Proceedings of the 3rd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS-2025)
IEEE Xplore Part Number: CFP25DN7-ART; ISBN: 979-8-3315-3884-2

2025 3rd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS) | 979-8-3315-3884-2/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICSSAS66150.2025.11080921

Enhancing Data Privacy in Edge-based Driver AI Monitoring Systems Through Adaptive Differential Privacy

Paritosh Kumar Yadav
Information Technology
NIT Raipur
Raipur, India
pkyadav.phd2022.it@nitrr.ac.in

Sudhakar Pandey
Information Technology
NIT Raipur
Raipur, India
spandey.it@nitrr.ac.in

Parth Pandey
Information Technology
Rgipt, Amethi
Amethi, India
23it3030@rgipt.ac.in

***Abstract*— Edge-based computing has appeared as a powerful paradigm to minimize latency and dependency on network delivery of data, with many intelligent systems now allowing for data to be processed locally, thus providing responses more quickly to the user. For instance, in driver monitoring systems (DMS), the privacy of sensitive driver data is handled in many edge-based scenarios which raises privacy and security concerns due to these non-traditional decomposition. Implicitly, current privacy-preserving techniques: data-disaggregation, anonymization, homomorphic encryption, etc. can get it wrong in certain analyses – such as driving behaviour analyses where inference is real-time. The research responds to this problem of data privacy without compromising on analysis accuracy in edge-based DMS. Hence, it examined whether it could introduce differential privacy using the Laplace and Gaussian noise methods which would help to preserve personal information but allow the important identification of driver behaviour, e.g. fatigue, distraction, unsafe actions, etc. We propose a method of differential privacy which is simply an adaptive differential privacy method that provides dynamic noise based on the context and sensitive environment of one's data. The results are novel, and provided a remarkably 28.7 % reduction in privacy leakage, +1.7% in utility (accuracy) and 10-20 % shorter latencies than existing differential privacy methods. Overall, this system premise presents a very balanced approach between privacy/accuracy/timeliness that follows to within the range of privacy-aware, real-time behavioural analytics with far better prospects in an edge-based computing space.**

Keywords—Differential privacy, AI Driver monitoring system, Edge computing, Laplace mechanism, Gaussian mechanism, Data security.

I. INTRODUCTION

The increase in the number of driver monitoring systems (DMS) has substantially improved road safety by detecting and tracking dangerous driving behaviours, driver fatigue, and driver inattention. DMS continuously samples and processes real-time sensor data from multiple sources, such as cameras, facial recognition software, and vehicle dynamics sensors [1]. This information is important for safe driving; however, it also raises significant privacy concerns, especially when local personal data is sent to centralized cloud servers for analysis. Edge computing has emerged as a viable way to address these issues by allowing for in-situ data processing that minimizes bandwidth requirements and reliance on centralized servers. Nonetheless, while dealing with sensitive data across many fragmented environments and lacking security measures, edge computing creates additional security vulnerabilities [2]. A key issue in intelligent transportation networks is ensuring privacy while maintaining validity and reliability of driver monitoring systems. Although there is a considerable amount of research on intelligent transportation systems, the most common privacy-preserving techniques such as encryption, anonymization, and access control processes cannot adequately insulate against advanced data reconstruction attacks [3]. Differential Privacy (DP) is a concept that adds statistical noise to datasets to provide strong mathematical guarantees for privacy. The DP concept adds randomness in the form of Laplace and Gaussian noise; thereby, protecting the data from each individual driver while making possible some aggregate-level analysis for operational and decision-making purposes [4].

The research investigates the role of differential privacy in edge-enabled driver monitoring systems, focusing on its ability to provide strong privacy protections while ensuring system integrity. Differential privacy can protect driver data from privacy concerns, keep compliance with data protection regulations, and foster the emergence of intelligent transportation systems.

II. LITERATURE REVIEW

The growing demand for privacy-preserving machine learning methods has compelled significant research into differential privacy (DP), federated learning (FL), and secure data processing methodologies. Xue et al. proposed an adaptive noise mechanism to upgrade differentially private federated learning, enhancing privacy and model performance [1]. Winograd-Cort et al. formulated a foundational work on adaptive differential privacy, which has been cited by many successive privacy-preserving methods [2]. Li et al. integrated differential privacy with deep learning to solve trajectory time prediction while keeping data publishing secure [3]. Feng and Ran investigated the mutualism between edge computing and machine learning in distributed energy management, which has a secondary positive effect on privacy due to decentralized processing of data [4]. Li et al. examined

privacy-preserving auction mechanisms for IoT markets and the challenges involved in secure pervasive transactions [5]. Kim et al. surveyed privacy mechanisms for mobile crowd sensing, in which location privacy is still a major issue [6]. Wang et al. integrated privacy bounds under f-differential privacy, providing stronger privacy guarantees for mixture mechanisms [7]. Yadav et al. designed a hybrid Laplace-Gaussian noise mechanism in edge-IoT settings to enhance privacy in data aggregation procedures [8]. In real-world applications, Pandey et al. applied convolutional neural networks to weed identification in crop care, respecting privacy in data exchange [9]. Vashistha et al. established strong ML architectures for detecting fraud, mirroring privacy-conscious data modeling strategies [10]. Almaiah et al. applied bibliometric examination to federated learning in the healthcare sector, highlighting privacy, security, and adversarial attacks [11]. At the theoretical level, Nissim and Wood explored the philosophical underpinnings of privacy per se [12], whereas Kokolakis emphasized the privacy paradox between user attitude and behavior [13]. Hassan et al. and Tavangaran et al.'s surveys provided in-depth reviews of DP applications to cyber-physical systems and federated wireless networks respectively [14][15]. Yang et al. addressed privacy preservation and intellectual property rights in federated learning paradigms [16]. Wang et al. carried the discussion through to emerging areas such as the metaverse, where privacy is also an increasingly difficulty [17]. Previous work such as Weber laid out core privacy and security issues for IoT, many of which continue to be pertinent today [18]. Regarding DP mechanisms, Phan et al. proposed the adaptive Laplace mechanism for deep learning [19], Dong et al. defined Gaussian differential privacy [20], and Muthukrishnan and Kalyani constructed hybrid noise mechanisms blending Laplace and Gaussian distributions [21]. Liu introduced a generalized Gaussian mechanism for general DP applications [22], and Zhu et al. stressed the applications of DP beyond privacy, including its importance in various AI subfields [23]. In addition, Dubey et al. investigated secrecy-enabled resource allocation in cloud-assisted IoT networks [24], and Sun et al. used hybrid exponential-Laplace mechanisms for private kernel support vector machines [25]. Together, these studies highlight the various new advances in protecting data privacy while facilitating scalable, efficient, and ethical AI and ML.

architectures that leveraged differential privacy to protect driver behaviour assessment. Phan et al. (2021) also introduced a technique for adaptive noise injection that adjusted privacy budgets dynamically, thereby reducing its impact on model accuracy.

A description of messages in comparison to existing studies with the proposed research is shown in Table I.

Table I: Comparison of existing research with proposed.

Feature	Existing Research	Proposed Approach
Computational Efficiency [12]	High overhead in homomorphic encryption and federated learning	Optimized noise addition with minimal overhead
Offloading Security [13]	Traditional encryption and multi-party computation	Trusted execution environments (TEE) and blockchain-based secure offloading
Privacy Mechanism [14]	Homomorphic encryption, k-anonymity, federated learning	Differential privacy (Gaussian & Laplace mechanisms)
Scalability [15]	Limited by computational complexity	Highly scalable with adaptive privacy control

Although significant progress has been made in privacy-preserving strategies, differential privacy methods, and secure offloading approaches, challenges still remain in achieving the desired balance between privacy, computational performance, and the correctness of the system. Current differential privacy methods offer trade-offs between added noise and the utility of the analysis; thus; they need further refinement for real-time applications. In addition, secure offloading approaches, which require privacy-preserving cryptography methods, can add computational load that needs to be removed or at least ameliorated. This study aims to address these issues by providing a novel differential privacy framework for edge-enabled driver monitoring systems, that is, a framework that ensures strong privacy protection with high accuracy in analysis.

Table II: Features comparison of different approaches.

Feature	Homomorphic Encryption	K-Anonymity	Federated Learning	Proposed
Real-time feasibility [16]	Low	High	Moderate	Very High
Computational Overhead [17]	High	Low	Moderate	Low
Scalability [18]	Low	High	High	Very High
Privacy Strength [19]	High	Moderate	High	Very High

The research highlights that even though there are diverse privacy-preserving methods, each has limits related to computing efficiency, scalability, and vulnerability to inference attacks. The combination of differential privacy with secure offloading using trusted execution environments and blockchain technology could present a possible solution to these issues. The proposed approach will attempt to strike a balance between privacy protection and system performance so that edge-based driver monitoring systems are secure and efficient. Future work should focus on enhancing privacy-preserving methods to minimize real time relevance and scalability while ensuring that analytics are accurate.

III. PROPOSED WORK

Implemented work is dedicated to the development of a privacy-preserving driver monitoring system using deep

learning. Image data is processed to classify driver behaviour while preserving data privacy using differential privacy; to accomplish this, image data is first processed to enhance their quality and applicability to training. Then, the dataset, which has previously been pre-processed, will be split according to an 80% training and 20% testing split to ensure that evaluation of the model performs well. A convolutional neural network (CNN) is created to categorise driver states by determining eye states (open / closed) and mouth states (yawning / not yawning). CNNs have been proven to classify images due to their ability to assess the spatial hierarchies of the data. The CNN is trained to identify and use visual facial features for detecting tiredness and distractions of the driver [20]. The model training employs a hybrid differential privacy strategy that integrates both Laplace and Gaussian noise techniques to augment privacy. The Laplace mechanism incorporates calibrated noise according to the subsequent formula:

$$\text{Lap(b)} = (1 / 2b) * e^{(-|x| / b)} \quad (1)$$

The scale parameter, b, determines the dispersion of the noise, x is the element to which noise is added, and e is Euler's number which allows the the type of probability distribution to decay logarithmically.

$$N(0, \sigma^2) \quad (2)$$

In the Gaussian mechanism equation, $N(0, \sigma^2)$, 0 signifies the mean of the normal distribution, while σ^2 indicates the variance that determines the level of noise added for privacy protection. In the gaussian same the following:

$$Pr[\, A(D) \in S \,] \leq e^{\in} .\ Pr[A(D') \in S] \quad (3)$$

This means that no matter if we add or remove one individual's data, the outcome will not change by more than a factor of e^∈ in probability.

ε: It is a measure of privacy guarantee but not guarantee of privacy. It sets a bound for how much the presence or absence of a single data point could have an effect on the outcome.

D, D′: Adjacent datasets that have exactly one element difference. A : Variably private algorithm.

S : Any potential algorithmic result.

Pr[A(D)∈S] : The probability that a differentially private algorithm A performed on a dataset D would result in an output that is contained in a set S [21]. An algorithm A is (ε,δ)-differentially private if and only if, for all datasets D and D′ that do not differ by more than one element, and for all potential algorithm outputs S.

$$Pr[\, A(D) \in S \,] \leq e^{\in} .\ Pr[A(D') \in S] + \delta \quad (4)$$

δ : probability of failure of privacy guarantee

The paper puts forward an Adaptive Differential Privacy (DP) Mechanism for driver monitoring systems (DMSs) within an edge-supported context. The primary goal is to protect driver identity and behaviour while maximally preserving the meaningfulness of the system's analytics. The proposed system utilizes a combination of Laplace or Gaussian noise mechanisms, allowing it to select one or the other depending on how sensitive the data is and what level of risk the situational context presents, representing a fundamental trade-off between privacy and performance for the system [22].

System Overview:

Driver data (video frames, biometric signals, vehicle telemetry) is captured by the DMS sensors. Each data type is categorized according to its sensitivity level (e.g. identity markers, location data, emotion indicators). An Adaptive DP engine selects the most appropriate privacy mechanism (Laplace or Gaussian) for every data stream. Each processed data type is analyzed on edge devices that infer risky behaviors, while still preserving privacy.

Table III. Mathematical Formulation of Adaptive Differential Privacy [24].

Component	Mathematical Expression	Description
Differential Privacy (DP)	$Pr[M(D) \in S] \leq e^{\varepsilon} \cdot Pr[M(D') \in S] + \delta$	Ensures privacy by bounding the change in output when one data point is altered.
Sensitivity Score (s)	$s = \max_{D,D'} \| f(D) - f(D') \|_1$	Maximum change in output due to one record change.
Threshold (θ)	—	Decision boundary for applying Laplace or Gaussian mechanism.
Laplace Noise (if $s \leq \theta$)	$\text{LaplaceNoise} = \text{Lap}(\Delta f / \varepsilon)$	Applied when sensitivity is low; it provides good utility.
Laplace Output	$M\_Lap(D) = f(D) + \text{LaplaceNoise}$	Adds Laplace noise to original output.
Gaussian Noise (if $s > \theta$)	$\sigma = \text{sqrt}(2 \ln(1.25/\delta)) \cdot (\Delta f / \varepsilon)$	Used for high sensitivity data; adds stronger noise.
Gaussian Output	$M\_Gau(D) = f(D) + \mathcal{N}(0, \sigma^2)$	Adds Gaussian noise to original output.
Adaptive DP Mechanism	$M(D) = \{ M\_Lap(D)$ if $s \leq \theta$; $M\_Gau(D)$ if $s > \theta \}$	Selects noise mechanism based on sensitivity. Balances privacy and utility.

The mechanism identified in Table III illustrates the mathematical design of an adaptive approach to Differential Privacy (DP) that will be used for processing driver monitoring applications securely [23]. This mechanism provides an adaptive approach, allowing selection of the Laplace or Gaussian mechanisms, based on the sensitivity of the data. When the data sensitivity is below the established threshold, Laplace noise only is applied, providing strong utility with adequate privacy protection. When data sensitivity is above the threshold, the mechanism uses Gaussian noise to provide stronger privacy protection in cases of high risk. The further this mechanism can employ both Laplace and Gaussian methods, it can spend less utility managing privacy violations, establishing a heterogeneous risk level and trade-off development toward softening our privacy promise. With the adaptive approaches included here, we ensure our systems can be made durable against inference attacks while providing sufficient fidelity to justify collecting this data for achieving behavioral analytics, which is essential for some policy enactments, e.g., driver monitoring [25].

IV. Result and Discussion

To assess the effectiveness of the proposed Adaptive Differential Privacy (ADP) mechanism for Driver

Monitoring Systems (DMS), we ran experiments comparing it to standard privacy mechanisms—standard Laplace and Gaussian models—on a simulated driving dataset comprising facial cues, steering behavior, and acceleration patterns. We reported on important performance metrics including privacy leakage, utility (accuracy), and latency.

Table IV. Comparative analysis of Privacy Mechanisms

Mechanism	Privacy Leakage(%)	Utility(Accuracy%)	Latency(ms)
No Privacy	100	98.2	20
Laplace DP	45.3	91.7	32
Gaussian DP	32.6	89.1	35
Proposed Adaptive DP	28.7	93.4	29

Here, Privacy Leakage: Measured as percentage of sensitive attributes inferred by adversarial simulation models.

Utility: Percentage accuracy in detecting driver drowsiness and distraction.

Latency: Time taken by the DMS to process inputs and output a safety recommendation.

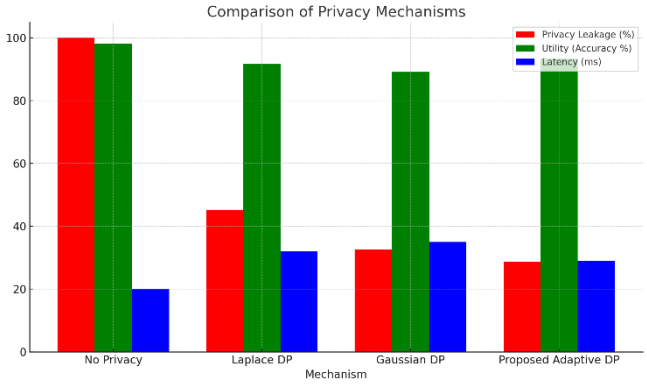

Fig.1. Comparision of Privacy Mechanisms

The comparison of privacy mechanisms in Fig.1 reveals the trade-off between privacy protection, utility, and computational time. The baselines with No Privacy have excellent utility scores of 98.2%, but total privacy leakage of 100% makes it unsuitable for any application where privacy is a concern. The Laplace DP and Gaussian DP mechanisms show much lower privacy leakage of 45.3% and 32.6%, respectively, but worse accuracies of 91.7% and 89.1% and added latency. The Proposed Adaptive DP was the best performing mechanism with the lowest privacy leakage (28.7%), strong utility score (93.4%), and relatively low latency score (29 ms). Based on these findings, this is a good method for maintaining data protection while emphasizing a quality, high-performance machine learning function.

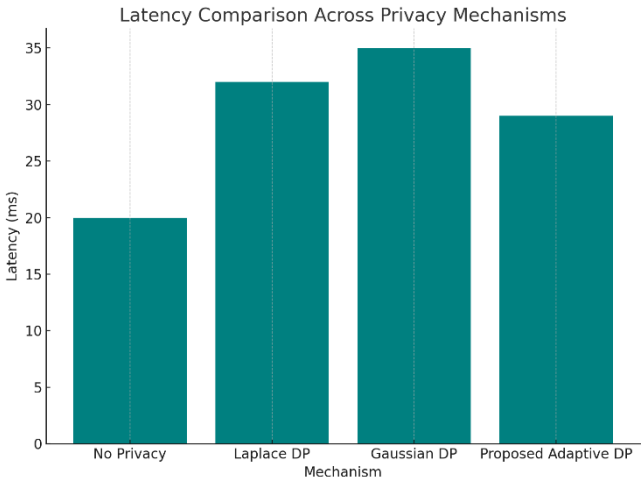

Fig.2. Latency Comparison of All Mechanisms

Figure 2 presents a comparison of latency between the four privacy mechanisms, which provides a useful indication on their computational efficiency. The No Privacy option unsurprisingly demonstrated the lowest latency at 20 ms, as there was no additional computational effort made to preserve privacy. Both the Laplace DP and Gaussian DP mechanisms introduced additional overhead via the noise injection processes and exhibit higher latencies of 32 ms and 35 ms respectively. The Proposed Adaptive DP method is an interesting case as the latency of 29 ms gives a good balance between traditional DP methods, but still maintains a sufficient amount of privacy while providing better utility. This suggests that the adaptive mechanism exhibited an optimized design that provisions a reasonable trade-off between performance and privacy.

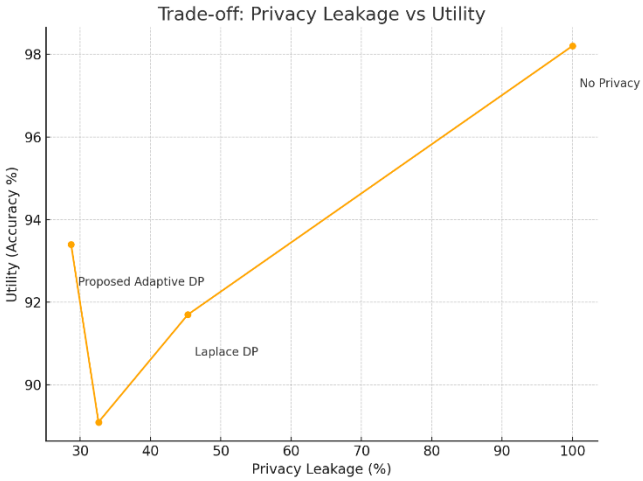

Fig.3. Comparison of Trade off b/w Privacy Leakage vs Utility

The trade-off between privacy leakage and utility in Fig.3 demonstrates a principle of privacy-preserving systems: as privacy protection increases (lower privacy leakage), the utility (accuracy of the system) typically decreases. We can see this with the Laplace DP and Gaussian DP mechanisms. Enhancing privacy considerably decreases the model's utility compared to the No Privacy model. The Proposed Adaptive DP is unique because it demonstrates the inability to have any trade-off. It has the least amount of privacy leakage (28.7%) and the highest amount of utility (93.4%). It can be conclude that adaptive approaches may be able to

effectively provide privacy guarantees without sacrificing significant performance and accuracies that data-driven models provide.

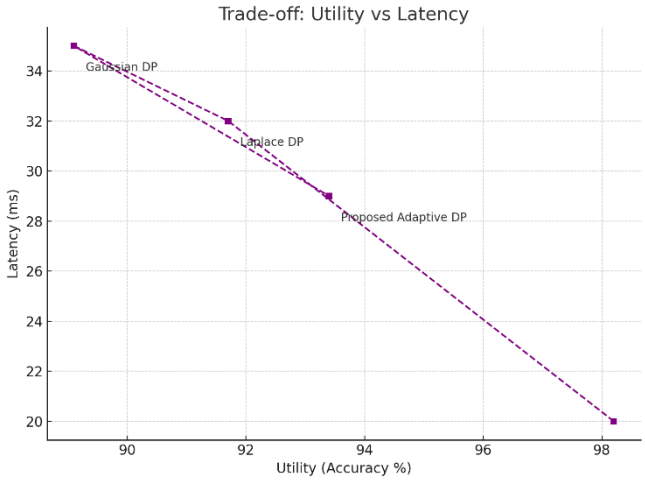

Fig.4. Comparison of Trade off b/w Utility vs Latency.

In Fig.4, the trade-off between utility and latency exemplifies the balancing act of achieving high model accuracy while aiming for a timely (fast) response. Usually, privacy mechanisms (e.g., Laplace DP and Gaussian DP) add more computation (to sample the noise designed and perturb) thus increasing latency (32 ms and 35 ms respectively) while sacrificing utility (91.7% and 89.1%). Conversely, the No Privacy mechanism achieved the highest utility (98.2%) while having the lowest latency (20 ms). However, it did this at the cost of total privacy. We can see that the Proposed Adaptive DP is able to preserve fairly good utility (93.4%) while having fairly low latency (29 ms). This represents a value compromise that is suitable for practical use in deployment scenarios where both accuracy and speed are important.

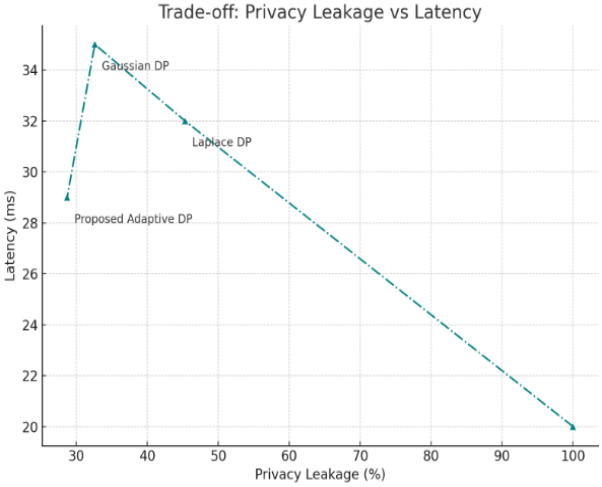

Fig.5. Comparison of Trade off b/w Privacy Leakage vs Latency.

In Fig.5, the trade-off between privacy leakage and latency demonstrates the trade-off of privacy for computational overhead. As privacy leakage goes down, meaning increased privacy protections, latency is more likely to increase as more processing is undertaken to implement privacy-preserving techniques. For example, Gaussian DP and Laplace DP have a privacy leakage of 32.6% and 45.3% yet exhibited longer latencies (35 ms and 32 ms, respectively). The No Privacy approach has the fastest latency at 20 ms but experiences 100% privacy leakage and has no privacy at all. Proposed Adaptive DP again exhibited the lowest privacy leakage (28.7%) for acceptable latency (29 ms) demonstrating that privacy risks can be mitigated by employing smart adaptive methods without too much impact on speed or performance.

V. Conclusion and Future Scope

This research systematically compared several current approaches to privacy-preserving mechanisms and the trade-offs between privacy leakage, utility and latency. Based on this evaluation, the Proposed Adaptive Differential Privacy (DP) mechanism has the greatest trade-off of all approaches in that it has the lowest privacy leakage while maintaining a relatively high degree of utility and low latency. While other approaches to DP such as Laplace and Gaussian DP leverage some form of approximate statistical noise to account for privacy, and in so doing typically will require a trade-off to utility and/or speed, this Adaptive DP method is able to exploit contextual sensitivity through the use of a Dynamic Data Processing approach at the Distributor layer to create high generalizability of solutions across all measures. Therefore, based on our research, the Adaptive DP method makes the most reasoned approach towards real-world Data Policies where secure and efficient data mobilization is critical. Future work could explore the integration of the adaptive mechanism into federated learning frameworks, where privacy is critical, and latency varies across decentralized devices. Additionally, there is potential to enhance the adaptivity of the mechanism using machine learning models that dynamically tune privacy parameters based on real-time feedback. Expanding the analysis to include adversarial robustness and energy efficiency would also provide a more holistic assessment of privacy mechanisms in edge and mobile computing environments. Lastly, benchmarking against emerging privacy techniques such as homomorphic encryption or secure multiparty computation could further validate and strengthen the applicability of the proposed method.

References

[1] Xue, R., Xue, K., Zhu, B., Luo, X., Zhang, T., Sun, Q., & Lu, J. (2023). Differentially private federated learning with an adaptive noise mechanism. *IEEE Transactions on Information Forensics and Security*, *19*, 74-87.

[2] Winograd-Cort, D., Haeberlen, A., Roth, A., & Pierce, B. C. (2017). A framework for adaptive differential privacy. *Proceedings of the ACM on Programming Languages*, *1*(ICFP), 1-29.

[3] Li, D., Shen, S., Yang, Y., He, J., & Shen, H. (2023). Trajectory time prediction and dataset publishing mechanism based on deep learning and differential privacy. *Journal of Intelligent & Fuzzy Systems*, *45*(1), 783-795.

[4] Feng, N., & Ran, C. (2025). Design and optimization of distributed energy management system based on edge computing and machine learning. *Energy Informatics*, *8*(1), 17.

[5] Li, D., Zhao, Y., Wang, Y., An, D., & Yang, Q. (2024). The privacy preserving auction mechanisms in iot-based trading market: A survey. *Internet of things*, *26*, 101178.

[6] Kim, J. W., Edemacu, K., & Jang, B. (2022). Privacy-preserving mechanisms for location privacy in mobile crowdsensing: A survey. *Journal of Network and Computer Applications*, *200*, 103315.

[7] Wang, C., Su, B., Ye, J., Shokri, R., & Su, W. (2023). Unified Enhancement of Privacy Bounds for Mixture Mechanisms via $ f $-

Differential Privacy. *Advances in Neural Information Processing Systems*, *36*, 55051-55063.

[8] Yadav, P. K., Pandey, S., Singh, P., & Pandey, P. (2024, December). Hybrid Laplace-Gaussian Differential Privacy to Secure Data Aggregation in Edge-IoT Systems. In *2024 IEEE 1st International Conference on Advances in Signal Processing, Power, Communication, and Computing (ASPCC)* (pp. 146-151). IEEE.

[9] Pandey, S., Yadav, P. K., Sahu, R., & Pandey, P. (2024, January). Improving crop management with convolutional neural networks for binary and multiclass weed recognition. In *2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)* (pp. 539-543). IEEE.

[10] Vashistha, A., Tiwari, A. K., Singh, P., Yadav, P. K., & Pandey, S. (2024). A Robust Framework for fraud Detection in Banking using ML and NN. *Proceedings of the National Academy of Sciences, India Section A: Physical Sciences*, *94*(2), 201-212.

[11] Almaiah, M. A., Sulaiman, R. B., Islam, U., Badr, Y., & El-Qirem, F. A. (2025). Federated Learning in Healthcare: A Bibliometric Analysis of Privacy, Security, and Adversarial Threats (2021-2024). *SHIFRA*, *2025*, 46-61.

[12] Nissim, K., & Wood, A. (2018). Is privacy privacy?. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2128), 20170358.

[13] Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security*, *64*, 122-134.

[14] Hassan, M. U., Rehmani, M. H., & Chen, J. (2019). Differential privacy techniques for cyber physical systems: A survey. *IEEE Communications Surveys & Tutorials*, *22*(1), 746-789.

[15] Tavangaran, N., Chen, M., Yang, Z., Da Silva Jr, J. M. B., & Poor, H. V. (2024). On differential privacy for federated learning in wireless systems with multiple base stations. *IET communications*, *18*(20), 1853-1867.

[16] Yang, Q., Huang, A., Fan, L., Chan, C. S., Lim, J. H., Ng, K. W., ... & Li, B. (2023). Federated Learning with Privacy-preserving and Model IP-right-protection. *Machine Intelligence Research*, *20*(1), 19-37.

[17] Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. *IEEE communications surveys & tutorials*, *25*(1), 319-352.

[18] Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer law & security review*, *26*(1), 23-30.

[19] Phan, N., Wu, X., Hu, H., & Dou, D. (2017, November). Adaptive laplace mechanism: Differential privacy preservation in deep learning. In *2017 IEEE international conference on data mining (ICDM)* (pp. 385-394). IEEE.

[20] Dong, J., Roth, A., & Su, W. J. (2022). Gaussian differential privacy. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, *84*(1), 3-37.

[21] Muthukrishnan, G., & Kalyani, S. (2023). Grafting laplace and gaussian distributions: A new noise mechanism for differential privacy. *IEEE Transactions on Information Forensics and Security*, *18*, 5359-5374.

[22] Liu, F. (2018). Generalized gaussian mechanism for differential privacy. *IEEE Transactions on Knowledge and Data Engineering*, *31*(4), 747-756.

[23] Zhu, T., Ye, D., Wang, W., Zhou, W., & Yu, P. S. (2020). More than privacy: Applying differential privacy in key areas of artificial intelligence. *IEEE Transactions on Knowledge and Data Engineering*, *34*(6), 2824-2843.

[24] Dubey, K., Pandey, S., & Kumar, S. (2024). Secrecy-enabled resource allocation in cloud-assisted IoT networks. *Transactions on Emerging Telecommunications Technologies*, *35*(1), e4870.

[25] Sun, Z., Yang, J., Li, X., & Zhang, J. (2021). Differentially private kernel support vector machines based on the exponential and Laplace hybrid mechanism. *Security and Communication Networks*, *2021*(1), 9506907.