BULLETIN of Cherkasy State Technological University

Journal homepage: https://bulletin-chstu.com.ua/en

Vol. 31 No. 3. 2026

UDC 004.75
DOI: 10.62660/bcstu/3.2026.49

ISSN: 2306-4412
E-ISSN: 2708-6070

Confidentiality threat modelling for data exchange in distributed systems

Nazarii Dmytriv*
Postgraduate Student
Private Higher Education Establishment "European University"
03115, 16V Akademik Vernadskyi Ave., Kyiv, Ukraine
https://orcid.org/0009-0007-0326-3622

Volodymyr Kotsun
PhD in Technical Sciences, Associate Professor
Higher Education Establishment "European University"
03115, 16V Akademik Vernadskyi Ave., Kyiv, Ukraine
https://orcid.org/0000-0003-2363-8157

Abstract. The relevance of the study is determined by the increasing complexity of contemporary distributed environments, in which sensitive data passes through multiple nodes, communication channels, application services, message brokers, and storage subsystems. Under such conditions, confidentiality assurance requires not only the use of separate cryptographic mechanisms, but also a formalised assessment of cumulative confidentiality risk along the entire data exchange route. The aim of the study was to develop a route-oriented mathematical model for the quantitative assessment of confidentiality breach risk in distributed systems, taking into account node compromise probability, channel interception probability, data sensitivity, and the effectiveness of security mechanisms. The study employed methods of system analysis, mathematical modelling, and scenario-based evaluation. The data exchange process was formalised as a sequence of stages, each of which was assigned a local confidentiality breach risk and an adjusted risk considering the effectiveness of cryptographic protection, access control, and monitoring. The proposed integral risk function made it possible to aggregate local risks along the entire exchange route and determine the contribution of individual architectural elements to the cumulative risk. According to the results of scenario-based modelling, the integral risk was 0.01405 for the baseline scenario, 0.00223 for the intermediate scenario, and 0.000196 for the comprehensive protection scenario. The transition from the baseline scenario to the intermediate scenario reduced the integral risk by more than six times, whereas the application of comprehensive protection ensured its reduction by more than seventy times. The analysis of local risks showed that the client application and the data storage subsystem made the largest contribution to cumulative risk in the baseline scenario. This substantiates the need to prioritise the strengthening of protection measures at these stages of the exchange route. The practical significance of the obtained results lies in the possibility of using the proposed model to compare alternative architectures of distributed systems, identify critical stages of data exchange, and justify the selection of a set of security mechanisms

Keywords: data protection; exchange route; integral risk; local risk; access control; cryptographic protection; security monitoring

INTRODUCTION

Distributed systems have become a technological basis for cloud services, microservice applications,enterprise integration platforms, and inter-organisational information exchange. Their widespread adoption is driven

Article's History: Received: 16.04.2026; Revised: 17.08.2026; Accepted: 21.09.2026; Published: 07.10.2026

Suggested Citation:
Dmytriv, N., & Kotsun, V. (2026). Confidentiality threat modelling for data exchange in distributed systems. *Bulletin of Cherkasy State Technological University*, 31(3), 49-57. doi: 10.62660/bcstu/3.2026.49.

*Corresponding author (nazarii.dmytriv@gmail.com)

Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/)

by scalability, modularity, flexibility of deployment, and fault tolerance. At the same time, these very properties complicate confidentiality assurance, since sensitive data is no longer processed within a single controlled perimeter. Instead, it moves through client endpoints, gateways, internal services, message brokers, storage subsystems, and communication channels, each of which may contribute to confidentiality exposure. Under such conditions, confidentiality should be treated not as a local property of an isolated component, but as an integral characteristic of the entire end-to-end data exchange route.

Contemporary studies increasingly address confidentiality in distributed environments from the standpoint of software architecture, data flow modelling, and security-aware system design. S. Hahner *et al.* (2021) showed that modelling data flow constraints improves design-time confidentiality analysis by allowing security requirements to be expressed in architectural terms. S. Seifermann *et al.* (2022) demonstrated that the joint representation of information flow restrictions and access control conditions makes it possible to identify confidentiality violations more effectively. Scientists S. Schneider & R. Scandariato (2023) further confirmed the practical value of security-rich data flow modelling for distributed and microservice-based applications. At the same time, broader studies on distributed information systems emphasise that confidentiality assessment should be considered within the wider context of architectural heterogeneity, route complexity, and interdependence of system components. A. Rahdari *et al.* (2025) highlighted the need to assess privacy and security mechanisms together with deployment constraints and scalability conditions in distributed cloud computing. Researchers I. Chereja *et al.* (2025) showed that privacy exposure may be assessed more systematically when propagation effects and vulnerability expansion are explicitly taken into account.

The Ukrainian research context also demonstrates increasing attention to cybersecurity risk assessment and secure data processing in distributed environments. D. Palko *et al.* (2023) proposed a cyber risk modelling approach for distributed information systems that takes into account structural complexity, large-scale system architecture, distributed metadata, and security metrics. This approach is relevant to the present study because it confirms the need to consider risk as a cumulative and multi-factor characteristic of distributed systems rather than as a property of isolated components. In the context of secure data exchange and personal data protection, V. Balatska *et al.* (2025) proposed a blockchain-based approach to ensuring the reliability and security of personal data in state register systems. This study is relevant to the present research because it considers confidentiality, integrity, controlled access, traceability of operations, and protection against unauthorised data modification as interconnected properties of secure information exchange. At the same time, the problem of compact route-oriented quantification of confidentiality risk along the full data exchange path remains insufficiently formalised.

Despite these advances, existing approaches do not provide a sufficiently compact and interpretable analytical mechanism for aggregating confidentiality exposure along the full end-to-end route of distributed data exchange. Some studies are focused primarily on architectural semantics, information flow consistency, or policy violations, whereas others address broader cybersecurity or privacy risk without concentrating specifically on cumulative confidentiality loss during data exchange. As a consequence, there remains a need for a route-oriented analytical model that would integrate route structure, local adverse event probabilities, data sensitivity, and the cumulative mitigating effect of security controls within a single quantitative framework suitable for comparative architectural assessment. Therefore, an important scientific and practical task is to develop a mathematical model for assessing confidentiality threats during data exchange in distributed systems. The purpose of this study was to develop such a model on the basis of route decomposition of distributed data exchange. To achieve this purpose, the following objectives were defined: to formalise the route of data exchange in a distributed system; to identify the key parameters influencing confidentiality risk; to construct an integral function for aggregating local confidentiality threats; and to evaluate the applicability of the proposed model by means of scenario-based analysis.

MATERIALS AND METHODS

The study was based on a formal analytical approach to assessing confidentiality threats during data exchange in distributed systems. The methodological idea was to represent data exchange not as a single event, but as a sequence of interconnected stages, each of which contributes to the overall confidentiality risk. Such a representation makes it possible to assess confidentiality loss along the full route of data movement while taking into account both the characteristics of individual nodes and the properties of communication channels between them. For the purposes of the study, the data exchange route in a distributed system is represented as an ordered set (1):

$$P = \{e_1, e_2, \ldots, e_n\}, \quad (1)$$

where e_i denotes the *i-th* stage of data exchange. Depending on the architecture under consideration, a stage may correspond to a client application, an API gateway, an application service, a message broker, an integration interface, or a storage subsystem. This representation allows the analysis to be performed at the level of the complete route rather than at the level of isolated system elements.

To describe confidentiality exposure at each stage, a set of normalised parameters is introduced. The first parameter, $p_i \in [0.1]$, denotes the probability of compromise of the node or service involved in stage e_i. The second parameter, $q_i \in [0.1]$, characterises the probability of interception or unauthorised disclosure on the communication channel associated with that stage. Since confidentiality loss depends not only on the probability of an adverse event but also on the value of the exposed information, the model additionally includes a sensitivity coefficient $w_i \in [0.1]$ which reflects the relative confidentiality significance of the data processed or transmitted at stage e_i. Under these assumptions, the baseline local confidentiality risk for stage e_i is defined as (2):

$$ri = w_i \cdot p_i \cdot q_i. \quad (2)$$

This expression reflects the idea that confidentiality loss becomes more probable when sensitive data is handled by a vulnerable node and transmitted through a channel with a non-negligible interception probability. Although the model is intentionally compact, it captures the core relationship between data sensitivity, local vulnerability, and channel-related exposure.

To take into account the effect of protection mechanisms, three additional coefficients are introduced. The coefficient $c_i \in [0.1]$ characterises the effectiveness of cryptographic protection $a_i \in [0.1]$ characterises the effectiveness of access control mechanisms; and $m_i \in [0.1]$ reflects the effectiveness of monitoring and audit measures. The adjusted local confidentiality risk is therefore determined as (3):

$$r_i\text{^}* = w_i \cdot p_i \cdot q_i \cdot (1\text{-}c_i)(1\text{-}a_i)(1\text{-}m_i), \quad (3)$$

where the normalised coefficients may be assigned on the basis of expert assessment, organisational security baselines, threat catalogs, or empirical telemetry obtained from the analysed environment. Such calibration makes it possible to adapt the proposed model to the specific architecture, data classification policy, and operational conditions of the distributed system under consideration. The integral confidentiality risk for the entire exchange route is then defined as the probability that at least one route stage results in confidentiality loss (4):

$$R = 1\text{-}\prod_{i=1}^{n}(1\text{-}r_i^*), \quad (4)$$

where the product is calculated for all i from 1 to n. This form of aggregation was chosen because it reflects the cumulative route-level nature of confidentiality exposure in distributed interaction. Even if the local risk at each individual stage is relatively small, the total confidentiality risk may become significant when data passes through multiple components and communication links. In order to identify the stages that contribute most strongly to the overall confidentiality exposure, the relative contribution of each stage is calculated as (5):

$$\delta_i = \frac{r_i^*}{\sum_{j=1}^{n} r_j^*}, \quad (5)$$

where the summation is calculated for all j from 1 to n. The value of δ_i is used to rank the stages of the exchange route according to their contribution to the cumulative confidentiality risk and, accordingly, to determine the architectural elements that require priority strengthening of protection measures. To improve the interpretability of the obtained results, the calculated integral confidentiality risk is additionally mapped to qualitative risk levels (6):

$$L(R) \in \{low, moderate, high, critical\}, \quad (6)$$

where the qualitative interpretation of the obtained values is defined as follows: $L(R) = low$ for $0 \leq R < 0.01$, $L(R) = moderate$ for $0.01 \leqslant R < 0.05$, $L(R) = high$ for $0.05 \leqslant R < 0.10$, and $L(R) = critical$ for $R \geqslant 0.10$. This makes it possible to use the model not only for numerical comparison of alternative scenarios, but also for a more explicit interpretation of the obtained results in the context of architectural decision-making.

The applicability of the proposed model is evaluated by means of scenario analysis. Three scenarios are considered: a baseline scenario with weak protection, an intermediate scenario with improved security controls, and a comprehensive protection scenario characterised by stronger cryptographic protection, stricter access control, and more effective monitoring. For all scenarios, the parameter values are normalised within the interval [0.1], which makes the model suitable for comparative analysis of alternative architectural solutions. The resulting values of the integral confidentiality risk are further interpreted using the qualitative scale defined by expression (6). Thus, the proposed methodological framework combines route-based formalisation of data exchange, local confidentiality risk estimation, integral aggregation of route risks, qualitative interpretation of the obtained risk values, and scenario-based comparison of protection levels. This makes it suitable for analytical evaluation of confidentiality threats in distributed systems at the design stage and for comparing alternative architectural configurations in terms of confidentiality assurance.

RESULTS

To evaluate the proposed model, a representative distributed data exchange route consisting of five stages was considered. The selected route reflects a typical configuration of a distributed information system in which sensitive data moves from a user-facing component to intermediate processing and integration

elements and then to a persistent storage subsystem. This configuration was selected because it makes it possible to demonstrate how confidentiality-related risks accumulate along the full route of data movement and how different levels of protection influence both integral and stage-level risk values:

$$P = \{e_1, e_2, e_3, e_4, e_5\},$$

where e_1 is a client application, e_2 is an API gateway, is an application service, e_3 is a message broker, and e_5 is a data storage subsystem. The route stages were interpreted as functionally different elements of distributed data exchange. The client application represents the user-facing entry point of interaction with the system. The API gateway performs routing, filtering, and access mediation functions. The application service processes business logic and may operate with sensitive data during request execution.

The message broker supports asynchronous data exchange between system components. The data storage subsystem accumulates and preserves processed information and therefore represents a critical point from the standpoint of confidentiality assurance. Such decomposition makes it possible to evaluate confidentiality risk not only at the level of the whole system, but also at the level of separate architectural stages. For the analysed route, the sensitivity coefficients were defined as:

$$w = \{0.9, 0.8, 0.7, 0.9, 1.0\},$$

the probabilities of node compromise as:

$$p = \{0.08, 0.05, 0.06, 0.04, 0.07\},$$

and the probabilities of interception on communication channels as:

$$q = \{0.10, 0.08, 0.07, 0.06, 0.09\}.$$

The model was evaluated under three protection scenarios. In the baseline scenario, the effectiveness coefficients of security controls were set to $c_i = 0.10$, $a_i = 0.20$, and $m_i = 0.10$. In the intermediate scenario, the corresponding values were $c_i = 0.65$, $a_i = 0.55$, and $m_i = 0.35$. In the comprehensive protection scenario, the values were increased to $c_i = 0.85$, $a_i = 0.80$, and $m_i = 0.70$.

The influence of these coefficients on the integral confidentiality risk follows directly from the structure of the adjusted local risk function. The coefficients , ai, and mi describe the effectiveness of cryptographic protection, access control, and monitoring, respectively. Since the residual local risk is multiplied by the factors $(1 - c_i)$, $(1 - a_i)$, and $(1 - m_i)$, an increase in any of these coefficients decreases the remaining unmitigated part of the risk at each route stage.

Cryptographic protection reduces the probability that intercepted data can be disclosed in a meaningful form. Access control decreases the probability of unauthorised interaction with system components and sensitive data. Monitoring reduces residual exposure by increasing the probability of detecting abnormal activity, policy violations, or suspicious data exchange events. Therefore, the simultaneous strengthening of all three controls has a cumulative effect: it reduces local confidentiality risks at individual stages and, consequently, decreases the integral confidentiality risk along the entire data exchange route. This is important for confidentiality assurance because sensitive data in distributed systems may be exposed not at one isolated point, but through the accumulation of risks across multiple nodes and communication channels. For the baseline scenario, the selected values of the protection coefficients describe a configuration in which the protective mechanisms are present but have limited effectiveness. In this case, the model reflects a situation where encryption, access control, and monitoring reduce confidentiality exposure only partially. Therefore, the residual risk remains relatively noticeable at several stages of the route. This scenario was used as a reference point for evaluating how the integral confidentiality risk changes when the level of protection is increased.

The intermediate scenario represents a strengthened configuration of the same distributed data exchange route. In this case, the effectiveness of cryptographic protection and access control was increased considerably, while monitoring was also improved. This scenario reflects a more mature security configuration in which sensitive data is protected during transmission and processing, unauthorised access is more effectively restricted, and suspicious activity is more likely to be detected. The purpose of this scenario was to determine whether partial but coordinated improvement of several controls can significantly reduce the cumulative confidentiality risk. The comprehensive protection scenario represents the highest level of security maturity among the three analysed configurations. In this scenario, cryptographic protection, access control, and monitoring were modeled as strong and mutually reinforcing mechanisms. Such a configuration corresponds to a distributed system in which sensitive data is protected both in transit and at rest, access to system components is strictly controlled, and security monitoring provides additional visibility into abnormal or unauthorised operations. This scenario was used to evaluate the lowest residual confidentiality risk that can be achieved under the selected model parameters.

The use of the same route structure and the same baseline values of sensitivity, node compromise probability, and channel interception probability in all three scenarios made it possible to isolate the influence of security control effectiveness. Therefore, the differences between the calculated risk values are caused

specifically by the change in the coefficients of cryptographic protection, access control, and monitoring. This makes the comparison methodologically consistent and allows the effect of protection strengthening to be interpreted directly. The calculated values of the integral confidentiality risk are presented in Table 1.

Table 1. Integral confidentiality risk values under different protection scenarios

Scenario	c_i	a_i	m_i	R	Risk level
Baseline scenario	0.10	0.20	0.10	0.01405	moderate
Intermediate scenario	0.65	0.55	0.35	0.00223	low
Comprehensive protection scenario	0.85	0.80	0.70	0.000196	low

Source: calculated by the authors

As shown in Table 1, the baseline configuration corresponds to a moderate confidentiality risk level, whereas both strengthened protection scenarios correspond to a low risk level according to expression (6). However, the numerical values show that the difference between the scenarios is substantial even when two of them belong to the same qualitative risk category. In the baseline scenario, the integral confidentiality risk is 0.01405. This value reflects the cumulative effect of confidentiality exposure across the full route of data exchange when cryptographic protection, access control, and monitoring have limited effectiveness. Under such conditions, the presence of several route stages increases the probability that confidentiality may be compromised at least at one point of the exchange process. In the intermediate scenario, the integral confidentiality risk decreases to 0.00223. Compared with the baseline scenario, this represents a reduction of more than six times. This result demonstrates that even partial but coordinated strengthening of cryptographic protection, access control, and monitoring can substantially reduce residual confidentiality exposure.

The reduction is achieved because the adjusted local risk at each route stage is decreased by the higher effectiveness of protection mechanisms. As a result, the cumulative risk along the entire data exchange route also decreases. This confirms that confidentiality assurance in distributed systems should be implemented through a coordinated set of controls rather than through isolated protective mechanisms. In the comprehensive protection scenario, the integral confidentiality risk decreases further to 0.000196. Compared with the baseline scenario, this means a reduction of more than seventy times. Such a result indicates that the simultaneous strengthening of cryptographic protection, access control, and monitoring produces a strong cumulative mitigation effect. Although both the intermediate and comprehensive scenarios are classified as low risk according to the qualitative scale, their numerical values differ significantly. Therefore, the use of numerical risk assessment is important because qualitative categories alone may hide meaningful differences between alternative protection configurations.

The obtained results also show that the proposed model is sensitive to changes in the effectiveness of security controls. When the coefficients of cryptographic protection, access control, and monitoring increase, the residual local risks decrease at each stage of the exchange route, and this leads to a lower integral confidentiality risk. This property makes the model suitable for comparative analytical assessment of alternative protection configurations. In practical terms, the model can be used to estimate how much the overall confidentiality risk may decrease when an organization improves encryption, strengthens access control, introduces more effective monitoring, or combines these measures within one protection strategy. To determine which architectural stages contribute most strongly to cumulative confidentiality exposure, the local adjusted risks were calculated for all three protection scenarios. This made it possible not only to compare the baseline, intermediate, and comprehensive configurations at the level of integral risk, but also to identify how the residual risk is distributed across the individual stages of the data exchange route. The results of the stage-level assessment are presented in Table 2.

Table 2. Stage-level adjusted confidentiality risks under different protection scenarios

Stage	Architectural element	Baseline scenario	Intermediate scenario	Comprehensive protection scenario	Relative contribution
e_1	Client application	0.004666	0.000737	0.0000648	0.330
e_2	API gateway	0.002074	0.000328	0.0000288	0.147
e_3	Application service	0.001905	0.000301	0.0000265	0.135
e_4	Message broker	0.001400	0.000221	0.0000194	0.099
e_5	Data storage	0.004082	0.000645	0.0000567	0.289

Source: calculated by the authors

As shown in Table 2, the local adjusted risk values decrease consistently when moving from the baseline scenario to the intermediate and comprehensive protection scenarios. In the baseline scenario, the highest

local adjusted risk is associated with the client application, where the value reaches 0.004666. The second most significant contribution is associated with the data storage subsystem, where the local adjusted risk is 0.004082. Together, these two stages account for approximately 61,9% of the total route-level contribution to confidentiality risk. This indicates that confidentiality exposure in the analysed route is concentrated primarily at the user-facing entry point and at the stage of persistent data accumulation.

The high contribution of the client application can be explained by its direct interaction with users, external requests, authentication procedures, and potentially heterogeneous operating conditions. At this stage, confidentiality may be affected by weak authentication, compromised endpoints, insecure sessions, or unauthorised attempts to initiate data exchange. Therefore, targeted measures at this stage should focus on strengthening access control, secure session management, endpoint hardening, strict validation of requests, and monitoring of abnormal user activity. In terms of the proposed model, these measures primarily increase the effectiveness of access control and monitoring coefficients and therefore reduce the residual local risk at the first stage of the route. The data storage subsystem also demonstrates a high local adjusted risk because it accumulates the most sensitive data and preserves it over time. Even if transmission and intermediate processing stages are sufficiently protected, unauthorised access to storage, improper privilege management, weak encryption at rest, or insufficient auditability of database operations may lead to significant confidentiality loss. For this reason, risk reduction at this stage should prioritise encryption of stored data, strict role-based access control, separation of privileges, secure key management, database activity monitoring, and integration of storage events with security monitoring systems. These measures increase the effectiveness of cryptographic protection, access control, and monitoring at the storage stage and therefore reduce its contribution to the integral confidentiality risk.

DISCUSSION

The obtained results support the idea that confidentiality in distributed architectures should be analysed as a property of data movement across the system rather than as a characteristic of isolated components. This interpretation is consistent with architecture-based approaches to confidentiality analysis developed in recent years. S. Hahner *et al.* (2021) demonstrated that explicit modelling of data flow constraints improves confidentiality analysis at the design stage by expressing security requirements in architectural terms. S. Seifermann *et al.* (2022) showed that confidentiality violations can be identified more effectively when information flow restrictions are considered together with access control conditions. S. Schneider & R. Scandariato (2023) confirmed the practical importance of security-rich data flow diagrams for distributed and microservice-based applications. The results of the present study are consistent with these approaches, since the proposed model also relies on the decomposition of data movement into separate route stages. However, unlike these works, the proposed approach additionally provides quantitative estimates of local and integral confidentiality risk.

The results also correspond to broader cybersecurity risk modelling studies in distributed information systems. D. Palko *et al.* (2023) emphasised that cyber risk modelling in distributed systems should take into account structural complexity, heterogeneity of subsystems, distributed metadata, and the interaction of multiple security factors. The obtained values in the present study confirm this position: the integral confidentiality risk is formed not by one isolated component, but by the cumulative contribution of several route stages. A. Rahdari *et al.* (2025) also highlighted that privacy and security mechanisms in distributed cloud computing should be assessed together with deployment constraints and scalability conditions. This is relevant to the proposed model because the scenario-based comparison demonstrates how different levels of cryptographic protection, access control, and monitoring influence residual confidentiality exposure along the full data exchange route. M. Zubair *et al.* (2024) designed an access control mechanism for trusted data sharing in a distributed data streaming system, emphasising fine-grained policies, dynamic enforcement, transparency, and confidentiality preservation. This is directly related to the proposed model because access control is one of the coefficients that reduces residual local risk at each stage of the exchange route.

A separate group of studies focuses on privacy-preserving and secure data sharing mechanisms. A. Ballesteros-Rodríguez *et al.* (2024) analysed privacy-preserving computing services for encrypted and distributed IoT data streams, A. Odeh *et al.* (2024) considered privacy-preserving data sharing in telehealth services, while K. Li *et al.* (2025) and D. Zhu *et al.* (2025) summarised broader approaches to secure and privacy-preserving data sharing. Z. Yu *et al.* (2025) proposed a privacy-preserving data sharing scheme with searchable encryption for health data space. I. Chereja *et al.* (2025) proposed an approach to privacy exposure assessment based on vulnerability expansion and propagation effects. T. Bontekoe *et al.* (2025) analysed verifiability for privacy-preserving computing on distributed data, while S.-Y. Kim *et al.* (2025) considered cross-company data sharing using distributed analytics. These works emphasise that confidentiality and privacy risks should be evaluated not only at the level of one data processing operation, but also across the broader data exchange environment. The proposed model develops this idea by introducing a compact route-oriented risk function that makes it possible to aggregate local

confidentiality risks and determine which stages contribute most strongly to the final risk value.

The comparison with blockchain-oriented studies is also important. K. Ansar *et al.* (2024) analysed blockchain-based data breach detection and emphasised the importance of integrity, traceability, and timely identification of security incidents. M.R. Hasan *et al.* (2023) proposed a smart contract-based access control framework for Internet of Things devices, which is relevant to the present study because access control is one of the key coefficients used to reduce residual confidentiality risk at each route stage. J. Yu *et al.* (2024) proposed a secure and verifiable blockchain-based framework for personal data validation. H. Tian & G. Huang (2024) considered a distributed secure storage framework for Industrial Internet of Things data based on blockchain, while W. Tong *et al.* (2024) focused on blockchain-based data sharing and privacy protection in Industrial Internet of Things environments. These studies demonstrate the relevance of distributed mechanisms for improving trust, auditability, access control, and resistance to unauthorised data modification. However, most of them focus primarily on the design of specific protection architectures or mechanisms. In contrast, the present study focuses on the analytical assessment of confidentiality risk along the route of data exchange and can therefore be used before selecting a specific technological implementation.

Thus, the proposed model complements existing studies in three main ways. First, it connects confidentiality assessment with the full route of data movement rather than with a single component or isolated protection mechanism. Second, it combines node compromise probability, channel interception probability, data sensitivity, and the effectiveness of cryptographic protection, access control, and monitoring within one analytical framework. Third, it provides both integral and stage-level results, which makes it possible not only to compare protection scenarios, but also to identify where targeted security improvements should be introduced first. This is why the model can be used as a design-stage analytical tool for comparing alternative distributed architectures and selecting priority confidentiality protection measures. When interpreting the obtained results, several limitations of the proposed model should be taken into account. First, the model assumes relative independence of local confidentiality-related events at different stages of the exchange route, whereas real distributed systems may exhibit correlated failures, cascading exposures, or dependencies caused by shared infrastructure. Second, the normalised coefficients used in the model are intended primarily for comparative analytical evaluation rather than for exact prediction of incident probability in a particular operational environment. Third, the assignment of parameter values requires expert judgment or empirical calibration. Therefore, the calculated values should be interpreted as structured comparative indicators for architectural decision-making rather than as deterministic forecasts.

CONCLUSIONS

The study developed a route-oriented mathematical model for assessing confidentiality threats during data exchange in distributed systems. The proposed approach represents the exchange route as a sequence of interconnected stages and evaluates confidentiality risk by combining node compromise probability, channel interception probability, data sensitivity, and the mitigating effect of cryptographic protection, access control, and monitoring. This made it possible to assess confidentiality not as a property of an isolated component, but as a cumulative characteristic of the entire data exchange route. The scenario-based evaluation showed that the integral confidentiality risk was 0.01405 in the baseline scenario, 0.00223 in the intermediate scenario, and 0.000196 in the comprehensive protection scenario. Thus, the transition from the baseline scenario to the intermediate scenario reduced the calculated risk by more than six times, while the comprehensive protection scenario reduced it by more than seventy times. These values confirm that the simultaneous strengthening of cryptographic protection, access control, and monitoring substantially decreases residual confidentiality exposure along the full route of data movement.

The stage-level analysis showed that in the baseline scenario the highest local adjusted risk was associated with the client application, where the value was 0.004666, and with the data storage subsystem, where the value was 0.004082. In the intermediate scenario, the corresponding local risks decreased to 0.000737 for the client application and 0.000645 for the data storage subsystem. In the comprehensive protection scenario, these values decreased further to 0.0000648 and 0.0000567, respectively. Therefore, the client application and data storage subsystem remain the priority stages for targeted confidentiality protection, even when the overall level of security controls is strengthened.

The obtained results demonstrate that the proposed model can be used for comparative assessment of alternative protection scenarios and for identifying the stages of a distributed data exchange route that require priority strengthening. In practical terms, the greatest reduction of confidentiality risk may be achieved by improving access control, secure session management, endpoint protection, encryption of stored data, secure key management, and monitoring of database and user activity at the most risk-contributing stages. Further research may be directed toward extending the model by incorporating dependencies between route stages, dynamic adaptation of trust levels, sensitivity analysis of model parameters, and

empirical calibration of coefficients based on telemetry obtained from real distributed environments.

ACKNOWLEDGEMENTS

None.

FUNDING

None.

CONFLICT OF INTEREST

None

REFERENCES

[1] Ansar, K., Ahmed, M., Helfert, M., & Kim, J. (2024). Blockchain-based data breach detection: Approaches, challenges, and future directions. *Mathematics*, 12(1), article number 107. doi: 10.3390/math12010107.

[2] Balatska, V., Poberezhnyk, V., & Opirskyy, I. (2025). Method for ensuring the reliability and security of personal data in blockchain systems of state registers. In *Proceedings of CPITS 2025: Workshop on cybersecurity providing in information and telecommunication systems* (pp. 293-310). Kyiv: CEUR-WS.

[3] Ballesteros-Rodríguez, A., Sánchez-Alonso, S., & Sicilia-Urbán, M.Á. (2024). Privacy-preserving computing services for encrypted personal data through streams over distributed ledgers. *International Journal of Networked and Distributed Computing*, 12, 362-384. doi: 10.1007/s44227-024-00038-9.

[4] Bontekoe, T., Karastoyanova, D., & Turkmen, F. (2025). Verifiability for privacy-preserving computing on distributed data – a survey. *International Journal of Information Security*, 24, article number 141. doi: 10.1007/s10207-025-01047-7.

[5] Chereja, I., Erdei, R., Delinschi, D., Pasca, E., Avram, A., & Matei, O. (2025). Privacy-conducive data ecosystem architecture: By-design vulnerability assessment using privacy risk expansion factor and privacy exposure index. *Sensors*, 25(11), article number 3554. doi: 10.3390/s25113554.

[6] Hahner, S., Seifermann, S., Heinrich, R., Walter, M., Bureš, T., & Hnětynka, P. (2021). Modelling data flow constraints for design-time confidentiality analyses. In *IEEE Software Architecture Companion Proceedings* (pp. 15-210). Stuttgart: IEEE. doi: 10.1109/ICSA-C52384.2021.00009.

[7] Hasan, M.R., Alazab, A., Joy, S.B., Uddin, M.N., Uddin, M.A., Khraisat, A., Gondal, I., Urmi, W.F., & Talukder, M.A. (2023). Smart contract-based access control framework for Internet of Things devices. *Computers*, 12(11), article number 240. doi: 10.3390/computers12110240.

[8] Kim, S.-Y., Berninger, S., Kocher, M., Perau, M., & Geisler, S. (2025). Cross-company data sharing using distributed analytics. *Systems*, 13(6), article number 418. doi: 10.3390/systems13060418.

[9] Li, K., Lohachab, A., Dumontier, M., & Urovi, V. (2025). Privacy preservation in blockchain-based healthcare data sharing: A systematic review. *Peer-to-Peer Networking and Applications*, 18, article number 302. doi: 10.1007/s12083-025-02148-9.

[10] Odeh, A., Abdelfattah, E., & Salameh, W. (2024). Privacy-preserving data sharing in telehealth services. *Applied Sciences*, 14(23), article number 10808. doi: 10.3390/app142310808.

[11] Palko, D., Babenko, T., Bigdan, A., Kiktev, N., Hutsol, T., Kuboń, M., Hnatiienko, H., Tabor, S., Gorbovyi, O., & Borusiewicz, A. (2023). Cyber security risk modelling in distributed information systems. *Applied Sciences*, 13(4), article number 2393. doi: 10.3390/app13042393.

[12] Rahdari, A., Keshavarz, E., Nowroozi, E., Taheri, R., Hajizadeh, M., Mohammadi, M., Sinaei, S., & Bauschert, T. (2025). A survey on privacy and security in distributed cloud computing: Exploring federated learning and beyond. *IEEE Open Journal of the Communications Society*. doi: 10.1109/OJCOMS.2025.3560034.

[13] Schneider, S., & Scandariato, R. (2023). Automatic extraction of security-rich dataflow diagrams for microservice applications written in Java. *Journal of Systems and Software*, 202, article number 111722. doi: 10.1016/j.jss.2023.111722.

[14] Seifermann, S., Heinrich, R., Werle, D., & Reussner, R.H. (2022). Detecting violations of access control and information flow policies in data flow diagrams. *Journal of Systems and Software*, 184, article number 111138. doi: 10.1016/j.jss.2021.111138.

[15] Tian, H., & Huang, G. (2024). Research on distributed secure storage framework of Industrial Internet of Things data based on blockchain. *Electronics*, 13(23), article number 4812. doi: 10.3390/electronics13234812.

[16] Tong, W., Yang, L., Li, Z., Jin, X., & Tan, L. (2024). Enhancing security and flexibility in the Industrial Internet of Things: Blockchain-based data sharing and privacy protection. *Sensors*, 24(3), article number 1035. doi: 10.3390/s24031035.

[17] Yu, J., Li, X., & Guo, Y. (2024). A secure and verifiable blockchain-based framework for personal data validation. *Computers*, 13(9), article number 240. doi: 10.3390/computers13090240.

[18] Yu, Z., Wang, H., Liu, Y., & Zhang, Q. (2025). A privacy-preserving data sharing scheme with searchable encryption for health data space. *Electronics*, 15(1), article number 63. doi: 10.3390/electronics15010063.

[19] Zhu, D., Zhou, Z., Li, Y., Zhang, H., Chen, Y., Zhao, Z., & Zheng, J. (2025). A survey of data security sharing. *Symmetry*, 17(8), article number 1259. doi: 10.3390/sym17081259.

[20] Zubair, M., Sabzevari, M., Khatri, V., Tarkoma, S., & Hätönen, K. (2024). Access control for trusted data sharing. *EURASIP Journal on Information Security*, 2024, article number 30. doi: 10.1186/s13635-024-00178-z.

Моделювання загроз конфіденційності під час обміну даними в розподілених системах

Назарій Дмитрів
Аспірант
Приватний вищий навчальний заклад «Європейський університет»
03115, бульв. Академіка Вернадського, 16В, м. Київ, Україна
https://orcid.org/0009-0007-0326-3622
Володимир Коцун
Кандидат технічних наук, доцент
Приватний вищий навчальний заклад «Європейський університет»
03115, бульв. Академіка Вернадського, 16В, м. Київ, Україна
https://orcid.org/0000-0003-2363-8157

Анотація. Актуальність дослідження зумовлена зростанням складності сучасних розподілених середовищ, у яких чутливі дані проходять через множину вузлів, каналів зв'язку, прикладних сервісів, брокерів повідомлень і підсистем зберігання. За таких умов забезпечення конфіденційності потребує не лише застосування окремих криптографічних механізмів, а й формалізованого оцінювання сукупного ризику втрати конфіденційності на всьому маршруті обміну даними. Метою дослідження було побудувати маршрутно-орієнтовану математичну модель кількісного оцінювання ризику порушення конфіденційності в розподілених системах з урахуванням імовірності компрометації вузлів, імовірності перехоплення в каналах передавання, чутливості даних та ефективності механізмів захисту. У роботі використано методи системного аналізу, математичного моделювання та сценарного оцінювання. Процес обміну даними було формалізовано як послідовність етапів, для кожного з яких визначено локальний ризик порушення конфіденційності та скоригований ризик з урахуванням ефективності криптографічного захисту, контролю доступу й моніторингу. Запропонована інтегральна функція ризику дала змогу агрегувати локальні ризики вздовж усього маршруту обміну та визначити внесок окремих архітектурних елементів у сукупний ризик. За результатами сценарного моделювання встановлено, що для базового сценарію інтегральний ризик становив 0,01405, для проміжного сценарію – 0,00223, а для сценарію комплексного захисту – 0,000196. Перехід від базового до проміжного сценарію зменшив інтегральний ризик більш ніж у шість разів, тоді як застосування комплексного захисту забезпечило його зниження більш ніж у сімдесят разів. Аналіз локальних ризиків показав, що найбільший внесок у сукупний ризик у базовому сценарії формували клієнтський застосунок і підсистема зберігання даних. Це обґрунтовує доцільність пріоритетного посилення захисту саме на цих етапах маршруту обміну. Практичне значення отриманих результатів полягає у можливості використання запропонованої моделі для порівняння альтернативних архітектур розподілених систем, визначення критичних ділянок обміну даними та обґрунтування вибору комплексу захисних механізмів

Ключові слова: захист даних; маршрут обміну; інтегральний ризик; локальний ризик; контроль доступу; криптографічний захист; моніторинг безпеки