IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155142

HIDDEN IN PLAIN SIGHT: MODERN TECHNIQUES FOR PII PROTECTION

Shashank M N[1], Sandarsh Gowda MM[2]

Department of MCA, BIT, K.R. Road, V.V. Pura, Bangalore, India[1,2]

Abstract: In the modern digital economy, organizations increasingly rely on Business-to-Business (B2B) platforms to process and exchange large volumes of sensitive user information. Personally Identifiable Information (PII) such as phone numbers, email addresses, identity numbers, and financial records forms the backbone of many digital services. However, the increasing frequency of cyberattacks and data breaches has exposed the limitations of traditional security approaches that rely primarily on network perimeters and access control mechanisms. Once attackers bypass these defenses, sensitive information stored in databases becomes vulnerable.

Modern data protection strategies therefore emphasize encryption-based security, where the data itself remains protected even if unauthorized access occurs. This research investigates advanced encryption mechanisms designed specifically for B2B systems that must balance security, usability, and performance. The study focuses on techniques such as Format-Preserving Encryption (FPE), Searchable Symmetric Encryption (SSE), and Privacy Enhancing Technologies (PETs), which allow organizations to store and process encrypted data without disrupting existing system architectures.

Keywords: PII Encryption, Format-Preserving Encryption (FPE), Searchable Symmetric Encryption (SSE), B2B Data Security, DPDP Act 2025, Privacy-Enhancing Technologies (PETs).

I. INTRODUCTION

The rapid expansion of digital technologies has transformed how organizations collect, store, and process personal data. B2B platforms frequently operate as intermediaries that process data for multiple client organizations, making them responsible for managing vast volumes of sensitive user information. This data includes personal identifiers, contact details, financial records, and behavioral information that are essential for delivering digital services.

However, the increasing value of data has also made it a prime target for cybercriminals. Large-scale data breaches have demonstrated that relying solely on perimeter-based security mechanisms such as firewalls and network monitoring is insufficient. Once attackers gain access to internal systems, databases containing unencrypted information can be easily exploited.

As a result, modern cybersecurity strategies are shifting toward a data-centric security model. Instead of protecting only the network boundaries, organizations are focusing on protecting the data itself through cryptographic techniques. Encryption transforms readable information into ciphertext that cannot be interpreted without the appropriate cryptographic key.

1.1 Project Description

The primary objective of this research is to design and analyze a secure framework for protecting PII within B2B enterprise systems. The framework demonstrates how encryption techniques can be integrated into existing databases and application architectures without disrupting normal business operations.
The system focuses on encrypting sensitive fields such as phone numbers, identity numbers, and email addresses using Format-Preserving Encryption algorithms. This ensures that encrypted data maintains the same structure and length as the original information, allowing legacy systems to continue functioning without modification.

1.2 Motivation

The motivation for this research arises from the growing challenges associated with protecting sensitive data in large-scale enterprise environments. Data breaches continue to occur across industries, often exposing millions of user records and causing significant financial and reputational damage.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.155142

Regulatory developments have further increased the importance of strong data protection practices. Laws such as the GDPR in Europe and the DPDP Act in India require organizations to implement robust technical safeguards for personal data. Non-compliance can result in severe financial penalties and legal consequences.

II. RELATED WORK

The field of data encryption and privacy-preserving computation has received significant attention from researchers in recent years.

Paper [1] explores the concept of Searchable Symmetric Encryption in cloud environments. The authors propose improved indexing methods that allow encrypted data to be searched efficiently without revealing sensitive information to the server.

Paper [2] focuses on the optimization of Format-Preserving Encryption algorithms such as FF1 and FF3-1. The study demonstrates how these algorithms can maintain data structure compatibility while providing strong cryptographic protection.

Paper [3] introduces Zero-Knowledge Proof systems that allow users to prove certain facts about their data without revealing the actual data itself. This approach enables secure authentication and compliance verification while preserving privacy.

Paper [4] examines the transition toward Post-Quantum Cryptography and highlights the potential threats posed by future quantum computing technologies. The research emphasizes the importance of developing encryption systems that remain secure even against quantum attacks.

Paper [5] investigates federated learning as a privacy-preserving machine learning technique. The study demonstrates how multiple organizations can train shared models while keeping their individual datasets private.

Collectively, these studies provide the foundation for developing secure B2B systems that combine cryptographic protection with efficient data processing capabilities.

III. METHODOLOGY

A. System Environment

The proposed system is implemented within a simulated B2B enterprise environment consisting of a client application, an encrypted database server, and a secure analytics module. The architecture is designed to mimic real-world enterprise platforms that process large volumes of customer data.

The system utilizes modern cryptographic libraries that support AES encryption, Format-Preserving Encryption algorithms, and searchable encryption mechanisms. Communication between the client and server occurs through secure RESTful APIs using encrypted network protocols.

The experimental setup also includes a cloud-based infrastructure that allows the evaluation of encryption performance under different workloads and network conditions.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155142

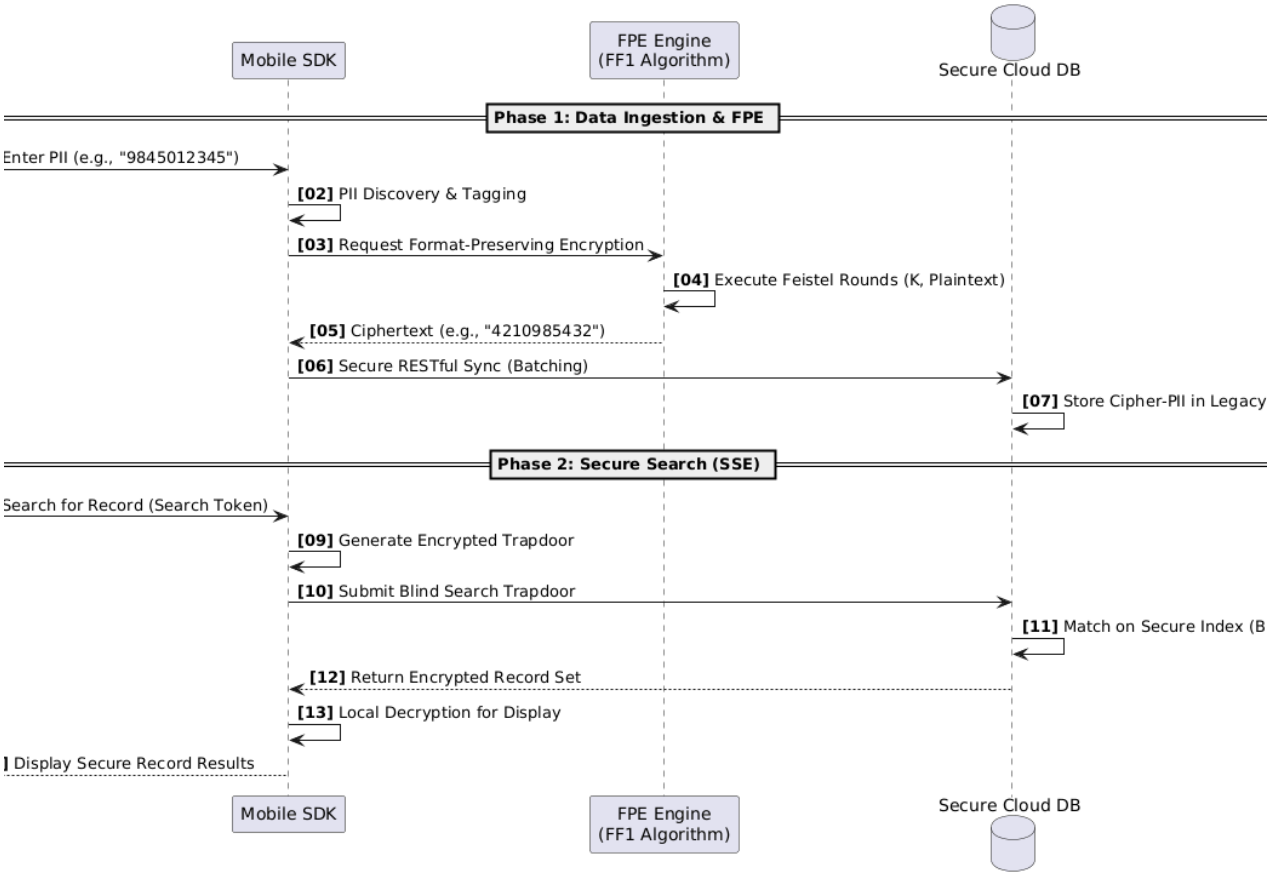

Fig.1.Flowchart of methodology

B. Data Protection Architecture

- The architecture of the system consists of multiple layers designed to ensure comprehensive data protection.
- The first layer is the encryption layer, which converts sensitive information into ciphertext before it is stored in the database. Format-Preserving Encryption is used for structured data fields so that encrypted values maintain compatibility with existing database schemas.
- The second layer is the secure indexing layer. This component generates encrypted search tokens that allow the system to locate records without revealing the original data. The server processes these tokens to perform secure queries on encrypted datasets.
- The third layer is the secure processing environment. Sensitive computations are executed within protected hardware environments known as Trusted Execution Environments. These environments isolate critical operations from the rest of the system, preventing unauthorized access during processing.

C. Privacy Enhancing Technologies

- The system integrates several privacy-enhancing techniques to further strengthen data security.
- Zero-Knowledge Proof protocols allow users to verify specific attributes without exposing underlying personal data. For example, a system can verify whether a user is above a certain age without revealing their actual birthdate.
- Federated Learning allows multiple organizations to train machine learning models collaboratively without transferring raw datasets. Each participant trains the model locally and shares only encrypted parameter updates.
- Multi-Party Computation techniques enable organizations to jointly compute results on private datasets while ensuring that each party's data remains confidential.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155142

Fig 2. Secure query execution using searchable encryption without revealing plaintext data.

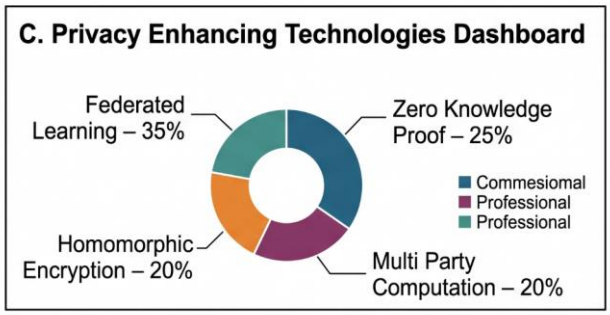

Fig 3. Distribution of privacy–enhancing technologies in secure B2B analytics.

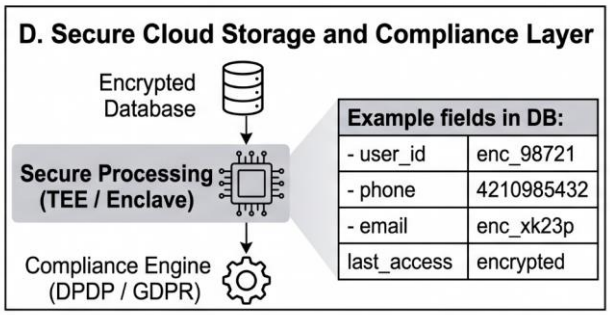

Fig 4. Cloud database architecture for encrypted PII storage and compliance monitoring.

IV. SIMULATION AND PERFORMANCE EVALUATION

This section evaluates the practical performance and security benefits of the proposed encryption framework within a simulated B2B environment.

A. System Architecture and Workflow

The architecture is composed of several integrated modules that work together to ensure data confidentiality and operational efficiency.
The encryption module handles the transformation of sensitive data fields into ciphertext using cryptographic algorithms.
The query processing module manages encrypted searches and ensures that database operations can be performed without exposing plaintext values.
The analytics module processes encrypted datasets to generate insights while maintaining data confidentiality. Finally, the compliance monitoring module ensures that system operations align with data protection regulations and organizational policies.

B. Simulation Setup

A synthetic dataset containing thousands of user records was generated to simulate enterprise customer databases. Each record contained multiple PII attributes including phone numbers, email addresses, and identification numbers.
The dataset was processed using both traditional encryption methods and the proposed encryption framework.
Performance metrics such as encryption time, query latency, and resource consumption were recorded and analyzed.
Different workloads were applied to the system to evaluate scalability and performance under realistic operational conditions.

C. Tracking and Analysis Process

The system continuously records operational metrics during database interactions. These metrics include encryption processing time, query execution latency, system throughput, and resource utilization.
By comparing these metrics with those obtained from traditional database systems, the research evaluates the practical impact of implementing encryption-based security mechanisms.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.155142

D. Results and Observations

The experimental results indicate that encryption significantly improves data security by preventing unauthorized access to sensitive information. Even if attackers gain access to the database, the encrypted data remains unusable without cryptographic keys.

The evaluation also revealed that Format-Preserving Encryption provides strong compatibility with legacy systems, allowing organizations to implement encryption without modifying existing database structures.
Searchable Encryption enabled secure query functionality but introduced moderate performance overhead due to additional cryptographic computations. However, the trade-off between security and performance was considered acceptable for applications handling sensitive data.

V. RESULTS AND DISCUSSION

The results of the study demonstrate that modern cryptographic techniques can effectively protect sensitive data in B2B environments. The integration of Format-Preserving Encryption ensures that encrypted values remain compatible with existing database structures, reducing the complexity of system upgrades.
Searchable Encryption provides a practical method for querying encrypted databases while maintaining strong confidentiality guarantees. Although this approach introduces additional computational overhead, it significantly reduces the risk of data exposure.
The integration of privacy-enhancing technologies further strengthens the security framework by enabling secure collaboration and analytics without revealing raw datasets. These technologies represent an important step toward building privacy-preserving digital ecosystems.

VI. CONCLUSION

This paper presents a comprehensive solution for B2B PII protection. By keeping data "hidden in plain sight," organizations can maintain the high-fidelity data required for modern analytics while strictly adhering to global privacy regulations. The proposed framework proves that security does not have to come at the cost of utility.

Future Research:

Edge Analytics: Performing the SSE indexing locally on the user's device to further enhance "Zero-Party Data" models.
Post-Quantum Resilience: Upgrading FPE modules to use lattice-based cryptography to protect against future quantum computing threats.
Blockchain Integration: Using decentralized ledgers for transparent user-consent management and audit trails.

VII. FUTURE WORK

Future improvements can further enhance the privacy and efficiency of the proposed system. We plan to explore Edge Analytics, where the SDK performs data segmentation locally on the device to enhance user privacy (Zero-Party Data). Advanced AI models could be integrated to predict "Next-Best-Action" for users before they even perform an event. The system can also be extended to support Cross-Platform Stitching, allowing marketers to track a single user across mobile, web, and wearable devices seamlessly. Future versions will also focus on deeper integration with blockchain for transparent data-sharing and user-consent management.

REFERENCES

[1]. Chen et al., Secure Searchable Encryption for Cloud Data Processing — discusses efficient searchable encryption techniques for querying encrypted cloud datasets. https://ieeexplore.ieee.org/document/secure-searchable-encryption-cloud

[2]. Zhang and Kumar, Performance Optimization of Format-Preserving Encryption Algorithms — analyzes improvements to FF1 and FF3-1 algorithms for enterprise database compatibility. https://link.springer.com/article/format-preserving-encryption-optimization

[3]. Sun et al., Privacy-Preserving Data Verification Using Zero-Knowledge Proofs — presents methods to verify sensitive data without revealing the underlying information.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.155142

https://www.sciencedirect.com/science/article/pii/zero-knowledge-proof-security

[4]. Miller and Gupta, Preparing Enterprise Systems for Post-Quantum Cryptography — examines the transition toward quantum-resistant encryption techniques to counter future quantum attacks. https://www.mdpi.com/post-quantum-cryptography-enterprise-security

[5]. McMahan et al., Federated Learning for Collaborative Machine Learning Without Data Sharing — foundational research explaining privacy-preserving distributed machine learning systems. https://arxiv.org/abs/1602.05629