THE USA JOURNALS
THE AMERICAN JOURNAL OF ENGINEERING AND TECHNOLOGY (ISSN – 2689-0984)
VOLUME 06 ISSUE12

PUBLISHED DATE: - 18-12-2024
DOI: - https://doi.org/10.37547/tajet/Volume06Issue12-13 PAGE NO.: - 141-149

RESEARCH ARTICLE Open Access

THE BASICS OF CREATING SECURE DATA ARCHITECTURES FOR FINANCIAL ORGANIZATIONS

Di Feng
Director of Cyber Data Risk & Resilience Division, China/Canada (Montreal, Quebec)

Abstract
The article discusses approaches to the development of systems that minimize the risks of unauthorized access, leaks, and data integrity violations. Special attention is paid to the introduction of security mechanisms at the design stage, the adaptation of architectural models to the conditions of the digital economy, and the use of modern technologies. Due to increased cyber threats and changes in the norms that determine the need to create secure data architectures in financial organizations. The work is based on the concepts of Privacy by Design and security by Design, as well as technological solutions, including blockchain, and adaptive authentication.
The approaches presented in the article include micro-segmentation of networks to isolate components, restriction of user privileges, and the use of cryptographic methods to protect information. These measures ensure compliance with the requirements of the digital environment. Scientific articles by foreign authors, as well as materials that are publicly available on the Internet, were used as sources.
The information presented in the article is intended for professionals involved in information security, system architecture development, and project management in the financial sector. They will also be useful to other scientific specialists. The focus of the work is on the need for an integrated approach, updating solutions in response to modern threats.

Keywords Data architecture, financial organizations, information security, blockchain, Privacy by Design, Security by Design.

INTRODUCTION

The financial sector is transforming the influence of digitalization, resulting in increased data volumes and their significance for business operations. Ensuring information security has become a primary concern for organizations in the financial domain. Modern threats, including cyberattacks, data breaches, and technological vulnerabilities, demand new architectural approaches to safeguard systems.

The rising number of incidents disrupting financial systems leads to asset losses and decreased client trust. The tightening of regulatory requirements, such as GDPR and PCI DSS, compels companies to revise their processes to align with current standards. Concepts such as Privacy by Design and Security by Design are increasingly applied in system development, driven by the adoption of technologies like blockchain and artificial intelligence.

The purpose of this study is to analyze approaches to designing architectures that ensure information security in the financial sector. The research examines principles that help minimize data leakage risks and provides recommendations aimed at improving system resilience against various threats.

METHODS

Contemporary research on data protection, architectural approaches in financial services, and the integration of technologies into the digital economy spans several thematic areas. Each direction focuses on developing resilient solutions capable of meeting the demands of digital transformation.

Studies on information security emphasize integrating security mechanisms into the design process. The concept of Privacy by Design, described in the work of Babu M. S., Raj K. B., and Devi D. A. [1], focuses on preserving confidentiality through architectural approaches. Ebad S. A. [3] explores secure programming as a means of eliminating vulnerabilities during development. The principles of Security by Design, highlighted in the study by Awaysheh F. M. et al. [5], aim to mitigate risks associated with data processing in cloud environments. Methods for building systems resistant to data leaks are presented in the publication by Yee G. O. M. A. [9].

Architectural approaches in financial services emphasize adapting systems to changes in the economic environment. The work of Wedha B. Y., Vasandani M. S., Wedha A. E., et al. [2] discusses the transformation of online services to meet market demands. Massacci F., and Ngo C. N. [4] examine challenges in designing distributed platforms and propose solutions for overcoming them. Pashtova, L. [6] investigates structural changes in corporate architecture driven by digitalization. The article by Cen T. [8] describes the application of blockchain technology in financial management.

The use of technology for developing architectural solutions involves studying innovative approaches. Boldrin L., Sellitto G. P., and Tepandi J. [10] analyze the TOOP architecture, aimed at creating a transparent interaction system between organizations. Pflughoeft K. A., Soofi E. S., and Soyer R. [7] present data management methods based on entropy models. Kristiana I. et al. [12] explore the use of data in banking, where architectural approaches enhance the efficiency of business processes.

The article China Data Protection and Cybersecurity: Annual Review of 2023 and Outlook for 2024 [14], published on www.twobirds.com, outlines changes in Chinese legislation, including data protection requirements for companies to comply with new regulations. The author organizes information on recent legislative initiatives, emphasizing the potential developments in cybersecurity. This enables professionals to prepare for potential adjustments in the application of new legal acts in advance.

The source 3-month Countdown to China's New Data Security Regulation [15], published on rouse.com, examines business preparations for implementing Chinese data security standards. It focuses on the practical aspects of compliance, reporting requirements, and mandatory measures for information protection. The article provides steps companies need to take to meet the new standards.

The article Financial Services [13], hosted on cpl.thalesgroup.com, centers on data security issues in the financial sector, emphasizing the importance of protecting confidential information and preventing leaks. It discusses technical solutions that ensure the security of transactions and data protection. Tools and methods aimed at reducing the risk of data breaches and ensuring operational stability amid digital threats are also described.

Different authors focus on various aspects of data protection and architectural solutions. Some concentrate on conceptual design issues, while others develop technological approaches. The implementation of new systems into existing financial sector structures presents challenges. The economic feasibility of using such solutions requires further study.

The analysis of the reviewed areas supports the development of solutions tailored to the conditions of the digital environment. Technological approaches that consider the specifics of organizational processes form the basis for creating integrated systems that ensure stability and security.

Various methods were employed in this study. The theoretical component included the examination of scientific works, regulatory acts, and practical recommendations related to the design of secure data architectures. The Privacy by Design, Security by Design, and Zero Trust approaches were evaluated using methods focusing on their features in the financial sector.

The results of the research formed the basis for recommendations aimed at creating reliable data protection mechanisms for financial organizations. The applied methods facilitated the organization of information, identification of significant risk factors, and the proposal of pathways for developing architectural solutions.

RESULTS AND DISCUSSION

The creation of secure data architectures in the financial sector relies on the application of technologies, organizational solutions, and compliance with regulatory requirements. Information related to client data, transactions, analytical reports, and management strategies is of significant interest to malicious actors. Threats originate from external sources and internal factors, including employee errors, vulnerabilities in integration processes, and violations of security policies. Figure 1 below illustrates the process of creating secure data architectures for financial organizations.

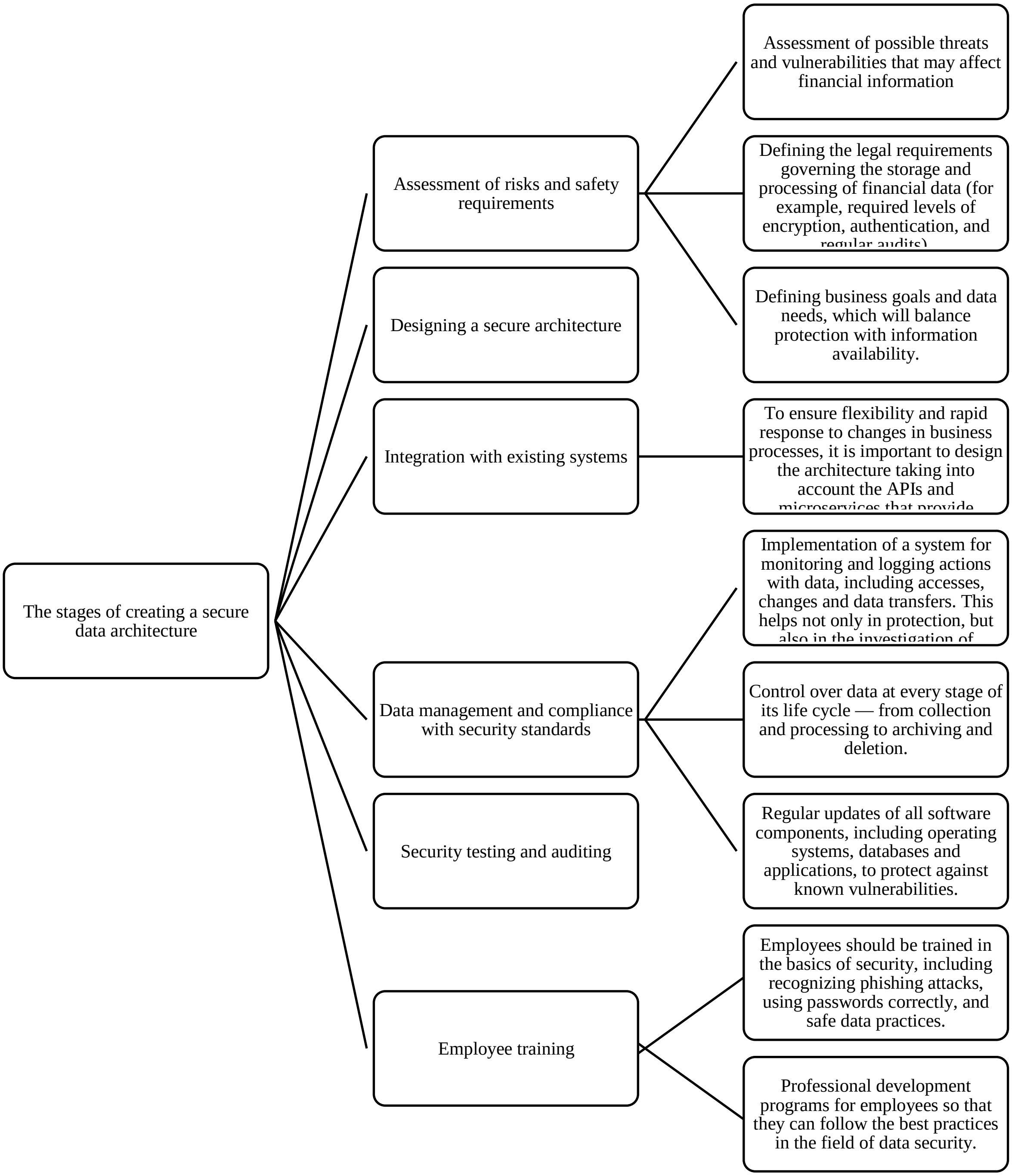
The stages of creating a secure data architecture
Assessment of risks and safety requirements
Designing a secure architecture
Integration with existing systems
Data management and compliance with security standards
Security testing and auditing
Employee training
Assessment of possible threats and vulnerabilities that may affect financial information
Defining the legal requirements governing the storage and processing of financial data (for example, required levels of encryption, authentication, and regular audits)
Defining business goals and data needs, which will balance protection with information availability.
To ensure flexibility and rapid response to changes in business processes, it is important to design the architecture taking into account the APIs and microservices that provide
Implementation of a system for monitoring and logging actions with data, including accesses, changes and data transfers. This helps not only in protection, but also in the investigation of
Control over data at every stage of its life cycle — from collection and processing to archiving and deletion.
Regular updates of all software components, including operating systems, databases and applications, to protect against known vulnerabilities.
Employees should be trained in the basics of security, including recognizing phishing attacks, using passwords correctly, and safe data practices.
Professional development programs for employees so that they can follow the best practices in the field of data security.

Fig.1. The process of creating secure data architectures for financial organizations [7].

Threats also emerge through partner chains, including cloud service providers and contractors working with infrastructure. Addressing these challenges requires revising security methods and updating systems [2]. The principles of creating secure data architectures are illustrated in Figure 2.

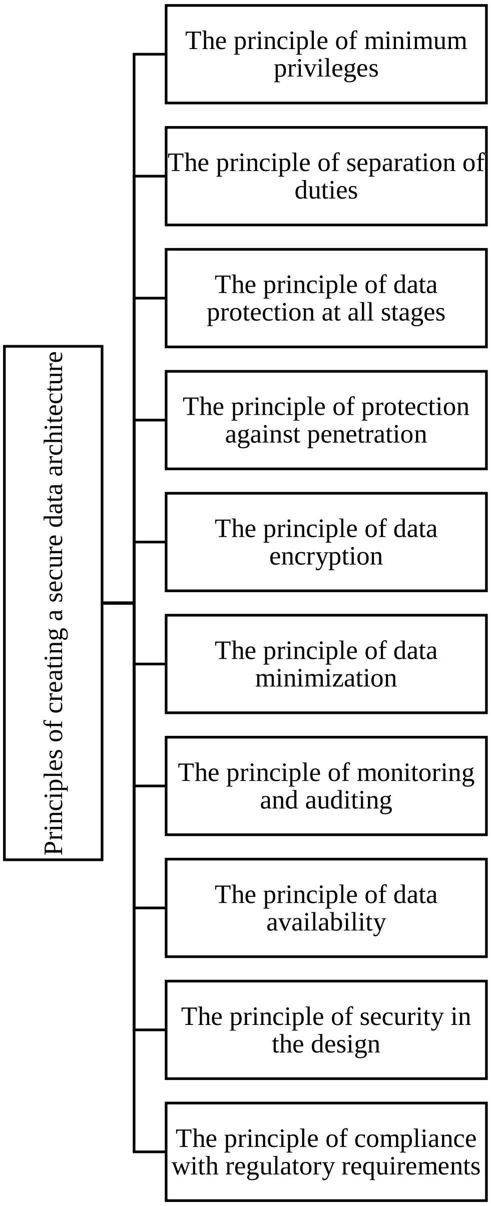
Principles of creating a secure data architecture
The principle of minimum privileges
The principle of separation of duties
The principle of data protection at all stages
The principle of protection against penetration
The principle of data encryption
The principle of data minimization
The principle of monitoring and auditing
The principle of data availability
The principle of security in the design
The principle of compliance with regulatory requirements

Fig.2. Principles of creating a secure data architecture [2,6].

One key principle is the restriction of interactions. Isolated network segments are introduced, strict access limitations to resources are enforced, and redundant connections between components are eliminated. The infrastructure is protected in stages to prevent the spread of threats. For instance, transaction data is stored in isolated segments, with access regulated by clear policies. Traffic is filtered by firewalls operating at packet and application levels.

Access management systems are implemented with a focus on minimizing user privileges. Role-based models and attribute-based approaches are used, where access parameters are determined by location, device, and operation context. Authentication methods based on biometrics, behavior analysis, and time-based codes enhance data security.

Encryption serves as a critical tool for ensuring security. Algorithms such as AES-256 and high-cryptographic-strength protocols like TLS 1.3 are employed. Key management is implemented through hardware modules, tokenization, and pseudonymization, reducing the risks of data breaches [6].

Threat monitoring is carried out using analytical platforms. Machine learning applications detect anomalies undetectable by traditional tools. Process automation accelerates threat mitigation, including connection blocking and system element isolation.

The Zero Trust concept eliminates assumptions about the reliability of internal elements. All interactions are verified, and network segmentation prevents the spread of threats. Even during localized incidents, the remaining parts of the system remain protected.

Organizational measures include developing clear regulations, conducting audits, penetration testing, and vulnerability assessments. Employee training reduces risks associated with human errors [3].

Compliance with standards such as GDPR, PCI DSS, and ISO 27001 regulates data processing, incident management, and encryption. Adherence to these norms enhances customer trust and reduces legal risks.

Artificial intelligence technologies enable the analysis of user actions, process automation, and prevention of suspicious operations. The integration of such approaches creates a comprehensive protection system.

Data architecture development requires consideration of changes, implementation of technological solutions, and the creation of approaches tailored to current challenges. Financial organizations focusing on these areas establish resilient systems that strengthen their market positions [5].

In China, financial institutions adopt information protection approaches aligned with regulatory requirements. The legislative framework includes the "Cybersecurity Law," the "Data Security Law," and the "Personal Information Protection Law." Since 2023, standards for cross-border data transfer based on contractual mechanisms have been in effect, simplifying operations for companies with limited data volumes [13].

Special attention is given to personal information processing audits. Companies conduct audits by the "Administrative Measures for Personal Information Processing Compliance Audits" of 2023. These procedures aim to ensure legal compliance, operational transparency and strengthened control over data processing.

In the Guangdong-Hong Kong-Macao Greater Bay Area, the GBA Certification has been introduced to facilitate cross-border data exchange. This tool, used in the financial sector, mandates adherence to regulatory requirements, enhancing information security.

As a result of these measures, a reduction in cyber threat incidents has been observed. However, compliance with regulatory requirements incurs significant financial costs, especially for large organizations, where expenses include the implementation of encryption technologies and control of data processing workflows.

Canadian financial institutions are governed by the federal Personal Information Protection and Electronic Documents Act (PIPEDA) and regional legislative acts, including Quebec's laws. Special emphasis is placed on encryption methods, access management, and data tokenization. Technological solutions offered by companies like Thales provide organizations with tools to secure data when interacting with cloud services. These approaches are aimed at strengthening information security [14].

In 2023, the financial sector experienced a decline in cyber incidents, attributed to the use of encryption technologies and advancements in data control methods. These measures demonstrate the effectiveness of selected solutions for ensuring security.

China and Canada actively participate in initiatives to improve data protection systems, including the development of cloud service standards and the application of artificial intelligence in threat analysis. However, the implementation of such solutions entails high financial costs and the need to meet complex regulatory requirements [15].

Table 1 presents the advantages and disadvantages of creating secure data architectures for financial organizations.

Table 1. Advantages and disadvantages of creating secure data architectures for financial organizations [12-15]

Advantages	Disadvantages
Enhanced security: Secure architectures protect data from unauthorized access, leaks, and attacks.	High costs: Developing and implementing secure architecture requires significant financial and time resources.
Compliance with regulations: Meets security standards and legal requirements (e.g., GDPR, PCI DSS).	Complexity in management: Continuous monitoring and managing data security can be labor-intensive and require specialized skills.
Threat protection: Reduces risks of cyberattacks, data breaches, and loss of confidential information.	Slower system performance: Security measures such as encryption and multi-factor authentication can slow data processing.
Increased customer trust: Data protection strengthens trust among clients and partners.	Integration challenges: Implementing secure architecture can face difficulties when integrating with existing legacy systems.
Reduced risk of financial losses: Minimizes losses from data security-related incidents.	Potential vulnerabilities: Design flaws or insufficient security measures may create exploitable weaknesses.
Lifecycle data management: Enables tracking and controlling the use and storage of data.	Need for regular updates: Architecture requires continuous updates to protect against new threats and vulnerabilities.
Long-term resilience: Security systems provide enduring protection and mitigate the impact of attacks.	High training requirements: Employees must be regularly trained in secure data handling practices and technologies.

The examples of efforts by the two countries illustrate a practical approach to data security, grounded in the adoption of advanced technologies, international coordination, and continuous development of the regulatory framework.

CONCLUSION

The development of data architectures for financial organizations serves as a foundation for ensuring resilience amid digital transformation. Analysis conducted in scientific studies has demonstrated the necessity of a systematic approach that incorporates the principles of Privacy by Design, Security by Design, and the use of technological solutions that align with regulatory requirements.

Methods such as micro-segmentation, privilege restriction, adaptive authentication, and cryptographic protection have proven effective in preventing data breaches and reducing the risks of cyberattacks. The implementation of automated platforms for monitoring and analytical data processing ensures prompt threat detection and mitigation of their consequences. Organizational measures, including employee training, the establishment of security protocols, and the execution of audits, contribute to enhancing protection levels.

REFERENCES

1. M Babu. S., Raj K. B., Devi D. A. Data security and protection of confidential data using the "projected confidentiality" technology //2nd International Conference of the Central Committee on Innovations in the field of big data for sustainable cognitive Computing: BDCC 2019. – Springer International Publishing House, 2021. – Pp. 177-189.
2. Vedha B. Yu., Vasandani M. S., Vedha A. E. P. B. Designing enterprise architecture for the transformation of online financial services //Syncron: Dan Penelian Tech Informatics magazine. – 2023. - vol. 7. – No. 4. – pp. 2670-2678.
3. Shbad S. A. Research on how to make decisions for software development //IEEE Access. – 2022. – Vol. 10. – pp. 128983-128993.
4. Massachusetts, N. K., N. N. Distributed servers: security and implementation problems //IEEE Security & Privacy. – 2020. – Vol. 19. – No. 1. – pp. 54-64.
5. Avaishe F. M. et al. Security in the design of big data processing platforms in cloud computing //IEEE Standards transactions on engineering management. – 2021. – vol. 69. – No. 6. – pp. 3676-3693.
6. Pashtova, L. Financial architecture of corporations in digital reality / L. Pashtova // Finance and credit. 2024. Volume 30. pp.507-526.
7. Flugheft K. A., Sufi E. S., Sawyer R. Information architecture for data disclosure //Entropy. – 2022. – Vol. 24. – No. 5. – p. 670.
8. Sen. T. Building a financial data control regime based on blockchain technology //ICIDC 2023: Proceedings of the 2nd International Conference on Information Economics, Data Modeling and Cloud Computing, ICIDC 2023, June 2-4, 2023, Nanchang, China. – European Alliance for Innovation, 2023. – vol. 4. – p. 193.
9. Yi G. O. M. An approach to design to minimize data theft // International Conference 2022 on Computational Science and Computational Intelligence (CSCI). – IEEE, 2022. – pp. 983-989.
10. Boldrin L., Sellitto G. P., Tepandi J. The architect of the TOOP // The principle of monotonous use: The TOOP project. - Cham: Springer International Publishing, 2021. – pp. 126-140.
11. Anikeeva V.V., Selifanov V.V. Risk assessment in the process of determining the architecture of the system // Security of digital

technologies. – 2022. – № 4 (107). – Pp. 52-62.

12. Christiana I. et al. Optimizing the implementation of big data to create business value and architecture in the proposed banking industry: a systematic review //The 2023 International Conference on Computer Science, Information Technology and Engineering (ICCoSITE). – IEEE, 2023. – pp. 667-672.

13. Financial services. [Electronic resource] Access mode: https://cpl.thalesgroup.com/industry/financial-data-security (date of access: 11/19/2024).

14. Data protection and cybersecurity in China: annual review for 2023 and prospects for 2024. [Electronic resource] Access mode:https://www.twobirds.com/en/insights/2024/china/china-data-protection-and-cybersecurity-annual-review-of-2023-and-outlook-for-2024 - 1 (date of application: 11/19/2024).

15. There are 3 months left before the new data protection rules come into force in China. [Electronic resource] Access mode: https://rouse.com/insights/news/2024/3-month-countdown-to-the-china-s-new-data-security-regulation-key-trends-and-compliance-insights (date of access: 11/19/2024).