Cyber Risk Assessment Model for Digital Transactions

Petya I. Petrova (p. petrova@utp.bg)
University of Telecommunications and Post, Sofia, 1700, Acad. St. Mladenov Str., Bulgaria

***Abstract*— The increasing use of electronic services, remote identification, digital signing and automated data exchange creates the need for cyber risk assessment mechanisms operating at the level of individual digital transactions. Conventional identity and authentication controls provide an essential security layer but may be insufficient to identify transactions performed with compromised credentials, hijacked sessions, anomalous devices or significant behavioural and contextual deviations.**

This paper proposes a multi-criteria model for automated cyber risk assessment of digital transactions. The model creates a transaction-specific risk profile based on six components: digital identity, authentication, transactional data, technical environment, behavioural deviation and transaction context. The components are normalized and aggregated into an integrated risk-indicator score, which is subsequently combined with the potential impact of the transaction. The resulting Digital Transaction Risk Score (DTRS) enables the transaction to be classified and associated with an adaptive security response. The functional behaviour of the model is demonstrated through three transaction scenarios representing low, elevated and critical risk conditions. The proposed approach provides a basis for transaction-oriented cyber risk assessment in dynamically changing digital environments.

***Keywords*— cyber risk, digital transaction, digital identity, authentication, behavioural analysis, contextual risk, DTRS.**

I. Introduction

Digital transformation is fundamentally changing the way citizens, organizations, and information systems interact. Administrative services, financial operations, electronic signing, remote identification, access-rights management, and automated data exchange are increasingly carried out without physical presence and through interconnected information systems [1], [4].

The growth of digital connectivity creates dependencies among digital identity, authentication mechanisms, endpoint devices, communication environments, and applications. Managing these dependencies is part of the contemporary approach to cyber risk developed in ISO/IEC 27001, ISO/IEC 27005, and the NIST Cybersecurity Framework 2.0 [7], [9], [11].

At the European level, NIS2 and DORA place additional emphasis on cyber risk management and digital operational resilience [2], [3]. The eIDAS Regulation and its amendment through Regulation (EU) 2024/1183 establish the regulatory framework for electronic identification, trust services, and the European Digital Identity [1], [4].

However, the security of a specific digital operation cannot be determined solely by the fact that the identity is valid and authentication has been successfully completed. Compromised credentials, hijacked sessions, or significant deviations in device characteristics, behaviour, and context may result in a technically valid but actually unauthorized operation [13], [14].

Therefore, the following assumption is rejected:

$$Successful\ Authentication \Rightarrow Low\ Transaction\ Risk$$

In other words, successful authentication does not automatically constitute evidence of low risk for a specific digital transaction.

This principle is consistent with the Zero Trust approach, in which access decisions are not based solely on previously established trust in the user or device [12].

For the purposes of this study, a digital transaction is defined as a logically completed electronic interaction between a subject, an information system, or a digital service in which information is requested, authenticated, processed, transmitted, confirmed, or modified, producing a specific administrative, financial, legal, or operational outcome.

Traditional risk assessment generally considers assets, processes, services, or information systems [6], [9]. In digital transactions, however, current technical, identity-related, and behavioural characteristics may change between two consecutive operations.

Therefore:

$$RT_i \neq RS$$

where RT_i is the risk of the specific transaction, while RS denotes the overall risk state of the system.

The objective of this study is to develop a multi-criteria model for automated cyber risk assessment of digital transactions based on identity-related, authentication, information, technical, behavioural, and contextual indicators.

To achieve this objective, the following tasks are defined:

1. define the digital transaction as an independent object of assessment;
2. identify the main components of transactional cyber risk;
3. develop a mechanism for normalizing and aggregating risk indicators;
4. formalize an integrated risk assessment;
5. link the quantitative assessment to a protective response;
6. verify the functional behaviour of the model.

II. Transaction-Oriented Cyber Risk Assessment

A. The Digital Transaction as an Object of Assessment

The life cycle of a digital transaction can be represented in a generalized form as:

initiation → *identification* → *authentication* → *request*

→ processing → execution → confirmation → logging.

At the individual stages, different risk signals may arise in relation to digital identity, authentication mechanisms, information integrity, the technical environment, and subject behaviour.

Contemporary digital identity guidelines distinguish identity proofing, authentication, authenticator management, and federation, supporting the need to analyse the reliability of digital interaction as a set of interrelated factors [13]. NIST SP 800-63-4 explicitly covers these key areas of digital identity.

B. Core Definitions

Transactional cyber risk is the risk of adverse consequences resulting from the compromise, manipulation, or unauthorized execution of a specific digital transaction.

Transaction-oriented risk assessment is the process of determining the risk state of an individual digital transaction on the basis of its current identity-related, authentication, information, technical, behavioural, and contextual characteristics.

A risk indicator is a measurable or categorizable characteristic of a transaction whose deviation from an established normal or expected state may be associated with increased risk.

Behavioural deviation is a measurable difference between the characteristics of the current digital activity and the subject's previously established reference profile.

Potential impact is an assessment of the severity of possible consequences if a specific transaction is compromised.

Digital Transaction Risk Score (DTRS) is a normalized quantitative value in the range from 0 to 100 through which the proposed model represents the overall risk state of a specific digital transaction.

C. Dynamic Nature of Transactional Risk

Transactional cyber risk is dynamic because it is formed on the basis of the current state of multiple characteristics of the specific operation.

A transaction may present low risk when associated with a known identity, reliable authentication, a managed device, and a usual context, while the same type of transaction may receive a significantly higher score when a combination of technical or behavioural deviations is present.

A similar logic is applied in risk-based authentication, where additional characteristics of an access attempt are used to adapt the authentication response [14].

Accordingly, the model should simultaneously consider:

who → how the subject is authenticated → through what technical environment → what action is performed → in what context → to what extent behaviour deviates → what the potential consequences may be.

III. Proposed Cyber Risk Assessment Model

A. Conceptual Structure

Let a specific digital transaction be denoted by T_i. For this transaction, the following vector is formed:

$$XT_i=[I_i,A_i,D_i,E_i,B_i,C_i]$$

where:

- I_i – risk indicator related to digital identity;
- A_i – authentication risk indicator;
- D_i – risk indicator related to transactional data;
- E_i – technical-environment risk indicator;
- B_i – behavioural deviation;
- C_i – contextual deviation.

Potential impact is represented separately by P_i because it characterizes the possible consequences of compromise rather than the presence of a risk signal.

The logic of the model is:

$$XT_i \rightarrow S_i \rightarrow Pi \rightarrow R_i \rightarrow DTRS_i \rightarrow Decision$$

where S_i represents an aggregated normalized score of the risk indicators.

S_i is not interpreted as a statistical probability of a successful cyberattack. It is a quantitative measure of the intensity of the observed risk signals associated with the specific transaction.

B. Risk Components

Digital Identity I reflects the validity and status of the identity, indications of compromised credentials, and atypical account usage.

$$I=f(i_1,i_2,\ldots,i_m)$$

Authentication A reflects the authentication mechanism used, MFA, failed attempts, and indicators of a compromised session.

$$A=f(a_1,a_2,\ldots,a_m)$$

Transactional Data D assesses content integrity, the validity of the electronic signature or timestamp, and the presence of unexpected modifications.

$$D=f(d_1,d_2,\ldots,d_m)$$

The sensitivity and criticality of the processed information are not included in D; instead, they are considered when determining the potential impact P_i. This reduces the possibility of double-counting the same factor.

Technical Environment E reflects device status, known vulnerabilities, protective mechanisms, and network context.

$$E=f(e_1,e_2,\ldots,e_m)$$

Behavioural Deviation B represents the difference between the current action and the subject's reference profile P_u:

$$B=\Delta(T_i,P_u)$$

The profile may account for temporal characteristics, devices used, location, frequency, and sequence of actions.

Context C reflects the current spatial, temporal, and session-related characteristics of the transaction.

$$C=f(c_1,c_2,\ldots,c_m)$$

C. Normalization of Indicators

To aggregate heterogeneous indicators, they are

transformed to a common interval $x_{ij}^{norm} \in [0,1]$, where a value of 0 indicates no identified risk deviation, while 1 represents the maximum identified deviation according to the selected parameterization.

For a quantitative indicator, min-max normalization may be used:

$$x_{ij}^{norm} = (x_{ij} - x_{min}) / (x_{max} - x_{min})$$

For categorical characteristics, a discrete scale may be used:

State	Value
Normal	0.00
Low deviation	0.25
Moderate deviation	0.50
High deviation	0.75
Critical deviation	1.00

Component X_k is determined as:

$$X_k = \Sigma_{j=1}^{mk} \alpha_{kj} \, x_{kj}^{norm}$$

subject to:

$$\Sigma_{j=1}^{mk} \alpha_{kj} = 1$$

where α_{kj} defines the relative importance of each sub-indicator within the corresponding component.

D. Aggregated Risk-Indicator Score

The aggregated score is determined as:

$$S_i = w_I I_i + w_A A_i + w_D D_i + w_E E_i + w_B B_i + w_C C_i$$

subject to:

$$w_I + w_A + w_D + w_E + w_B + w_C = 1$$

For implementation, the following initial parameterization is used:

Component	Weight
Identity *I*	0.20
Authentication *A*	0.20
Transactional Data *D*	0.10
Technical Environment *E*	0.15
Behaviour *B*	0.20
Context *C*	0.15
Total	1.00

The weights represent an initial expert-based parameterization and should not be treated as universal constants. In practical deployment, they should be calibrated using historical data, known incidents, and statistical evaluation of the results.

E. Potential Impact

Potential impact is determined separately $P_i \in [0,1]$.It may reflect service criticality, information sensitivity, possible consequences for confidentiality, integrity, and availability, financial and operational impact, and the effect on interconnected information systems.

Separating P_i from the indicator components enables the model to distinguish observed risk signals from the severity of potential consequences.

F. Integrated Assessment of Transactional Cyber Risk

For the purposes of the proposed model, the integrated assessment is defined as:

$$R_i = S_i P_i$$

subject to:

$$0 \le R_i \le 1$$

This relationship constitutes an operational formalization within the proposed model, where S_i characterizes the intensity of the risk indicators and P_i represents the potential impact.

For practical interpretation:

$$DTRS_i = 100 R_i$$

Therefore:

$$DTRS_i \in [0,100]$$

The preliminary classification is:

DTRS	Level	Response
0–20	Low	Allow
>20–40	Moderate	Allow and monitor
>40–60	Elevated	Step-up authentication
>60–80	High	Temporarily suspend and review
>80–100	Critical	Block

The thresholds are model parameters and are subject to subsequent empirical calibration.

IV. Model Verification

The verification aims to determine whether changes in the values of the risk indicators produce distinguishable DTRS levels. Three scenarios are used, representing low, elevated, and critical risk profiles. The verification is functional and does not constitute statistical validation.

A. Low-Risk Transaction

For the following values: $I=0.05,\ A=0.05,\ D=0.10,\ E=0.10,\ B=0.05, C=0.10$ the result is $S_1=0.070$. For $P_1 = 0.40$: $R_1=0.028$, $DTRS_1=2.80$.

The transaction is classified as low risk and may be allowed.

B. Elevated-Risk Transaction

For $I=0.35,\ A=0.65,\ D=0.45,\ E=0.70,\ B=0.80,\ C=0.75,$ the result is: $S_2=0.6225$. For $P_2=0.90$: $R_2=0.56025$, $DTRS_2=56.03$.

The transaction falls into the elevated-risk category, for which the model activates additional authentication or review.

C. Critical-Risk Transaction

For: $I=0.85, A=0.90, D=0.80, E=0.90, B=0.95, C=0.90$ the result is: $S_3=0.890$. For $P_3=1.00$: $R_3=0.890$, $DTRS_3=89.00$

The transaction is classified as critical, and the model prescribes blocking or immediate referral for review.

Indicator	Scenario 1	Scenario 2	Scenario 3
S_i	0.070	0.623	0.890
P_i	0.40	0.90	1.00

Indicator	Scenario 1	Scenario 2	Scenario 3
R_i	0.028	0.560	0.890
DTRS	2.80	56.03	89.00
Level	Low	Elevated	Critical
Response	Allow	Step-up authentication	Block

The obtained values show the expected increase in DTRS as the intensity of the risk indicators and the potential impact increase. The demonstration confirms the model's functional sensitivity to different combinations of transaction characteristics, but it should not be interpreted as an empirical assessment of its accuracy.

V. Architecture for Practical Implementation

The model may be implemented as a standalone analytical module or as part of an information system for the provision of digital services.

The functional architecture is:

Data Sources →Feature Extraction →Risk Engine →DTRS →Decision

Data Sources provide input from IAM and authentication systems, SIEM, EDR/XDR, log records, device-management systems, and transaction systems.

Feature Extraction transforms the acquired telemetry into normalized indicators.

The Risk Engine forms the *I, A, D, E, B*, and *C* components, calculates Si, incorporates Pi, and determines Ri and DTRS.

The Decision Module converts the quantitative score into a technical response:

Allow →Monitor →Step−up Authentication →Review →Block

The architecture is consistent with Zero Trust principles, in which identity, device state, and current context contribute to the decision-making process [12].

VI. Scientific and Applied Contribution and Limitations

The main scientific and applied contribution of this study is the development of a formalized multi-criteria model in which the specific digital transaction is treated as an independent unit of cyber risk assessment.

The distinguishing characteristics of the model are:

1. Formation of a multidimensional risk profile for each transaction;
2. Separation of the risk indicators Si from the potential impact Pi;
3. Integration of identity-related, authentication, information, technical, behavioural, and contextual characteristics;
4. Normalization of heterogeneous indicators into a unified quantitative score;
5. Transformation of the integrated assessment into DTRS;
6. Direct linkage of DTRS to an adaptive protective response.

The formalized sequence is:

$$T_i \rightarrow XT_i \rightarrow S_i \rightarrow P_i \rightarrow R_i \rightarrow DTRS_i \rightarrow Decision$$

The proposed model also has limitations. The weighting coefficients and thresholds used are expert-defined and have not been statistically calibrated. Si represents an aggregated score of risk indicators rather than the probability of a successful attack. The presented scenarios demonstrate the functional logic of the model but do not establish statistical accuracy. A subsequent stage of the research should validate the model using real or reliably anonymized transaction data and determine optimal weights and thresholds through empirical analysis.

VII. Conclusion

This study develops a multi-criteria model for automated cyber risk assessment of digital transactions. Unlike approaches in which risk is assessed primarily at the level of an asset, system, or service, the proposed model treats the specific transaction as a dynamic object of assessment.

By integrating six groups of risk indicators, a separate assessment of potential impact, and the Digital Transaction Risk Score, the model enables current transaction characteristics to be transformed into a quantitative assessment and linked to a specific protective response.

The verification demonstrates the functional capability of the model to distinguish transactions with low, elevated, and critical risk profiles. Future research should focus on empirical validation, statistical calibration of weights and thresholds, and analysis of false-positive and false-negative results.

References

[1] European Parliament and Council. (2014). Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS). Official Journal of the European Union, L 257, 73–114.

[2] European Parliament and Council. (2022a). Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA). Official Journal of the European Union, L 333, 1–79.

[3] European Parliament and Council. (2022b). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2). Official Journal of the European Union.

[4] European Parliament and Council. (2024). Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. Official Journal of the European Union.

[5] Fridman, L., Weber, S., Greenstadt, R., & Kam, M. (2015). Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location. IEEE Systems Journal.

[6] ISO. (2018). ISO 31000:2018 Risk management — Guidelines. International Organization for Standardization.

[7] ISO/IEC. (2022a). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization.

[8] ISO/IEC. (2022b). ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. International Organization for Standardization.

[9] ISO/IEC. (2022c). ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks. International Organization for Standardization.

[10] Makowski, J.-P., & Pöhn, D. (2023). Evaluation of real-world risk-based authentication at online services revisited: Complexity wins. arXiv preprint arXiv:2308.15156.

[11] National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. National Institute of Standards and Technology.

[12] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. NIST Special Publication 800-207. National Institute of Standards and Technology.

[13] Temoshok, D., Proud-Madruga, D., Choong, Y.-Y., Galluzzo, R., Gupta, S., LaSalle, C., Lefkovitz, N., & Regenscheid, A. (2025). Digital Identity Guidelines. NIST Special Publication 800-63-4. National Institute of Standards and Technology.

[14] Wiefling, S., Lo Iacono, L., & Dürmuth, M. (2020). Is this really you? An empirical study on risk-based authentication applied in the wild. Proceedings of the IFIP SEC Conference.

[15] Wiefling, S., Dürmuth, M., & Lo Iacono, L. (2021). What's in score for website users: A data-driven long-term study on risk-based authentication characteristics. arXiv preprint arXiv:2101.10681.