International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)
https://ijcjournal.org/index.php/InternationalJournalOfComputer/index

Best Practices for Personal Data Protection in Scalable Enterprise Applications

Serhii Onishchenko*

Senior Software Engineer, Scalable Solutions Expert, Architectural Innovator & AI Specialist, Caterpillar, 540 W, Chicago, USA

Email: serhiy.onishchenko@gmail.com

Abstract

This article examines existing methods for protecting personal data in corporate applications, considering modern challenges in dynamic and distributed cloud environments. The study includes an extensive analysis of encryption techniques, such as proxy encryption, DNA encryption, dual encryption with fragmentation, and homomorphic encryption, as well as mechanisms for ensuring data integrity and access control. These mechanisms include cryptographic hash functions, digital signatures, message authentication codes (MAC), role-based and attribute-based access control, federated authentication, and multi-factor authentication. The research also reviews publicly available studies found on the Internet. Particular attention is given to the specifics of data protection in cloud infrastructures, where high intensity, data fragmentation, and the lack of physical security control necessitate architectural solutions such as Trusted Virtual Data Centre (TVDc) and Tera Architecture, along with the integration of security measures into the software development lifecycle (SDLC). The materials presented in this study are relevant to researchers, system architects, and corporate IT infrastructure practitioners seeking to synthesize theoretical and empirical approaches to achieve a high level of information security in the face of rapidly evolving threats.

Keywords: personal data protection; scalable corporate applications; proxy encryption; homomorphic encryption; data integrity; access control; cloud computing; dynamic cloud environments; TVDc; SDLC.

1. Introduction

With the rapid development of scalable corporate applications and the continuous growth of processed personal data, ensuring data security has become a critical challenge.

Received: 2/3/2025
Accepted: 4/10/2025
Published: 4/22/2025

---

* Corresponding author.

Modern enterprises increasingly rely on cloud technologies, which provide flexibility and scalability but also introduce new vulnerabilities and increase the risk of unauthorized access to confidential information. In this context, the application of advanced encryption methods, such as proxy encryption, DNA encryption, dual encryption with data fragmentation, and homomorphic encryption, along with comprehensive access control and data integrity mechanisms, has become essential for enhancing the protection of personal information in dynamic and distributed IT environments.

The current landscape of personal data protection in scalable corporate applications exhibits a variety of approaches, as reflected in the literature. Raja and his colleagues in [1] analyze security and privacy challenges in cloud computing, identifying existing gaps in modern approaches and proposing solutions to overcome them. Similarly, Mahalingam and her colleagues in [2] present an innovative approach to cryptographic key generation based on neural network attractors using DNA-coded schemes. Their methodology combines neural network modeling with empirical validation, highlighting the scientific novelty of the proposed solution.

Shuford and his colleagues in [5] explores the application of artificial intelligence algorithms to enhance accessibility technologies for individuals with disabilities. Meanwhile, the studies conducted by Schwartz and his colleagues in [6] and Pindi and his colleagues in [7] demonstrate the use of complex computational models for analyzing dynamic processes in biological systems. Additional perspectives on methodological advancements are presented by Ahsan and Senapati[8] and Dixit and her colleagues in [9], who integrate quantum mechanics/molecular mechanics (QM/MM) calculations with experimental validation to study biochemical reaction mechanisms, such as epoxide ring cleavage and the inhibition of key biomolecular processes.

Hasan and his colleagues in [10] investigate interpretable artificial intelligence models for credit card fraud detection. Their study hypothesizes that explainable AI algorithms enhance the transparency and reliability of automated systems, which is particularly relevant for scalable corporate applications. Padmapriya and her colleagues in [3] demonstrate, for the first time, the integration of elliptic curve cryptography (ECC) with SC-FDMA technology for secure data transmission in mission-critical environments. Similarly, Sowmya and her colleagues [4] develop and implement the Chao-Cryptic architecture based on FPGA, designed to secure audio communication.

A notable research gap lies in the insufficient integration of modern encryption methods with data integrity and access control measures within a unified security framework for dynamic and distributed cloud environments. While individual technologies have been analyzed, the lack of a comprehensive approach to combining advanced cryptographic solutions with infrastructural security mechanisms presents a research gap that requires further investigation.

The objective of this article is to analyze methods for protecting personal data in scalable corporate applications.

The scientific novelty of the study lies in the analysis of existing publications, which has identified previously unexplored interconnections between personal data protection methods in scalable corporate applications,

outlining their advantages and limitations.

A limitation of this study is the lack of empirical verification of the integration of the proposed data protection methods, making it difficult to assess their effectiveness and adaptability in real-world dynamic distributed cloud infrastructures. Additionally, the high computational costs and complexity of managing processes related to homomorphic encryption and dual encryption with fragmentation limit the practical scalability and applicability of these methods in corporate systems.

The proposed hypothesis suggests that implementing a multi-layered security system that integrates advanced encryption methods with robust access control mechanisms and continuous security monitoring will reduce the risk of personal data breaches and unauthorized collection in scalable corporate applications, even within dynamically evolving cloud infrastructures.

To achieve this objective, an extensive review of contemporary literature covering research in cryptography and information security has been conducted.

2. Modern encryption methods for personal data protection

Modern encryption methods not only protect data from external attacks but also enable computations on encrypted data without exposing the original information. Proxy encryption is a technique that allows a trusted intermediary to convert encrypted text from one key to another without revealing the underlying data. This approach significantly reduces the risk of key material compromise, as the intermediary itself does not have access to plaintext data. DNA encryption, in turn, utilizes bio-inspired algorithms that model the structure and complexity of DNA, adding another layer of security against adversaries and enhancing system resilience to attacks [1, 2]. The combination of proxy encryption and DNA encryption presents a promising approach for developing adaptive and multi-layered personal data protection systems.

Dual encryption is based on the sequential application of two independent cryptographic algorithms to the original data. This approach increases decryption complexity, even if one of the algorithms is compromised. Additionally, data fragmentation—the process of dividing an information block into multiple parts stored on different servers or network segments—provides an additional layer of security. Even if a single node is breached, this method ensures that the complete dataset remains protected. The combination of dual encryption with data fragmentation minimizes potential vulnerabilities in distributed systems.

Homomorphic encryption is an advanced method that enables computations on encrypted data without the need for decryption. This approach ensures that confidential information remains secure throughout the entire processing cycle, which is particularly crucial for cloud computing and distributed systems [1, 5]. Despite its clear security advantages, homomorphic encryption requires significant computational resources and is currently limited in practical application for high-performance systems. Modern research is focused on optimizing homomorphic encryption algorithms to reduce computational overhead while maintaining a high level of data security.

To provide a clearer understanding of each approach, Table 1 presents a comparative analysis of encryption methods.

Table 1: Comparative analysis of modern encryption methods for personal data protection [3, 7].

Encryption Method	**Key Features**	**Advantages**	**Limitations / Application Scope**
Proxy Encryption	Enables the transformation of encrypted data using different keys without revealing plaintext	Flexible access management; reduced key compromise risk	Requires a trusted intermediary; increased implementation complexity
DNA Encryption	Utilizes algorithms that mimic the complex biological structure of DNA	Enhanced resistance to cryptanalysis; inherent structural complexity	Experimental stage; limited processing speed
Dual Encryption with Fragmentation	Applies two sequential encryption algorithms and splits data into fragments	Minimizes leakage risk in case of node compromise; distributed storage	Increased computational overhead; complex management of fragmented data
Homomorphic Encryption	Enables computations on encrypted data without decryption	High confidentiality during data processing	Requires substantial computational resources; limited scalability in real-world systems

The integration of proxy encryption, DNA encryption, dual encryption with data fragmentation, and homomorphic encryption establishes a multi-layered system for protecting personal data. Each of these methods offers distinct advantages and limitations, making their combination an effective strategy for achieving optimal security in scalable corporate applications. Ongoing research in this field continues to focus on enhancing algorithm efficiency and reducing computational complexity, which remains a key direction for advancing data protection systems.

3. Mechanisms for ensuring data integrity and access control

Ensuring data integrity involves applying cryptographic methods that maintain the immutability of information during storage and transmission. The following mechanisms play a fundamental role in this field:

- Cryptographic hash functions: Any modification to the original data results in a drastic change in the hash value, allowing for the rapid detection of data compromise [1].

- Digital signatures: This mechanism combines data integrity and authentication. Using asymmetric algorithms (e.g., RSA or elliptic curve cryptography), the sender generates a digital signature that allows the recipient to verify that the data has not been altered and originates from the stated source [5].
- Message Authentication Code (MAC): By utilizing a secret key in combination with a hashing algorithm, MAC generates an authentication code for a message. This approach ensures both data integrity and authentication in symmetric encryption environments, making it particularly effective for secure data exchange between trusted parties [9].

Each of these mechanisms has specific advantages and limitations. Hash functions provide high computational speed but do not guarantee sender authentication. Digital signatures enable source verification but require greater computational resources. MAC reduces computational overhead but relies on the secure distribution of secret keys.

Access control is a crucial aspect of data security, as even robust integrity protection cannot prevent information leakage in cases of unauthorized access. Modern access management approaches include the following mechanisms:

- Role-Based Access Control (RBAC): Based on assigning permissions according to user roles, RBAC simplifies access rights management in scalable systems. This centralized control minimizes errors in permission assignments.
- Attribute-Based Access Control (ABAC): Unlike RBAC, ABAC uses attributes related to users, resources, and environmental factors. This enables a more flexible and granular access control model, adapting to the dynamic requirements of modern corporate systems [1].
- Federated Authentication and SAML: Standards such as Security Assertion Markup Language (SAML) facilitate Single Sign-On (SSO), allowing users to access distributed resources using a single authentication process. This simplifies access management in multi-service and cloud environments.
- Multi-Factor Authentication (MFA): MFA requires multiple independent factors for user verification (e.g., password, token, biometric data). This significantly reduces the risk of credential compromise, even if one factor is compromised [2, 7].

An effective combination of these mechanisms creates a multi-layered security system where data integrity measures are closely integrated with access control strategies, minimizing both internal and external threats.

To illustrate the advantages and limitations of different data integrity and access control methods, Table 2 presents a comparative analysis.

Table 2: Comparative analysis of data integrity and access control mechanisms [1, 4, 5].

Mechanism Type	**Example/Method**	**Key Advantages**	**Limitations / Considerations**
Hash Functions	SHA-256, SHA-3	High computational speed; one-way function allows for detecting unauthorized modifications	Do not ensure sender authentication; vulnerable to collisions in outdated algorithms (e.g., MD5)
Digital Signatures	RSA, ECDSA	Guarantee data integrity, authenticity, and immutability; provide legally recognized verification	Computationally intensive; require public key infrastructure (PKI) management
MAC	HMAC (based on SHA-256)	Ensures integrity and authentication with low computational cost; effective for trusted data exchange	Relies on secret key distribution; complexity in securely managing shared keys
Role-Based Access Control (RBAC)	Role-based models	Simplifies access rights management; centralized control of access policies; suitable for static organizational structures	Limited flexibility in dynamic role and permission changes; does not consider request context
Attribute-Based Access Control (ABAC)	Attribute-based models	High flexibility; accounts for context (location, time, device type); scalable	Complex policy implementation and management; requires precise attribute definition and updates
Federated Authentication (SSO, SAML)	SAML 2.0, OpenID Connect	Enables Single Sign-On and simplifies account management in distributed systems; enhances convenience and security through centralized authentication	Depends on a central identity provider; potential risks if the central service is compromised
Multi-Factor Authentication (MFA)	Combination of password, token, and biometrics	Significantly reduces the risk of unauthorized access, even if one factor is compromised; enhances security levels	Requires additional hardware and configuration; may reduce user convenience

Thus, integrating cryptographic integrity mechanisms (hash functions, digital signatures, MAC) with modern access control methods (RBAC, ABAC, federated authentication, and MFA) establishes a robust foundation for securing information in scalable corporate systems. A comprehensive approach not only enables the timely detection and prevention of unauthorized data modifications but also ensures effective access management, which is particularly important in dynamic cloud environments.

4. Data protection features in dynamic and distributed cloud environments

Cloud environments are characterized by high intensity, elasticity, and workload fragmentation, creating opportunities for scalability while also posing significant challenges to information security. Traditional security measures often prove insufficient under these conditions, and emerging threats require specialized approaches that consider the unique aspects of distributed architecture and dynamically changing configurations.

One of the primary challenges is the dynamic nature of cloud environments. Automatic scaling, periodic migration of virtual machines, and changes in resource configurations require continuous monitoring and adaptive security management. While elasticity enables timely responses to workload fluctuations, it complicates centralized asset management, as cloud workloads may be distributed across multiple geographic regions [1]. This distribution introduces synchronization and access control challenges and complicates the timely application of security updates.

Furthermore, data fragmentation in distributed systems increases the risk of compromise. Data divided into fragments and stored on different servers or data centers requires specialized protection mechanisms. Concepts such as Trusted Virtual Data Centre (TVDc) are employed to create isolated and trusted service execution environments within Infrastructure-as-a-Service (IaaS) frameworks. Additionally, architectural solutions like Tera Architecture establish isolated "closed spaces" for virtual machines, restricting attackers' capabilities even if they obtain privileged access [9, 10].

In cloud computing, the responsibility for physical infrastructure security largely shifts to service providers. This situation removes direct physical security control from the client organization, necessitating compensatory measures such as enhanced encryption, network segmentation, and access control. As a result, the risk of data leakage during transmission between distributed nodes increases, requiring additional transport-level security measures such as VPN, TLS, and SSL.

Another critical challenge is inter-virtual machine attacks, including side-channel attacks, where attackers can extract information by analyzing parallel computing processes between virtual machines. To mitigate these threats, independent security policies are developed to limit attackers' capabilities through strict isolation of virtual instances and the implementation of specialized monitoring mechanisms.

Modern approaches to cloud data protection include not only infrastructure-level measures but also security integration throughout the software development lifecycle (SDLC). This approach ensures that security principles are embedded from the outset, significantly reducing vulnerabilities in the final product. In addition to technical measures, attention is given to the role of service providers, who offer configurable security

parameters through various platform-as-a-service (PaaS) solutions [1].

To provide a better understanding of data protection specifics in dynamic and distributed cloud environments, Table 3 presents a comparative analysis of key aspects.

Table 3: Comparative analysis of data protection features in dynamic and distributed cloud environments (compiled by the author based on [1, 3, 6]).

Protection Aspect	**Key Challenges**	**Solutions**	**Advantages / Limitations**
Cloud environment dynamism	Rapid scaling, frequent configuration changes, difficulty in centralized monitoring	Continuous monitoring, adaptive security systems, integration of security measures into SDLC	Flexibility and rapid response; high computational and monitoring system demands
Data fragmentation and distribution	Data spread across multiple locations, challenges in centralized asset management	Use of TVDc and Tera Architecture for creating isolated and trusted environments	Increased security through isolation; complexity in integration and administration
Lack of physical security control	Responsibility for physical security lies with cloud service providers, risk of data leaks during transmission	Transport-level encryption (TLS, VPN), independent security policies, regular audits	Reduced data leakage risks; dependency on provider reliability and difficulty in physical infrastructure control
Inter-virtual machine threats (side-channel attacks)	Potential data leaks through inter-VM process analysis	Virtual machine isolation, independent security measures, dedicated monitoring mechanisms	High security through isolation; possible performance impact and increased implementation costs

Thus, the characteristics of dynamic and distributed cloud environments necessitate a comprehensive and multi-layered approach to data protection. Integrating infrastructure solutions such as TVDc and Tera Architecture with transport-level security measures and embedding security principles into the SDLC allows for robust protection even in rapidly evolving and distributed architectures. Despite the evident advantages of these approaches, their implementation entails high computational costs and requires continuous monitoring, highlighting the need for further research and refinement of cloud security systems.

5. Conclusion

Modern personal data protection in scalable corporate applications requires a multi-layered and integrated approach. The analysis of the presented methods demonstrated that the application of advanced cryptographic technologies, such as proxy encryption with DNA-based encryption elements, dual encryption with fragmentation, and homomorphic encryption, enhances information security by minimizing the risk of key material compromise, even in cases of attacks on individual system nodes.

Additionally, the comprehensive use of data integrity mechanisms, including hash functions, digital signatures, and MAC, in combination with modern access control systems (RBAC, ABAC, federated authentication, and multi-factor authentication), provides additional protection against unauthorized access and internal threats.

Security challenges in distributed cloud environments necessitate the implementation of specialized architectural solutions such as TVDc and Tera Architecture, along with the integration of security measures into the SDLC. This approach ensures that security aspects are proactively considered during the development and operation of systems.

Thus, a comprehensive strategy that combines advanced encryption methods, data integrity assurance, and sophisticated access control mechanisms represents an effective solution for safeguarding personal data in modern scalable corporate applications.

References

[1]. V. Raja et al. “Exploring challenges and solutions in cloud computing: A review of data security and privacy concerns.” *Journal of Artificial Intelligence General science (JAIGS)*, vol. 4, pp.121-144, 2024.

[2]. H. Mahalingam et al. “Neural attractor-based adaptive key generator with DNA-coded security and privacy framework for multimedia data in cloud environments.” *Mathematics*, vol. 11, pp.1–10, 2023.

[3]. V. M. Padmapriya et al. “ECC joins first time with SC-FDMA for Mission “security”.” *Multimedia Tools and Applications*, vol.79, pp. 17945-17967, 2020.

[4]. B. Sowmya et al. “Design and Implementation of Chao-Cryptic Architecture on FPGA for Secure Audio Communication.” *Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS*, vol.3, pp. 135-144, 2020.

[5]. J. Shuford. “Contribution of Artificial Intelligence in Improving Accessibility for Individuals with Disabilities.” J*ournal of Knowledge Learning and Science Technology*, vol. 2, pp. 421-433, 2023.

[6]. E. A. Schwartz et al. “RNA targeting and cleavage by the type III-Dv CRISPR effector complex.” *Nature communications*, vol. 15, pp. 1-9, 2024

[7]. C. Pindi et al. “Molecular basis of differential stability and temperature sensitivity of ZIKA versus dengue virus protein shells.” *Scientific Reports*, vol. 10, pp. 1-10, 2020.

[8]. M. Ahsan and S. Senapati. “Water plays a cocatalytic role in epoxide ring opening reaction in aspartate proteases: a QM/MM study.” *The Journal of Physical Chemistry B*, vol.123, pp. 7955-7964, 2019.

[9]. S. M. Dixit, M.Ahsan and S. Senapati. “Steering the lipid transfer to unravel the mechanism of cholesteryl ester transfer protein inhibition.” *Biochemistry*, vol. 58, pp. 3789-3801, 2019.

[10]. M. R. Hasan, M. S. Gazi and N. Gurung. “Explainable AI in Credit Card Fraud Detection: Interpretable Models and Transparent Decision-making for Enhanced Trust and Compliance in the USA.” *Journal of Computer Science and Technology Studies*, vol. 6, pp.1-12, 2024.