ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ / INFORMATION TECHNOLOGY

УДК 004.056.2:004.65

Bohdan Vasylenko, Kseniia Kugai
(Kyiv, Ukraine)

METHODS OF ENSURING DATA INTEGRITY AND VERIFICATION IN AUTOMATED EVALUATION SYSTEMS

The article analyzes technical methods for maintaining data integrity within automated evaluation systems. It focuses on implementing cryptographic hashing, server-side validation, and audit logging to prevent unauthorized data modification. The proposed architectural solutions aim to ensure the reliability and transparency of results in distributed environments.

Keywords: *data integrity, automated evaluation, cryptographic hashing, audit log, information security, distributed systems.*

Стаття аналізує технічні методи забезпечення цілісності даних в автоматизованих системах оцінювання. Основну увагу приділено впровадженню криптографічного хешування, серверної валідації та логування аудиту для запобігання несанкціонованій модифікації даних. Запропоновані архітектурні рішення спрямовані на забезпечення надійності та прозорості результатів у розподілених середовищах.

Ключові слова: *цілісність даних, автоматизоване оцінювання, криптографічне хешування, аудит дій, інформаційна безпека, розподілені системи.*

Digital systems are now common in both educational and competitive settings, especially where results are processed automatically. Such platforms work with data that directly influences scores, rankings, and final decisions. Because of this, the issue is not only how the system functions, but also how well it protects records from unauthorized changes. In the article, data integrity is defined as the ability to maintain the correctness and consistency of information while it is stored, transferred, and processed. In evaluation systems, even small unauthorized edits may affect the fairness of the final result. For that reason, the article examines several practical technical methods to help reduce this risk.

Theoretical Foundations of Data Reliability. Data protection begins with the system's overall structure. On many digital platforms, multiple clients interact with a central server, creating multiple points where inconsistencies may arise. As M. Kleppmann notes, systems that process large volumes of data should be designed with fault tolerance and consistency in mind so that concurrent operations do not damage the correctness of records [2, p. 18]. In an automated evaluation system, this means that different authorized users should see the same verified version of the data. Database constraints and foreign keys are useful here, but on their own, they are not enough to prevent deliberate interference. Because of this, integrity checks should be built into multiple levels of the system.

Analysis of Integrity Threats. Automated evaluation platforms may be exposed to several threats that affect the correctness of stored results. One common risk is SQL injection, when malicious input is used to interfere with database operations and alter records. Another threat arises during data transmission: if communication between the client and the server is not properly protected, an attacker may intercept and modify the transmitted data. Internal misuse must also be considered, as users with extended access rights may influence results without obvious signs of interference. Under such conditions, ordinary data storage is not sufficient. The system must include verification mechanisms that detect unauthorized modifications.

System Architecture and Design. The proposed solution involves a multi-tier architecture where each component is responsible for a specific stage of data verification. This design separates the user interface from the processing logic and the storage layer.

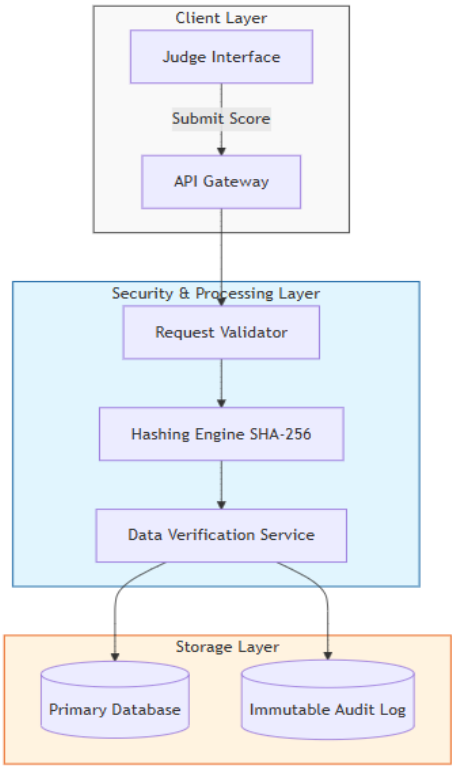

Fig. 1. Multi-tier architecture of the evaluation system

The API Gateway acts as the first line of defense by performing initial request filtering. Every incoming packet undergoes validation to ensure that the sender has the necessary permissions. This separation between the interface and the validation layer reduces the risk that a compromise in the web interface will automatically affect the entire data processing chain. The validation service checks the range and format of the evaluation data before passing it to the next module.

Cryptographic Hashing for Data Verification. One practical way to ensure data integrity is to use cryptographic hashing. In this approach, a data record is converted into a fixed-length value that acts as its verification signature. Such a value cannot be used to restore the original content, but it can be used to detect whether the record has been changed. According to W. Stallings, a secure hash function must make it computationally infeasible to produce identical outputs for different inputs [3, p. 312]. In the proposed system, SHA-256 is applied to a combination of the score, the participant identifier, and a secret salt in order to generate a unique control value for each submission.

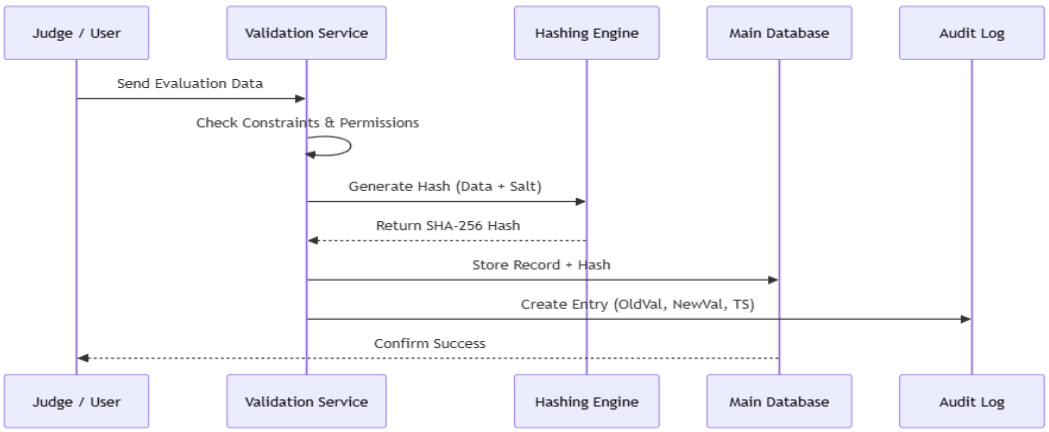

Fig. 2. Sequence of hashing and storage

The resulting hash is stored in the database alongside the evaluation record. Whenever the record is accessed or checked later, the system generates a new hash from the current values and compares it with the saved one. If both values match, the record is treated as unchanged. If they differ, the system identifies the record as potentially altered and excludes it from trusted processing. In this way, hashing acts as a control mechanism that helps reveal modifications made outside the expected application workflow.

Implementation of Immutable Audit Logs. Hash verification is more effective when the system also keeps a history of important changes. For this reason, an audit log may be used to record actions related to sensitive evaluation data. In a safer design, such entries are added in sequence and should not be edited or deleted later. Hash-based mechanisms described in ISO/IEC 10118-3 can support integrity control when tampering resistance is critical [1]. In this model, database triggers automatically record the previous value, the new value, the update time, and the user who made the change.

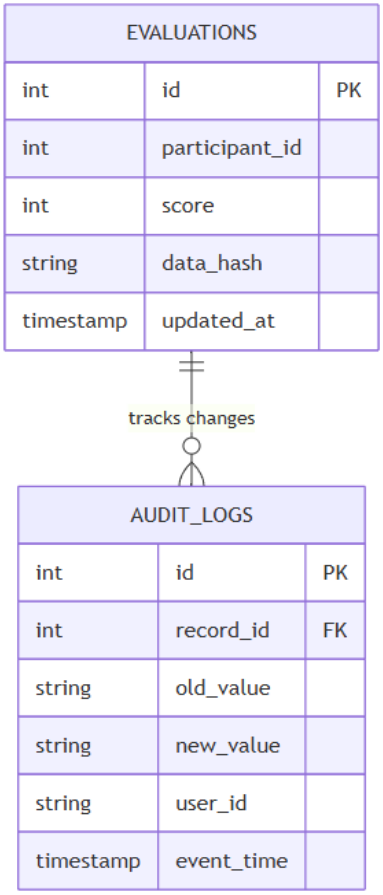

Fig. 3. Relationship between evaluations and audit logs

This approach enables the reconstruction of the sequence of events associated with a particular evaluation record. If inconsistencies appear in the final results, administrators can review when the change occurred and which user account was involved. In this sense, the audit log works as an additional layer of control alongside cryptographic hashing. It improves the system's transparency and strengthens accountability for actions performed on the platform.

Data Transmission Security. Data protection matters not only in storage but also while information moves between system components. In this system, JSON Web Tokens are used to support access control and confirm user identity. Each token is signed by the server and contains role-related data needed for verification. When a user submits an evaluation, the token is sent together with the request and checked before any further processing begins. It does not remove every possible threat, but it helps reduce unauthorized submissions and makes misuse less likely. Together with server-side validation, this measure creates a more reliable environment for handling evaluation data.

Thus, data integrity in automated evaluation systems cannot be supported by a single mechanism alone. Hashing helps identify changes in records, while audit logs make those changes easier to trace over time. Separating validation, processing, and storage functions also improves overall system control. Taken together, these measures make evaluation results more transparent and easier to verify. As a result, they can improve confidence in digital assessment platforms used in educational and competitive practice.

REFERENCES

1. International Organization for Standardization. (2018). *ISO/IEC 10118-3:2018 Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions.* URL: https://cdn.standards.iteh.ai/samples/67116/35affcb89e9c4fafb695cf3fe7d0a534/ISO-IEC-10118-3-2018.pdf

2. Kleppmann, M. (2017). Designing Data-Intensive Applications. The Big Ideas Behind Reliable, Scalable, and Maintainable Systems. O'Reilly. URL: https://unidel.edu.ng/focelibrary/books/Designing%20Data-Intensive%20Applications%20The%20Big%20Ideas% 20Behind%20Reliable,%20Scalable,%20and%20Maintainable%20Systems%20by%20Martin%20Kleppmann%20(z-lib.org).pdf

3. Stallings, W. (2022). Cryptography and Network Security: Principles and Practice. Pearson. URL: https://www.uoitc.edu.iq/images/documents/informatics-institute/Competitive exam/Crypto graphy_and_Network_Security.pdf

УДК 004.89:681.518

Максим Галькевич
(Одеса, Україна)

ОГЛЯД НЕЙРОМЕРЕЖЕВИХ МЕТОДІВ У ЗАДАЧАХ АВТОМАТИЧНОГО КЕРУВАННЯ ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ

У статті проведено аналіз застосування штучних нейронних мереж (ШНМ) як інструменту вдосконалення класичних систем автоматичного керування технологічними процесами (АКТП). Розглянуто архітектури нейро-ПІД регуляторів, методи прогнозного керування на основі нейромережевих моделей (NMPC) та підходи до навчання з підкріпленням для оптимізації нелінійних динамічних об'єктів. Визначено переваги нейромережевих методів у порівнянні з традиційними методами ідентифікації та керування в умовах невизначеності параметрів об'єкта.

Ключові слова: *штучний інтелект, нейронні мережі, автоматичне керування, ПІД-регулятор, нейроуправління, ідентифікація систем, нелінійні системи, промислова автоматизація.*

The article analyzes the use of artificial neural networks (ANN) as a tool for improving classical automatic control systems. Neural-PID controller architectures, model predictive control (NMPC) based on neural networks, and reinforcement learning approaches for optimizing non-linear dynamic objects are considered. The advantages of neural network methods compared to traditional identification and control methods under uncertainty are determined.

Keywords: *artificial intelligence, neural networks, automatic control, PID controller, neurocontrol, system identification, non-linear systems, industrial automation.*

Класичні методи автоматичного керування, що базуються на лінійних моделях (зокрема ПІД-регулятори), часто виявляються недостатньо ефективними при роботі зі складними технологічними процесами, що мають суттєве запізнення та нелінійність. Як