DOI https://doi.org/10.36059/978-966-397-491-0-42

ENSURING THE SECURITY OF INFORMATION SYSTEMS IN DISTRIBUTED ENTERPRISES IN CONDITIONS OF UNSTABLE COMMUNICATION SYSTEM OPERATIONS

Khniunin S. H.
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Department of Information Technologies
International Humanitarian University
Odesa, Ukraine

Shvedu M. I.
2nd-year Master's student in Cybersecurity and Information Protection
International Humanitarian University
Odesa, Ukraine

In recent years of the war, one of the most critical tasks for many enterprises in Ukraine is maintaining the operational status of their energy systems and communication networks. There are numerous distributed enterprises with one or more main offices and multiple branches. The operation of such enterprises, located across vast areas, with remote sites or operating across multiple countries, heavily depends on the connection with branches, which require continuous (or periodic) access to a unified database.

In the functioning of distributed enterprises, maintaining communication lines and energy infrastructure is of paramount importance. While energy independence can be achieved through the use of diesel generators or battery-powered power stations, the loss of communication between separate enterprise structures can negatively impact the overall performance of the system.

Such circumstances have affected not only Ukraine but also other countries in Europe and Asia. For example, one can mention the cable breaks, both power and communication cables, in the Baltic Sea between 2023 and 2025 [1], as well as the damage to the communication cable connecting Taiwan to the mainland by the anchor of a Chinese ship on February 22, 2025 [2].

Previously, the server's connection with nodes was commonly made via a dedicated communication channel. However, in today's realities, it is necessary to switch to alternative methods, including the use of external data carriers delivered by couriers or special postal services [3].

In such cases, to ensure the system's functionality, it is essential to convert the information that needs to be transmitted into a standardized electronic format, represented as individual dedicated files. The input/output, storage, and transfer

processes, illustrated in Fig. 1, must be carried out in standard formats among all participants in the system's lifecycle.

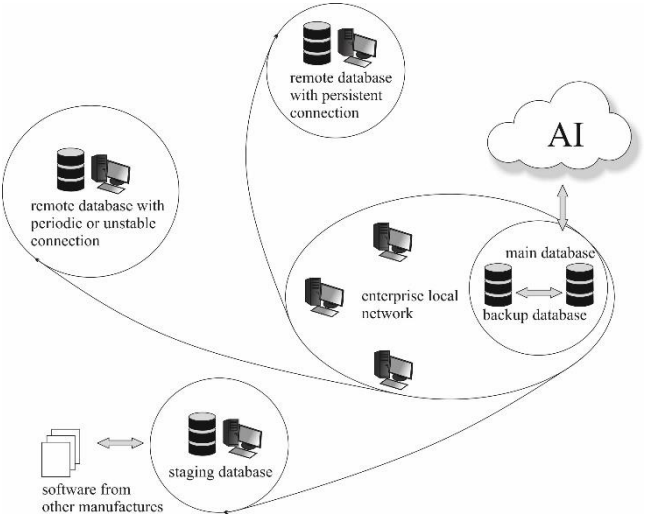

Fig. 1. Data Transmission Organization in a Distributed Enterprise System

In addition to the problems of information transmission, which are addressed through technical means, an important aspect is the synchronization of databases [4]. This previously simple task becomes significantly more complex in the case of a distributed system that lacks a constant real-time connection between geographically remote sites.

Modern Database Management Systems (DBMS) have built-in mechanisms to ensure data integrity and security, which minimizes the likelihood of errors. However, data verification cannot be fully automated, as it depends on the human factor.

The main issue is tracking the accuracy of modifications to existing data that occur between two communication sessions. This becomes particularly challenging when data is simultaneously modified in both databases. At first glance, it may seem that a simple method of linking, which prioritizes the operation that occurred first, is not possible for several reasons. The first reason is the inability to synchronize clocks between computers. Hardware failures (such as motherboard clock resets) or insufficient qualifications of the personnel working with the software (many users rarely check the system time, and some are unaware of the basic operating system settings) may interfere with accurate

clock synchronization. All of this leads to confusion in the temporal display of records. Another reason is that both changes to the records could be legitimate, but their simultaneous existence in one database is impossible. This synchronization challenge grows proportionally with the number of data copies (three or more).

To work effectively in such conditions, a comprehensive approach is necessary, involving the application of various methods, each of which addresses specific difficulties. In 2025, the Digital Development Strategy for Innovation in Ukraine up to 2030 was approved, which identified AI (Artificial Intelligence) as one of the key areas for innovation development – specifically, the implementation of decision support systems based on data in priority sectors [5]. AI plays an increasingly important role in ensuring data accuracy when modifying data in DBMS. Some issues can be resolved through its application, such as:

– anomaly and error detection;
– prevention of unauthorized changes;
– automatic error correction;
– analysis and forecasting.

The use of AI in DBMS will significantly improve data accuracy during modifications, reduce the risk of errors, and ensure data security and integrity.

Bibliography:

1. Economic Pravda. Underwater warfare in the Baltic Sea: Why is Russia destroying critical infrastructure of the EU and NATO countries? https://epravda.com.ua/svit/obriv-kabeliv-u-baltiyskomu-mori-chim-ce-zagrozhuye-krajinam-yes-ta-nato-802785/ (accessed: March 4, 2025).

2. Taiwan detains Chinese vessel that severed underwater cable. https://nv.ua/ukr/world/countries/poshkodzhennya-pidvodnogo-kabelyu-u-tayvani-zatrimali-kitayske-sudno-50492977.html (accessed: March 4, 2025).

3. State Service of Special Communication and Information Protection. https://www.cip.gov.ua/en (accessed: March 4, 2025).

4. Connolly, Thomas M., Begg, Carolyn E. Database Systems: A Practical Approach to Design, Implementation, and Management. 6th edition. Longman (Pearson Education), 2015, 1442 p.

5. Government approves the Digital Development Strategy for Innovation in Ukraine (WINWIN) until 2030. https://biz.ligazakon.net/news/233397_uryad-zatverdivstrategyu-tsifrovogo-rozvitku-nnovatsyno-dyalnost-ukrani-winwin-do-2030-roku (accessed: March 4, 2025).