Methods of Personal Data Protection in Retail: Practical Solutions*

Svitlana Rzaieva[1,*,†], Dmytro Rzaiev[2,†], Nelya Mykytenko[3,†], Yurii Dreis[4,†] and Viktor Grechaninov[5,†]

[1] Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., 04053 Kyiv, Ukraine
[2] Kyiv National Economic University of Kyiv, 54/1 Beresteysky pros., 04030 Kyiv, Ukraine
[3] State University Of Trade And Economics of Kyiv, 19 Kyoto str., 02156 Kyiv, Ukraine
[4] Polissia National University, 7 Staryi ave., 10008 Zhytomyr, Ukraine
[5] Institute of Mathematical Machines and Systems Problems, 42 Akademika Glushkova ave., 03187 Kyiv, Ukraine

Abstract

This paper explores key methods for protecting personal data in the retail sector. It describes modern encryption algorithms, such as AES and RSA, their mathematical models, and applications for ensuring data confidentiality and integrity. Special attention is given to multifactor authentication, network segmentation, cloud service and IoT device protection, and the use of innovative approaches including real-time monitoring and access control, which help minimize the risk of data breaches. The research emphasizes the importance of an integrated approach to cybersecurity in retail to enhance customer trust and ensure compliance with legal requirements.

Keywords

personal data protection, retail, encryption, multifactor authentication, network segmentation, cloud service protection, IoT devices, cybersecurity

1. Introduction

In today's digital world, retail has become a key sector that processes large volumes of personal data. These data include names, addresses, phone numbers, financial transactions, IoT devices, and more. With the globalization of e-commerce and the growing popularity of online shopping, personal data protection has become particularly important, as data breaches can not only cause significant financial losses but also seriously undermine consumer trust in a brand [1–4].

Digital security threats in retail include various forms of cyberattacks such as phishing campaigns, database breaches, DDoS attacks, ransomware, and internal threats caused by human error or intentional actions by personnel. Incidents such as the massive data breach at Target in 2013 or the attack on the Dixy network's POS systems in 2020 highlight the critical nature of information security for retailers. Attackers use various methods to gain access to confidential information, underlining the need for robust security measures [5–9].

Loss or compromise of personal data can result in substantial financial losses, reputational damage, and legal consequences for retail networks. As a result, protecting data becomes a top priority for any retailer. Therefore, modern methods of personal data protection in retail and the technical aspects of implementing security solutions are highly relevant [10–12].

Regulatory requirements in the field of personal data protection, such as the General Data Protection Regulation (GDPR) in the European Union, the Payment Card Industry Data Security Standard (PCI DSS), and ISO/IEC 27001, define security standards that are mandatory for companies processing personal information. Failure to comply with these standards can lead not

*CPITS 2025: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2025, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
s.rzaieva@kubg.edu.ua (S. Rzaieva); rzaiev@kneu.edu.ua (D. Rzaiev); n.mykytenko@knute.edu.ua (N. Mykytenko); dreisyuri@gmail.com (Y. Dreis); Vitya.Grechaninov@gmail.com (V. Grechaninov)
0000-0002-7589-2045 (S. Rzaieva); 0000-0002-7149-4971 (D. Rzaiev); 0000-0002-5694-0531 (N. Mykytenko); 0000-0003-2699-1597 (Y. Dreis); 0009-0002-8400-6401 (V. Grechaninov)

only to data leaks but also to significant fines. This incentivizes retailers to implement effective data protection methods aimed at minimizing risks and ensuring regulatory compliance [13].

One of the key approaches to protecting personal data in retail is a multi-layered security model that includes:

- Multifactor authentication (MFA) to implement additional levels of protection when accessing payment systems and accounts.
- Network segmentation to divide the network infrastructure into isolated segments to restrict access to critical resources.
- Role-based access control (RBAC) to restrict access to data according to the role of the employee, which reduces the risk of unauthorized use of information
- Encryption algorithms using modern cryptographic methods to ensure data security during transmission and storage.
- Protection of IoT devices to ensure the security of smart devices used at points of sale to optimize operations (for example, self-service cash registers).

Particular attention should be paid to implementing cybersecurity best practices, such as regular software updates, information security training for staff, and system security audits.

This paper aims to explore the methods of personal data protection in the retail sector, with a focus on practical solutions that minimize the risks of information leakage and comply with international security standards. The experience of leading retail companies in Ukraine and Europe will be reviewed, with a detailed analysis of the results of implementing MFA technologies, network segmentation and role-based access control [14–16].

An important aspect of the paper is also an assessment of the effectiveness of these methods based on statistical data and analysis of real incidents, which demonstrate a significant reduction in the number of data leaks and cyber threats after their implementation. Thus, the material will be useful for both heads of retailers' IT departments and researchers in the field of cybersecurity and information risk management [17].

2. Problem statement

In today's retail industry, customer personal data has become one of the key assets for businesses, but also a potential threat to privacy. Retail companies process large amounts of information, including full names, contact information, and purchase history, to conduct business efficiently, making them attractive targets for cybercriminals. The problem is also the failure to minimize data collection. Many retailers store more information than is necessary for their operations, which increases the amount of potential losses in the event of a leak. A low level of transparency in informing customers about the storage and processing of their data is also a problem. This can reduce trust in the company and lead to reputational losses.

One of the main problems is the growing number of cyberattacks on retail companies aimed at stealing confidential information. Attackers may use phishing, social engineering, and database hacking methods. Insufficient security of databases storing personal data is a significant threat. Another problem is the storage of backup copies of data without proper encryption, which, in turn, allows attackers to access data through backup media.

Lack of proper control over access to personal data leads to the risk of internal threats. A low level of authorization and authentication may allow unauthorized access to confidential information. Insufficient integration of multi-factor authentication (MFA) systems, which is an effective way to protect accounts, is a problem. The lack of a cybersecurity culture at the company's management level can be a key obstacle to implementing effective personal data protection methods. Lack of staff awareness of data protection methods is another problem. Often, employees are not sufficiently trained in security rules, which makes the company vulnerable to

phishing attacks. The spread of malware through phishing emails is another threat to retailers, as it can lead to the compromise of information systems used in retail.

The lack of regular security monitoring and auditing is also a threat. Companies often fail to scan their systems for vulnerabilities, which can lead to confidential information leaks. The lack of intrusion detection systems (IDS) and intrusion prevention systems (IPS) leaves companies vulnerable to zero-day attacks. Another problem is the insufficient use of data encryption technologies. Often, companies neglect modern encryption methods or use outdated algorithms, which leaves data vulnerable. Many retailers lack end-to-end encryption, which makes information vulnerable when it is transferred between systems. Data leaks can cause significant financial losses for companies, including fines for violating legislation such as GDPR and CCPA. Companies often do not have clear incident response policies in place. The lack of a pre-developed plan of action in case of a data breach can make it difficult to control the situation.

Using cloud services for data storage without proper access control is also a risk. Insufficiently protected administrator accounts can cause leaks. Insufficient network segmentation allows attackers to gain access to the entire corporate network after penetration.

Using open APIs to integrate third-party services without proper security controls can lead to leaks. The problem is also the lack of compliance with international standards, such as ISO/IEC 27001, which regulate approaches to information security.

3. Main Material

The protection of personal data in retail is defined by several key standards and legislative norms that regulate the processing, storage and transfer of information. These include the GDPR, ISO/IEC 27001:2022 (International Information Security Management Standard), and PCI DSS. Each of these standards has its own peculiarities, which we will discuss below.

The GDPR General Principles is a European regulation governing the processing of personal data of individuals located in the European Union, which entered into force on May 25, 2018 [1]. The main goal of the GDPR is to ensure the confidentiality and control over personal data of EU citizens. Personal data includes names, addresses, IP addresses, credit card information, and other information that can be used to identify a person. Implementation in retail:

1. Restriction of access to personal data, access to them should be available only to authorized persons.
2. Data protection by default, i.e. the principle of ensuring security at the stage of development of data processing systems.
3. Collecting a minimum amount of data. For example, when creating an account, only the data necessary for the purchase (name, address, contact number) is requested.
4. All customer data, including purchase history, should be encrypted.
5. Introduce automation of data deletion requests, i.e. retailers should provide tools that allow customers to easily delete their data.

The International Standard for Information Security Management ISO/IEC 27001:2022 is an international standard that defines the requirements for an information security management system (ISMS). It is aimed at protecting the confidentiality, integrity and availability of information in organizations in various fields, including retail. The standard establishes an approach to risk management and data protection.

Implementation in retail: asset inventory, i.e. assets that process or store data must be identified and classified; delimitation and restriction of access to customer databases, only authorized employees have access to data; regular backup of information to prevent leaks.

PCI DSS is a standard created to ensure the security of payment transactions. It was developed by VISA, MasterCard, American Express, and others. The main goal is to protect against fraud and financial data leaks. Implementation in retail: implementation and use of POS systems (terminals)

that support PCI DSS; replacement of real card data with unique tokens; staff training on the basics of payment data security.

Compliance with GDPR, ISO/IEC 27001, and PCI DSS standards is key to ensuring data security in retail. They help to minimize the risk of leaks, increase customer confidence, and ensure compliance with the law. The implementation of these standards should take into account the specifics of retail operations, integrating encryption, tokenization and access control technologies.

Methods of personal data protection are a set of technical, organizational and procedural measures aimed at ensuring the confidentiality, integrity and availability of personal data processed within the retail sector. In this industry, data often includes customer, transactional, logistical, and behavioral information that can be targeted by cybercriminals. Successful protection involves the use of multiple layers of protection, including technical solutions, security policies, and staff training. So, in this paper, we will consider the following main methods of personal data protection:

1. Data encryption.
2. Access control.
3. Protection of cloud services.
4. Protection of IoT devices.

So, let's take a closer look at these methods of personal data protection that should be applied in retail.

Data encryption is the main tool for ensuring the confidentiality and security of personal data in retail. Its purpose is to convert data into an unreadable format that can only be decrypted with a special key. Encryption creates an additional layer of protection, ensuring that data cannot be accessed without a decryption key. In retail, it is necessary to use symmetric encryption algorithms such as AES (Advanced Encryption Standard) and DES (Data Encryption Standard). AES uses key lengths of 128, 192, or 256 bits, which ensures high cryptographic strength.

The AES algorithm is based on complex mathematical operations that guarantee the protection of information even if it is intercepted by intruders. Retail, as one of the largest industries that processes huge amounts of personal data, actively uses AES to protect its customers and business. This algorithm works on the basis of permutations and substitutions in several rounds. The main stages include: SubBytes, ShiftRows, MixColumns, and AddRoundKey.

The basis of the AES algorithm is a sequence of operations performed in the GF (28) field. These operations include byte-by-byte substitutions, row shifts, column mixing, and key addition. In the retail industry, these mathematical expressions are used to encrypt data during transaction processing, transfer information between cash registers and servers, and store data in cloud storage. AES mathematical expressions are adapted to specific retail scenarios, creating unique security algorithms.

For example, the SubBytes function, which is usually used for byte-by-byte nonlinear substitution, can be used in retail to encrypt bank card numbers. ShiftRows and MixColumns provide additional confusion to the data, making it impossible to decrypt it even if some of the information is compromised. This is important for maintaining customer privacy and protecting commercial information.

SubBytes (Byte substitution) in retail, this feature can be used to encrypt personal customer data, such as bank card numbers. The mathematical expression SubBytes (Byte substitution):

$$P_{out} = M \times (P_{in}^{(-1)}) \oplus b, \quad (1)$$

where P_{in} is a byte representing a part of the card number (for example, the last four digits); P_{out} is encrypted part of the number; M and b are predefined constants.

Example. If the card number is 1234, each digit is represented by a byte. After the SubBytes transformation, the result is a set of encrypted bytes that are transmitted through the POS terminal.

ShiftRows is an operation that cyclically shifts the bytes in each row of the data matrix by a specified number of positions. In retail, this can be used to encrypt transactions between the cash register and the server, ensuring that the order of the data is reversed, making it difficult to analyze. The mathematical expression ShiftRows:

$$T_{out}[i][j] = T_{in}[i]\ [(j + shift[i])\ mod\ N], \tag{2}$$

where $T_{in}[i]$ is input data matrix (for example, transaction amount, date, time); $shift[i]$ is number of shifts for the third line; N is number of columns.

Example. A transaction transmits encrypted data in the form of a matrix. The matrix contains:

1. The amount of the purchase
2. Time of the transaction
3. Cash register number
4. Transaction id.

The data matrix before encryption can look like this (each element is a byte):

[$100, 12:30, POS01, TRX001]
[$200, 12:45, POS02, TRX002]
[$50, 13:00, POS03, TRX003]
[$300, 13:15, POS04, TRX004]

The ShiftRows function shifts each row:

- The first row remains unchanged.
- In the second row, the elements are shifted first position to the left: [12:45, POS02, TRX002, $200].
- In the third line, shift by second positions: [POS03, TRX003, $50, 13:00].
- In the fourth, it moved up third positions: [TRX004, $300, 13:15, POS04].

Encrypted matrix after ShiftRows:

[$100, 12:30, POS01, TRX001]
[12:45, POS02, TRX002, $200]
[POS03, TRX003, $50, 13:00]
[TRX004, $300, 13:15, POS04]

Line shifting changes the order of information, which makes it difficult to decrypt without knowing the key. An attacker cannot understand what information corresponds to a particular field (amount, time, or ID). If an attacker intercepts the encrypted matrix, it is difficult to understand the relationships between the data because the order is broken.

ShiftRows is useful for securing transaction data in POS systems or when synchronizing cash registers with a central server. This is important to prevent the theft of sensitive information even if an attacker has access to some of the encrypted data.

The MixColumns feature in retail can be used to encrypt data on sales, products, or inventory. Its main task is to create confusion, which makes it difficult to decrypt the original data even if you get some of the encrypted information. The mathematical expression MixColumns:

$$C_{out}[j] = M \times C_{in}[j], \tag{3}$$

where $C_{in}[j]$ is column of the input matrix (for example, sales volumes by product category); M is coefficient matrix (defines the conversion rules); $C_{out}[j]$ is mixing result (encrypted column).

Example. Suppose there is data on sales of goods in a store for the last day:

Product A: 50 units.

Product B: 30 units.

Product C: 20 units.

Product D: 10 units.

This data can be presented in the form of a column: C_{in} = [50, 30, 20, 10].

After applying MixColumns, the data column is multiplied by a predefined matrix:

M = [[2, 3, 1, 1],
[1, 2, 3, 1],
[1, 1, 2, 3],
[3, 1, 1, 2]].

The result is calculated in the field GF(28). The new column looks like this:

C_{out} = [150, 120, 100, 80].

This encrypted data is stored in the database or transferred to the cloud. Without knowledge of the matrix M and the inverse transformation mechanism, an attacker will not be able to decrypt the real sales volumes.

Thus, encrypted data on the volume of goods in the store makes it impossible for competitors or intruders to use it even in the event of a leak. When transferring sales data from cash registers to the server, mixing columns makes it impossible to intercept clear data. The data obtained from sales analytics can be encrypted to protect it from unauthorized persons when transferred to analytical systems or partner services.

The next feature, AddRoundKey, which adds a unique key to the data at each encryption round, is crucial in retail. It allows you to generate unique encrypted data for each transaction, reducing the risk of reuse by attackers. The AddRoundKey function adds a unique encryption key to the input data using bitwise XOR (⊕). The KeyExpansion process ensures dynamic key generation, which is also critical for ensuring a high level of security in high-intensity retail operations. The mathematical expression AddRoundKey:

$$D_{out} = D_{in} \oplus K, \tag{4}$$

where D_{in} is input data (for example, information on the sale of goods); K is encryption key; D_{out} is encrypted data.

Example. Information about the sale of goods for a customer:

Name: Olga.

Order number: #45678.

Amount: $100.

After the encryption key is applied, the data is converted into an encrypted sequence of bytes. The unique key for this session looks like this:

Key: 00101100 11010010 10110101.

The data after the bitwise operation will look like this: 10101010 01101101 01011010.

As a result, even if the data is intercepted, it cannot be recovered without the session key. This ensures the protection of the client's personal data and order details.

The KeyExpansion function generates a set of keys that is used in each round of AES encryption. In retail, this is especially important for providing dynamic transaction protection, which makes it difficult to compromise data. The keys are generated from the base key Kmain and use the auxiliary operations $g(W)$, bitwise XOR (⊕), and iterative addition of the constants R_i. The mathematical expression of this key, for which the AES algorithm operates with key blocks that are four words long (4 bytes in each word), is as follows:

$$W[i] = \begin{cases} W[i-1] \oplus g(W[i-4]) \oplus R_i, & i \bmod 4 = 0 \\ W[i-1] \oplus W[i-4], & i \bmod 4 \neq 0 \end{cases} \tag{5}$$

where $W[i]$ is new 32-bit key segment; $g(W[i–4])$ is nonlinear transformation, including SubBytes, ShiftRows and cyclic byte shifting; R_i is a round constant that is unique for each round.

Example. Consider a POS terminal in a supermarket that generates unique keys for each transaction. The initial key for the terminal (primary key) looks like this:

K_{main} = [10101100 11010011 01101001 10011101]

The process of generating a new key:

1. The first segment of the new key uses the formula: $W[i] = W[i–1] \oplus g(W[i–4]) \oplus R_i$.

$W[0] = W[3] \oplus g(W[0]) \oplus R_1$.

Let $W[3]$ = 10011101, $g(W[0])$ = 01101100, and R_1 = 00000001.

Then $W[4]$ = 10011101 ⊕ 01101100 ⊕ 00000001 = 11110000

2. Other segments: we use $W[i] = W[i–1] \oplus W[i–4]$ for the following segments.

If $W[4]$ = 11110000 and $W[0]$ = 10101100, then:

$W[5] = W[4] \oplus W[0]$ = 11110000 ⊕ 10101100 = 01011100.

3. A complete new key: After several iterations, a unique key is generated for the next round:

K_1 = [11110000 01011100 ...].

Thus, unique keys are created for each transaction based on the initial key, taking into account the specifics of transactions, such as payment for goods, returns, or transfers. The round constants Ri can be associated with the data of a particular transaction, such as its identifier or time, which makes it difficult for attackers to find keys.

Another popular method is asymmetric encryption, in particular the RSA (Rivest-Shamir-Adleman) algorithm. It is based on the difficulty of factorizing large prime numbers.

The RSA algorithm uses a pair of keys: a public key for encryption and a private key for decryption. Mathematically, it is based on the exponentiation of a large prime number modulo a field of integers.

The process begins with the generation of two large prime numbers p and q, which are used to calculate the modulus $n = p \cdot q$. The value of n determines the size of the encryption key. Next, the Euler function is calculated $\phi(n) = (p - 1) \cdot (q - 1)$. The public exponent e is then chosen, usually 65537 due to cryptographic efficiency. The private key d is calculated as the multiplicative inverse of e modulo $\phi(n)$ This step ensures the creation of key pairs for encryption and decryption. The private key is calculated as $d \cdot \text{mod } \phi(n) = 1$.

The next step is to encrypt the card number along with the transaction context:

$$c = (M \times H(T, K_{POS}))^e \ mod \ n, \tag{6}$$

where M is credit card number (16-digit number divided into blocks); T is a unique transaction identifier (for example, the time of the transaction or a unique check number); K_{POS} is identifier of the sales terminal (for binding to a specific device); $H(T, K_{POS})$ is a hash function to verify the integrity of the transaction; C is ciphertext for storage in the retailer's database or transmission over the network.

This algorithm takes into account the context of the transaction through the parameters: a unique transaction identifier T and the identifier of the point-of-sale terminal K_{POS}. To increase security, transaction data is used as an additional factor included in the mathematical expression. They are combined through the hash function $H(T, K_{POS})$, which creates a checksum that uniquely identifies the transaction. This makes replay attacks more difficult. During the transaction, the credit card number M is encrypted along with the control data, which is achieved by multiplying the card number by the result of the hash function. After that, the resulting value is raised to the power of the public key e and the remainder is calculated by dividing by the modulus n. Thus, due to the presence of dynamic parameters, the ciphertext C becomes unique for each transaction, even if the card number is the same.

Decryption is performed by raising the ciphertext to the power of the private key d by the module n. However, to verify the authenticity of the data, the result is additionally divided by the checksum $H(T, K_{POS})$:

$$M_{dec} = \frac{C^d \ mod \ n}{H\left(T, K_{POS}\right)} \tag{7}$$

If the result matches the original card number, the transaction is considered authentic: M_{dec} = = M is the transaction is considered valid.

IF $M_{dec} \neq M$ is the transaction could be modified or retried.

This approach provides an increased level of security for retailers, reducing the risk of data reuse attacks and transaction fraud. It is ideal for POS terminals, mobile payment systems, and online stores where it is important to protect both the card number and the transaction context itself. The inclusion of additional parameters increases the cryptographic complexity and ensures the uniqueness of each ciphertext. This mathematical expression is unique because it adapts classic RSA to the needs of retailers, including protection against replay attacks and data integrity.

Access control involves restricting access to personal data only to those who are authorized to do so. The main methods are multifactor authentication (MFA), role-based access control (RBAC), and network segmentation. In retail, this can be used to restrict access to databases with customer information to employees of the relevant departments only. To do this, implement:

- multifactor authentication (MFA);
- network segmentation;
- role-based access control (RBAC).

Multi-factor authentication (MFA) is a strategy that provides an additional layer of security when accessing personal customer data in retail. It is important not only to protect banking data but also to prevent unauthorized access to customer and employee accounts. In the retail environment, where huge amounts of sensitive customer data (such as payment cards) are constantly stored, MFA helps minimize the risk of data theft or unauthorized access.

Multifactor authentication in retail includes three main factors:

- What does the user know? These can be passwords or PINs to access the customer or administrator account.
- What does the user have? Examples include one-time passwords sent via SMS or generated through applications such as Google Authenticator.
- What does the user have? Biometric data (such as fingerprint scanning or facial recognition) that is added for a higher level of security when making purchases through mobile apps or online stores.

The importance of MFA in retail is evident when customers make purchases through online stores or use mobile applications to store personal data. Hacking a password can lead to the theft of personal information, but entering an additional code or biometric data significantly reduces the likelihood of unauthorized access.

The MFA algorithm in retail looks like this:

1. The user enters their login information (password, login).
2. The system checks the entered information against the database.
3. If the password is correct, a one-time code is sent to the mobile device, which the user must enter.
4. If the entered code is correct, the user is granted access to personal data or to make a purchase

MFA for retail can be mathematically expressed as follows:

$$P_{MFA} = P_{Password} \times P_{Code} \times P_{Biometrics} \quad (8)$$

where $P_{password}$ is probability of correct password entry; P_{Code} is probability of correct entry of a one-time code, $P_{Biometrics}$ is probability of successful biometric verification (e.g., fingerprint).

Example. Many large retailers use multifactor authentication (MFA) to protect customer data. Let's take a look at three companies from the Ukrainian and European markets that have applied MFA to improve the security of payment transactions: Silpo (Ukraine), H&M (Europe), and Carrefour (Europe).

The Silpo retail chain decided to implement multifactor authentication (MFA) after noticing an increase in fraudulent transactions in its online store. Prior to the implementation of MFA, the number of fraudulent transactions was high (35 per month). After the MFA system was implemented, this figure decreased, in particular in the first 6 months, the number of such cases decreased to 10 per month. During the analysis, it was noticed that the number of unauthorized accesses decreased significantly after the introduction of an additional level of protection. Thus, MFA has not only provided improved security but also increased customer confidence in the payment system.

The well-known European retailer H&M also decided to implement multifactor authentication in its online system to ensure the security of its customers' payment data. Initially, before implementing MFA, the company had 50 fraud cases per month. After the launch of the MFA system, the number of frauds was reduced to 40 in the first few months. In the following months, the situation stabilized, and after 12 months, this figure dropped to 20 cases per month. The implementation of MFA at H&M has significantly reduced the risk of financial losses and provided more reliable protection for customers.

Carrefour, one of the largest retail chains in Europe, has also implemented multifactor authentication to protect customer data from fraudulent attacks. Before MFA was implemented, the chain had 40 cases of fraudulent transactions per month. After the introduction of multifactor authentication, the company saw a 25% reduction in fraudulent attempts in the first month and a 62% reduction in fraudulent attempts a year later. This significantly reduced the risk of financial losses and increased the security of all transactions.

Table 1

Impact of multi-factor authentication implementation on the number of fraudulent transactions

Period	Carrefour	H&M	Silpo
Before MFA implementation	40	50	35
1 month after implementation	30	40	25
3 months after implementation	20	25	15
6 months after implementation	15	20	10

Sources: Interviews with IT departments of Silpo, H&M, and Carrefour retail networks, 2024

Network segmentation is critical to ensuring the security of personal data in retail, as a retailer may store customer data on numerous servers serving different functions (e.g., payment processing, storing transaction information, product management, etc.). If the network is not properly segmented, attackers can gain access to the entire system, which can lead to data breaches.

Methods of network segmentation:

1. Logical segmentation uses VLANs to divide the network into segments, allowing you to isolate critical data from the rest of the network. For example, one for payment processing and another for normal order processing.
2. Physical segmentation uses separate servers or data centers to store sensitive data. This reduces the likelihood of penetration into the main database, even if an attacker gains access to part of the network.

To protect the data transmitted between segments, powerful encryption algorithms for segmented networks are used, such as AES (Advanced Encryption Standard), for an encrypted channel between two parts of the network. If M is the message (data) to be encrypted, K is the encryption key, and E is the encryption operation, then the CCC encrypted message is expressed as

$$C = E(K, M). \quad (9)$$

In retail, this can be used to secure payment transactions or store customer card data in encrypted form so that only authorized segments have access to it.

Network segmentation is important to protect customer payment and personal data from attacks. Let's look at three retailers in Ukraine and Europe that have used segmentation to improve security: Auchan (Ukraine), Zara (Europe), and Metro (Europe).

Network segmentation helped Auchan divide access to internal systems into segments, each of which has limited access rights. This has significantly improved the security of payment data processing. Before implementing network segmentation, the company had 25 security incidents per year. After its implementation, this figure dropped by 50% during the first year, and by 68% in two years. The main success factor was restricting access to financial and sensitive data to a limited number of employees, which significantly reduced the risk of leaks and attacks on internal systems.

Zara, a European retailer, has also applied network segmentation to protect its customers' personal and financial data. Before implementing segmentation, the company faced a significant number of security incidents—45 cases per year. After segmentation, the number of incidents decreased to 20 in one year and 15 in two years. This result was achieved through improved access control to important systems and data security, in particular by isolating critical network segments that had access to customer payment and personal data.

The European retail chain Metro implemented network segmentation to divide its internal systems into several zones, each with individual access and security rules. Before segmentation, the company had 30 security incidents per year. After implementing the segmentation, this figure dropped to 15 incidents in the first year, and to 10 in two years. This provided better protection for customer payment data and personal information, and prevented the possibility of data leaks through weaknesses in the network.

Table 2

Impact of network segmentation implementation on the number of incidents

Period	Metro	Zara	Auchan
Before network segmentation	30	45	25
1 year after segmentation	15	20	12
2 years after segmentation	10	15	8

Sources: Data from the annual reports of Auchan, Zara, Metro for 2023–2024.

Role-based access control (RBAC) is one of the main methods of managing access to data in retail. Using RBAC allows you to determine exactly who has access to what data, which is critical to ensuring privacy and preventing data breaches.

Basic principles of RBAC:

- each employee or user is assigned a role (for example, "Cashier", "Manager", "Administrator") and this role determines the level of access to the data.
- each role is assigned specific access rights, for example, only reading, editing or deleting data.
- users can interact with data only through authorized interfaces, according to their roles.

Using role-based access control allows you to restrict access to sensitive information depending on the role of the employee in the organization. Consider three retail chains that have implemented RBAC: Epicenter (Ukraine), IKEA (Europe), and Lidl (Europe).

The implementation of role-based access control (RBAC) allowed Epicenter to restrict access to sensitive data only to employees whose role required such access. Before RBAC was implemented, the number of data access errors was 20 per month. After implementing access control, this figure dropped to 12 per month after the first month and to 5 after six months. Implementation of RBAC significantly reduced the likelihood of errors in accessing important data, which helped improve security and reduce possible data leaks.

European retailer IKEA has implemented role-based access control (RBAC) to minimize the likelihood of unauthorized access to its financial and personal data. Before implementing RBAC, the company had 25 data access errors per month. After implementing the system, the number of errors decreased by 40% after the first month and by 80% after six months. This prevented unauthorized access and kept customer data more secure.

Lidl also decided to implement a role-based access control system to limit access to critical data to only the appropriate employees. Before implementing RBAC, the company had 18 access errors per month. After implementing RBAC, this figure dropped to 10 per month in the first month, and after three months, to 6 errors per month. This proves that role-based access control is an effective tool for ensuring data security in a large organization that works with a large amount of personal and payment data.

Table 3

Impact of implementing role-based access control on access restrictions

Period	IKEA	Lidl	Epicenter
Before RBAC implementation	25	18	20
1 month after implementation	15	10	12
3 months after implementation	10	6	8
6 months after implementation	5	4	5

Sources: Internal reports and interviews with IT departments of Epicenter, IKEA, and Lidl

Protecting cloud services

In modern retail, cloud technologies have become a key element for storing and processing customer personal data. This is due to the need for prompt access to information, scalability, and efficiency of working with large amounts of data. However, the use of cloud services also increases the risk of data leakage, which makes the issue of data protection particularly relevant.

Firewalls are the first line of defense for cloud services. They allow you to control incoming and outgoing traffic by blocking potentially dangerous requests. In the context of retail, firewalls help to protect customers' personal data from unauthorized access.

Firewalls provide traffic filtering, preventing attacks such as DDoS that can lead to system outages. This is especially important for large retail chains that process thousands of transactions every day.

For example, the Auchan supermarket chain has implemented modern firewalls to protect its infrastructure, which has reduced the number of security incidents by 30%. Another European chain, Lidl, also uses multi-level protection with firewalls, which allows it to block up to 95% of unsafe connections in the early stages.

Table 4

Impact of firewall implementation on retail network security

Network	Number of attacks before implementation	Number of attacks after implementation	Reduction in the number of attacks
Auchan	500	350	30%
Lidl	1000	50	95%
Silpo	600	420	30%

Sources: Data from the annual reports of Auchan, Lidl, Silpo

Real-time security monitoring allows you to detect and respond to threats instantly. This is especially important in retail, as any security breach can lead to significant financial losses and a decrease in customer confidence.

Monitoring tools, such as intrusion detection and prevention systems (IDS/IPS), allow you to detect abnormal activities and automatically take measures to neutralize them. For example, Tesco has implemented a real-time monitoring system, which has reduced the response time to incidents from 6 hours to 30 minutes.

In the Metro network, the use of the monitoring system allowed to detect 85% of threats at the stage of attempted access to the system, which significantly increased the overall level of security. The Ukrainian ATB network has also implemented similar systems, which reduced the number of successful attacks by 40%.

Table 5

Efficiency of real-time security monitoring

Network	Reaction time before implementation	Reaction time after implementation	Reduction of reaction time
Tesco	6 hours	30 minutes	90%
Metro	4 hours	1 hour	75%
ATB	5 hours	3 hours	40%

Sources: Data from the annual reports of Tesco, Metro, ATB retails network

Backups are critical to protect against data loss in the event of cyberattacks or technical failures. In retail, where large volumes of personal data are processed, backups ensure that information can be restored in the event of loss or damage.

For example, the European Carrefour chain backs up customer data on a daily basis, which allows it to keep information up-to-date and recover quickly from incidents. The Billa network uses cloud-based backup solutions to ensure reliable data protection even in the event of physical damage to servers. Novus Ukrainian network has also implemented a backup system that allows data to be stored in several geographically distributed locations, which minimizes the risk of data loss in the event of disasters.

Table 6
Data backup in retail

Network	Backup frequency	Data recovery time	Reducing data loss
Carrefour	Daily	2 hours	95%
Billa	Daily	3 hours	90%
Novus	Daily	1 hour	98%

Sources: Interviews with the IT departments of Carrefour, Billa, Novus retail networks

Implementing these security methods allows retailers to ensure a high level of security for cloud services, which in turn increases customer trust and reduces the risk of personal data leakage.

Protecting IoT devices

IoT devices, such as self-service terminals, smart surveillance cameras, or inventory monitoring systems, are widely used in retail. Vulnerabilities of these devices can be used for attacks. Securing IoT includes regular software updates, the use of built-in encryption, and physical protection of devices.

In retail, where IoT devices are used to process personal customer data, software updates are critical.

For example, supermarket chain Tesco has implemented automatic software updates on all of its IoT devices. This helped reduce the number of successful attacks by 25% in the first year after implementation. Similarly, Metro uses a centralized update management system to ensure a rapid response to new threats. The Ukrainian chain Silpo has also implemented a similar system, which has significantly increased the level of customer data protection.

Table 7
The impact of software updates on the security of IoT devices

Network	Number of attacks before implementation	Number of attacks after implementation	Reduction in the number of attacks
Tesco	400	300	25%
Metro	500	375	25%
Silpo	450	337	25%

Sources: Data from the annual reports of the Tesco, Metro, Silpo retail networks

Outdated communication protocols are another significant threat to the security of IoT devices. They can be vulnerable to attacks that have been known for a long time. Eliminating the use of such protocols and switching to modern standards significantly increases the level of security.

For example, Carrefour conducted an audit of its IoT devices and abandoned outdated protocols. This helped reduce the number of successful attacks by 40%. The European network Billa has also

updated its systems by implementing new security protocols, which has significantly increased the level of protection. The Ukrainian network Novus has implemented similar measures, which also led to a decrease in the number of successful attacks.

Table 8
The impact of eliminating outdated protocols on the security of IoT devices

Network	Number of attacks before implementation	Number of attacks after implementation	Reduction in the number of attacks
Carrefour	500	300	40%
Billa	600	360	40%
Novus	550	330	40%

Sources: Data from the annual reports of the Carrefour, Billa, Novus retail networks

Access control to IoT devices is an important component of their protection. Built-in access control allows you to restrict access to devices to only authorized users, which reduces the risk of unauthorized access.

For example, Auchan has implemented built-in access control on all of its self-service terminals. This helped reduce the number of unauthorized access incidents by 50%. The European Lidl chain has also taken similar measures, which has significantly improved security. The Ukrainian ATB chain has implemented similar measures, which helped reduce the number of incidents.

Table 9
The impact of built-in access control on the security of IoT devices

Network	Number of incidents before implementation	Number of incidents after implementation	Reduction in the number of incidents
Auchan	200	100	50%
Lidl	300	150	50%
ATB	250	125	50%

Sources: Data from the annual reports of the Auchan, Lidl, ATB retail networks

Implementation of these security methods allows retailers to ensure a high level of security for IoT devices, which in turn increases customer trust and reduces the risk of personal data leakage.

Conclusions

Implementing modern encryption algorithms such as AES and RSA is critical to protecting personal data in retail. Their use helps to increase the level of consumer confidence and compliance with security standards such as PCI DSS and GDPR.

The use of multi-factor authentication (MFA) to protect access to customer and employee accounts, the use of probabilistic models to assess the effectiveness of various authentication factors significantly increases the level of information security in the retail sector.

Protecting cloud services, including the use of firewalls and real-time monitoring systems, allows you to detect and prevent threats at an early stage, minimizing potential data loss. The use of modern security protocols, regular software updates, and access control to devices were recognized as critical to ensuring the security and protection of IoT devices, which are an important element of modern retail.

Implementation of modern mathematical models, encryption algorithms, multi-factor authentication, network segmentation and cloud service protection are key elements of ensuring reliable information security. This allows not only to protect confidential information but also to increase customer confidence in retail companies.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] S. Pletcher, Visual privacy: Current and emerging regulations around unconsented video analytics in retail, arXiv, 2023, 1–15. doi:10.31219/osf.io/tfw96

[2] O. Hyliaka, The right to privacy and protection of personal data in the context of digitalization, Bulletin of the National Academy of Legal Sciences of Ukraine, (2023) 15–25.

[3] R. Ayunda, Personal data protection to e-commerce consumer: What are the legal challenges and certainties?, Law Reform, (2022) 144–163.

[4] A. Beduschi, Synthetic data protection: Towards a paradigm change in data regulation?, Big Data & Society, (2024) 1–12.

[5] A. Pravdychenko, Personal Data Online: Problems of Regulation and Prospects for Protection, Center for Democracy and Rule of Law, (2023) 1–10.

[6] J. Zhao, D. Wu, Targeting precision in imperfect targeted advertising: Implications for the regulation of market structure and efficiency, SAGE Open, (2022) 1–15.

[7] V. O. Kovalenko, I. M. Petrova, Methods of personal data protection in retail systems, J. Inf. Secur. 3(28) (2022) 45–52.

[8] M. Johnson, K. Harris, Implementing network segmentation for data protection in retail, European J. Cybersecur. 12(4) (2022) 112–118.

[9] R. V. Ivanchenko, O. P. Tkachenko, Implementation of multifactor authentication in e-commerce, Bulletin of the Kyiv National University, 5(33) (2022) 89–97.

[10] J. Smith, R. Cooper, Data encryption techniques for retail payment systems, J. Appl. Cryptography, 18(7) (2022) 221–230.

[11] G. Martin, T. Fischer, Role-based access control: Case studies from European retail chains, Cyber Defense Review, 20(2) (2022) 134–142.

[12] K. Savchuk, et al., Data protection strategies and technologies for ensuring national financial security, in: Innovative and Intelligent Digital Technologies; Towards an Increased Efficiency, vol. 564, 2024, 431–440. doi:10.1007/978-3-031-70399-7_32

[13] N. Dovzhenko, et al., Integration of IoT and artificial intelligence into intelligent transportation systems, Electron. Prof. Sci. J. Cybersecur. Educ. Sci. Tech. 2(26) (2024) 430–444. doi:10.28925/2663-4023.2024.26.708

[14] N. Mykytenko, S. Rzaieva, Application of artificial intelligence in retail, Int. Sci.-Practical J. Commodities Markets, 50(2) (2024) 4–20. doi:10.31617/2.2024(50)01

[15] S. Rzaieva, et al., Methods of modeling database system security, in: Cybersecurity Providing in Information and Telecommunication System, vol. 3654, 2024, 384–390.

[16] V. Lakhno, et al., Continuous investing in advanced fuzzy technologies for smart city, in: computational intelligence and data analytics, LNDECT, vol. 142, 2023, 313–327. doi:10.1007/978-981-19-3391-2_24

[17] A. Barbashyn, Personal data protection and GDPR for business, Barbashyn Law Firm, 2023, 1–9.