**International Journal of Independent Research Studies**
*Vol. 15, No. 2, 1-5, 2026*
*ISSN(E) 2226-4817*
*DOI: 10.55220/2304-6953.v15i2.875*


# Development of a Secure Customer and Personnel Management Platform

**Murat Bayri**[1]
**Ceren Ulus**[2]
**Nazlı Yusufoğlu**[3]
**M. Fatih Akay**[4]✉

[1]*Innovance Information Technologies, Dept. of Software Development, Türkiye.*
[2,3]*EFA Innovation Consulting and Technology, Dept. of Research and Development, Türkiye.*
[4]*Çukurova University, Dept. of Computer Engineering, Türkiye.*
*(✉ Corresponding Author)*

**Abstract**

Customer and personnel management play a crucial role in today's business processes. Effective personnel management significantly impacts employee motivation, which is directly related to employee engagement and performance. Similarly, proper customer management processes allow for the analysis of customer needs and feedback. These elements contribute to enhancing the company's brand image. Consequently, customer and personnel management platforms are becoming increasingly important. However, ensuring security on these platforms is a significant challenge. This study aims to increase transparency, security, and efficiency within the scope of customer and personnel management. To this end, a user-friendly platform has been developed, offering a web-based management panel and a mobile application. The platform can secure financial data using strong encryption algorithms such as Advanced Encryption Standard – 256-bit (AES-256) and Rivest–Shamir–Adleman – 2048-bit (RSA-2048). It can implement Role-Based Access Management (RBAC) and Multi-Factor Authentication (MFA) to control user access. The developed platform offers a solution that prioritizes digitalization and security in financial processes with its robust technical infrastructure, security-focused architecture, and innovative technologies, providing an innovative digital platform for use in customer and personnel management processes.

**Keywords:** Data security, Digitalization, Management platform.

## 1. Introduction

In today's evolving world, effectively managing customers and personnel is a crucial strategic action for a business to plan its customer relationships and employee dynamics in a planned, efficient, and sustainable manner. Customer Relationship Management (CRM) aims to increase customer satisfaction, build a loyal customer base, boost sales and profitability, and establish long-term relationships with potential and actual customers by considering their needs and desires [1]. This includes analyzing customer needs and expectations, managing complaints and feedback, and organizing pre- and post-sales services. Personnel management, on the other hand, is the effective and efficient management of a company's employees and organization [2]. This process includes various practices such as recruitment, training, personnel management, leave, advances, asset management, payroll, and benefits management. Through effective personnel management, employee productivity is maximized, the right person is placed in the right job, thereby increasing the service-personnel matching efficiency, and employee motivation and commitment are ensured. Motivated and trained personnel provide higher quality service. High-quality service, in turn, makes high customer satisfaction possible. High customer satisfaction ultimately leads to increased brand value and sustainable success. Consequently, the need for customer and employee management platforms has increased.

Customer and employee management platforms are software solutions that reduce manual tasks, increase efficiency, and simplify decision-making processes, enabling businesses to manage their customers and employees digitally, efficiently, and in a planned manner through a single system. The security of these platforms is crucial for protecting customer and employee data. This directly impacts company credibility. However, protecting financial data has become more complex today with the rise of cyberattacks and malicious software. Failure to ensure security for information can lead not only to financial losses but also to significant reductions in customer trust. The disclosure of customer personal information, payment information, and employee personal information, including salary and health data, is extremely risky. Such situations can cause financial losses, operational disruptions, and damage to the company's brand image.

The need for digital transformation for businesses to gain a competitive advantage and have a more effective operational structure has become increasingly evident today. The integration of technologies such as Robotic Process Automation (RPA) into financial processes reduces costs and accelerates business processes by automating repetitive tasks. In addition, national and international regulations regarding data security are increasing the

obligation for companies to comply with regulations in their financial processes. Regulations such as the European Union's General Data Protection Regulation (GDPR) and Turkey's Personal Data Protection Law (PDPL) mandate security standards such as encryption, traceability, and reportability of financial data.

This study aims to increase transparency, security, and efficiency within the scope of customer and personnel management. To this end, a platform has been developed that can ensure the security of financial data with strong encryption algorithms such as AES-256 and RSA-2048, implement RBAC and MFA to control user access, and offer a user-friendly experience with a web-based management panel and a mobile application.

This study is organized as follows: The relevant literature is presented in Section 2. After that, the details of the platform are provided in Section 3. Following this, the result of the study has been given in Section 4. And finally, the conclusion of the study is included with Section 5.

## 2. Literature Review

[1] examined problems such as difficulties in ensuring data privacy and security in digital finance transactions, cyber-attacks, and data breaches. To address these issues, the complexity of protecting personal and financial data has been analyzed. Current regulations, including the GPDR used worldwide and a standard for data provision in the field of payment cards have been examined. The findings underscored the necessity for robust encryption methods, the importance of MFA, and the necessity for continuous monitoring systems to mitigate potential vulnerability.

[2] highlighted browser and device compatibility, improved accessibility, and robust security and fraud protection systems for web-based platforms. It emphasized that platforms should take precautions against possible cyber-attacks, implement Application Programming Interfaces (APIs) comprehensively, and use CoPilot during the digital platform design phase. Additionally, the use of agile development has been touched upon to prevent issues that may arise in integrating third-party services, adopt AI-driven features, and improve user experience.

[3] aimed to systematically examine the impact of cybersecurity threats on digital banking security, adoption, and regulatory compliance. For this purpose, 78 peer-reviewed articles published between 2015 and 2024 have been examined. The investigation revealed that phishing and malware attacks are the most common types of cyberattacks and can cause large financial losses as well as consumer distrust. In this context, it has been determined that MFA and biometric security solutions are widely adopted in response to the problem of unauthorized access. In addition, it has been observed that the use of artificial intelligence-supported fraud detection and blockchain technologies for the security of financial transactions is widespread. On the other hand, the integration of third-party FinTech solutions has led to the use of stringent regulatory oversight and cybersecurity protocols. In this context, it has been highlighted that compliance with global cybersecurity regulations such as GDPR, Payment Services Directive, and Gramm–Leach–Bliley Act enhances digital banking security by mandating stringent authentication measures, encryption protocols, and real-time fraud monitoring.

[4] examined the integration of artificial intelligence into CRM and the effective applicability of artificial intelligence. Practical activities have been identified. Ethical design, centralization of customer data, model retraining, and continuous user engagement features have been highlighted. The study also presented a framework for integrating artificial intelligence into CRM.

[5] discussed encryption algorithms which are often used in the field of financial technology. In this context, symmetric, asymmetric and hybrid encryption methods, end-to-end encryption and homomorphic encryption techniques have been examined; each method has been evaluated in terms of criteria such as its strengths and weaknesses, practical applications in the field of Fintech, computational efficiency, scalability, and regulatory compliance. The findings revealed that encryption plays a critical role in ensuring the security and integrity of financial data. In addition, it has been revealed that end-to-end encryption is a highly ideal solution for data privacy in digital payments and mobile banking, while homomorphic encryption offers significant potential for secure data analysis by allowing transactions to be made without decrypting the data.

[6] proposed a framework called DPFedBank, which enables financial institutions to both develop machine learning models and provide data privacy with Local Differential Privacy (LDP) mechanisms. This framework enables organizations to provide insights while protecting the confidentiality of private information. For this purpose, possible security vulnerabilities have been investigated in depth and policies have been developed to prevent these vulnerabilities. A new combination of adaptive LDP mechanisms and encryption techniques developed specifically for financial data have been introduced, ensuring data privacy while maintaining model utility. Furthermore, advanced authentication protocols, encryption techniques for secure data exchange, and continuous monitoring systems to detect and respond to cyberattacks in real-time have been also included in the framework.

[7] aimed to provide a modern approach to creating an effective personnel management system. To identify key threats, the Delphi method, an expert analysis method, has been used. The hierarchical analysis method has been employed to organize threats, and the pairwise comparison method has been used to compare threats. The output presents a list of the most significant threats to the creation of a personnel management system. Based on the findings, it has been concluded that in the second half of the 2020s, the impact of internal threats on personnel management systems and the competitiveness of businesses increased, potentially negatively affecting the protection of workers' rights. The study concludes that establishing an effective personnel management system is a complex process influenced by various factors and threats.

[8] aimed to analyze the relationship between big data and digital marketing by taking data into consideration. The implementation and realization of blockchain technologies are largely dependent on environmental factors. Transactions on the blockchain ensure the privacy of user data by storing records in a decentralized ledger. When a block is determined to originate from an unverified source, the accuracy of the data is first supported by storing it on the blockchain and ensuring its accuracy is always verifiable. On the blockchain, information about data blocks, their origins, and other blocks they interact with is recorded and then automatically verified. This information is then verified by the network.

[9] have proposed a blockchain-based deep learning approach for interbank Know Your Customer (KYC) for a secure retail banking system. The aim is to protect customer privacy. To this end, deep biometric fingerprint data has been used to model KYC and anonymize the collected fingerprint data.

[10] have proposed an automated deep learning-based framework for interbank KYC for robot-based cyber-physical banking. The aim is to model the customer's KYC and ensure customer privacy by anonymizing the collected visual data, and a deep biometric architecture is used for this purpose. In addition to the blockchain network, a symmetric-asymmetric encryption-decryption module is also used for secure and decentralized transmission and verification of biometric information. Z6 and A6 lattice vector quantization is proposed for secure transmission and storage of face-to-face banking documents. In addition, a high-capacity fragile watermarking algorithm based on integer-to-integer discrete wavelet transform is presented. The Pepper humanoid robot is used for the automated biometric-based collection of handwritten bank checks from customers. Biometric information such as fingerprints and names of bank customers are placed as watermarks on the relevant bank documents using the proposed framework. In the results obtained, it has been observed that the proposed security protection framework can place more biometric data on bank documents compared to similar algorithms. The quality of secured bank documents has been observed to be 20% higher compared to other proposed algorithms.

[11] have examined the potential of blockchain technology to ensure the security of customer data in CRM systems in the age of digital transformation. This study provides case studies of successful blockchain-based CRM applications in loyalty reward programs, supply chain management in the life sciences sector, identity management, data sharing, and product traceability. The results of the study show that the implementation of blockchain-based solutions can provide effective cost savings, increased efficiency, and improved business profitability.

## 3. Details of the Platform

An integrated software architecture has been created for the web and mobile application. Additionally, a microservices-based approach has been adopted, aiming to provide flexibility and scalability. The database design is structured to meet the requirements for secure data storage. RBAC and MFA methods have enhanced the security of user authorization processes. The platform architecture has been built from 3 layers, namely the presentation layer, the application layer, and the data layer. The architectural scheme is given in Figure 1.

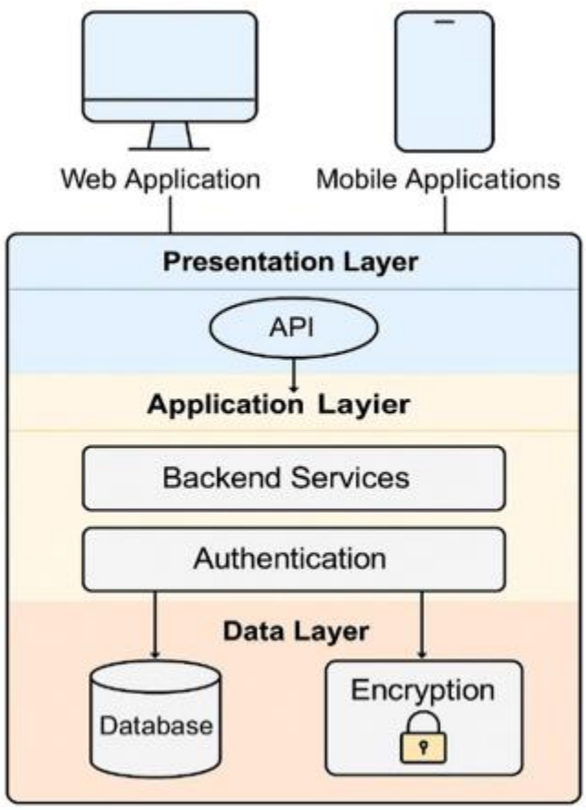


**Figure 1.** Platform Architecture.

The presentation layer of the platform architecture consists of Web Application and Mobile Applications components. These components are the interfaces that users interact with. This layer connects to the Application layer via API. The application layer consists of Backend Services and Authentication modules. All business logic, data processing, and authentication take place at this layer. The last layer, the Data Layer, includes the Database and Encryption modules. Financial data is encrypted with AES-256 and RSA-2048 algorithms, stored here and transmitted from here.

### *3.1. Data Encryption and Secure Storage*

In the study, the AES-256 encryption algorithm has been applied to store financial data securely. To ensure data transmission security, data transfer mechanisms encrypted with RSA-2048 have been used. Thus, both static and dynamic data are protected against unauthorized access. In addition, parallel processing algorithms have been used to optimize performance in data encryption processes. The code details for the process are given in Figure 2.

```php
<?php
// INV58

$data = '30.000'; // Şifrelenecek örnek veri

// === AES-256-CBC ile Şifreleme ===
$aes_key = random_bytes(32);   // 256 bit key
$iv      = random_bytes(16);   // 128 bit IV

// Veriyi AES-256-CBC ile şifrele
$ciphertext = openssl_encrypt(
    $data,
    'AES-256-CBC',
    $aes_key,
    OPENSSL_RAW_DATA,
    $iv
);

// IV ve şifreli veriyi tek pakette base64 ile sakla
$payload = base64_encode($iv . $ciphertext);

// === RSA-2048 ile AES Anahtarını Şifreleme ===
$publicKey  = openssl_pkey_get_public(file_get_contents('public.pem'));
openssl_public_encrypt($aes_key, $enc_key, $publicKey, OPENSSL_PKCS1_OAEP_PADDING);
$enc_key_b64 = base64_encode($enc_key);

// ---------- Buradan sonrası çözme işlemleri ----------

// RSA ile AES anahtarını çöz
$privateKey = openssl_pkey_get_private(file_get_contents('private.pem'));
openssl_private_decrypt(base64_decode($enc_key_b64), $dec_aes_key, $privateKey, OPENSSL_PKCS1_OAEP_PADDING);

// AES-256-CBC ile veriyi çöz
$payload_dec = base64_decode($payload);
$iv_dec      = substr($payload_dec, 0, 16);
$cipher_dec  = substr($payload_dec, 16);

$plain = openssl_decrypt(
    $cipher_dec,
    'AES-256-CBC',
    $dec_aes_key,
    OPENSSL_RAW_DATA,
    $iv_dec
);

echo "Çözülen veri: " . $plain;
```

**Figure 2.** Encrypting the AES key with RSA 2048

The AES key and IV initial vector have been primarily generated by random_bytes (32) and random_bytes (16). The data is then encrypted in AES-256-CBC mode with openssl_encrypt. The IV is added to the beginning of the encrypted data and stored together in base64 format. The AES key is encrypted using RSA-2048 and converted to base64 format. In the decoding phase, the AES key is decoded with RSA first, then the actual data is decoded with AES-256-CBC and printed on the screen.

### *3.2. Development of User Interface*

The user interface development section of the platform has created a design that includes intuitive interfaces and easy navigation features for both the web-based management panel and the mobile application. For the realization of customer and personnel management processes, a customizable access structure is offered according to user roles. A sample application screen is given in Figure 3.

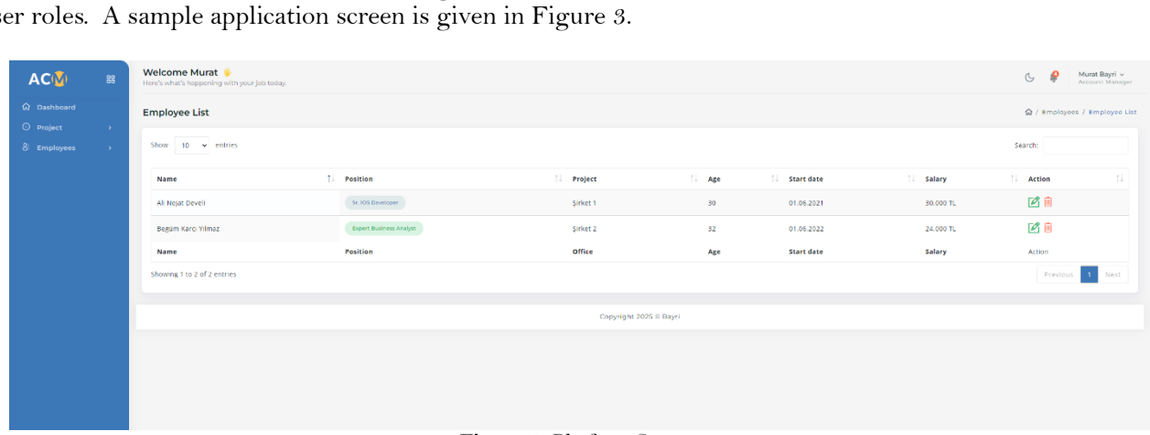


**Figure 3.** Platform Screen.

The screen given in Figure 3 shows the "Employee List" page of the Customer and Personnel Management Platform. The left menu provides quick access to the Dashboard, Project, and Employees menus. A welcome message and notification area is presented to the user (Account Manager) who logs in to the Top Panel. Employees' name, position, project assignment, age, start date, and salary information are listed in a table. The action buttons for editing and deleting are located on the right.

On this page, salary information is stored in the database encrypted with strong cryptography methods such as AES-256 and RSA-2048. The user interface securely decrypts this encrypted data and displays it on the screen. Thus, both data security is ensured and it is possible to protect financial information against unauthorized access

## 4. Results and Discussion

With the developed platform,

- An innovative digital platform developed for use in customer and personnel management processes has been introduced.
- With its robust technical infrastructure, security-focused architecture, and innovative technologies, a solution has been provided that prioritizes digitalization and security in financial processes.
- It has been enabled that businesses to manage their financial processes more securely, quickly, and efficiently. Data security has been maximized with the protection of financial data with strong encryption algorithms.
- A security infrastructure compliant with international standards is provided for data transmission and storage. This increases businesses' resilience against cybersecurity risks while strengthening their reputation by ensuring full compliance with legal regulations, especially PDPL and GDPR.
- The existing processes of businesses have been optimized, and contributions have been made to their digital transformation processes.
- A user-friendly interface is provided, offering access from both web-based and mobile devices. This interface increases the operational flexibility of businesses. Thus, companies can increase their competitiveness by having a more modern and technological infrastructure. The reliable and fast execution of financial transactions increased customer satisfaction and strengthened trust in the platform.

## 5. Conclusion

This study aims to develop a solution that will enable companies to improve security and efficiency standards by digitizing their financial transactions in customer and personnel management processes. To this end, a platform has been developed that can secure financial data with strong encryption algorithms such as AES-256 and RSA-2048, implement RBAC and MFA to control user access, and offer a user-friendly experience through a web-based management panel and a mobile application. The developed platform provides a security infrastructure compliant with international standards for data transmission and storage. This enables businesses to increase their resilience against cybersecurity risks, achieve full compliance with legal regulations such as PDPL and GDPR, and strengthen their reputation.

## References


Zhekova, M., Katrandzhiev, N., & Petkov, M. (2025). Design and development of a customer management system in the food industry. *BIO Web of Conferences, 170*, 03002. https://doi.org/10.1051/bioconf/202517003002

Muleme, G., Kaijage, S., & Ruhinda, B. (2022, November). A web-based human resource management system with machine learning techniques: A case study of the Inter-University Council for East Africa (IUCEA). In *International Conference on Technological Advancement in Embedded and Mobile Systems* (pp. 35–45). Cham, Switzerland: Springer Nature.

Adegbite, M. A. (2025). Data privacy and data security challenges in digital finance. *Journal of Digital Security and Forensics, 2*(1), 6–19.

Ekeh, S. A., Tahi, S., & Mohaisen, L. (2025). Enhancing cyber-security and user experience in digital banking platforms: A comprehensive approach. In C. E. Hewage, M. H. Zafar, & N. Kesswani (Eds.), *AI applications in cyber security and privacy of communication networks: ICCS 2024* (pp. xx–xx). Singapore: Springer. (Lecture Notes in Networks and Systems, Vol. 1453). *(Complete page numbers needed if available)*

Waliullah, M., Hossain George, M. Z., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: A systematic literature review. *American Journal of Advanced Technology and Engineering Solutions, 1*(1), 226–257.

Ledro, C., Nosella, A., Vinelli, A., Dalla Pozza, I., & Souverain, T. (2025). Artificial intelligence in customer relationship management: A systematic framework for a successful integration. *Journal of Business Research, 199*, Article 115531. https://doi.org/10.1016/j.jbusres.2025.115531

Olaiya, O. P., Adesoga, T. O., Adebayo, A. A., Sotomi, F. M., Adigun, O. A., & Ezeliora, P. M. (2024). Encryption techniques for financial data security in fintech applications. *International Journal of Science and Research Archive, 12*(01), 2942–2949. https://doi.org/10.30574/ijsra.2024.12.1.1210

He, P., Lin, C., & Montoya, I. (2024). *DPFedBank: Crafting a privacy-preserving federated learning framework for financial institutions with policy pillars* (arXiv preprint). arXiv. https://doi.org/10.48550/arXiv.2410.13753

Kopytko, M., Liubokhynets, L., Panchenko, V., Moysa, T., & Malanchuk, A. (2024). Formation of a personnel management system as a factor of increasing competitiveness and the enterprise security level in the context of digital transformation and new legal challenges. *Social and Legal Studios, 1*(7), 210–220.

Saxena, M., Senthilkumar, N., Girimurugan, B., & Hasan, K. S. (2024, March). Customer relationship management in the digital age by implementing blockchain for enhanced data security and customer trust. In *2024 2nd International Conference on Disruptive Technologies (ICDT)* (pp. 56–59). IEEE.

Srinivas, K., Nandini, J., Spoorthy, B., & Rahul, K. (2024). Secure customer management mechanism for online banking system. In *Sustainable Materials, Structures and IoT* (pp. 195–198). CRC Press.

Hajiabbasi, M., Akhtarkavan, E., & Majidi, B. (2023). Cyber-physical customer management for Internet of Robotic Things-enabled banking. *IEEE Access, 11*, 34062–34079. https://doi.org/10.1109/ACCESS.2023.3263859

Kumari, S., Sarkar, B., & Singh, G. (2023). Blockchain-based CRM solutions: Securing customer data in the digital transformation era. *International Journal of Computer Trends and Technology, 71*(4), 27–36.