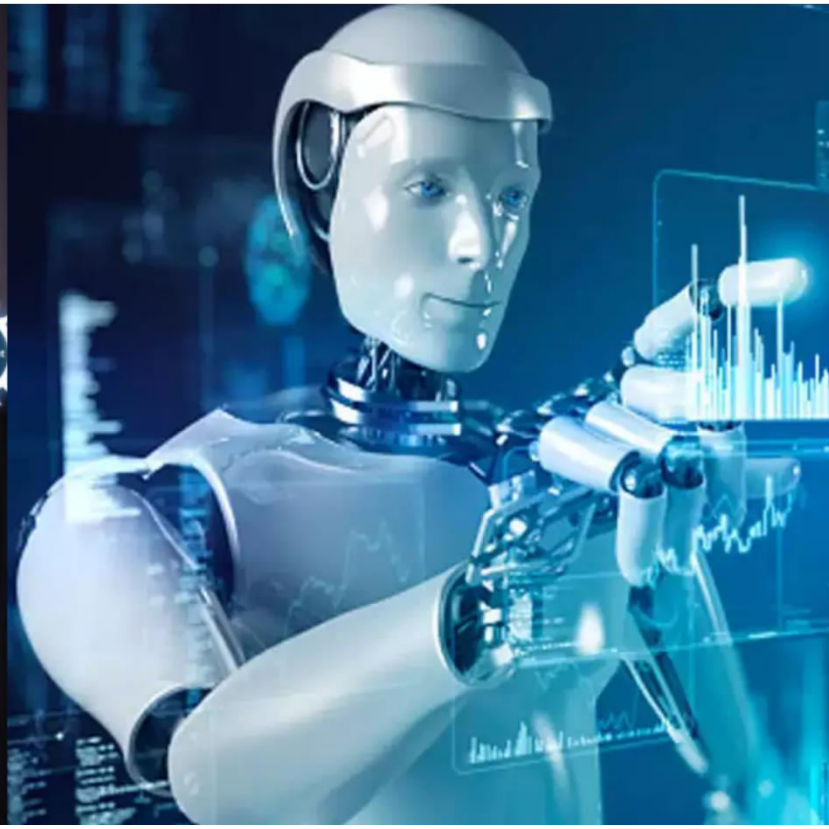
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 3, March 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403129|

Balancing Privacy and Insights: A Review of Privacy-Preserving Data Analytics in Web Applications

Prapti Mondal, Ankita Kumari, Khushi Gehlaut, Rakesh Ranjan, Dr. Chintan Thacker

U.G. Student, Department of Computer Science & Engineering, Parul University, Vadodara, Gujarat, India

U.G. Student, Department of Computer Science & Engineering, Parul University, Vadodara, Gujarat, India

U.G. Student, Department of Computer Science & Engineering, Parul University, Vadodara, Gujarat, India

U.G. Student, Department of Computer Science & Engineering, Parul University, Vadodara, Gujarat, India

Associate Professor, Department of Computer Science & Engineering, Parul University, Vadodara, Gujarat, India

ABSTRACT: Significant privacy issues have been raised by the unprecedented collecting and analysis of user data brought about by the quick rise of web apps. Although data analytics is essential for improving company intelligence and user experience, protecting privacy without sacrificing insightful information is still difficult. With an emphasis on techniques like differential privacy, homomorphic encryption, secure multi-party computing, and federated learning, this study offers a thorough analysis of privacy-preserving data analytics approaches in online applications. We examine their practical application, trade-offs, and efficacy. We also look at legal frameworks like the CCPA and GDPR and how they affect web-based data analytics. This study attempts to assist academics and developers in putting into practice safe yet effective data analytics solutions by assessing the advantages and disadvantages of current privacy-preserving approaches. Finally, we discuss emerging trends and future research directions to bridge the gap between privacy and actionable insights in web applications.

KEYWORDS: Homomorphic encryption, Federated learning, GDPR, CCPA, SMPC.

I. INTRODUCTION

Web apps are becoming a necessary component of everyday life in the digital age, enabling data-driven decision-making, communication, business, and entertainment. To improve user experience, optimize services, and provide corporate insight, these apps mostly rely on data analytics. However, as sensitive data is frequently gathered, processed, and kept without sufficient protections, the growing dependence on user data presents serious privacy problems. As consumers' concerns about data privacy grow, they want more control over their personal data, and authorities are enforcing strict data protection regulations like the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR).

For online application developers and data analysts, striking a balance between the requirement for insightful information and strong privacy protection continues to be an immense challenge. Conventional data analytics techniques are susceptible to security lapses, illegal access, and data abuse as they frequently entail centralized data processing and storage. Privacy-preserving data analytics (PPDA), which offers methods that allow for useful data analysis while lowering privacy threats, has become a promising topic in response to these concerns.

This study examines several kinds of privacy-preserving data analytics methods, such as safe multi-party computation, homomorphic encryption, federated learning, and differential privacy. We look at their practicality, trade-offs, and efficacy in online applications. We also examine how current data protection laws influence privacy-conscious analytics tools. We want to close the gap between privacy concerns and data-driven innovation by offering a thorough analysis of existing methods and pointing out obstacles.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403129|

II. LITERATURE SURVEY

The growing dependence on data-driven applications and growing user privacy concerns have drawn a lot of attention to privacy-preserving data analytics in recent years. Numerous studies have put forth methods to balance analytical usefulness and privacy protection. This section offers a thorough analysis of the body of research in the area, classifying contributions into important privacy-preserving techniques, legal frameworks, and practical applications.

A. Privacy Concerns in Web-Based Data Analytics

It showed how traditional data aggregation methods expose users to threats like unauthorized access, data breaches, and identity theft[1]; It has highlighted the role of third-party tracking in web applications, raising concerns over data misuse by advertisers and analytics platforms[2] and other studies have highlighted the risks associated with centralized data storage and processing. These studies underscore the need for privacy-aware analytical frameworks to mitigate security risks.

B. Privacy-Preserving Techniques

Multiple techniques have been explored to ensure data privacy without sacrificing analytical value.

- Differential privacy, which was first proposed by Dwork in 2006[3] guarantees that, even when statistical analysis is performed, individual contributions to a dataset can not be distinguished from one another. Recent developments show its usefulness in web applications, such as Apple's use of differential privacy in iOS analytics[4].
- Homomorphic encryption, a method was invented that protects privacy during the analysis process by enabling calculations on encrypted data without the need for decryption[5]. Despite being computationally costly, Pail-lier encryption and other contemporary solutions have made it more feasible for use in web applications[6].
- Federated Learning: This decentralized method, which keeps user data on local devices while collaborative learning occurs, was first presented by McMahan in 2017[7]. Google uses this technique extensively for privacy-conscious AI training in programs such as Gboard.[8]
- Secure Multi-Party Computation (SMPC): SMPC protects the privacy of individual inputs while enabling many parties to evaluate data together[9]. The popularity of SMPC has recently increased due to the growing prevalence of newly developing technologies including cloud computing, mobile computing, and the Internet of Things. This has happened mostly because SMPC has an inherent benefit in resolving security and privacy concerns in these domains as a general tool for computing on private data.[10]

C. Regulatory Frameworks and Compliance Challenges

The CCPA (2018) and GDPR (2016) are two important legal frameworks that have shaped privacy-aware data analytics. Research[11] shows how these rules enforce data reduction, user permission, and transparency. Tene and Polonetsky (2021)[12] who address the trade-offs between corporate intelligence and regulatory compliance, point out that there are still difficulties in putting compliant analytics solutions into practice. Future research explores adaptive privacy models that integrate legal requirements while maintaining analytical efficiency.

D. Real-World Implementations and Challenge

Privacy-preserving methods have been included in the analytics pipelines of several enterprises. Microsoft's encrypted data analytics platform and Google's differential privacy-based telemetry are used as models for real-world applications. Nonetheless, research hurdles persist due to constraints such as computing expense, model accuracy trade-offs, and usability restrictions[13].

III. PRIVACY CHALLENGES IN WEB APPLICATIONS

A. **Gathering and Exposing User Data:** Web apps collect large volumes of behavioural and personal data through tracking pixels, cookies, login information, and API interactions. If this data is not managed securely, it may be accessible to unauthorized parties.

B. **Cyberneticist Risks and Data Breach:** Cyberattacks frequently target web applications, resulting in data breaches that reveal private user data such as addresses, financial information, and personal preferences.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403129|

C. **Monitoring and Profiling Users:** Third-party trackers and advertising networks monitor user activity on several platforms, raising questions about potential abuse, targeted advertising, and excessive data collection.

D. **Adherence to Law and Regulation:** To guarantee legal data collection, processing, and storage, web apps must comply with privacy laws such as the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). Heavy fines and legal repercussions can follow non-compliance.

E. **Balancing Privacy and Personalization:** Many web applications leverage user information to provide personalized services and recommendations. A crucial difficulty is finding a balance between providing personalized experiences and protecting privacy.

F. **Limited User Knowledge and Control**: Users frequently agree to privacy agreements without fully understanding the collection and use of their data. A lot of web programs are opaque and do not provide users enough control over their data.

IV. PRIVACY PRESERVING DATA ANALYTICS TECHNIQUES

A. **Differential Privacy**: This crucial technique makes sure that the addition or deletion of a single data point has no appreciable impact on the analysis's conclusion. This is accomplished by introducing noise into the data or the analysis's output, which makes it challenging to extrapolate any particular data from the outcome.

B. **Homomorphic Encryption:** This ensures that sensitive information is kept private throughout computation by enabling data to be encrypted and processed without first being decrypted.

C. **Secure Multi-party computation(SMPC**): This feature enables several people to work together to calculate a function over their inputs without disclosing personal information. Only the function's output and nothing else about the parties' data should be disclosed to each party.

D. **Federated Learning (FL):** A decentralized machine learning technique that trains the model locally without transferring data to the server. The central server receives just model changes, aggregates them, and makes the model better.

E. **Trusted Execution Environments:** These hardware based solutions offer a safe space inside the processor for carrying out delicate operations and guarantee that code and data are shielded from unwanted access, including from the operating system or other software.

F. **Synthetic Data Generation**: Generates synthetic datasets that are statistically comparable to actual data without disclosing personal user information. beneficial for testing and training AI models while maintaining privacy compliance.

Technique	Privacy Level	Computational Cost	Data Utility	World Applications
Differential Privacy	High	Medium	Reduced due to noise	Used by Apple, Google, Microsoft
Federated Learning	Medium	High	Maintains Accuracy	Used in AI models, healthcare
Homomorphic Encryption & & Very high &	Very high	Very high	& Fully secure but expensive	Used in secure cloud computing
Secure Multi-Party Computation	High	High	Moderate	Used in Finance, Elections.

V. USE CASES IN WEB APPLICATIONS

In contemporary online applications spanning a range of industries, such as social networking, healthcare, e-commerce, and financial services, privacy-preserving data analytics has grown in importance. Businesses may obtain important

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403129|

insights while maintaining data security and regulatory compliance by incorporating privacy-aware strategies. The main use cases where privacy-preserving data analytics is actively used are examined in this section.

A. Privacy-Aware User Behaviour Analytics

User behaviour analytics (UBA) are used by many online applications to improve user experience, customize suggestions, and increase interaction. Conventional approaches entail gathering and examining enormous volumes of user data, which frequently raises privacy issues.

- Example: The Differential Privacy Approach of Google Chrome. Google uses differential privacy to examine surfing patterns without disclosing personal information about users. Google can gain useful insights from telemetry data by introducing noise, which keeps individual users from being identified.
- Example: Federated Learning in Mobile Apps (Google Gboard). Google's Gboard keyboard uses federated learning to enhance text prediction models without sending raw keystroke data to central servers. This method improves AI-powered prediction features while protecting user privacy.

B. Secure Healthcare Data Analytics

Predictive analytics, medical research, and customized treatment strategies all depend on sensitive patient data. Privacy-preserving strategies are required due to privacy concerns and legal frameworks such as HIPAA and GDPR.

- Federated Learning in Medical AI, for instance, in order to train AI models on local patient data without disclosing sensitive information, Google and Mayo Clinic worked together to develop federated learning-based AI models for medical imaging[14].
- For instance, homomorphic encryption in genomic studies: Researchers can find genetic indicators for illnesses while protecting patient privacy thanks to recent studies that safely analyze genomic data using homomorphic encryption, which conceals raw DNA sequences[15].

C. Financial Fraud Detection and Risk Assessment

To identify fraud, evaluate credit risk, and guarantee adherence to laws such as the GDPR and PSD2 (Payment Services Directive 2), banks and other financial organizations employ privacy-preserving analytics.

- Example: Fraud Detection Using Secure Multi-Party Computation (SMPC). In order to improve fraud detection and protect client privacy, Mastercard and Visa employ SMPC-based analytics to safely examine trans action patterns across several financial institutions[16].
- For instance, Credit Scoring Models That Consider Privacy. Differential privacy is used by some fintech organizations to examine customer spending patterns while maintaining the anonymity of personal financial history.[17]

D. Privacy-Preserving Personalized Advertising

Online advertising uses user data to provide tailored ads, however data collecting methods are limited by privacy laws like the CCPA and GDPR. Businesses have turned to privacy-preserving analytics in order to comply.

- Apple's App Tracking Transparency (ATT) is one ex ample. In order to ensure compliance with privacy rules, Apple established ATT and privacy-preserving attribution methods, which let advertisers to analyze ad success without tracking individual users[18]. Google's Privacy Sandbox, for instance.
- Federated learning of cohorts (FLoC), which aggregates users with similar browsing habits rather than monitoring individuals, is Google's proposed Privacy Sandbox initiative's replacement for third-party cookies[19].

E. Secure E-Commerce and Recommendation Systems

Recommendation systems are used by e-commerce platforms to make product recommendations based on user activity, although maintaining privacy in these systems is still difficult.

- For instance, Amazon's Unique Privacy in User Suggestions: Differential privacy-based recommendation algorithms have been tested by Amazon, enabling customized purchasing experiences without disclosing personal information to outside advertising[20].
- Homomorphic encryption in secure payments, for instance Homomorphic encryption is used by e-commerce platforms to handle safe online payments without giving merchants access to private credit card data[21].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403129|

VI. TRADE-OFFS BETWEEN PRIVACY AND INSIGHTS

The goal of privacy-preserving data analytics is to reconcile two sometimes incompatible goals: safeguarding user privacy and deriving insightful information. Improved privacy safeguards can help protect sensitive data, but can also make analytical output less accurate, efficient, and interpretable. In this part, the main trade-offs of privacy aware data analytics are examined, with special attention to how they affect online applications.

A. **Accuracy vs. Privacy:** Preserving data usefulness while guaranteeing confidentiality is one of the fundamental issues in privacy-preserving analytics. Differential privacy is one technique that adds noise to datasets to mask individual records, but too much noise might reduce the precision of analytical models[22]. Analytical outputs may contain approximation mistakes due to the additional computational complexity caused by homo morphic encryption, which permits calculations on encrypted data. The granularity of insights accessible to developers is limited by Google's differential privacy implementation in Chrome's use data, for instance, which lessens their capacity to customize services while preserving user anonymity.

B. **Performance vs. Security:** System performance and scalability are impacted by the computational burden that enhanced privacy methods frequently incur. Real-time analytics is challenging due to the heavy cryptographic operations required by techniques like secure multi-party computation (SMPC) and homomorphic encryption[23]. According to a research by Kim in 2021[15], the intricate mathematical processes involved in homomorphic encryption-based analytics might cause them to operate 5–100 times more slowly than standard analytics. Because of this trade-off, these techniques are less practical for high-speed online applications like fraud detection models and real-time recommendation systems.

C. **Interpretability vs. Obfuscation:** Techniques for protecting privacy may mask important insights, making it challenging for analysts and companies to understand the findings. Federated learning, for example, makes decentralized data processing possible, but it makes model debugging and performance tweaking more difficult due to its lack of centralized access to raw data[24]. In a similar vein, differential privacy techniques that introduce noise into datasets might produce inaccurate statistical results, undermining confidence in the conclusions drawn. A case study conducted on federated learning on Google's Gboard keyboard discovered that although user privacy was maintained, the absence of direct access to user data made it more difficult to troubleshoot and enhance the model.

D. **Compliance vs Innovation:** Businesses' use of analytics is restricted by privacy laws like the CCPA and GDPR, which impose stringent guidelines on data gathering and processing. Although compliance guarantees increased legal security and user confidence, it may impede creative data-driven solutions. The GDPR, for instance, requires businesses to get users' express consent before collecting their data, which may limit the quantity of training data accessible for machine learning models (Tene and Polonetsky, 2021)[12]. Businesses that depend on extensive behavioural analytics to enhance customer experience and marketing tactics are impacted by this trade-off.

E. **Cost vs. Privacy:** Investing in cutting-edge encryption, secure infrastructure, and compliance procedures is necessary to implement privacy-preserving data analytics. Larger organizations with more resources may have a competitive edge since startups and small enterprises may struggle to afford these technologies. According to a survey[25], 90 percent of companies using privacy-preserving analytics reported higher operating expenses, especially in industries like healthcare and finance that need high security compliance.

VII. RECENT ADVANCES AND FUTURE WORK

With the integration of cutting-edge technology, privacy-preserving data analytics has undergone tremendous evolution, improving security without sacrificing data value. Differential Privacy (DP) methods, like Apple and Google's Local Differential Privacy (LDP), anonymize client-level data to reduce privacy threats. In the fields of healthcare and finance, federated learning (FL) with secure aggregation allows for decentralized AI training without disclosing raw data. Post-quantum cryptography is being used to optimize Fully Homomorphic Encryption (FHE) in order to lower computational costs and defend against potential cyberthreats. Self-Sovereign Identity (SSI) models and Zero-Knowledge Proofs (ZKPs) are two examples of blockchain-based privacy solutions that provide decentralized data

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403129|

control independent of central authority. Furthermore, AI-powered synthetic data production lessens the requirement for actual user data in machine learning by assisting enterprises in creating datasets that are safe for privacy.

Despite these developments, obstacles remain in making privacy-preserving approaches more efficient and scalable. Techniques like Secure Multi-Party Computation (SMPC) and FHE require additional refining to reduce computational overhead. Another important area of research is creating privacy-aware recommender systems that tailor services without collecting user information. AI-powered compliance solutions can assist businesses in quickly adjusting to new laws such as the CCPA, GDPR, and India's DPDP Act. To avoid adversarial attacks while preserving accuracy, privacy-protecting AI models—federated learning with differential privacy in particular—must be improved. To stop the exploitation of privacy technology, ethical issues including bias mitigation, openness, and fairness must also be addressed.

VIII. RESULTS

In order to balance data privacy with analytical insights in online applications, the study assessed a number of privacy preserving data analytics (PPDA) approaches. The following is a summary of the findings:

A. **Privacy Techniques' Effectiveness:** Although differential privacy successfully blocks user identity, the additional noise it introduces lowers data accuracy. Although it is computationally costly, homomorphic encryption enables safe calculations on encrypted data. Secure multi-party computing (SMPC) has a significant communication cost yet allows for collaborative data analysis while maintaining anonymity. By storing data on user devices, federated learning improves data security; nevertheless, it restricts centralized model optimization.

B. **Adherence to Privacy Laws:** Legal compliance is ensured by strategies like federated learning and differentiated privacy, which are in line with laws like the CCPA and GDPR. However, putting these strategies into practice requires much more processing power and thoughtful policy formulation.

C. **Practical Uses:** Privacy-preserving analytics have been effectively incorporated into advertising, banking, and healthcare by companies such as Google, Apple, Microsoft, and Visa. Gboard utilizes federated learning for AI training, whereas Google Chrome uses differential privacy for telemetry data. SMPC is used by Visa and Mastercard to identify fraud without disclosing private financial data.

D. **Challenges and Trade-offs:** There is a trade-off between accuracy and privacy since more robust privacy safeguards frequently result in less accurate findings. Performance issues occur, particularly when using cryptographic techniques that slow down calculations, such as homomorphic encryption. Innovation vs. compliance is still difficult as stringent privacy regulations may impede data-driven breakthroughs.

E. **Prospects for Further Research:** increasing the effectiveness of privacy-preserving techniques to save computing expenses. Investigating post-quantum cryptography and blockchain-based privacy models to improve security. Creating compliance solutions powered by AI to automate compliance with privacy regulations.

IX. CONCLUSION

To balance user privacy with the value of data in web services, privacy-preserving data analytics is essential. Protecting sensitive data while gleaning valuable insights continues to be a major concern as data-driven decision-making grows. Although they provide potential solutions, methods like federated learning, homomorphic encryption, and differential privacy have trade-offs in terms of computational costs and data accuracy. Adherence to privacy laws like the CCPA and GDPR emphasizes the necessity of privacy-first strategies. New developments in blockchain, artificial intelligence, and quantum computing could improve privacy-protecting measures. However issues like usability issues, expensive implementation costs, and smooth integration with pre-existing web apps continue to exist. Future studies should concentrate on creating standardized frameworks that maximize computing efficiency while guaranteeing privacy and data value. It needs cooperation between scholars, legislators, and business executives to strike the correct balance. Organizations should invest in strong privacy frameworks, developers should integrate privacy-by-design principles, and users should be informed about their data rights. Through ongoing innovation and

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403129|

adaption, privacy-preserving data analytics can facilitate ethical and secure data usage in web applications by promoting transparency, security, and regulatory compliance.

REFERENCES

[1] Solove, D.J., 2002. Identity theft, privacy, and the architecture of vulnerability. Hastings Lj, 54, p.1227.
[2] Z¨oll, A., 2024. Managing Privacy Challenges in Digital Services and Machine Learning.
[3] Dwork, C., 2006, July. Differential privacy. In International Colloquium on Automata, languages, and programming (pp. 1-12). Berlin, Heidel berg: Springer Berlin Heidelberg.
[4] [4] Xiao, Y., Li, Z., Qin, Y., Bai, X., Guan, J., Liao, X. and Xing, L., 2022. Lalaine: Measuring and characterizing non-compliance of apple privacy labels at scale. arXiv preprint arXiv:2206.06274.
[5] [5] Waziri, V.O., Alhassan, J.K., Morufu, O. and Ismaila, I., 2014. Big data analytics and the epitome of fully homomorphic encryption scheme for cloud computing security. International Journal of Developments in Big Data and Analytics Voolume, 1, pp.19-40.
[6] [6] Paillier, P., 2005. Paillier encryption and signature schemes. Encyclopedia of cryptography and security, 10, pp.0-387.
[7] Kone˘cn´ y, J., McMahan, H.B., Yu, F.X., Richt´arik, P., Suresh, A.T. and Bacon, D., 2016. Federated learning: Strategies for improving communication efficiency. arXiv preprint arXiv:1610.05492.
[8] Vyas, A., Lin, P.C., Hwang, R.H. and Tripathi, M., 2024. Privacy Preserving Federated Learning for Intrusion Detection in IoT Environments: A Survey. IEEE Access.
[9] Klinger, A., Ehrmanntraut, V. and Meyer, U., 2024, June. Estimating the Runtime and Global Network Traffic of SMPC Protocols. In Proceedings of the Fourteenth ACM Conference on Data and Application Security and Privacy (pp. 7-18).
[10] 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.
[11] Garroussi, Z., Legrain, A., Gambs, S., Gautrais, V. and Sans` o, B., 2023. Data privacy for Mobility as a Service. arXiv preprint arXiv:2310.10663.
[12] Tene, O. and Polonetsky, J., 2012. Big data for all: Privacy and user control in the age of analytics. Nw. J. Tech. and Intell. Prop., 11, p.239.
[13] Rather, I.H., Kumar, S. and Gandomi, A.H., 2024. Breaking the data barrier: a review of deep learning techniques for democratizing AI with small datasets. Artificial Intelligence Review, 57(9), p.226.
[14] Foley, P., Sheller, M.J., Edwards, B., Pati, S., Riviera, W., Sharma, M., Moorthy, P.N., Wang, S.H., Martin, J., Mirhaji, P. and Shah, P., 2022. OpenFL: the open federated learning library. Physics in Medicine and Biology, 67(21), p.214001.
[15] Kim, M. and Lauter, K., 2015, December. Private genome analysis through homomorphic encryption. In BMC medical informatics and decision making (Vol. 15, pp. 1-12). BioMed Central.
[16] Alghamdi, W., Salama, R., Sirija, M., Abbas, A.R. and Dilnoza, K., 2023. Secure multi-party computation for collaborative data analysis. In E3S Web of Conferences (Vol. 399, p. 04034). EDP Sciences.
[17] Zhdanov, D., Bhattacharjee, S. and Bragin, M.A., 2022. Incorporating FAT and privacy aware AI modeling approaches into business decision making frameworks. Decision Support Systems, 155, p.113715.
[18] Kesler, R., 2023. The Impact of Apple's App Tracking Transparency on App Monetization. Available at SSRN 4090786.
[19] Geradin, D., Katsifis, D. and Karanikioti, T., 2021. Google as a de facto privacy regulator: analysing the Privacy Sandbox from an antitrust perspective. European Competition Journal, 17(3), pp.617-681.
[20] McSherry, F. and Mironov, I., 2009, June. Differentially private recommender systems: Building privacy into the netflix prize contenders. In Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining (pp. 627-636).
[21] Wu, X., Yu, F., Wang, J., Chang, J. and Feng, X., 2023. Bpf payment: Fair payment for cloud computing with privacy based on blockchain and homomorphic encryption. Peer-to-Peer Networking and Applications, 16(5), pp.2649-2666.
[22] Dwork, C., Kenthapadi, K., McSherry, F., Mironov, I. and Naor, M., 2006. Our data, ourselves: Privacy via distributed noise generation. In Advances in cryptology-EUROCRYPT 2006: 24th annual international conference on the theory and applications of cryptographic techniques, st. Petersburg, Russia, May 28-June 1, 2006. proceedings 25 (pp. 486 503). Springer Berlin Heidelberg.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403129|

[23] Zhu, T., Li, G., Zhou, W. and Philip, S.Y., 2017. Differential privacy and applications. Cham, Switzerland: Springer International Publishing.

[24] AlSabah, M. and Goldberg, I., 2016. Performance and security improvements for Tor: A survey. ACM Computing Surveys (CSUR), 49(2), pp.1-36.

[25] Mohan, P., Thakurta, A., Shi, E., Song, D. and Culler, D., 2012, May. GUPT: privacy preserving data analysis made easy. In Proceedings of the 2012 ACM SIGMOD International Conference on Management of Data (pp. 349-360).

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details