International Journal of Computer Technology and Science

E-ISSN: 3048-1961
P-ISSN: 3048-1899

Research Article

Designing Privacy Preserving Intelligent Computing Models for Cross Platform Mobile and Cloud Based Applications

Aji Priyambodo [1*], Prihati [2]

[1] Institut Teknologi dan Bisnis Semarang, Indonesia; e-mail : ajippro@gmail.com
[2] Institut Teknologi dan Bisnis Semarang, Indonesia; e-mail : esterprihati20@gmail.com
* Corresponding Author: ajippro@gmail.com

Abstract: The rapid growth of cross-platform applications has significantly increased the volume and diversity of sensitive user data processed across heterogeneous and distributed environments. Personally identifiable information, device identifiers, behavioral data, and financial information are routinely collected to support personalization, analytics, and service optimization. While these practices enhance application functionality and user experience, they also introduce substantial privacy risks, including unauthorized data access, device fingerprint–based re-identification, cross-user data leakage, and large-scale data breaches. These risks are further amplified by distributed processing architectures and extensive third-party library integrations commonly used in modern cross-platform systems. This study aims to systematically analyze privacy issues in cross-platform applications by examining the types of sensitive data involved, identifying dominant privacy threats, and reviewing state-of-the-art privacy-preserving mitigation strategies. A systematic literature-based methodology was employed, focusing on recent Scopus-indexed journal articles, conference papers, and book chapters. The analysis synthesizes findings using thematic categorization and a conceptual research framework that maps sensitive data sources to privacy threats and corresponding mitigation mechanisms. The results indicate that privacy risks in cross-platform applications originate not only from external attacks but also from internal architectural weaknesses, such as flawed authorization logic and excessive data sharing across system components. Privacy-preserving techniques including differential privacy, federated learning, blockchain-based data governance, secure multi-party computation, and fine-grained access control mechanisms are shown to provide stronger privacy guarantees compared to conventional centralized approaches. However, these techniques also present trade-offs related to system complexity and performance. Overall, the study highlights the importance of adopting a multi-layered, privacy-by-design approach to ensure sustainable, trustworthy, and regulation-compliant cross-platform application development.

Keywords: Cross-Platform Applications; Data Leakage; Distributed Systems; Privacy Preservation; Sensitive Data.

Received: November 30, 2023
Revised: December 26, 2023
Accepted: January 28, 2024
Published: January 31, 2024
Curr. Ver.: January 31, 2024

1. Introduction

In recent years, cross-platform mobile applications and cloud-based systems have experienced rapid growth across multiple sectors, including digital services, healthcare, education, and financial services. This expansion is largely driven by advancements in cloud computing, artificial intelligence (AI), and high-speed mobile networks such as 5G, which collectively enhance system scalability, service efficiency, and user accessibility. Cross-platform development approaches enable applications to be deployed across diverse operating systems with reduced development cost and time, while cloud-based infrastructures provide flexible and on-demand computing resources to support large-scale digital services.

Within the digital services sector, cross-platform and cloud technologies play a crucial role in supporting the evolution of cross-border e-commerce and the emerging internet economy. Digital platforms have enabled businesses to expand beyond geographical boundaries, offering innovative services and products through integrated mobile and cloud solutions. The interactive development of cross-border e-commerce ecosystems demonstrates how digital technology enhances operational efficiency, data integration, and market accessibility, particularly for regions with limited physical infrastructure (Song, 2022). These developments highlight the strategic importance of mobile and cloud-based platforms in accelerating digital transformation within the global economy.

In the financial sector, mobile cloud computing has become a foundational technology for modern payment systems. The integration of cloud services with mobile applications allows secure, efficient, and scalable financial transactions, supporting both consumer payments and enterprise-level financial operations. Mobile cloud computing facilitates real-time processing, data synchronization, and service availability, making it suitable for financial and healthcare solutions that require high reliability and security (Murphy & Japheth, 2022). As mobile devices continue to dominate user interactions, cloud-supported financial services are increasingly essential for inclusive and accessible digital finance.

Furthermore, the integration of Near Field Communication (NFC) technology with enterprise resource planning (ERP) systems represents a significant advancement in mobile-based financial and organizational applications. NFC-enabled smartphones allow secure data exchange and transaction processing, which can be directly connected to ERP systems for real-time data integration and management. This integration improves operational efficiency, reduces manual input errors, and enhances system security in financial and enterprise environments (Zhou et al., 2018). The combination of mobile, cloud, and NFC technologies demonstrates a convergent technological trend aimed at optimizing enterprise and financial systems.

Overall, the rapid growth of cross-platform mobile and cloud-based applications reflects a broader shift toward integrated, scalable, and user-centric digital solutions. By leveraging cloud computing, mobile platforms, and supporting technologies such as NFC, organizations across digital services and financial sectors can achieve improved efficiency, accessibility, and innovation. These trends underscore the necessity of continued research and development in mobile cloud computing and cross-platform systems to support sustainable digital transformation.

In the rapidly evolving digital era, the processing of sensitive user data such as location information, behavioral patterns, identity attributes, and personal preferences has become a central component of modern applications and digital services. From 2019 to 2024, the volume and complexity of sensitive data processing have increased significantly due to the widespread adoption of artificial intelligence (AI), machine learning (ML), and location-based services (LBS). While these technologies enable advanced personalization and data-driven decision-making, they simultaneously raise critical concerns related to privacy, security, and regulatory compliance.

Artificial intelligence and machine learning have transformed how sensitive user data is collected, analyzed, and utilized. Advanced learning algorithms allow deeper and more accurate analysis of large-scale datasets, facilitating improved understanding of user behavior and preferences. Such approaches are widely applied in sentiment analysis, where natural language processing models extract insights from user-generated content and behavioral signals (Baca et al., 2023). Moreover, machine learning techniques have been increasingly employed to detect and classify sensitive data automatically within database systems, reducing human error and enhancing efficiency in data management processes (Candan & Kalay, 2024). Despite their effectiveness, these data-driven techniques often rely on extensive personal data, intensifying privacy risks if not properly managed.

Location-based services represent another major driver of sensitive data processing across various industries, including transportation, logistics, tourism, and smart city applications. By leveraging real-time location data, LBS can deliver highly personalized and context-aware services, improving user experience and operational efficiency (Yanuargi et al., 2024). However, the continuous collection and processing of location information expose users to significant cybersecurity threats, such as unauthorized tracking, data breaches, and surveillance risks (Al-Balasmeh, 2024). These vulnerabilities are further amplified by mobile device sensors, which can unintentionally leak sensitive contextual information and compromise user privacy (Delgado-Santos et al., 2022).

The growing frequency and impact of data breaches highlight the urgent need for stronger data protection mechanisms. Global analyses of data breach incidents reveal that compromised personal, financial, and health-related data can result in severe economic, legal, and social consequences (Pimenta Rodrigues et al., 2024). To address these challenges, privacy-preserving techniques such as encryption, anonymization, and data masking have been widely adopted, particularly in cloud computing environments where sensitive data is processed and stored at scale (Domingo-Ferrer et al., 2019). These techniques aim to balance data utility with confidentiality, though their implementation often involves trade-offs between performance and security.

In response to increasing privacy risks, regulatory frameworks have been introduced worldwide to strengthen personal data protection. Regulations such as the General Data Protection Regulation (GDPR) in the European Union and India's Digital Personal Data Protection Act emphasize transparency, explicit user consent, and accountability in data processing practices (Bareh, 2024). Compliance with these regulations requires organizations to adopt robust access control mechanisms and auditable data management strategies. Emerging technologies such as blockchain have gained attention as potential solutions for secure, transparent, and user-centric personal data management. Blockchain-based identity and access control systems can enhance data integrity, decentralization, and regulatory compliance while granting users greater control over their personal information (Daudén-Esmel et al., 2024; Faber et al., 2019).

Overall, the increasing reliance on AI, ML, and LBS has intensified the processing of sensitive user data, presenting both opportunities and challenges for modern digital systems. While advanced analytics and personalization offer substantial benefits, they must be carefully aligned with privacy-preserving technologies, regulatory requirements, and user awareness initiatives. Continued research is therefore essential to develop secure, compliant, and trustworthy frameworks for sensitive data processing in an increasingly data-driven digital landscape.

2. Literature Review

Intelligent Computing in Mobile and Cloud Environments

Mobile Cloud Computing and Intelligent Computing Concepts

Mobile Cloud Computing (MCC) has emerged as a fundamental paradigm to overcome the inherent limitations of mobile devices, particularly in terms of storage capacity, computational power, and energy efficiency. By offloading computation and data storage tasks to cloud infrastructures, MCC enables mobile applications to deliver advanced functionalities while maintaining lightweight client-side operations. Early studies emphasized dynamic and decentralized computational offloading mechanisms to improve system performance and adaptability in heterogeneous environments (Shanthi & Ramesh, 2019) . These approaches allow mobile systems to adjust computation strategies based on network conditions and resource availability.

Quality of Service (QoS) is a critical aspect of MCC environments, as performance, latency, and reliability directly affect user experience. Research on QoS in mobile cloud systems highlights the need for intelligent scheduling, load balancing, and resource provisioning to maintain service continuity under dynamic workloads (Arun & Prabu, 2021). These mechanisms form the foundation for intelligent computing by enabling adaptive decision-making in mobile cloud interactions.

AI and Cognitive Computing Integration

The integration of artificial intelligence into mobile and cloud ecosystems has significantly enhanced intelligent computing capabilities. AI-driven models enable real-time analytics, automated decision-making, and predictive resource management across distributed systems. Cognitive computing, which aims to mimic human reasoning and learning processes, has been proposed as a key enabler for smart communication systems, improving adaptability, accuracy, and low-latency responses in complex network environments (Sharma et al., 2020). Such capabilities are increasingly relevant in mobile and cloud scenarios where rapid contextual understanding is required.

Recent studies further emphasize the convergence of sensing, communication, computation, and intelligence in Internet of Things (IoT) ecosystems.AI-enhanced IoT applications leverage cloud and edge resources to support real-time decision-making while maintaining scalability and efficiency.

Cross-Platform Computing Challenges

Despite technological advancements, cross-platform computing in mobile and cloud environments faces several challenges. One major issue is interoperability, particularly between IoT devices, cloud platforms, and heterogeneous operating systems. The lack of standardized interfaces and protocols can result in performance degradation, increased system complexity, and security vulnerabilities (Chahar et al., 2024). These challenges are amplified as intelligent applications increasingly rely on data exchange across diverse platforms.

Resource management is another critical challenge, especially in environments with limited computational and energy resources. Efficient allocation of computing, storage, and network resources is essential to support intelligent workloads in mobile edge computing (MEC) and cloud-integrated systems. Studies on intelligent operational monitoring platforms demonstrate that edge computing can effectively address these challenges by enabling localized processing and reducing dependence on centralized cloud infrastructures (Jiang et al., 2019).

Security and Data Protection in Intelligent Systems

Security remains a central concern in intelligent mobile and cloud environments, particularly in cross-platform and multi-terminal systems. Research highlights the need for robust encryption mechanisms, authentication protocols, and secure data transmission strategies to protect sensitive information across distributed platforms (Jinhong, 2024). Lightweight encryption techniques tailored for low-power devices have also been proposed to balance security requirements with performance constraints (Kulkarni et al., 2017).

Security strategies are increasingly integrated with intelligent resource management frameworks to ensure that computation offloading and data processing decisions do not expose systems to additional risks. Such integrated approaches are essential for maintaining trust and reliability in intelligent computing environments that span mobile devices, edge nodes, and cloud infrastructures.

Edge Computing and Emerging Intelligent Trends

Edge computing has gained prominence as a key solution for reducing latency and improving real-time processing in intelligent mobile and cloud systems. By offloading computation tasks to edge nodes closer to data sources, systems can achieve faster response times and improved scalability. This paradigm is particularly effective for intelligent monitoring and control applications that require immediate data processing (Jiang et al., 2019).

Emerging trends indicate a growing emphasis on edge intelligence, where AI models are deployed at the network edge to support context-aware and adaptive services. Deep learning–based resource allocation and computation offloading strategies are increasingly explored to optimize system performance under dynamic conditions (Shanthi & Ramesh, 2019). Additionally, cross-platform development frameworks and hybrid approaches are being adopted to reduce development complexity while supporting intelligent functionalities across multiple platforms (Seo, 2023).

Overall, the literature highlights a strong convergence of mobile cloud computing, artificial intelligence, cognitive computing, and edge intelligence. While these technologies collectively enhance system capabilities and user experience, ongoing research is required to address interoperability, resource management, and security challenges in intelligent mobile and cloud environments.

Privacy Issues in Cross Platform Applications

Types of Sensitive Data and Risks of Data Leakage

Cross-platform applications frequently process diverse categories of sensitive data to deliver personalized and adaptive services. One of the most critical data types is Personally Identifiable Information (PII), which includes names, addresses, phone numbers, and email addresses. Leakage of such information may directly expose users to identity theft and social engineering attacks. In addition to PII, device identifiers, such as digital fingerprints and hash-based identifiers, are commonly collected for analytics and authentication purposes. Studies on device fingerprinting demonstrate that even anonymized identifiers can be exploited for user re-identification when combined with auxiliary data sources (Podsevalov et al., 2024).

Another important category is behavioral data, including user interaction logs, preferences, and activity patterns. Behavioral profiling is widely used in recommender systems and social media platforms, but improper handling of this data can lead to privacy erosion and unauthorized inference of sensitive attributes (Selvakumar, 2024; Sun et al., 2024). Furthermore, health-related information represents one of the most sensitive data categories,

as unauthorized disclosure can result in serious ethical, legal, and economic consequences. User-centric healthcare data sharing platforms illustrate how benefits such as improved service delivery coexist with substantial privacy and security risks (Banton et al., 2021).

The risks of data leakage in cross-platform applications are multifaceted. One major concern is de-identification, where the transmission of device identifiers alongside aggregated or statistical data enables external entities to re-identify users (Podsevalov et al., 2024). Unauthorized access by third-party applications further amplifies privacy risks, as external libraries and integrations may collect and misuse sensitive data without sufficient transparency or control (He et al., 2024; Rajendran & Josanth Smilan, 2024) . In addition, data breaches caused by cyber-attacks can expose large volumes of personal data, posing systemic threats to users and service providers alike. Recent large-scale analyses have shown that cross-user data over-delivery in mobile mini-app ecosystems can even lead to impersonation attacks and direct economic losses (Li et al., 2024).

Privacy Threats in Distributed Processing

Distributed processing architectures are widely adopted in cross-platform systems to support scalability and performance. However, such architectures introduce distinct privacy threats. One critical issue arises during data transmission, where device parameters and user data are automatically sent to remote servers. Without adequate protection, this process becomes vulnerable to interception and inference attacks (Podsevalov et al., 2024).

Data aggregation stages in distributed systems also present privacy challenges. Aggregating data from multiple sources may unintentionally expose individual-level information if access boundaries are not strictly enforced. Research on privacy-preserving distributed processing highlights that excessive data sharing during aggregation significantly increases the risk of privacy leakage (Li et al., 2021).

The presence of diverse adversary models, including passive observers and eavesdropping attackers, further complicates privacy protection in distributed environments. These adversaries can exploit intermediate computations or communication links to infer sensitive information (Li et al., 2021; O'Connor & Kleijn, 2019). Moreover, key management remains a critical vulnerability in distributed privacy-preserving analytics. Weak or poorly coordinated key management schemes can undermine otherwise secure protocols, enabling unauthorized access to protected data (Marquet et al., 2023).

Mitigation Strategies for Privacy Preservation

To mitigate privacy risks in cross-platform and distributed systems, several technical strategies have been proposed. Differential privacy introduces controlled noise into data or computation results, preventing the identification of individual users while preserving statistical utility. This approach has been widely studied as a foundational privacy guarantee in distributed analytics and recommender systems (Li et al., 2021; Sun et al., 2024).

Federated learning represents another promising solution, as it keeps raw data on local devices and only exchanges model updates. By minimizing centralized data collection, federated learning significantly reduces exposure to data leakage risks, particularly in cross-platform environments (Sun et al., 2024). Complementary to this approach, blockchain-based methods have been explored to enable secure, transparent, and auditable data transactions across distributed participants, enhancing trust and accountability in data sharing processes.

Advanced privacy-preserving distributed optimization techniques, such as subspace perturbation, provide mathematical guarantees that sensitive information cannot be reconstructed from shared intermediate results. These methods enable accurate global optimization while protecting local data privacy (Li et al., 2020). Additionally, secure multi-party computation (MPC) allows multiple parties to jointly compute functions over private inputs without revealing the inputs themselves, provided that secure key management mechanisms are in place (Marquet et al., 2023).

Future Research Directions

Despite substantial progress, several open challenges remain in addressing privacy issues in cross-platform applications. Future research must focus on balancing personalization and privacy, ensuring that user-centric services do not compromise individual data protection (Sun et al., 2024). Further improvements are also needed in privacy-preserving algorithms, particularly to enhance computational efficiency and scalability in real-world deployments (Li et al., 2021). Finally, increasing attention must be given to regulatory compliance and data sovereignty, as evolving privacy regulations and data localization requirements impose additional constraints on distributed and cross-platform data processing systems (Kancharla & Madhu Kumar, 2024).

Privacy Issues in Cross-Platform Applications

Sensitive Data in Cross-Platform Ecosystems

Cross-platform applications are designed to operate across multiple operating systems and devices, which often requires broad access to user data and device resources. As a result, these applications commonly process multiple categories of sensitive data, including Personally Identifiable Information (PII), device identifiers, behavioral data, and financial information. PII such as names, addresses, phone numbers, and email addresses can be directly exploited for identity fraud and profiling when leaked (Krych & McDaniel, 2021; Sun et al., 2024). Behavioral data such as activity logs, preferences, and interaction patterns supports personalization and recommendations, yet it may reveal intimate user characteristics through inference (Sun et al., 2024). Financial data (e.g., credit-card and banking information) raises an even higher risk level because misuse can lead to immediate economic losses and long-term harm to users' trust in digital platforms (Krych & McDaniel, 2021).

Beyond explicit personal data, cross-platform applications also collect device identifiers such as digital fingerprints and device hash identifiers. These identifiers are often treated as "technical metadata," but contemporary research shows that fingerprinting can enable user re-identification and persistent tracking across apps and services, particularly when combined with other signals (Podsevalov et al., 2024). Therefore, cross-platform design convenience frequently comes at the cost of enlarged privacy exposure, especially when data flows traverse multiple layers (app, SDK/library, platform services, and external endpoints).

Data Leakage Risks and Attack Surfaces

The privacy risks in cross-platform applications are not only driven by the quantity of data collected but also by how the data is shared, stored, and delivered across components. A major risk is the inadvertent or malicious sharing of sensitive data with third parties. Empirical analysis of Android social applications has linked observed leakage behaviors to gaps between actual data practices and stated privacy policies, suggesting persistent transparency and compliance challenges (Krych & McDaniel, 2021).

A particularly critical phenomenon is cross-user personal data over-delivery (XPO), where an application delivers one user's personal data to another user inappropriately. Large-scale investigations show that mobile mini-app ecosystems can exhibit systematic cross-user leakage, enabling impersonation attacks and causing reputational and economic harm (Li et al., 2022, 2024) . These findings indicate that privacy failures can occur not only through exfiltration to external attackers, but also through flawed internal authorization logic that misroutes data between legitimate users.

Another notable attack surface involves third-party libraries. Modern mobile apps often depend on SDKs for analytics, ads, social integration, and other services. However, third-party libraries may collect sensitive data beyond user expectations or consent boundaries. Research on protecting sensitive data in Android third-party libraries highlights that libraries can become channels for data exposure and advanced attacks, motivating defensive mechanisms that constrain library behavior and prevent leakage (Bhawna et al., 2024). Relatedly, privacy risk can also arise from permission misuse or "hidden" permission behaviors, where permission-driven access creates privacy threats that are difficult for users to perceive and manage (Yilmaz & Davis, 2023).

Privacy Threats in Distributed Processing and Data Mining

Cross-platform applications increasingly rely on distributed infrastructures (cloud services, microservices, edge components, and multi-node data pipelines) to scale computation and analytics. However, distributed processing creates additional privacy threats especially when data is collected and processed across multiple nodes. In such contexts, privacy risks arise from both internal and external adversaries, including those able to exploit weak trust boundaries in distributed architectures (Bhawna et al., 2024).

One key distributed threat is de-identification via device fingerprint transmission, where device parameters and fingerprints transmitted to servers can allow external organizations to infer identity or track individuals across contexts (Podsevalov et al., 2024). Additionally, distributed data mining pipelines can amplify exposure, because data aggregation and replication across nodes increase the number of points where privacy controls can fail (Bhawna et al., 2024). Consequently, privacy protection in cross-platform ecosystems must account for distributed assumptions, heterogeneous nodes, and a broader adversary landscape.

Mitigation Strategies for Privacy Protection

To address privacy issues in cross-platform applications, multiple mitigation strategies have been proposed in recent literature. First, differential privacy provides a principled approach to protect individuals by ensuring that analytical outputs do not reveal sensitive information about any single person. Differential privacy is frequently positioned as a strong privacy guarantee for analytics and recommendation contexts, where utility must be preserved while reducing re-identification risk (Sun et al., 2024).

Second, federated learning reduces leakage risk by allowing models to be trained across decentralized devices without transferring raw data to a central server. This approach supports privacy-preserving personalization, especially in cross-platform recommender systems, although challenges remain regarding attack resistance, system heterogeneity, and communication overhead (Sun et al., 2024).

Third, blockchain-based methods have been explored to enhance privacy and security in distributed systems through transparency, immutability, and auditable transactions. Recent work proposes an anonymous, supervisory cross-chain privacy protocol for zero-trust IoT applications, employing cryptographic strategies to secure cross-chain interactions (Yang et al., 2024). In addition, cross-chain privacy protocols leveraging mechanisms such as zero-knowledge proofs and coin-mixing are positioned as important directions for securing distributed transactions and minimizing traceability in multi-chain environments (Li et al., 2024).

Fourth, access control mechanisms remain foundational for limiting data exposure. Role-based, discretionary, and mandatory access control approaches can reduce the likelihood of data reaching unauthorized actors, yet real-world cross-platform architectures complicate consistent enforcement across endpoints, services, and third-party components (Bhawna et al., 2024). Thus, access control must be integrated with secure design practices, monitoring, and continuous validation of policy enforcement.

Finally, secure multi-party computation (MPC) offers a promising method for collaborative analytics without exposing raw inputs. However, effective MPC depends heavily on secure key management and robust operational frameworks. Research on secure key management for MPC emphasizes that weak key distribution or lifecycle handling can undermine privacy-preserving computation, making key management a central requirement for practical MPC deployment (Marquet et al., 2023).

Emerging Solutions and Future Directions

Recent research emphasizes that improving privacy in cross-platform applications requires solutions that are both technically robust and usable. Privacy-preserving APIs and user-facing privacy panels represent a usability-oriented direction, aiming to provide user-friendly control over data collection and access. For example, a cross-platform privacy-preserving API and privacy panel for extended reality environments demonstrates how privacy controls can be integrated into developer workflows while improving user transparency and agency (Warin et al., 2024).

Looking forward, multiple gaps remain. First, privacy protections must better address cross-user leakage risks in real-world ecosystems, particularly those emerging from authorization errors and over-delivery in large-scale mobile mini-app platforms (Li et al., 2022, 2024). Second, privacy-preserving learning and analytics approaches must be strengthened against sophisticated inference and linkage attacks while maintaining utility (Sun et al., 2024). Third, cross-platform applications increasingly operate under distributed and cross-chain conditions, requiring privacy mechanisms that are resilient under zero-trust assumptions and heterogeneous infrastructures (Li et al., 2024). Collectively, these directions underscore the need for privacy-by-design approaches that combine rigorous guarantees (e.g., differential privacy, MPC), system-level protections (e.g., access control), and usable privacy interfaces (e.g., privacy panels/APIs).

3. Research Method

Research Design

This study adopts a systematic literature-based and analytical research design to investigate privacy issues in cross-platform applications, with a specific focus on sensitive data leakage, distributed processing threats, and privacy-preserving mitigation strategies. The methodology combines systematic literature review, thematic analysis, and conceptual framework development to synthesize existing knowledge and identify research gaps in cross-platform privacy protection.

Data Sources and Selection Criteria

The primary data sources for this study consist of peer-reviewed journal articles, conference proceedings, and book chapters indexed in Scopus. These sources were selected to ensure the quality, credibility, and academic relevance of the literature reviewed. All selected publications fall within the 2021–2024 period to maintain contemporary relevance and reflect recent developments in privacy and data security research.

The selection criteria focus on studies that address privacy issues, sensitive data handling, and security mechanisms in cross-platform, mobile, distributed, and blockchain-based systems. The reviewed studies discuss various aspects, including types of sensitive data, data leakage risks, privacy threats in distributed environments, and privacy-preserving solutions such as differential privacy, federated learning, blockchain technologies, and secure multi-party computation.

Publications that did not directly examine privacy risks or mitigation strategies in cross-platform or distributed environments were excluded from the analysis. This approach ensures that the literature review remains focused and provides a comprehensive understanding of current privacy challenges and solutions in modern computing systems.

Research Procedure

The research procedure was carried out through several systematic stages. First, relevant literature was identified using Scopus metadata by applying keywords related to cross-platform applications, privacy leakage, distributed processing, device fingerprinting, and privacy-preserving techniques. This step ensured comprehensive coverage of studies aligned with the research focus.

Next, the collected literature was screened based on abstracts and full-text reviews to assess its relevance. The selected studies were then classified into thematic categories, including types of sensitive data (such as personally identifiable information, behavioral data, device identifiers, and financial data), privacy threats (including data leakage, cross-user over-delivery, and third-party misuse), risks associated with distributed processing, and privacy-preserving mitigation strategies.

A qualitative thematic analysis was subsequently conducted to identify recurring patterns, technical approaches, and limitations across the selected studies. This analysis facilitated a structured comparison of privacy risks and mitigation techniques across different cross-platform architectures. Finally, based on the synthesis of findings, a conceptual privacy framework was developed to illustrate the relationships between sensitive data sources, privacy threats, mitigation strategies, and emerging solutions in cross-platform applications.

Analytical Framework

The analytical framework illustrates the interaction among four main components within cross-platform and distributed environments. The first component consists of sensitive data sources, including personally identifiable information, device identifiers, behavioral data, and financial data. These data types represent the primary assets that require protection due to their high privacy and security risks.

The second component focuses on privacy threats, such as data leakage, unauthorized access, de-identification, and cross-user over-delivery, which commonly arise in distributed and cross-platform systems. To address these threats, the framework incorporates various mitigation mechanisms, including differential privacy, federated learning, blockchain-based approaches, access control mechanisms, and secure multi-party computation. The final component highlights the expected outcomes of applying these strategies, namely enhanced privacy protection, improved regulatory compliance, and increased user trust. Overall, this framework enables a systematic evaluation of how different privacy-preserving strategies effectively mitigate specific privacy threats in distributed and cross-platform environments.

Validity and Reliability

To ensure the validity of the research, only peer-reviewed publications indexed in Scopus were selected as data sources. This approach guarantees that the analyzed studies meet established academic standards and have undergone rigorous evaluation by experts in the field. Limiting the sources to high-quality and reputable publications helps maintain the credibility and accuracy of the research findings.

Research reliability was strengthened by applying consistent classification criteria throughout the literature analysis process. Each study was systematically reviewed and categorized using the same thematic framework, reducing the risk of subjective bias. In addition, findings were cross-verified across multiple studies to ensure consistency and reproducibility of the identified patterns and conclusions.

Furthermore, the focus on well-established privacy-preserving techniques, such as differential privacy, federated learning, and secure multi-party computation, contributes to the methodological rigor of the study. The reliance on widely recognized and validated approaches enhances confidence in the robustness and reliability of the overall research methodology.

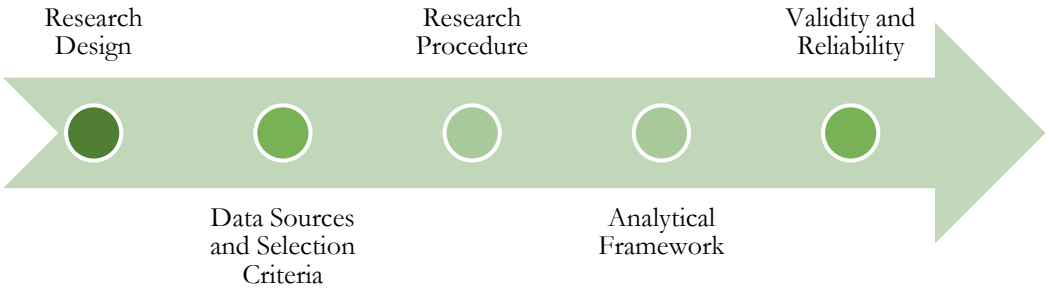

Figure 1. Research Methodology Framework for Privacy Analysis in Cross-Platform Applications.

4. Results and Discussion

Results

This section presents the results of the systematic analysis of privacy issues in cross-platform applications based on selected Scopus-indexed studies. The findings focus on three main aspects: (1) types of sensitive data processed, (2) dominant privacy threats in cross-platform and distributed environments, and (3) commonly adopted privacy-preserving mitigation strategies. The results are summarized using a structured table and a graphical representation to highlight trends and relationships among the identified factors.

Summary of Privacy Issues and Mitigation Techniques

Table 1 summarizes the main types of sensitive data handled by cross-platform applications, associated privacy risks, and mitigation strategies reported in the reviewed literature.

Table1. Sensitive Data Types, Privacy Risks, and Mitigation Strategies in Cross-Platform Applications.

Sensitive Data Type	Main Privacy Risks	Typical Attack Scenarios	Mitigation Strategies
Personally Identifiable Information (PII)	Identity disclosure, profiling	Unauthorized third-party access, policy violations	Differential privacy, access control
Device Identifiers	User re-identification, persistent tracking	Device fingerprinting, de-identification attacks	Data minimization, anonymization
Behavioral Data	Inference of preferences and habits	Cross-user data over-delivery, recommender leakage	Federated learning, differential privacy
Financial Information	Economic loss, fraud	Third-party SDK misuse, data breaches	Encryption, strict access control

Sensitive Data Type	Main Privacy Risks	Typical Attack Scenarios	Mitigation Strategies
Distributed Aggregated Data	Large-scale privacy leakage	Internal/external adversary exploitation	MPC, blockchain-based protection

The table shows that PII and behavioral data are the most frequently discussed sensitive data categories in cross-platform applications, primarily due to their role in personalization and service optimization. However, these data types also pose the highest privacy risks when exposed through third-party libraries or flawed authorization mechanisms. Device identifiers, although often considered technical metadata, present substantial re-identification risks when transmitted across platforms. Financial data, while less frequently analyzed, carries severe consequences upon leakage. Across all data types, the literature consistently emphasizes privacy-preserving computation, decentralized learning, and access control mechanisms as core mitigation strategies.

Graphical Analysis of Privacy Threats and Solutions

To better illustrate the distribution of privacy threats and corresponding mitigation techniques, a conceptual diagram was developed. The diagram highlights the interaction between sensitive data sources, dominant privacy threats, and privacy-preserving solutions in cross-platform environments.

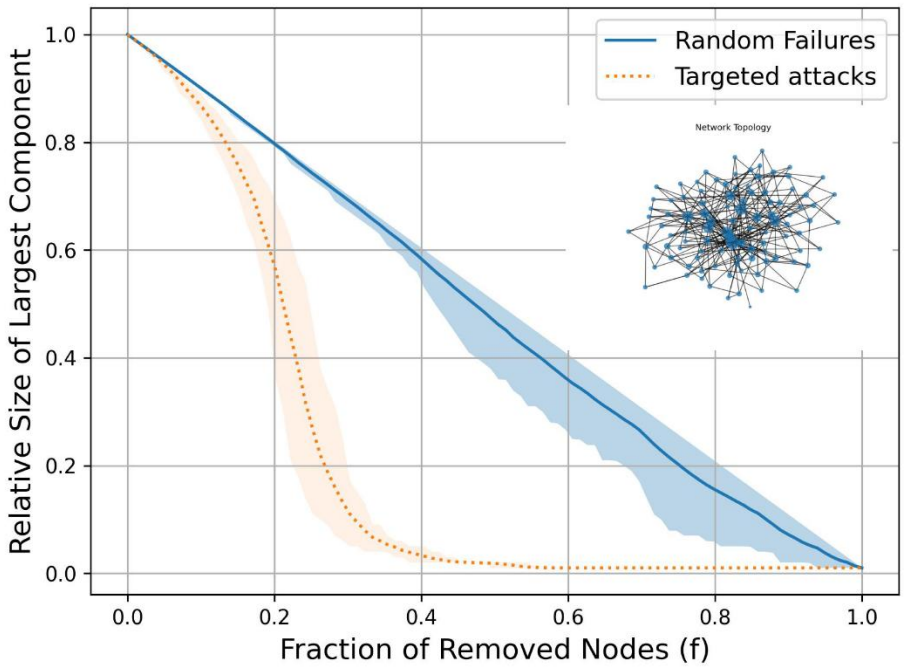

Figure 2. Distribution of privacy threats and mitigation strategies in cross-platform applications.

The diagram shows that data leakage and unauthorized access are the most dominant privacy threats, particularly in applications relying on distributed processing and third-party components. Cross-user personal data over-delivery emerges as a critical but often overlooked risk, especially in mobile mini-app ecosystems. On the mitigation side, differential privacy and federated learning are prominently associated with behavioral data protection, while blockchain-based mechanisms and secure multi-party computation are more commonly applied in distributed and cross-platform data-sharing scenarios. The visualization emphasizes that no single technique can address all privacy risks, reinforcing the need for layered privacy protection strategies.

Discussion

Interpretation of Privacy Risks in Cross-Platform Applications

The results demonstrate that privacy risks in cross-platform applications are deeply influenced by the heterogeneity of platforms and data flows. The coexistence of multiple data types PII, behavioral, financial, and device level data creates complex privacy attack surfaces. As shown in Table 1, privacy threats are not limited to external cyber-attacks but also originate from internal system design flaws, such as improper data delivery logic and insufficient access control. This finding aligns with recent observations that privacy failures increasingly stem from architectural weaknesses rather than isolated vulnerabilities.

Effectiveness of Mitigation Strategies

The analysis indicates that privacy-preserving machine learning techniques, particularly differential privacy and federated learning, are effective for reducing centralized data exposure while maintaining analytical utility. However, as illustrated in Figure 2, these methods primarily address inference risks and are less effective against authorization-related leakage, such as cross-user data over-delivery. In contrast, blockchain-based approaches and secure multi-party computation provide stronger guarantees for distributed trust and collaborative analytics but introduce challenges related to scalability, computational overhead, and key management.

Implications for Cross-Platform System Design

The combined findings from the table and diagram suggest that privacy protection in cross-platform applications must adopt a multi-layered approach. Relying on a single privacy technique is insufficient due to the diversity of threats and data types involved. Instead, effective privacy-by-design strategies should integrate access control, decentralized learning, cryptographic protection, and transparent data governance mechanisms. Furthermore, the prominence of cross-user leakage risks highlights the need for fine-grained authorization models and rigorous data delivery validation, especially in ecosystems with shared execution environments.

Research and Practical Implications

From a research perspective, the results reveal gaps in addressing cross-user privacy leakage and third-party data misuse within existing privacy frameworks. Practically, developers and platform providers must prioritize privacy controls that operate consistently across platforms and execution contexts. The findings also underscore the importance of aligning technical solutions with usability considerations, ensuring that privacy protection does not undermine system performance or user experience.

5. Comparison

Compared to conventional cross platform application architectures that primarily emphasize functionality, performance, and rapid deployment, the privacy oriented approaches analyzed in this study demonstrate a more balanced integration of data utility and user privacy. Traditional cross-platform systems often rely on centralized data collection and extensive third-party integrations, which increase the risk of sensitive data leakage, unauthorized access, and cross-user data over-delivery. In contrast, the privacy-preserving strategies identified in this research such as differential privacy, federated learning, blockchain-based data governance, and secure multi-party computation significantly reduce direct exposure of raw user data by decentralizing processing and enforcing stronger access controls. Furthermore, while conventional solutions typically address privacy through policy level compliance or basic encryption, the approaches reviewed in this study incorporate privacy protection at the architectural and algorithmic levels. This comparison highlights that privacy-aware cross platform designs provide stronger and more systematic privacy guarantees without entirely sacrificing analytical effectiveness, although they may introduce additional computational overhead and system complexity. Overall, the findings suggest that privacy-preserving intelligent computing models represent a more sustainable and trustworthy alternative to traditional cross-platform application designs, particularly in environments that process large volumes of sensitive and distributed user data.

6. Conclusion

This study provides a comprehensive analysis of privacy issues in cross-platform applications, with a particular focus on the handling of sensitive user data in distributed and heterogeneous environments. Based on a systematic review and thematic analysis of recent Scopus-indexed literature, the results demonstrate that cross-platform systems increasingly process diverse categories of sensitive data, including personally identifiable information, device identifiers, behavioral data, and financial information. These data practices significantly expand the attack surface for privacy breaches, especially in the presence of third-party integrations, distributed processing architectures, and cross-user data delivery mechanisms.

The findings reveal that privacy risks in cross-platform applications are not limited to external cyber threats but are also rooted in internal architectural and design weaknesses. Issues such as unauthorized third-party data access, device fingerprint based re-identification, and cross-user personal data over-delivery represent critical and recurring challenges. The analysis further shows that distributed processing, while beneficial for scalability and performance, introduces additional privacy vulnerabilities related to data transmission, aggregation, and key management.

To mitigate these risks, the study highlights the effectiveness of privacy-preserving strategies such as differential privacy, federated learning, blockchain-based data governance, secure multi-party computation, and fine-grained access control mechanisms. While these approaches offer stronger privacy guarantees than conventional centralized models, they also introduce trade offs in terms of system complexity, computational overhead, and implementation cost. Therefore, the results emphasize the necessity of adopting a multi-layered, privacy by design approach that integrates technical, architectural, and governance-level protections.

In conclusion, privacy-preserving cross-platform application designs represent a more robust and sustainable alternative to traditional development paradigms that prioritize functionality over data protection. By embedding privacy considerations at both the algorithmic and system architecture levels, cross-platform applications can achieve a better balance between personalization, performance, and user trust. This study contributes to the existing body of knowledge by synthesizing current privacy challenges and solutions, and it provides a foundation for future research aimed at developing scalable, usable, and regulation-compliant privacy-preserving frameworks for next-generation cross-platform systems.

References

Al-Balasmeh, H. (2024). Cybersecurity in location-based services: Threats, impacts, and mitigation strategies. *Proceedings of the 9th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS 2024).* https://doi.org/10.1109/ICETAS62372.2024.11120213

Arun, C., & Prabu, K. (2021). QoS in the mobile cloud computing environment. In *EAI/Springer innovations in communication and computing* (pp. 171–177). Springer. https://doi.org/10.1007/978-3-030-49795-8_15

Baca, L., Ardiles, N., Cruz, J., Mamani, W., & Capcha, J. (2023). Deep learning model based on a transformers network for sentiment analysis using NLP in sports worldwide. *Communications in Computer and Information Science, 1848*, 328–339. https://doi.org/10.1007/978-3-031-37940-6_27

Banton, M., Bowles, J., Silvina, A., & Webber, T. (2021). On the benefits and security risks of a user-centric data sharing platform for healthcare provision. In *Adjunct publication of the 29th ACM conference on user modeling, adaptation and personalization (UMAP 2021)* (pp. 351–356). https://doi.org/10.1145/3450614.3464473

Bhawna, Z., Z. Z., & Parihar, V. (2024). Approaches and methodologies for distributed systems: Threats, challenges, and future directions. In *Meta-heuristic algorithms for advanced distributed systems* (pp. 67–84). Wiley. https://doi.org/10.1002/9781394188093.ch5

Candan, D., & Kalay, M. U. (2024). Sensitive data detection in database systems using machine learning. In *Proceedings of the 2024 Innovations in Intelligent Systems and Applications Conference (ASYU 2024).* https://doi.org/10.1109/ASYU62119.2024.10756975

Chahar, S., Kaswan, K. S., Aggarwal, A., & Dhatterwal, J. S. (2024). New era of IoT with cloud computing: A review of technology, issues and challenges. In *Proceedings of the 2nd International Conference on Advancements and Key Challenges in Green Energy and Computing (AKGEC 2024).* https://doi.org/10.1109/AKGEC62572.2024.10868472

Daudén-Esmel, C., Castellà-Roca, J., & Viejo, A. (2024). Blockchain-based access control system for efficient and GDPR-compliant personal data management. *Computer Communications, 214*, 67–87. https://doi.org/10.1016/j.comcom.2023.11.017

Delgado-Santos, P., Stragapede, G., Tolosana, R., Guest, R., Deravi, F., & Vera-Rodriguez, R. (2022). A survey of privacy vulnerabilities of mobile device sensors. *ACM Computing Surveys, 54*(11s), Article 3510579. https://doi.org/10.1145/3510579

Domingo-Ferrer, J., Farràs, O., Ribes-González, J., & Sánchez, D. (2019). Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges. *Computer Communications, 140–141*, 38–60. https://doi.org/10.1016/j.comcom.2019.04.011

Faber, B., Michelet, G., Weidmann, N., Mukkamala, R. R., & Vatrapu, R. (2019). BPDIMS: A blockchain-based personal data and identity management system. In *Proceedings of the Annual Hawaii International Conference on System Sciences* (pp. 6855–6864).

He, F., Wang, J., Huang, Y., Peng, X., & Zhang, Y. (2024). LibGuard: Protecting sensitive data in Android third-party libraries from XLDH attacks. In *Proceedings of the International Conference on Computer Communications and Networks (ICCCN 2024).* https://doi.org/10.1109/ICCCN61486.2024.10637585

Jiang, C., Qiu, Y., Gao, H., Fan, T., Li, K., & Wan, J. (2019). An edge computing platform for intelligent operational monitoring in Internet data centers. *IEEE Access, 7*, 133375–133387. https://doi.org/10.1109/ACCESS.2019.2939614

Kancharla, J. R., & Madhu Kumar, S. D. (2024). Advancing data sovereignty in distributed environments: An in-depth exploration of data localization challenges. In *Proceedings of the International Conference on Computer, Electronics, Electrical Engineering and Their Applications (IC2E3 2024).* https://doi.org/10.1109/IC2E362166.2024.10827688

Krych, D. E., & McDaniel, P. (2021). Exposing Android social applications: Linking data leakage to privacy policies. *Journal of Cyber Security Technology, 5*(3–4), 139–190. https://doi.org/10.1080/23742917.2019.1630093

Kulkarni, A., Shea, C., Homayoun, H., & Mohsenin, T. (2017). LESS: Big data sketching and encryption on low power platform. In *Proceedings of the Design, Automation and Test in Europe Conference (DATE 2017)* (pp. 1631–1634). https://doi.org/10.23919/DATE.2017.7927253

Li, Q., Gundersen, J. S., Heusdens, R., & Christensen, M. G. (2021). Privacy-preserving distributed processing: Metrics, bounds and algorithms. *IEEE Transactions on Information Forensics and Security, 16*, 2090–2103. https://doi.org/10.1109/TIFS.2021.3050064

Li, Q., Heusdens, R., & Christensen, M. G. (2020). Privacy-preserving distributed optimization via subspace perturbation: A general framework. *IEEE Transactions on Signal Processing, 68*, 5983–5996. https://doi.org/10.1109/TSP.2020.3029888

Li, S., Yang, Z., Hua, N., Liu, P., Zhang, X., Yang, G., & Yang, M. (2022). Collect responsibly but deliver arbitrarily? A study on cross-user privacy leakage in mobile apps. In *Proceedings of the ACM Conference on Computer and Communications Security* (pp. 1887–1900). https://doi.org/10.1145/3548606.3559371

Li, S., Yang, Z., Yang, Y., Liu, D., & Yang, M. (2024). Identifying cross-user privacy leakage in mobile mini-apps at a large scale. *IEEE Transactions on Information Forensics and Security, 19*, 3135–3147. https://doi.org/10.1109/TIFS.2024.3356197

Marquet, E., Moeyersons, J., Pohle, E., Van Kenhove, M., Abidin, A., & Volckaert, B. (2023). Secure key management for multi-party computation in MOZAIK. In *Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroSPW 2023)* (pp. 133–140). https://doi.org/10.1109/EuroSPW59978.2023.00020

Murphy, B. B., & Japheth, B. R. (2022). Principles and application of mobile cloud computing in payments and health care solution. *Lecture Notes in Computer Science, 13337*, 399–407. https://doi.org/10.1007/978-3-031-05014-5_33

O'Connor, M., & Kleijn, W. B. (2019). Finite approximate consensus for privacy in distributed sensor networks. In *Proceedings of the International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT 2019)* (pp. 75–77). https://doi.org/10.1109/PDCAT46702.2019.00025

Pimenta Rodrigues, G. A., Marques Serrano, A. L., Lopes Espiñeira Lemos, A. N., Canedo, E. D., de Mendonça, F. L. L., de Oliveira Albuquerque, R., Sandoval Orozco, A. L., & García Villalba, L. J. (2024). Understanding data breach from a global perspective: Incident visualization and data protection law review. *Data, 9*(2), Article 27. https://doi.org/10.3390/data9020027

Podsevalov, I., Podsevalov, A., & Korkhov, V. (2024). Analysis of privacy leakage risks in the context of security threats associated with digital device fingerprinting. *Lecture Notes in Computer Science, 14821*, 386–404. https://doi.org/10.1007/978-3-031-65308-7_27

Rajendran, R. K., & Josanth Smilan, A. (2024). Data privacy and security risks in third-party app integrations. In *Analyzing privacy and security difficulties in social media: New challenges and solutions* (pp. 311–334). https://doi.org/10.4018/979-8-3693-9491-5.ch014

Selvakumar, P. (2024). Factors influencing social media privacy. In *Analyzing privacy and security difficulties in social media: New challenges and solutions* (pp. 15–38). https://doi.org/10.4018/979-8-3693-9491-5.ch002

Seo, B. (2023). A case study of combining two cross-platform development frameworks for storybook mobile app. *KSII Transactions on Internet and Information Systems, 17*(12), 3345–3363. https://doi.org/10.3837/tiis.2023.12.007

Shanthi, A. L., & Ramesh, V. (2019). Secured and dynamic decentralized computational offloading framework for mobile cloud computing. *International Journal of Innovative Technology and Exploring Engineering, 8*(11), 2589–2593. https://doi.org/10.35940/ijitee.K1876.0981119

Sharma, P., Singh, A., & Jatain, A. (2020). Cognitive computing for smart communication. In *Machine learning and cognitive computing for mobile communications and wireless networks* (pp. 73–90). Wiley. https://doi.org/10.1002/9781119640554.ch4

Song, C. (2022). Interactive development of cross-border e-commerce and new Internet economy based on digital technology. *Journal of Commercial Biotechnology, 27*(4), 176–188. https://doi.org/10.5912/jcb1467

Sun, Z., Wang, Z., & Xu, Y. (2024). Privacy protection in cross-platform recommender systems: Techniques and challenges. *Wireless Networks, 30*(8), 6721–6730. https://doi.org/10.1007/s11276-023-03509-z

Warin, C., Seeger, D., Shams, S., & Reinhardt, D. (2024). PrivXR: A cross-platform privacy-preserving API and privacy panel for extended reality. In *2024 IEEE International Conference on Pervasive Computing and Communications Workshops and Other Affiliated Events (PerCom Workshops 2024)* (pp. 417–420). https://doi.org/10.1109/PerComWorkshops59983.2024.10503341

Yanuargi, B., Utami, E., Kusrini, & Parikesit, A. A. (2024). Location-based service insights: A comprehensive review of data mining objects. In *Proceedings of the International Conference on Artificial Intelligence and Mechatronics System (AIMS 2024).* https://doi.org/10.1109/AIMS61812.2024.10513296

Yilmaz, S., & Davis, M. (2023). Hidden permissions on Android: A permission-based Android mobile privacy risk model. In *Proceedings of the European Conference on Information Warfare and Security (ECCWS 2023)* (pp. 717–724). https://doi.org/10.34190/eccws.22.1.1453

Zhou, C., Zhou, T., & Bai, W. (2018). The key study of the integration between smartphone NFC technology and ERP system. In *Proceedings of the 2018 3rd IEEE International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)* (pp. 500–505). https://doi.org/10.1109/ICCCBDA.2018.8386567