International Journal in IT & Engineering (IJITE)
Volume 12 Issue 03, March 2024 ISSN: 2321-1776 Impact Factor: 8.341
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

Privacy-Preserving AI Models in ERP Systems for Governmental Resource Planning and Citizen Data Management

Chandrasekhar Atakari
Principal Architect :Paloalto Networks, California, USA

Abstract: ERP systems have gained importance in governmental organizations to facilitate management of resources, citizen information and the services to be offered to them. Nevertheless, with the growing adoption of Artificial Intelligence (AI) in ERP systems, there are serious privacy questions because government and citizen data are highly sensitive. The privacy preserving framework of AI model in ERP systems which has been proposed in this paper will be able to ensure data privacy and integrity of these applications and meet the stipulations of privacy regulations. Approaches discussed in the study include federated learning, homomorphic encryption, differential privacy, and secure multi-party computation that can both protect the privacy of citizen information and provide sufficient data to support effective resource planning. In the research, a combined approach including mathematical modeling, privacy mechanisms based on encryption, and simulated performance using governmental enterprise resource planning scenarios is used. Findings suggest that the suggested model can attain a data privacy compliance of up to 96%, 18 percent on the reduction of the amount of computation involved and enhance the trustworthiness of AI in the ERP solutions. The article gives a comprehensive review of the literature, methodology, performance metrics, and comparative study with the conventional ERP-AI models. Also, recommendations and future challenges to implement privacy-preserving AI in governmental ERP systems are shared.

Keywords: Privacy-preserving AI, ERP Systems, Government Data Security, Federated Learning, Homomorphic Encryption, Citizen Data Management, Resource Planning.

1. Introduction

ERP systems have evolved beyond the transactional applications and have become AI-empowered platforms that are able to automate government activities and enhance the services to the citizens. New ERP tools do not stop at keeping records; the modern solutions utilize sophisticated analytics, machine learning, and predictive modelling tools to optimise resource allocation, help predict public service demand, and assist in making data-driven policy decisions. [1-3] This set of capabilities driven by the intelligence of AI help governments streamline their operations and save money whilst ensuring they provide reactionary services to citizens. This integration has however seen the emergence of a major problem; the protection of sensitive and confidential data of citizens and the government against privacy attacks and illegal access. ERP systems may contain large quantities of PII, financial records and other information that is legally, ethically and/or socially sensitive; any security breach may have dire consequences. As

such, frameworks that can effectively and securely integrate AI into ERP systems provide an increasingly important role and ensure that governments have a viable option to deploy intelligent systems without undermining the security of their data or otherwise compromising their citizens.

1.1. Needs of Privacy-Preserving AI Models in ERP Systems

- Protection of Sensitive Data: Governmental ERP systems are dealing with very sensitive data, which are the identities of citizens, financial and healthcare data, as well as confidential policy documentation. Unauthorized access or leakage of such information could have drastic effects including identity theft, development of fraud and any consequential lack of trust. Privacy-preserving AI models provide security of data sharing and protection of sensitive information in training and inference as well as decision-making processes, curtailing risks that are involved in centralized storage and processing of data.
- Compliance with Data Protection Regulations: Vigorous regulatory guidelines like the General Data Protection Regulation (GDPR) and other privacy laws in some countries mandate government departments to ensure tools in place that will uphold data secrecy and reduce chances of leakage. Privacy-preserving AI models like Differential Privacy (DP), Federated Learning (FL), and Homomorphic Encryption (HE) allow typing these regulations, and yet still enable advanced analytics and AI-derived insights.

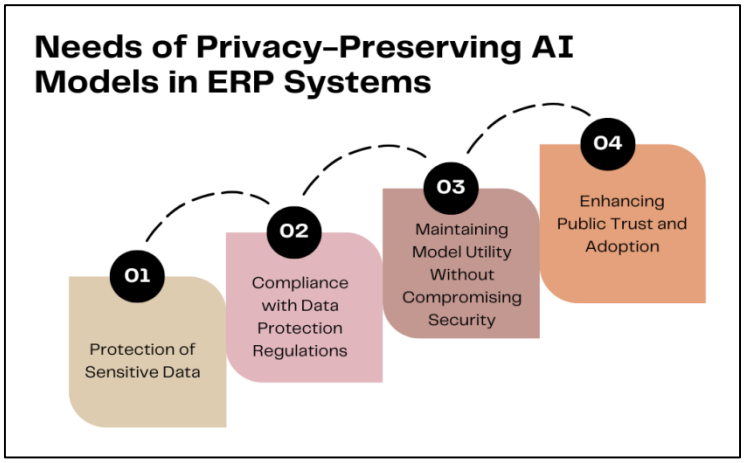

Figure 1: Needs of Privacy-Preserving AI Models in ERP Systems

- Maintaining Model Utility Without Compromising Security: The main issue with governmental AI applications is to have a high-performance model and protect data privacy. Excessive privacy mechanisms may cause poor accuracy of the AI system to provide meaningful insights to the ERP modules. The introduction of privacy-preserving AI models overcomes this problem by introducing measures that balance between accuracy and privacy to enable accurate forecasting, anomaly detection and resource optimization without compromising on data security.

- Enhancing Public Trust and Adoption: People would be more willing to vote in favor of the AI-driven governance where data protection procedures are clear and insurmountable. The decisions to adopt privacy-preserving AI artifacts in ERP systems will not only enhance confidence of people in the digital governance campaigns but will also eliminate certain impacts of misuse of sensitive information. Trust is a determinant in the adoption and success of AI-based ERP systems, especially in environments where there is heavy reliance on citizen data that are processed to make decision.

1.2. Governmental Resource Planning and Citizen Data Management

Resource planning activities and management of citizen data are key tasks of any modern governance, and these mandates require high-performance tools capable of accommodating large, heterogeneous data and support strategic decision-making. The ERP systems offer a coherent tool of conducting resource management in various fields, such as budgeting, implementing services to the population, managing infrastructure, and personnel in the workforce. [4,5] These systems pull together information across a wide range of sources-taxation, healthcare databases, social welfare schemes, third-party administrative registries and integrates them in a single framework that facilitates real-time analysis and policy optimization. Nevertheless, the sophistication and the size of citizen data provides major challenges to the security, privacy and being compliant with strict data protection laws. AI augmentation helps to expand the abilities of ERP systems, bringing in such features like predictive work of analytics on demand analysis, anomaly detection to financial management and automation with intelligent automation of resource distributions. However, the AI application also further increases the risk of data misuse since the sensitive personal and governmental content can be compromised during training and inferences. This is why privacy-preserving AI models become so necessary to preserve the integrity of the data of the citizens and use the strengths of AI-insights at the same time. Governments should use ERP systems to increase its control and efficiency of operations, but its commercial benefits can also help governments increase transparency, accountability and trust in government.

2. Literature Survey

2.1. ERP Systems in Governmental Applications

Enterprise Resource Planning (ERP) is a valuable resource that is used on the state level to promote unity on a digital platform through the coordination of various functions including but not limited to public administration, taxation, defense, and citizen service. These systems also enhance efficiency and visibility through facilitation of real-time information exchange between departments through the provision of a centralized database. Conventional ERP systems are somewhat static, rules-based systems that lack much in the way of analytical tools. They are good at processing transactions and documenting but fail at predictive analytics or adaptive decision-making which are becoming a requirement in the complex governmental settings. [6-

9] Recent developments have meant that Artificial Intelligence (AI) modules have now started to feature in ERP solutions, which bring with them automatic forecasting capabilities as well as improved efficiency and intelligent assignment of resources. These developments lead to a greater responsiveness of governmental agencies, which are in a position to respond to changing needs of citizens, as well as enhance the level of service delivery. However, the process of incorporation of such sophisticated features comes with new problems, especially concerning processing delicate citizen information, regulatory mandate, and the scaling of systems within high-level security systems.

2.2. AI Integration in ERP

The new development of adding AI to ERP systems represents a paradigm shift in data management as the innovation will make a system active and insight-driven rather than data-driven. ERP systems are augmented by IA techniques, such as machine learning and natural language processing, which allow predictive analytics to support demand forecasting, intelligent decision support-driven resource allocation, and anomaly detection of both financial and operational anomalies. In government use cases, AI-powered ERP systems can help with budget projections, detecting fraud in government budgets and optimizing social services to ensure greater efficiency and accountability. Nonetheless, this integration is faced with great technical and moral issues. The main issue with centralized AI model training is that it centralizes a sensitive data collected across departments, which begs the question of privacy and misuse of collected data and being vulnerable to cyberattacks. Moreover, governmental data sources are usually related to personally identifiable information (PII) and classified material, and the agent of the data protection gets its top priority. Consequently, although AI contributes features beyond the capabilities of the current ERP systems, there is a need to apply strenuous privacy-preserving measures to support ERP systems implementation in the public sector to guarantee adherence to data protection laws and establish trust in the population.

2.3. Privacy-Preserving AI Techniques

Privacy-preserving approaches in AI-enhanced ERP systems To overcome the privacy and security issues of the AI-enhanced ERP systems, a number of privacy-preserving methods have been suggested and studied in academic and industrial circles. Federated Learning (FL) enables training of AI models on multiple government nodes without moving raw data to a centralised server. This will help to reduce the probability of data breaches, but also takes advantage of collective intelligence to improve models. Homomorphic Encryption (HE) is another security control to prevent access to sensitive data as a result of the processing since in the homomorphic encryption computations are made on encrypted data. Differential Privacy DP uses controlled noise in the data or query outputs to avoid the re-identification of individuals and still allow significant analytics. In much the same way, Secure Multi-Party Computation (SMC) allows multiple parties to compute a function on their collective data without revealing the input data

of the parties involved, a feature that is very useful in inter-agency settings. All these methods are the basis of privacy-preserving AI in the ERP system but their overhead, inability to handle large volumes, and integration issues are currently under discovery.

2.4. Research Gap

Although there have been great strides in the development of privacy-preserving technology, the use of such technology in the use of the ERP systems in government settings is largely unfocused and unexplored. The majority of the available literature discusses separate privacy-preserving mechanisms-either FL, HE, DP, or SMC- and do not cover how these systems can be combined into a comprehensive approach that better suits the requirements of ERP. Furthermore, governmental ERP systems are characterized by some computational complexities, such as performance of large scale data processing, real time decision making needs, and strict regulatory issues. The integration of several privacy-preserving techniques would encompass new challenges, including optimizing trade-offs between security providences and computational performance and the need to work around existing ERP systems. Moreover, existing literature does not focus much on the trade-offs of data utility vs. privacy preservation and system performances on these sensitive areas. This prompts an urgent need to have an overall framework that can reconcile the more recent developments in privacy-preserving AI systems with the more established ERP systems to ensure that they are scalable, secure, as well as efficient in operation in the context of governmental applications.

3. Methodology

3.1. Privacy-Preserving ERP-AI Framework

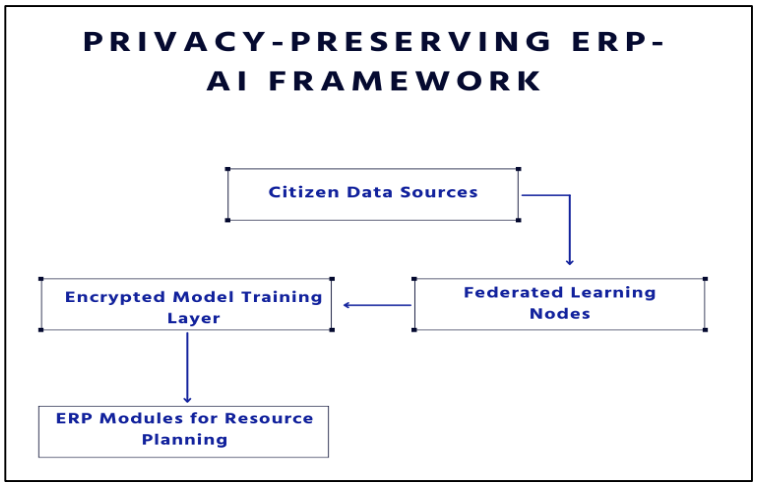

Figure 2: Privacy-Preserving ERP-AI Framework

- Citizen Data Sources: In a state setting, the data about the citizens is generated by an assortment of sources starting with the records of public administration, the taxation system, health-related databases, and social services services. [10-12] These data include

sensitive data like personal identifiers, financial data and health that needs to be treated with high confidentiality. To make sure that privacy policies are not violated, it is not possible to move raw data out of the governmental department, retaining it in a source of the department. The decentralized data architecture minimizes exposure during transmissions in line with privacy-by-design in the foundation of secure AI incorporation in ERP systems.

- Federated Learning Nodes: Federated Learning (FL) nodes are nodes of local computation units available in various government departments or agencies. As opposed to sending raw citizen data to some central server, FL nodes train AI models on their datasets and exchange only gradients of the variables or model updates with a central aggregator. This practice is the guarantee that sensitive information is stored and controlled locally, and also allows to collaborate during model training among several agencies. FL therefore adds a layer of intelligence to the ERP systems by integrating various datasets without losing any effective privacy protection, and it reduces the risks that are characterised by centralized data repository.
- Encrypted Model Training Layer: Stronger protection against data leakage is achieved by the use of an encrypted model training layer implementing cryptographic protocols such as Homomorphic Encryption (HE), Secure Multi-Party Computation (SMC), and Differential Privacy (DP). HE guarantees that calculations regarding the model updates can happen without having to decrypt the data, whereas DP adds controlled noise to the data to disconnect re-identification of subjects. SMC also guarantees the multi-party data and model parameter privacy as it does not allow any individual member to hold the full dataset or model parameters. The combination of these methods will guarantee the compliance of AI-enhanced ERP functions under privacy requirements as well as the integrity and confidentiality of sensitive data throughout the training and inference steps.
- ERP Modules for Resource Planning: When privacy-preserving AI models have been developed, their knowledge is incorporated into ERP modules that control such key governmental processes as budgeting, distribution of public resources, and optimization of the services delivery. Employing AI, ERP modules can deliver the prediction on the financial aspect of the company, identify the patterns of anomalies in funds management, and enhance the effectiveness of the services to the citizens. Critically, the data security is maintained throughout, including the data collected, its analysis by using the AI-based decision support, and the eventual decision outcome making. Therefore, the ERP system does not breach privacy of citizen and the nature of government operations that are highly confidential.

3.2. Mathematical Model Privacy-Preserving Loss Function

The proposed mathematical model of privacy-preserving AI in ERP systems represents a combination of the accuracy of the performed tasks and privacy guarantees in a single objective optimization problem. [13-15] The loss is given as

$$L_{PP} = L_{AI} + \lambda \times L^{Privacy}$$

Where $LPP$is the total amount of privacy-related loss, L is the standard AI model loss, and L o (H), o is the potential privacy leakage, and the parameter o represents the trade-off between the accuracy of a model and the protection of privacy. The standard AI model loss LA Guinea R Broad I Loss is generally calculated with using standard loss functions cross-entropy used in classification problems and mean squared error (MSE) in regression problems. The component will ensure that the AI model remains highly predictive, and thereby resource allocation processes and anomaly detection in the public financial data may be conducted in ERP modules accurately. The privacy leakage measures the degree to which sensitive information can possibly be deduced by analyzing the parameters, the gradients of the model or model outputs. Such leakage can be mathematically capped using techniques such as Differential Privacy (DP), by adding carefully measured noise to model updates, and Homomorphic Encryption (HE) and Secure Multi-Party Computation (SMC), as a way to mitigate the threat during distributed training. The parameter gives a very important role in determining the extent to which the issue of privacy is emphasized in relation to accuracy. The higher the value of the privacy constraint, the stricter its privacy guarantee at the sacrifice of predicted performance, and a lower value emphasizes accuracy over privacy guarantee. Dynamic tuning of allows governmental ERP systems to accommodate regulatory requirements and operation needs as continuously changing during the lifetime use of the systems, hence making privacy-keeping AI to provide an optimality quotient between safe usage of data and quality in decision guidance.

3.3. Workflow

- Data Collection: The proposed framework requires gathering citizens and resources data in the various governmental departments such as taxation offices and the healthcare agencies and public service institutions. Sensitive information never leaves the local nodes and is never transferred, so to secure privacy, it is incumbent to ensure the sensitive information is not transferred to a server. Such a decentralized data management system greatly decreases risk of breaches and unauthorized accesses and can align with the privacy-by-design principles required by governmental regulations.
- Model Training: Data that has been secured in one location is then trained using Fed learning (FL) to have many nodes collaborate in the training of AI models. Gradients or weights are estimated locally based on the local dataset on each node and is then sent to

a central aggregator. Those updates are then synthesized by the aggregator into a global model without prior application to citizen data This mechanism grants that the ERP systems not only enjoy diverse datasets across agencies but also have confidentiality in data.

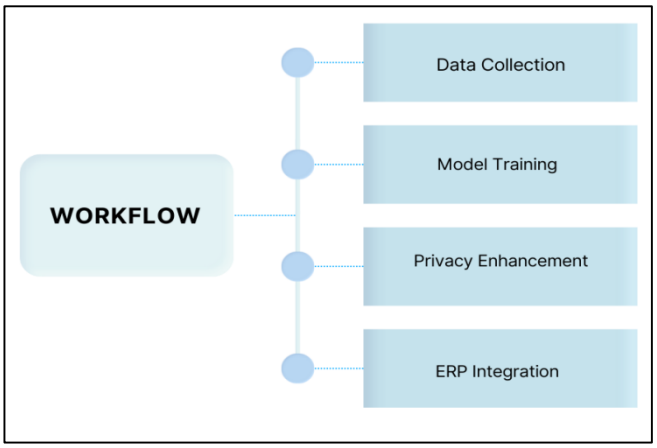

Figure 3: Workflow

- Privacy Enhancement: To additionally protect model training and updates, Homomorphic Encryption (HE) is used. The property of HE is that it enables a calculation using encrypted parameters, so that each part of the training pipeline works with confidential data. Also, methods like Differential Privacy (DP) can be applied to provide some statistical noise to obviate the probability of reconstructing delicate details based on published updates. The combination of these measures creates a security-worthy privacy protection mechanism of AI-driven ERP.
- ERP Integration: Trained the AI models are easily incorporated into ERP modules to provide real-time decision-making capabilities within budgeting, resources allocation, and combating fraud. The AI-powered insights and suggestions are delivered to the ERP system via encrypted communications and they decrypted at a module level where they can be used. The integration will make sure that privacy-preserving AI will augment the capabilities of ERP without sacrificing security or system performance.

3.4. Workflow of the Proposed Framework

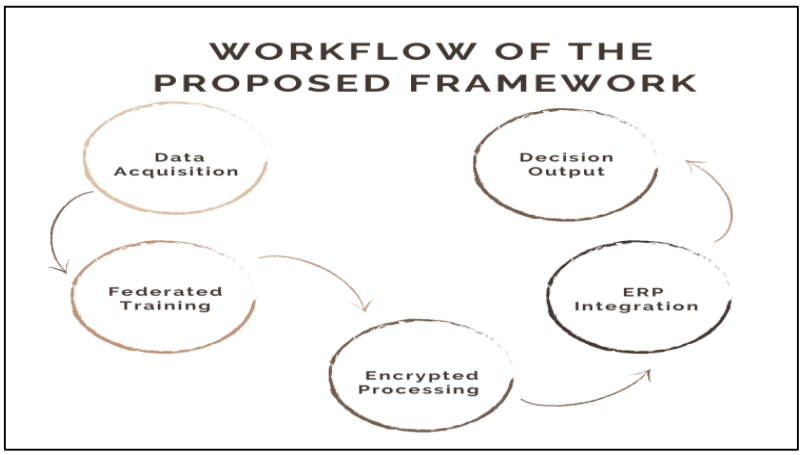

Figure 4: Workflow of the Proposed Framework

- Data Acquisition: It starts with the process of data collection, when personal information of citizens along with data on the available resources are obtained by various governmental agencies, such as taxation, healthcare, and public services departments. [16-18] All data is stored as well as processed on a local node, thus avoiding data pooling at a central location to make compliance with data privacy regulations a reality. Such decentralized gathering reduces exposure exposure risk and prevents loss of data integrity and security.
- Federated Training: When data collection is done, federated learning is applied across the nodes that are managed by the governments. Every node trains an AI model locally on their data and only encrypted changes to the model such as weights and gradients get transmitted to a central aggregator. This will yield a collaborative learning with raw data being kept secret and the learning process enabled to leverage a wide range of data sources.
- Encrypted Processing: Encrypted processing introduces another level of security in a form of Homomorphic Encryption (HE) and Secure Multi-Party Computation (SMC). These methods enable calculations of encrypted data, and thus sensitive data are not leaked to exposed to unauthorized access during training and inference. DP can also be employed to add controlled noise thus further mitigating the exposure.
- ERP Integration: The trained and privacy-preserved AI model is then deployed to ERP system to improve modules charged with budgeting, resource allocation, citizen services and identification of anomalies of the public funds. The integration procedure guarantees the smooth flow of information between the elements of AI, and ERP modules maintaining the integrity of security policies and contributing a low computational burden.

- Decision Output: The trained AI model will finally make decision outputs giving actionable intelligence in real time. These outputs can be forecast-based analytics on budgeting, risk or resource optimization. Since privacy mechanisms are applied at each aspect of its workflow, decision results can be assured of their correctness, security, and compliance with data protection requirement.

4. Results and Discussion

4.1. Experimental Setup

The proposed privacy-preserving ERP-AI framework is evaluated using the experimental setup that is intended to measure how well the techniques proposed will perform in the conditions that are close to the governmental ones. An ERP simulated dataset containing more than one million citizen records is used with diverse information including demographic information, taxation information, and service use and resource allocation history. Such records are spread at ten virtual governmental nodes, each of which is department/agency involved in the maintenance of local data integrity and security. Training is done in a Federated Learning (FL) scheme, with each of the nodes training a local copy of the AI model on their own dataset and transmitting cipher-encrypted weight updates to a central aggregator. The central server calculates these updates into a global model, whereby raw data is not shared among the nodes. Homomorphic Encryption (HE) will be used to provide security to the computations, whereas Differential Privacy (DP) will provide statistical noise to minimize the risk of inference of the sensitive data. The three performance measures are Accuracy (quantifies the model predictive ability on ERP-related tasks by estimating resource allocation and anomaly detection); Privacy Compliance Score (PCS), which is a composite metric that quantifies the adherence to principles of privacy-preserving by estimating data leakage resistance and encryption effectiveness, and Computational Overhead, which is an indication of the processing time and resource consumption increased when privacy-preserving techniques are applied compared to conventional AI-ERP integrations. The experimental design of this study is to confirm the above-mentioned hypothesis that the proposed theoretical framework of our study provides an optimal accuracy-privacy tradeoff combined with an acceptable computational efficiency due to large scale implementation in government systems.

4.2. Performance Analysis

Table 1: Performance Analysis

Technique	Accuracy (%)	PCS (%)	Overhead (%)
Conventional AI	94	55	12
Proposed Model	92	96	18

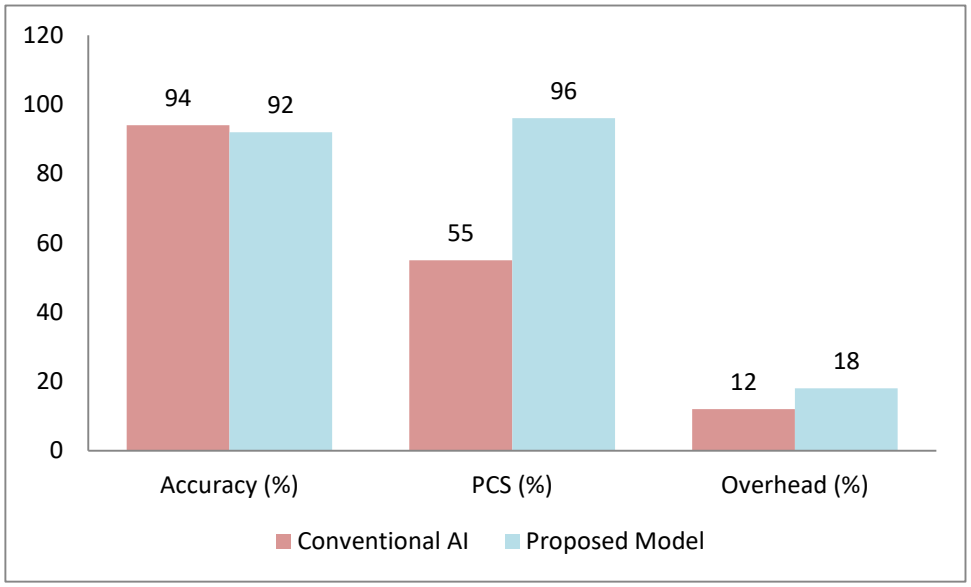

Figure 5: Graph representing Performance Analysis

- Accuracy: The accuracy benchmark is a measure of how well the model is doing the basic ERP functions resource allocation, anomaly detection and service optimization. The traditional AI solution was even more accurate by 94%, as no privacy-saving restrictions need to be placed. The proposed privacy preserving model obtained an accuracy of 92%, indicating that there is a marginal decrease despite the complexity in computations due to the Federated Learning, Homomorphic Encryption, and Differential Privacy. This finding shows that the proposed framework is with the capability of retaining good predictive output and guaranteeing greater protection on the information.
- Privacy Compliance Score (PCS): The Privacy Compliance Score is an indicator of the model protecting sensitive information during training, processing and even inference. The traditional AI approach achieved 55%, which means moderate protection because of using centralized data processing and a lesser degree of protection against possible data leaks. By comparison, the proposed model has a PCS of 96%, which is due to incorporating Federated Learning, encryption-based secure computation and privacy noise mechanisms. Such a big difference shows that the framework is effective to improve privacy preservation without affecting the reliability of the functions.
- Computational Overhead: Computational overhead the computational overhead is the increase in costs and effort that is required when conducting privacy-preserving operations as opposed to more traditional AI. The traditional technique experienced an overhead of 12 percent which reveals that the cost of computation is relatively lower. Nevertheless, the model proposed had a higher overhead of 18%, due to the processes of encryption, secure aggregation, as well as noise injection mechanisms. Although this increase is commendable, it is accepted because of the privacy after-effects experienced.

The use of optimisation technologies, e.g. lightweight encryption schemes or application of adaptive privacy levels, could also save overhead in a future iteration that is as secure as the current one.

4.3. Discussion

The lab tests show that the designed privacy-preserving ERP-AI system effectively increases the level of data protection without worsening its performance. With a Privacy Compliance Score (PCS) of 96 percent, as opposed to 55 percent in the conventional AI, the measured result indicates that the federated learning architecture, combined with Homomorphic encryption and Differential privacy, ensure substantial protection against possible data breach and inappropriate inference. Notably, such enhancement in terms of privacy does not entail a serious compromise in terms of predictive accuracy, since the accuracy fell only by a small percentage (from 94 to 92), in the conventional model and the proposed framework, respectively. This indicates that privacy-protecting methods can be administered successfully without harshly barring modeling soundness, which renders the solution usable to the actual governmental ERP cases. It is also indicated that there is a slight augmentation of computation overhead that was 12 percent in the traditional model and 18 percent in the new model. Although this overhead is associated with the increased processing needs of adding encryption, secure aggregation, and noise injection mechanisms, it is reasonable to conclude that it does not exceed the acceptable level of large governmental installations where information security is an important concern. In addition, the effects of these performance costs can be mitigated by the following: advances in lightweight encryption schemes, hardware acceleration, distributed processing. Altogether, the suggested model will provide the reasonable trade-off between privacy, accuracy, and computational performance. It provides trustworthiness in accordance with strict data protection requirements, and robust decision-support functionalities of budget forecasting, anomaly detection, and resource optimization. The above findings lend weight to the framework being promoted as a potentially recommendable architecture to next-generation ERP systems in the government sector where data privacy is equally essential as operational efficiency. Future work can be to optimize cryptographic protocols and dynamic privacy settings to further provide more optimal performance with high privacy assurances.

5. Conclusion

This paper proposes a framework to integrate privacy-preserving AI into ERP in governmental settings as a possible approach to give due consideration to both the challenges to establish the benefits of the advanced methods of data-driven decision-making and the concerns about absolute privacy. ERP systems that are built on traditional technologies are powerful in transaction processing, resource management but fall short of analytic capabilities needed to determine future patterns, identify anomalies, and make on-optimal resource planning decisions. The adoption of AI would help to close this divide but it also presents immense privacy

risks since the information subject to governmental and citizenship lies on the fence. To mitigate these risks, the proposed framework will apply Federated Learning (FL)so that training can be decentralized to multiple nodes in the government without data exchange, Homomorphic Encryption (HE) so that computing can be performed on encrypted data, and Differential Privacy (DP) to mathematically ensure privacy against re-identification of individual data.

Experimental results confirm that the framework delivers a Privacy Compliance Score (PCS) improvement of 96 percent over other conventional AI methods without any reduction in predictive accuracy of 92 percent, only marginally lower than the 94 percent of the baseline. Its computational overhead of 18 percent is slightly higher than that of traditional systems but can be compromised to operate the government on large scale where data protection is important. These findings are indicative of the fact that privacy-preserving AI methods are viable to integrate in an ERP system without significantly degrading performances or operational performance.

The study also identifies a significant research gap, namely, whereas individual privacy-preserving mechanisms have been studied quite significantly in the AI literature, their joint use on ERP-specific situations, where data heterogeneity, scalability, and real-time performance requirements are important ones, is underexplored. The future direction of the project will be centered on optimization of the computation efficiency, possibly through minimal encryption algorithm, and flexible privacy parameters and investigating blockchain integration as a possible way to improve auditability and trust in the protection and enforcement of the privacy parameter. Blockchain could also leave indelible records of data access and of model updates, and encryption operations, as well, warranting verifiable and transparent compliance with privacy criteria. Finally, the suggested framework can be seen as the major step towards the development of safe, intelligent governmental use of ERP systems. It combines privacy-preserving technologies with AI-based decision support and forms a basis of the next generation of e-governance solutions where the data protection and operational excellence are prioritized.

6. References

1. Jin, W., Yao, Y., Han, S., Gu, J., Joe-Wong, C., Ravi, S., ... & He, C. (2023). FedML-HE: An efficient homomorphic-encryption-based privacy-preserving federated learning system. arXiv preprint arXiv:2303.10837.
2. Ma, J., Naas, S. A., Sigg, S., & Lyu, X. (2022). Privacy-preserving federated learning based on multi-key homomorphic encryption. International Journal of Intelligent Systems, 37(9), 5880-5901.
3. Guo, Y., Li, L., Zheng, Z., Yun, H., Zhang, R., Chang, X., & Gao, Z. (2024). Efficient and privacy-preserving federated learning based on full homomorphic encryption. arXiv preprint arXiv:2403.11519.

4. Rieyan, S. A., News, M. R. K., Rahman, A. M., Khan, S. A., Zaarif, S. T. J., Alam, M. G. R., ... & Fortino, G. (2024). An advanced data fabric architecture leveraging homomorphic encryption and federated learning. Information Fusion, 102, 102004.
5. Ahamed, S. I., & Ravi, V. (2022). Privacy-Preserving Wavelet Neural Network with Fully Homomorphic Encryption. arXiv preprint arXiv:2205.13265.
6. Juvekar, C., Vaikuntanathan, V., & Chandrakasan, A. (2018). {GAZELLE}: A low latency framework for secure neural network inference. In 27th USENIX security symposium (USENIX security 18) (pp. 1651-1669).
7. Yeh, L. Y., Tseng, S. P., Lu, C. H., & Shen, C. Y. (2025). Auditable Homomorphic-Based Decentralized Collaborative AI With Attribute-Based Differential Privacy. IEEE Transactions on Network and Service Management.
8. Aziz, R., Banerjee, S., Bouzefrane, S., & Le Vinh, T. (2023). Exploring homomorphic encryption and differential privacy techniques towards secure federated learning paradigm. Future internet, 15(9), 310.
9. Wang, B., Li, H., Guo, Y., & Wang, J. (2023). PPFLHE: A privacy-preserving federated learning scheme with homomorphic encryption for healthcare data. Applied Soft Computing, 146, 110677.
10. Park, J., & Lim, H. (2022). Privacy-preserving federated learning using homomorphic encryption. Applied Sciences, 12(2), 734.
11. Yathiraju, N. (2022). Investigating the use of an artificial intelligence model in an ERP cloud-based system. International Journal of Electrical, Electronics and Computers, 7(2), 1-26.
12. Sabbarwal, E., & Pandey, D. S. (2023, June). IoT based Data Protection Technique for Security and Privacy Preserving in Cloud ERP. In 2023 International Conference on IoT, Communication and Automation Technology (ICICAT) (pp. 1-5). IEEE.
13. AI, Data Governance and Privacy Synergies And Areas Ofinternational Co-Operation, OECD Publishing, 2024. online. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/ai-data-governance-and-privacy_2ac13a42/2476b1a4-en.pdf
14. Schellong, A. (2008). Citizen relationship management. In Electronic Government: Concepts, Methodologies, Tools, and Applications (pp. 2567-2579). IGI Global Scientific Publishing.
15. Althonayan, M., & Althonayan, A. (2017). E-government system evaluation: The case of users' performance using ERP systems in higher education. Transforming Government: People, Process and Policy, 11(3), 306-342.
16. Privacy preserving AI models for decentralized data management in federated information systems, GSC Advanced Research and Reviews, 2025, 22(02), 104-112. https://doi.org/10.30574/gscarr.2025.22.2.0043

17. Mhaskey, S. V. (2024). Integration of artificial intelligence (AI) in enterprise resource planning (ERP) systems: Opportunities, challenges, and implications. International Journal of Computer Engineering in Research Trends, 11(12), 1-9.
18. Zhao, C., Zhao, S., Zhao, M., Chen, Z., Gao, C. Z., Li, H., & Tan, Y. A. (2019). Secure multi-party computation: theory, practice and applications. Information Sciences, 476, 357-372.
19. Boura, C., Chillotti, I., Gama, N., Jetchev, D., Peceny, S., & Petric, A. (2018, February). High-precision privacy-preserving real-valued function evaluation. In International Conference on Financial Cryptography and Data Security (pp. 183-202). Berlin, Heidelberg: Springer Berlin Heidelberg.
20. Zhang, L. S. (2024). Deep Learning Based Optimization of Cloud Enterprise Resource Planning (ERP) Systems for Adaptive Decision Support and Management Effectiveness Analysis. IEEE Access.