Informatyka techniczna i sztuczna inteligencja
Technical informatics and Artificial Intelligence
Engineer of XXI Century'2024

Development of a secure method for data storage in databases and its visualization on web platforms

Oleh Koval [1], Oleh Harasymchuk [2,*], Vasyl Ramsh [3]

[1] *Lviv Polytechnic National University, 12 Bandera St., Lviv 79013, Ukraine, oleh.koval.mkbbi.2024@lpnu.ua*
[2] *Lviv Polytechnic National University, 12 Bandera St., Lviv 79013, Ukraine, oleh.harasymchuk@gmail.com*
[3] *Separated Subdivision of National University of Life and Environmental Sciences of Ukraine Berezhany agrotechnical institute, 20 Academichna St., Berezhany 47501, Ukraine, ramsh_v@ukr.net*
* *Corresponding author, oleh.harasymchuk@gmail.com*

Abstract: This article is dedicated to the research and improvement of methods for data storage in the Database and their transmission to a web platform for further display. As Databases contain and process various data, often of a confidential nature, security issues during their storage, processing, and transmission to web resources, become very important. The primary focus is on developing enhanced methods of data storage in the database and ensuring their security during transmission. This research is based on studying current scientific sources and informational resources of various kinds, including database protection methods and the most common security issues. Specifically, we explore the top 10 security risks for web applications, as identified by OWASP.

Keywords: Databases, Data storage, Database security, Web platform, XSS, DDos, HTTP, SSL/TLS, cryptography, hashing, OWASP security risks;

Opracowanie bezpiecznej metody przechowywania danych w bazach danych i ich wizualizacji na platformach internetowych

Oleh Koval [1], Oleh Harasymchuk [2,*], Vasyl Ramsh [3]

[1] *Uniwersytet Narodowy Politechnika Lwowska, ul. St. Bandery 12, Lwów 79013, Ukraina, oleh.koval.mkbbi.2024@lpnu.ua*
[2] *Uniwersytet Narodowy Politechnika Lwowska, ul. St. Bandery 12, Lwów 79013, Ukraina, oleh.harasymchuk@gmail.com*
[3] *Oddzielny oddział Narodowego Uniwersytetu Nauk Przyrodniczych i Środowiskowych Ukrainy, Instytut agrotechniczny Bereżany, ul. Academichna 20, Bereżany 47501, Ukraine, ramsh_v@ukr.net*

* *Corresponding author, oleh.harasymchuk@gmail.com*

Streszczenie: Artykuł poświęcony jest badaniom i udoskonalaniu metod przechowywania danych w bazie danych i ich transmisji na platformę internetową w celu dalszego wyświetlania. Ponieważ bazy danych zawierają i przetwarzają różne dane, często o charakterze poufnym, kwestie bezpieczeństwa podczas ich przechowywania, przetwarzania i przesyłania do zasobów internetowych stają się bardzo ważne. Główny nacisk kładzie się na opracowanie ulepszonych metod przechowywania danych w bazie danych i zapewnienie ich bezpieczeństwa podczas przesyłania. Badania te opierają się na badaniu bieżących źródeł naukowych i zasobów informacyjnych różnego rodzaju, w tym metod ochrony baz danych i najczęstszych problemów bezpieczeństwa. W szczególności badamy 10 największych zagrożeń bezpieczeństwa dla aplikacji internetowych, zidentyfikowanych przez OWASP.

Słowa kluczowe: Bazy danych, Przechowywanie danych, Bezpieczeństwo baz danych, Platforma internetowa, XSS, DDos, HTTP, SSL/TLS, kryptografia, hashowanie, Zagrożenia bezpieczeństwa OWASP;

DOI: https://doi.org/10.53052/9788367652292.06

1. Introduction

As information technology has become more integrated into daily life, information itself has become a key element of modern society. Consequently, information security is essential and must be continually improved, as weak security can lead to sensitive data loss. Recent years have seen an increase in security incidents, such as the Facebook breach (2020) and BlueLeaks (2020), highlighting vulnerabilities in even the largest systems. Beyond direct losses, companies suffer reputational damage, losing trust from customers and partners. Data breaches also carry legal consequences, particularly with regulations like GDPR [1-3].

Given the significance of secure databases and web platforms for organizations, ensuring the safety of data is crucial. Common vulnerabilities include weak authentication mechanisms, SQL injections, and cross-site scripting (XSS). This research focuses on analyzing vulnerabilities in databases and web platforms, developing methods for securely encrypting data and safely displaying it on web platforms to protect user privacy.

The goal is to analyze existing vulnerabilities and develop security measures to ensure the integrity and confidentiality of data during storage, processing, and use across these systems.

Research tasks include:

1. Analyzing the use of databases with web platforms.
2. Identifying potential threats in storing unprotected data.
3. Proposing an improved method for encrypted data storage and secure retrieval.
4. Implementing and testing this method for effectiveness.

The study aims to enhance data protection, offering practical solutions for secure data handling at every stage, including encryption and defense against XSS and SQL injection attacks.

2. Databases and Web platform

2.1. Databases

A database (DB) is an organized structure designed to store, modify, and process interrelated data, typically in large volumes [4-7]. Databases are crucial for dynamic websites with significant data demands, such as online stores, portals, or corporate websites. They consolidate vast amounts of information, including customer details, order histories, product catalogs, and more, allowing for flexible grouping of data .

One key advantage of databases is their speed in both inputting and retrieving information. Thanks to specialized algorithms, necessary data can be accessed within seconds. Additionally, databases enable complex interactions, where a change in one record can affect others . For instance, a web-based database stores essential information such as customer data, product lists, and price points, ensuring the smooth operation of websites.

```
SELECT TOP (1000) [id]
      ,[code]
      ,[firstName]
      ,[lastName]
      ,[locationID]
  FROM [SampleDB].[dbo].[employees]
```

100 %

Results | Messages

	id	code	firstName	lastName	locationID
1	1	code1	firstName 1	lastName 2	1
2	2	code2	firstName 2	lastName 2	2
3	3	code3	firstName 3	lastName 3	2
4	4	code4	firstName 4	lastName 4	3

Figure 1. Example of SQL Query

In relational databases, data is organized in tables with rows and columns. Rows represent objects (such as customer details), while columns represent attributes of those objects. These databases allow modeling complex relationships

between data using foreign keys. This not only reduces data redundancy through normalization but also maintains the system's integrity by ensuring all entries are connected properly. For example, in a restaurant's menu database, dishes are linked to categories using foreign keys, minimizing duplication and simplifying the addition of new items .
The primary tool for querying relational databases is SQL (Structured Query Language). SQL is used to create, modify, and query data stored in these databases. Common SQL operations include selecting data, inserting new entries, updating existing records, and deleting entries. For example, the command retrieves the first and last names of all customers from the database.

When designing a database, it's essential to visualize all relationships between data elements. This is part of the conceptual design phase, where an ER (Entity-Relationship) diagram is often used to depict entities and their relationships in the database.

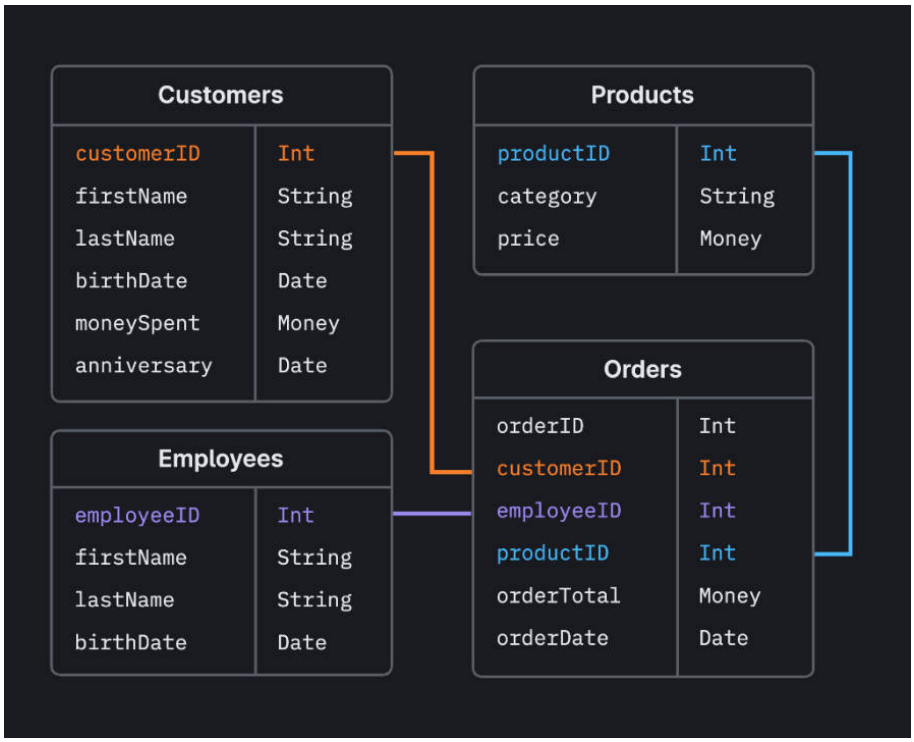

Figure 2. Entity-Relationship in relation Database

2.2. Web platform

The Web Platform is a collection of technologies developed as open standards by the World Wide Web Consortium (W3C) and other standardization bodies such as WHATWG, Unicode Consortium, IETF, and Ecma International [8]. It was introduced as a hypernym by W3C and defined in 2011 by CEO Jeff Jaffe as "a platform for innovation, consolidation, and economic efficiency." The creation of standards considering the Evergreen Web has enabled the addition of new capabilities while addressing security and privacy risks. The Web Platform includes technologies like HTML, CSS, SVG, MathML, ECMAScript, WebGL, and various APIs that facilitate the publication of web pages.
It serves as an interactive online environment designed to enhance user interaction and provide access to diverse content and functionalities through web browsers. The main objective is to analyze, visualize, and interpret statistical data via web browsers, allowing users to upload, process, and display data using a wide range of statistical methods and tools.
Key quality criteria for the platform include:

1. Data Display Speed: Users expect instant responses when viewing pages.
2. Reliability During Data Loading: The platform must handle data uploads efficiently, ensuring accuracy and integrity.
3. Database Query Optimization: The effectiveness of database interaction relies on the quality of SQL queries and database structure.
4. Scalability: The system must handle increased data volumes and user loads without performance loss.

5. Data Security: Access must be limited and protected from unauthorized access, requiring authentication, authorization, and encryption mechanisms.
6. User Session Support: Maintaining user sessions improves user experience by preserving interaction context throughout server requests.

3. Analysis of potential threats to the Database and Web platform

3.1. Analysis of potential threats to the Database

In the contemporary era of rapid advancements in cyberspace, the necessity for implementing information technologies is increasingly prominent. Among these technologies, the utilization of databases (DBs) has emerged as an optimal approach for managing large volumes of information within organizations. Recent statistics reveal a worrying trend: the frequency of data breaches has been steadily rising. This alarming increase underscores the importance of protecting data from unauthorized access, which has become a critical priority in the design and development of any information system [9].

To address these challenges, it is essential to conduct a thorough analysis of the threats faced by databases and to explore effective prevention methods. The potential destruction of corporate data storage or the loss of access to vital information can result in catastrophic consequences for organizations. Notable incidents in recent years highlight the risks involved. For instance, in 2016, the cybersecurity firm Threat Connect investigated attacks on voter databases in two U.S. states and discovered that these attacks originated from the same IP address associated with previous cyber assaults on Ukraine, Turkey, and Germany. In a similar vein, the World Anti-Doping Agency (WADA) accused Russia of hacking into secret databases concerning doping practices among American athletes. Additionally, a significant cyberattack by Chinese hackers in 2014 targeted the personnel records of the U.S. Office of Personnel Management, compromising sensitive information about federal employees seeking access to classified data.

Given that databases represent some of the most valuable corporate assets, they must be adequately protected using appropriate methods and techniques. The primary threats to databases include data theft and falsification, loss of confidentiality, breaches of personal data integrity, loss of data integrity, and loss of availability. Other concerns involve misconfigured database privileges and poor data management practices. The interconnected nature of these threats means that a breach in one area often diminishes security in others, making it crucial for organizations to maintain constant vigilance and monitor all possible channels for information leaks.

Protecting the confidentiality of sensitive information is vital, as it involves keeping data secret and ensuring that access is restricted to authorized individuals. Furthermore, the loss of data integrity can lead to corruption or destruction of information, which may have severe repercussions for an organization's operations, such as losing competitive advantages or the validity of overall data. In cases where data or systems become unavailable, organizations that rely on continuous operation may find themselves facing significant financial threats and disruptions in management systems that depend on databases.

In addressing these overarching issues of information security and data protection, it is important to consider traditional methods and tools for safeguarding databases. Although protection strategies can vary depending on the database management systems (DBMS) in use, common practices often include user authorization to control access, the use of views to present data securely, regular backup and recovery procedures, integrity maintenance mechanisms, encryption of sensitive information, and the application of hardware fault tolerance to prevent system failures.

3.2. Analysis of potential threats to the Web platform

Ensuring the security of web resources has become one of the most pressing issues in information security due to the widespread vulnerabilities that many websites exhibit and their constant exposure to cyberattacks. Web applications face a variety of threats, primarily encompassing issues of confidentiality, integrity, and availability. External attackers are often the main source of these threats, typically motivated by commercial interests and possessing substantial expertise in network security.

Hacker attacks represent the most significant threat to website security. These attacks can be either targeted or indiscriminate, often relying on the principle of “attack everything and see what breaks.” Targeted attacks focus on identifying various vectors of attack to exploit specific vulnerabilities, whereas indiscriminate attacks utilize mass methods to exploit superficial weaknesses in many systems at once [10].

Among the most common vulnerabilities is SQL injection, a method where attackers inject malicious SQL code into web application queries. This allows them to gain unauthorized access to databases, manipulate or destroy data, and execute harmful commands on the server.

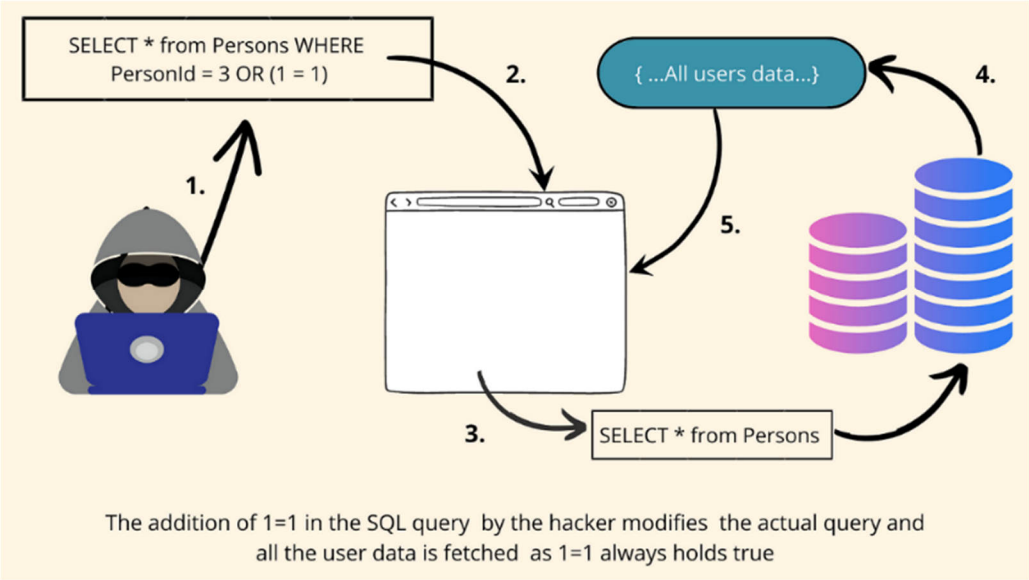

Figure 3. Attack principle SQL-injection

Another prevalent threat is Cross-Site Scripting (XSS), where attackers inject harmful scripts into web pages. These scripts execute in the browsers of unsuspecting users, potentially stealing cookies or performing actions on behalf of the user without their consent.

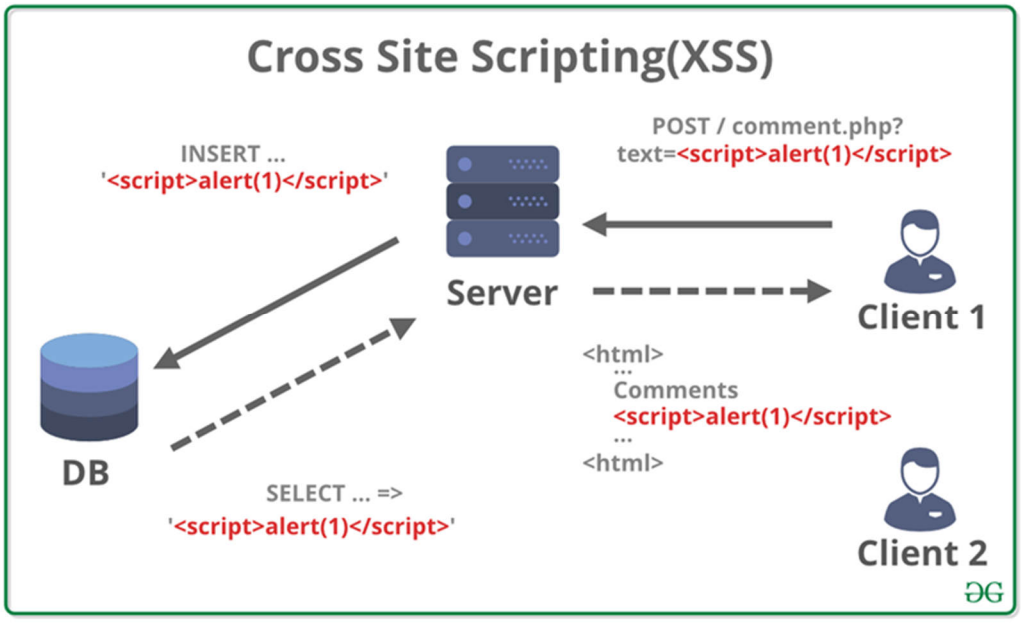

Figure 4. Attack principle Cross-Site Scripting (XSS)

Denial-of-Service (DoS) attacks aim to disrupt the normal functioning of a server by overwhelming it with excessive requests, making it unable to respond to legitimate users. Distributed Denial of Service (DDoS) attacks amplify this tactic by utilizing multiple computers to launch a coordinated attack, making it much harder for the targeted system to defend itself.

The increasing prevalence of attacks on websites can be attributed to two primary factors: lax security measures and inadequate defenses against potential attackers.

The proliferation of security tools and scanners for websites has lowered the barriers to entry for potential attackers. Communities, forums, and repositories foster the sharing of attack techniques among users, and the rapid dissemination of information regarding new vulnerabilities exacerbates the situation.

To mitigate these risks, organizations can enhance their security posture by adhering to guidelines from initiatives like the Open Web Application Security Project (OWASP). OWASP actively collects and publishes information about common web application vulnerabilities, including the OWASP Top Ten—a list of the most prevalent risks threatening web applications. By following these recommendations, developers and security teams can better identify and address serious vulnerabilities, ultimately providing more robust protection for web resources [11].

4. Development of an improved data protection method and its visualization

4.1. Conception of protection mechanism

It's essential to recognize that there is no absolute protection against cyberattacks, but you can significantly reduce risks by focusing on the most vulnerable areas where data theft commonly occurs. Protecting these critical points can minimize the chances of data breaches.

One of the most effective methods for safeguarding data in databases is encryption. Encrypting data before storing it ensures a high level of security. Even if attackers gain access to the database, they will not be able to interpret the encrypted data without the encryption key. This process maintains data confidentiality even in case of security breaches. The use of strong encryption algorithms is crucial for securing data both at rest and in transit. AES (Advanced Encryption Standard) is widely recommended for its reliability. The AES_CBC encryption function works in several steps to ensure secure data handling:

1. Salt Generation: Random data is added to the password before deriving the encryption key to make brute-force attacks more difficult.
2. Key Derivation: The password is transformed into a more complex key using a hash function, like PBKDF2 with SHA-256, to generate a secure key.
3. IV Generation: An Initialization Vector (IV) ensures unpredictability during the encryption process.
4. Cipher Creation: AES-CBC mode is used for encryption with the derived key and IV.
5. Data Encryption: Data is encrypted in fixed-size blocks, ensuring security at each step.
6. Ciphertext Formation: Encrypted blocks are combined to create the final encrypted text.
7. Base64 Encoding: The encrypted text is encoded for easy storage and transmission in a text format.

To enhance data security, it's crucial to design a database architecture where each user gets their own isolated schema upon registration. This schema-per-user approach ensures data isolation and privacy, as each user has their own space within the database, reducing the risk of unauthorized access. A central schema manages user metadata and maps users to their respective schemas, while sensitive data is encrypted before storage for an added layer of protection.

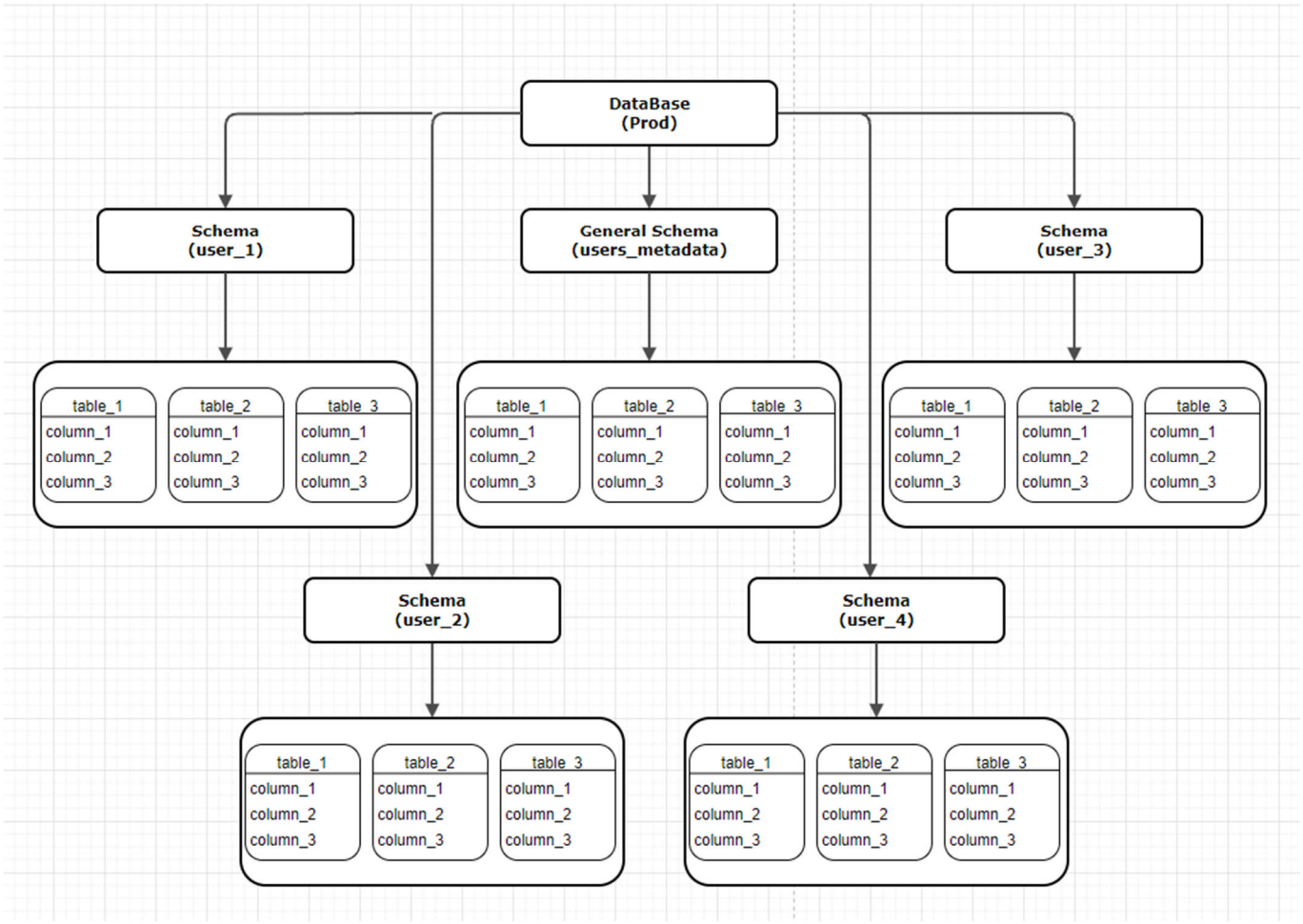

Figure 5. Database Architecture Schema per user

Proper access control is vital. Developers must rigorously manage who has access to specific data to prevent unauthorized changes or deletions, much like guarding a vault. Without this control, the risk of data manipulation increases significantly.

The architecture also supports scalability—schemas can be distributed across servers as the user base grows, balancing system load and improving performance. Additionally, security tools like Fortify should be used to monitor and analyze code for vulnerabilities, while regular audits and penetration testing are essential to maintain system integrity.

Frequent backups are another key element of this strategy. Isolated schemas make it easier to back up and restore individual user data without impacting the entire database, ensuring data recovery in case of unforeseen events.

However, encryption and security measures can slow down data processing, creating a trade-off between security and performance. Careful consideration is needed to balance these factors when designing and optimizing data storage systems.

Developers must ensure that all critical keys and credentials are stored securely to avoid potential security threats. Access should be restricted to authorized users only. One effective way to safeguard these keys and credentials is by using specialized secret management systems like HashiCorp Vault or AWS Secrets Manager. These systems are designed to store, manage, and automate the handling of secrets, providing strong protection. They offer features like data encryption at rest, automated access control, and user activity auditing. Implementing such systems helps maintain the confidentiality and security of keys and credentials, ensuring that external users cannot access critical components of your platform and database.

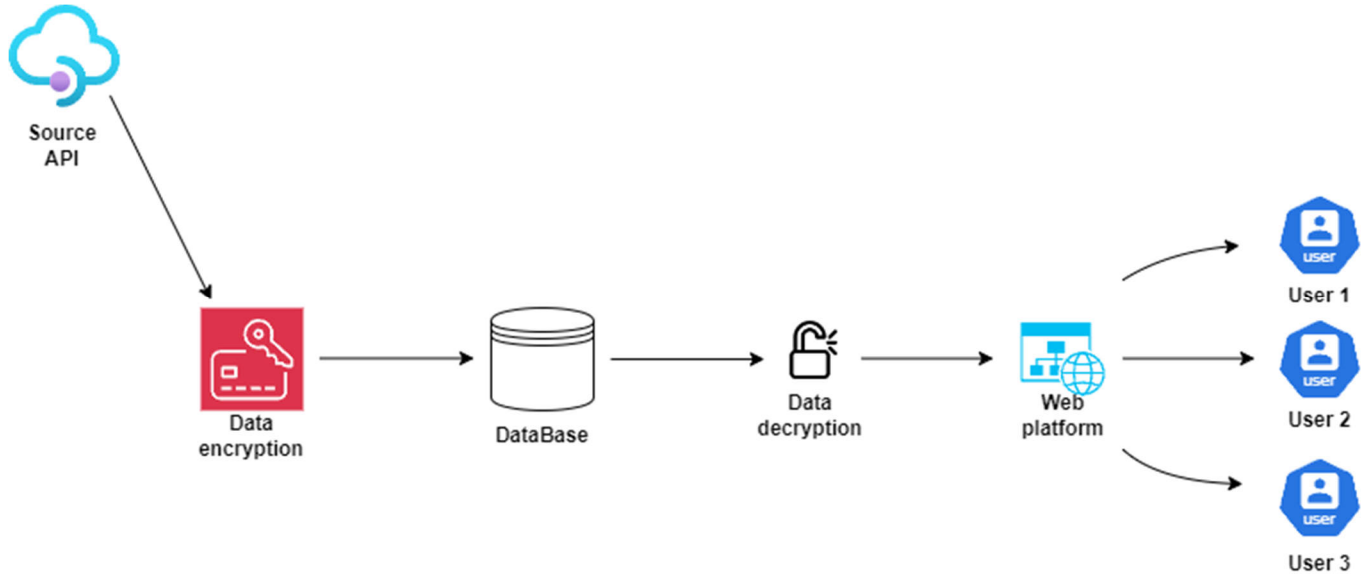

Figure 6. Flow of getting, writing, encrypting and display data

4.2. Security recommendations for Database and Web platform security

To ensure robust data security on a web platform, it's essential to implement a comprehensive set of protection measures. These strategies help safeguard sensitive information, maintain data integrity, and prevent unauthorized access. With growing sophistication in cyber-attacks, it's critical to address vulnerabilities that could lead to data breaches, service disruptions, or manipulation of information. The following are key measures to strengthen data transmission security, both at the network and application levels:

1. Protection from SQL Injection:
   - Use parameterized queries to pass user data as parameters, preventing malicious SQL code from being executed within the database.
   - Input validation should be enforced to ensure data meets expected formats (e.g., checking for the presence of only valid characters and ensuring data types are correct). This step reduces the risk of executing unwanted commands.
   - ORM frameworks (like Hibernate or Entity Framework) automatically generate SQL queries based on code-level objects, reducing the likelihood of SQL injection by abstracting the query-writing process.
2. Cross-Site Scripting (XSS) Protection:
   - Escape special characters (such as `<`, `>`, `&`, etc.) before displaying user input in the browser, ensuring malicious scripts cannot be injected into web pages.
   - Input validation should be performed to check for potentially harmful data before it is processed or rendered on the web page.
   - Implement security headers like Content Security Policy (CSP), which restricts which sources are allowed to execute scripts on the page, thereby mitigating XSS attacks.
3. Protection from Packet Sniffing:
   - Enforce the use of HTTPS for all connections, which ensures that data is encrypted in transit using SSL/TLS protocols, preventing attackers from intercepting and reading data.
   - Implement end-to-end encryption on both the client and server sides, so that even if packets are intercepted, the data remains unreadable without the proper decryption key.
   - Use multi-factor authentication (MFA) to add an extra layer of protection, ensuring that even if a password is compromised, unauthorized access is less likely.
4. DDoS Protection:
   - Leverage cloud-based DDoS protection services like Cloudflare, WS Shield, or Akamai that automatically detect and block large volumes of malicious traffic designed to overwhelm the server.
   - Real-time traffic monitoring is crucial for detecting abnormal activity patterns that may indicate an impending DDoS attack. Automatic alerts can trigger defensive responses before the attack causes significant damage.

- Deploy network filters and firewalls to block traffic from suspicious IP addresses and limit the number of requests from any single source. This helps mitigate DDoS attacks by filtering out harmful traffic before it reaches the server.

5. Conclusion

The foundation of this work stems from the urgent need to analyze and improve the methods used for storing data in databases and ensuring its secure transmission to web platforms. In today's digital landscape, where data integrity and confidentiality are paramount, this work addresses critical vulnerabilities that could compromise user data and application performance.

Throughout this research, substantial improvements have been made to bolster data security within databases and during data transfer. These enhancements include implementing additional encryption before data is recorded and optimizing the architecture of data storage and transmission channels, which safeguard sensitive information and enhance overall system reliability.

The specific tasks undertaken in this thesis include:

- Analyzing Database Use in Web Platforms: Exploring how databases integrate with web platforms and ensuring secure integration.
- Conducting In-Depth Threat Analyses: Investigating risks associated with storing unprotected data in databases and the impact on information displayed on web platforms.
- Proposing an Improved Method for Encrypted Data Storage: Developing a secure method for storing and transferring encrypted data to web platforms.
- The scientific novelty of this work includes:
- Enhancing Data Storage Methods: Presenting a refined technique for data storage that incorporates additional encryption, boosting reliability and confidentiality.
- Addressing Common Data Security Issues: Exploring prevalent security concerns in web platforms and databases, particularly during data processing and transmission.
- Developing a Comprehensive Data Protection Strategy: Establishing an integrated method for protecting data in databases and web platforms, including encryption, secure connections, and defenses against attacks like XSS and SQL injection.

In summary, this thesis addresses critical data security issues and contributes to the field of cybersecurity by enhancing methodologies for safeguarding databases and web platforms against cyber threats. The work aims to provide practical solutions and insights applicable in real-world scenarios to protect sensitive information and maintain data integrity.

References

1. Sotheby's Is Selling the First NFT Ever Minted—and Bidding Starts at $100. Available online: https://news.artnet.com/market/sothebys-is-hosting-its-first-curated-nft-sale-featuring-the-very-first-nft-ever-minted-1966003, (accessed on 07.10.2024).
2. Security challenges and solutions in web development-protecting data in SQL and NOSQL Available online: ttps://www.researchgate.net/publication/379947810_security_challenges _and_solutions_in_web_development-protecting_data_in_sql_and_nosql_databases, (accessed on 10.10.2024).
3. Threat Intelligence Sharing Platforms: Enhancing Cyber Defense Collaboration. Available online: https://www.researchgate.net/publication/380511842_threat_intelligence_sharing_platforms_enhancing_cyber_defense_collaboration, (accessed on 10.10.2024).
4. A web-based platform for the annotation and analysis of NAR-published databases. Available online: https://www.researchgate.net/publication/374938887_A_web-based_platform_for_the_annotation_and_analysis_of_NAR-published_databases, (accessed on 12.10.2024).
5. What is Database? Available online: https://www.geeksforgeeks.org/what-is-database/, (accessed on 12.10.2024).
6. Koval O., Harasymchuk O. Development of a Hybrid Method for Data Warehouse Construction.CSN. 2024; Volume 6, Number 1 : pp. 67 – 80. https://doi.org/10.23939/csn2024.01.067
7. Harasymchuk O., Buzhovych O. Strategies and innovative approaches to database protection in the age of growing cyber threats// Ukrainian Scientific Journal of Information Security, 2024, vol. 30, issue 1, pp. 166-178. https://doi.org/10.18372/2225-5036.30.18618.

8. ZION: A Scalable W3C Web of Things Directory. Available online: https://www.researchgate.net/publication/379056585_ZION_A_Scalable_W3C_Web_of_Things_Directory, (accessed on 12.10.2024).
9. Web Application Security Education Platform Based on OWASP API Security Project. Available online: https://www.researchgate.net/publication/367084892_Web_Application_Security_Education_Platform_Based_on_OWASP_API_Security_Project (accessed on 14.10.2024).
10. Essentials of Big Data Security Introduction to Big Data Security. Available online: https://www.researchgate.net/publication/379054076_Essentials_of_Big_Data_Security_Introduction_to_Big_Data_Security (accessed on 14.10.2024).
11. OWASP Top 10 API Security Risks – 2023. Available online: https://owasp.org/API-Security/editions/2023/en/0x11-t10/ (accessed on 14.10.2024).