Reconstruction of the Chronology of Events in Information and Communication Systems for Cyber Security Purposes based on the Coordination of Local Time Spaces*

Vitalii Fesokha[1,*,†], Ihor Subach[1,2,†]

[1] *Kruty Heroes Military Institute of Telecommunications and Information Technologies, st. Knyaziv Ostrozkyh, 45/1, Kyiv, 01011, Ukraine*

[2] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", st. Verkhnoklyuchova, 4, Kyiv, 03056, Ukraine*

Abstract

This paper examines the current scientific challenge of chronological reconstruction of events in information and communication systems (ICS) under conditions of asynchrony among their subsystems (components) and timestamp errors. In practice, the sequence of events recorded in monitoring logs often does not correspond to the actual sequence due to system clock drift, data transmission or processing delays, as well as the asynchrony of the time scales of different event sources. Modern cyber defense systems focused on event correlation often rely on such distorted chronology, which leads to erroneous conclusions during the analysis of cyber incidents and significantly complicates the establishment of cause-and-effect relationships between events. A method for chronological reconstruction of events is proposed, which is based on abandoning the assumption of a single global system time, does not require synchronization of monitoring sources, and restores global order based on reference relationships between events from different event logs. The method involves forming a set of local time spaces from event logs, determining reference and stabilizing relationships between them, finding optimal time offsets using a grid search method, and integrating the results into a single chronology of ICS events. An experimental study conducted using generated data based on MITRE ATT&CK cyberattack techniques confirms the effectiveness of the proposed approach – a reconstruction accuracy of 97% was achieved. The proposed method can be used in cyber incident monitoring and analysis systems for industrial control systems to improve the accuracy of event correlation and the reliability of reconstructing cause-and-effect chains between them.

Keywords

Information and communication systems, events, cyber security, local time space, time relativity, event correlation.

1. Introduction

Modern ICSs are characterized by highly dynamic data processing, distributed components, and intensive real-time information exchange. Under such conditions, it is extremely difficult to avoid distortions in the timestamps of the event lifecycle within ICSs due to various delays in data transmission and processing, the asynchronous operation of subsystems, or system clock drift. This results in the order of events recorded in logs often not reflecting their actual chronological sequence.

For cybersecurity systems whose functional core is focused on analyzing events to detect cyberattacks, malware, or signs of anomalous activity – such as Splunk, Elastic SIEM, Microsoft

*ITS-2025: Information Technologies and Security, December 11, 2025, Kyiv, Ukraine

* Corresponding author.

† These authors contributed equally.

vitaliifesokha@gmail.com(V. Fesokha); igor_subach@ukr.net (I. Subach);

0000-0001-6612-1970 (V. Fesokha); 0000-0002-9344-713X (I. Subach)

© 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

published 2026-11-26

CEUR-WS.org/Vol-4337/paper10.pdf

Sentinel, and IBM QRadar – such a mismatch is critical [1-4]. Thus, incorrect ordering of event sequences destroys the true cause-and-effect relationships between them, which ultimately leads to erroneous correlation results and a loss of understanding of their underlying structure.

This highlights the relevance of further research on reconstructing the actual (most probable) chronology of events in ICS systems to restore their contextual relationships for cybersecurity purposes.

1.1 Recent research and publications analysis

Research into the reconstruction of event chronologies in heterogeneous information systems has evolved from causal models to the intelligent analysis of temporal data [5–12]. The first fundamental ideas were formulated in [5], where the concept of logical dependence of events and the use of logical clocks to determine their partial order were proposed. Although this approach became the basis for event consistency in ICS, it assumes synchronized interaction of processes and does not account for distortions of timestamps in event logs. Further development is presented in [6], which examines the concept of virtual time, vector clocks, and global system states. Each process has a vector of values relative to events in other processes, and each event records the current state of this vector, based on which a decision is made regarding the chronology of events (if event $_A$ has a smaller vector than event $_B$, then $_A$ preceded $_B$).

Another approach to solving this problem is based on interval logic [7], which operates on a set of basic relations between event time intervals (only certain possible relations can exist between two event intervals). However, this approach has significant limitations regarding the analysis of life cycle phases for large volumes of events from various sources, where time may be incomplete or distorted. Similarly, temporal database models [8] focus on describing the chronology of events using two attributes: actual time and recording time, but they require the reliability of timestamps and do not account for delays during event recording.

The next stage of research [9] was devoted to the stream processing of unstructured data in large-scale computing environments. The concepts of “event time,” “processing time,” and “synchronization marks” were proposed, which made it possible to minimize delays during stream analysis. Although the approach is oriented toward real-time computation, it is not aimed at reconstructing causal relationships between events that have already been recorded in logs.

Recent scientific works [10–12] advance the field of digital forensics and the analysis of the chronology of cyber incidents. In particular, [10] proposes a conceptual model for describing the relationship between the actual sequence of events and their reconstruction based on digital artifacts. The model divides these spaces into quadrants (events: known, partially known, assumptions, unknown), which reflect different levels of data reliability, allowing for the systematization of the process of reconstructing event sequences in ICS. A drawback of this approach is the lack of a formal mechanism for reconciling events across independent sources. The paper [11] focuses on the issues of a narrow approach to describing cause-and-effect relationships in event logs. An improved logging method is proposed using identifiers of event-initiating sources, which allows tracking cause-and-effect relationships across multiple applications. Drawback: complex implementation in heterogeneous ICSs, lack of a global event synchronization algorithm. In [12], the use of large language models for automating the construction of cyber incident chronologies is investigated. The model analyzes textual descriptions of events, establishes their sequence, and generates explanations, which ensures a high level of automation; however, it does not guarantee correct temporal alignment and may generate illogical sequences.

Despite significant progress in the studies cited, the task of reconstructing the chronology of events in the ICS remains unresolved. Existing approaches do not ensure reliable reconstruction of event sequences in cases where time data is distorted or out of sync between different subsystems. Therefore, reconstructing the chronology of events in the ICS requires accounting for their

temporal relativity, where time data are not absolute but depend on the context of the subsystem within which they were recorded [13]. Each ICS subsystem forms its own local time space, in which events are perceived in a specific sequence that may differ from others.

Thus, the task of reconstructing the overall chronology of events in the ICS lies not in converting them to "universal time," but in reconciling the local time spaces that reflect the individual temporal perspective of each observation source.

The purpose of this paper is to develop a method for chronological reconstruction of events in an ICS for cybersecurity purposes based on the synchronization of local time spaces.

2. Reconstruction of the chronology of events

The proposed method is based on combining the advantages of the aforementioned approaches, but it rejects the assumption of a single global time in the ICS and shifts to a model of multiple time-based observation systems, which allows for the reconstruction of the most probable sequence of events under conditions of time relativity, where time data from different subsystems may be distorted or inconsistent [14]. It is based on the formation of local time spaces for each event source in the ICS and the subsequent coordination of their relationships, taking into account functional dependencies and logical constraints.

A local time space refers to the intrinsic time reference system of a specific source or context for recording events in the ICS (agent, subsystem, session, process), within which the order of events is considered internally consistent and is observed without necessarily corresponding to external time scales.

To form local time spaces, a sliding analysis window T is used, which is determined by the monitoring parameters of the cyber defense system. Window T covers the most recent events in the ICS received from various sources and corresponds to the time interval over which the cyber defense system performs data aggregation.

Input data:

$LS = \{L_1, L_2, \dots, L_K\}$ – a set of local time spaces (event logs) of the ICS;

$E = ¿\, i = 1 ¿\, k\, L_i -$ ¿the set of all events in the ICS within the time window T;

$\forall L_i \in LS$ a known sequence of events $\{e_{i1}, e_{i2}, \dots, e_{\text{in}}\}$ through the window of time T;

$\forall e_{ij} \in L_i$ it is known:

- local timestamp $t_i(e_{ij})$;
- event attributes $a_i(e_{ij})$ – type, process/session/user, identifiers of the current and parent processes;

$D = \{(e_{ij}, e_{ij+1}), | , e_{ij}\, e_{ij+1} \in E\, e_{ij} \to e_{ij+1}\}$ – a set of mandatory functional dependencies between view events:

- "process creation ⟶ process start";
- "request ⟶ response";
- "parent process ⟶ child process";
- "authentication ⟶ command execution".

Requirements: Construct a global chronology of events in the ICS over time T that:

- aligns local event sequences with LS;
- takes into account the temporal relativity of events (different subsystems have different times).

Constraints and assumptions:

- timestamps from different subsystems are not synchronized;
- the absence of some events in the logs is permitted.

2.1 Initialization of local time spaces

In this step, each event log of the ICS sources is formalized as a separate local time space $L_i \in LS$, within which the recorded sequence of events $L_i = \{e_{i1}, e_{i1}, \ldots, e_{\text{in}}\}$ is considered reliable [14]. This statement is based on the property of internal causal consistency of processes within a single event source. Thus, even if absolute timestamps are distorted, the relative order of events in the log remains valid, since it is determined by the actual order of request processing in the write queue.

The goal of this step is to transform the actual sequence of events L_i into a formal set of invariant constraints that must be preserved when constructing a global chronology of events. For each L_i, we define a set of event pairs that reflect the internal order in which they were recorded (1).

$$SP_{L_i} = \{(e_{ij} \prec e_{ij+1}), |, i = 1 \ldots n-1\}, \quad (1)$$

where ... where $e_{ij} \prec e_{ij+1}$ – e_{ij} precedes e_{ij+1}, $n-1$ – the number of event pairs in L_i.

The set of pairs formed for each time space L_i serves as the basis for preventing situations where event e_{i5} from L_i appears earlier in the global order of events than event e_{i2} from L_i when coordinating the set of local time spaces LS.

2.2 Defining reference relationships between local spaces

In this step, relationships are established that reflect functional dependencies between events in different ICS subsystems (the occurrence of one event triggers another), but within a single context (transaction or ICS session) [14]. The goal is to identify, based on the detected functional dependencies, such pairs of events in local sequences whose cause-and-effect relationship remains unchanged regardless of distortions in the timestamps.

In the previous stage, for each L_i, a sequence of events was recorded, where each event is described by a vector of attributes (type, timestamp, user ID, process ID, session ID) (2).

$$A(e_{ij}) = \{a_1, a_2, \ldots, a_m\}. \quad (2)$$

For each pair of local time spaces L_p and L_q, an event mapping is performed based on (3):

$$AF_{\text{sim}}(e_{pi}, e_{qj}) = w_f S_f + w_a S_a + w_t S_t, \quad (3)$$

where S_f is functional compatibility according to the rules, which includes D; S_a is contextual compatibility of events (event attributes); S_t – temporal proximity; w_f, w_a, w_t – weight coefficients of significance for each component (w_f – [0.45-0.5], w_a – [0.35-0.4], w_t – [0.1-0.2]).

A pair of events is considered to be correctly matched if $F_{\text{sim}}(e_{pi}, e_{qj}) \geq 0.7$, in accordance with the generally accepted concept of similarity thresholds [15, 16]. All pairs of events that satisfy this condition form the set of reference inter-space relationships (4).

$$F_{hard} = \{(e_{pi} \prec e_{qj}) | F_{\text{sim}}(e_{pi}, e_{qj}) \geq 0.7\}, \quad (4)$$

whereas all pairs of events that do not satisfy condition (4) form a set of weak connections, represented by the analytical expression (5).

$$F_{soft} = \{(e_{pi} \prec e_{qj}) | F_{\text{sim}}(e_{pi}, e_{qj}) < 0.7\}. \quad (5)$$

Thus, the set F_{hard} serves as a reference framework for event sequences, thereby ensuring the consistency of their chronology across independent observational sources. The set F_{soft} performs a stabilizing function in the process of reconciling the chronology of events between independent sources in the event of a shortage of reference relationships or incomplete logging. Fig. 1 schematically depicts the defined inter-space reference relationships of the local time spaces L_p and L_q.

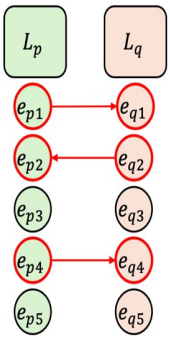


Figure 1: Determined reference relations between the local time spaces L_p and L_q.

2.3 Alignment of local time spaces

Given the temporal relativity of events, as defined earlier, the synchronization of local time spaces does not involve converting all timestamps to a single absolute system time, but rather involves mutually aligning their local scales [14]. Each ICS subsystem records events according to its own time scale; therefore, the purpose of this step is to establish correlations between such spaces, as well as to compensate for relative time shifts based on the reference relationships F_{hard} and stabilizing relationships F_{soft} obtained in the previous step.

In the context of heterogeneous ICSs, selecting a single reference local space for synchronization is inappropriate, since none of them can be considered a priori more reliable than the others; moreover, each of them may be subject to destructive interference. Therefore, the alignment of time spaces should be viewed as a combinatorial optimization problem, in which it is necessary to find such time shifts Δt_k for each local time space L_k as to minimize the number of violated reference li between events in different L_k. For each set $\Delta t = \{\Delta t_1, \Delta t_2, \ldots, \Delta t_m\}$, the following check is performed: whether the internal sequence of events is preserved within each L_k and how many inter-space reference relationships are violated.

The individual time shifts Δt_k for each L_k are selected using a grid search method [17]. In this case, the objective function is given by (6):

$$\min_{\Delta t} C(\Delta t) = \sum_{(e_p, e_q) \in F_{hard}} + w_{soft} \sum_{(e_p, e_q) \in F_{soft}} = (e_p, e_q, \Delta t_p, \Delta t_q) =, \quad (6)$$

where $u(e_p, e_q, \Delta t_p, \Delta t_q) = \begin{cases} 1, if\ t(e_p) + \Delta t_p > t(e_q) + \Delta t_q, \\ 0, otherwise. \end{cases}$ w_{soft} – weighting coefficient of influence F_{soft}.

After checking all grid options, the optimal combination of time shifts $\Delta t^* = arg\min_{\Delta t} C(\Delta t)$ is selected, which minimizes the number of violated constraints. In the event of an equal number of violations of reference constraints, preference is given to the solution with smaller absolute time shifts. The use of a set of weak constraints F_{soft} allows preventing the fragmentation of event sequences (soft preservation of logic even where a cause-and-effect relationship is not proven).

The result of the reconciliation is a set of adjusted timestamps $C(\Delta t)$ that maximally preserve the functional order of events between local time spaces (Fig. 2).

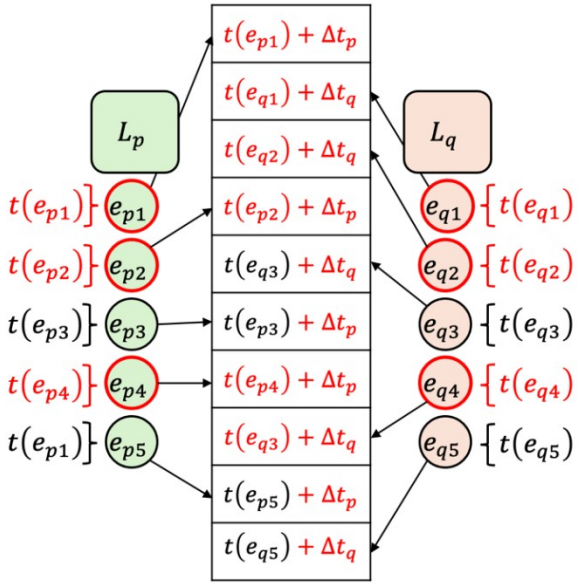


Figure 1: Generalized diagram of the alignment of the local time spaces L_p and L_q of the ICS.

2.4 Reliability Estimation of the Reconstructed Event Chronology

In the real-world operation of ICSs, there is no reference (true) sequence of events, which makes it impossible to directly assess the quality of the reconstruction. Consequently, it becomes necessary to evaluate the reliability of the reconstructed chronology based on the intrinsic properties of the data itself.

The proposed method for reconstructing the chronology of events is based on the use of constraints that reflect causal and functional dependencies between events. These constraints are formulated as sets of reference F_{hard} and stabilizing F_{soft} relationships between events in different local time spaces.

Since these relationships reflect only partial information about the connections between events, they form a set of partial constraints rather than a complete cause-and-effect graph. Accordingly, the assessment of the reliability of the reconstructed chronology should be based not on verifying its absolute correctness, but on the degree of consistency with the existing constraints.

To this end, a reconstruction reliability metric has been introduced, defined as the proportion of preserved reference relationships after the alignment of local time spaces, in accordance with [18, 19] (7):

$$F_{trust} = 1 - \frac{N_{viol}}{N_{hard}}, \tag{7}$$

where N_{viol} – number of disrupted support ligaments, N_{hard} – total number of support ligaments.

This indicator reflects the degree to which the derived sequence of events aligns with known cause-and-effect relationships. Only those relationships identified during the constraint formulation stage are taken into account. The absence of a relationship between events does not affect the reliability assessment.

Thus, the proposed indicator does not determine the absolute correctness of the reconstruction, but characterizes its internal logical consistency with the known operational structure of the ICS.

2.5 Integration into the cybersecurity process

In the final step, the results of the alignment of local time spaces are integrated into a unified information model of ICS events, which is compatible with the cyber defense system's analytics, correlation, and response processes.

Based on the results obtained, a harmonized global chronology of events is established, which preserves the local sequence of events from each observation source while ensuring the most plausible order of events in the IKS over a sliding window T (8).

$$H = \{ e_1', e_2', \dots, e_m' \} \subseteq E . \quad (8)$$

For each $e_i' \in H$ an entry is created (9):

$$e_i' = \langle id_i, t_i, src_i, type_i context_i \rangle , \quad (9)$$

where t_i – adjusted timestamp, src_i – source of the event, $type_i$ – type of event (what happened), $context_i$ – context of event.

The resulting timeline of events can be directly applied to cybersecurity tasks, specifically for:

- correlating events in SIEM systems to detect complex, multi-step attacks;
- constructing cause-and-effect chains of cyber incidents and analyzing their development scenarios;
- reducing the number of false positives caused by incorrect event ordering;
- improving the quality of anomaly detection, as a correct chronology allows for a more accurate assessment of deviations from normal behavior;
- supporting digital forensics processes, where it is crucial to reconstruct the actual sequence of the attacker's actions.

An important feature of the proposed approach is that it does not require prior clock synchronization between ICS subsystems. This allows the method to be applied in heterogeneous environments where event sources operate independently and use different time scales.

Furthermore, the use of a consistent event chronology reduces the number of false positives and false negatives in cybersecurity systems that arise from incorrect temporal ordering of events. This is particularly important for systems that perform automatic analysis of large volumes of events in real time or near real time.

Thus, integrating the proposed method into cybersecurity processes improves the quality of event analytics by creating a consistent, interpretable, and logically consistent representation of the chronology of events in the ICS.

3. Performance Evaluation

To evaluate the effectiveness of the proposed method for chronological reconstruction of events in information and communication systems, an experimental dataset was created that simulates the operational processes of such systems in the context of cyberattack scenarios [20].

Typical sequences of actions corresponding to cyberattack techniques were used as the basis for generating events. Each sequence of events was formed as an ordered set of interrelated actions (authentication, process creation, command execution, network interactions, data exfiltration, etc.) that reflect cause-and-effect relationships within sessions and processes.

General characteristics of the experiment:

- total number of generated events – 1500;
- number of events after forming the mixed set – 1455;
- number of event logs (local time spaces) – 3;
- number of reference relationships (hard relationships) – 283;
- total number of detected relationships (including stabilizing ones) – 346.

To simulate real-world operating conditions of the ICS, the generated events were distributed across several event logs (local time spaces). Each event was described using both timestamps and contextual attributes (session, process, and request identifiers, etc.), which remained constant. Distortion was applied exclusively to event timestamps in the form of individual shifts and time drifts within each log. As a result, a mixed (distorted) chronology of events was generated, in

which the global order of events does not correspond to their actual sequence of occurrence.

Prior to the application of the reconstruction method, the overall sequence of events was characterized by a significant number of disruptions in the cause-and-effect relationships between events in different subsystems.

Specifically, the number of disrupted causal relationships was 75.

After applying the method of reconciling local chronological frameworks, a reconstructed global chronology of events was obtained, in which the number of broken reference relationships was 29.8.

Thus, the application of this method made it possible to significantly reduce the number of violations of cause-and-effect relationships between events, indicating an improvement in the consistency of the global chronology.

Additionally, given the availability of a reference (ground truth) event sequence within the experimental setup, a direct comparison of event ordering was performed. The quality of reconstruction was evaluated using [18, 19], which measures the consistency of pairwise event ordering, as well as a reconstruction accuracy metric defined as the proportion of events occupying the correct position relative to the ground truth.

The obtained results are as follows:

- reconstruction accuracy of the mixed (distorted) sequence – 7.35%;
- reconstruction accuracy of the reconstructed sequence – 97.11%.

The results obtained confirm the high effectiveness of the proposed method in reconstructing the actual sequence of events.

3.1 Assessment of the Reliability of the Reconstructed Chronology

For each proceedings volume published with CEUR-WS, the titles of its papers should either all use the emphasizing capitalized style or the regular English (or native language) style. Check with the editors of your volume which style you should adopt.

Under the actual operating conditions of the ICS, there is no reference sequence of events, which makes it impossible to directly assess the accuracy of the reconstruction. In this regard, it is advisable to use an approach based on evaluating the consistency of the reconstructed chronology with known inter-event dependencies.

The reliability index of the reconstruction was determined as the proportion of preserved structural connections based on (7).

For the experimental results obtained: $F_{trust} = 1 - \frac{29.8}{283} \approx 0.895$.

Thus, following the reconstruction, approximately 89.5% of the underlying cause-and-effect relationships between events were preserved.

The results presented in Table 1 indicate a significant improvement in the consistency of the chronology of events following the application of the method.

Table 1

Results of the assessment of the effectiveness of reconstructing the chronology of events

Indicator	Before reconstruction	After reconstruction
Number of events	1455	1455
Number of hard relationships	283	283
Number of violation relationships	75	29.8
Violation rate	0.265	0.105
Reliability metric	0.735	0.895
Reconstruction accuracy	7.35%	97.11%

In particular, the number of violation relationships decreased by more than 2.5 times, accompanied by an increase in the reliability metric from 0.735 to 0.895 and a significant improvement in reconstruction accuracy.

It should be noted that inter-event dependencies are partial in nature and do not cover the entire set of events. In this regard, the reliability metric reflects not the absolute correctness of the reconstruction, but the degree of its consistency with known cause-and-effect relationships.

At the same time, the obtained values of the reliability metric are consistent with the results of direct assessment of the reconstruction's accuracy, indicating that it can be used to evaluate the quality of the reconstructed chronology in the absence of reference data.

4. Conclusion

This paper addresses the problem of reconstructing the chronology of events in information and communication systems for cybersecurity purposes based on the synchronization of local time spaces.

A method is proposed that is based on rejecting the assumption of a single global time and involves reconstructing the local time scales of ICS subsystems, taking into account functional dependencies between events. The method involves forming a set of local time spaces, identifying reference and stabilizing inter-event relationships, finding optimal time shifts, and integrating the results into a single coordinated chronology of events.

Additionally, an approach to assessing the reliability of the reconstructed chronology is proposed, which is based on the degree of preservation of reference cause-and-effect relationships between events.

The results of an experimental study conducted using generated data based on MITRE ATT&CK cyberattack techniques confirm the effectiveness of the proposed approach: the reconstruction accuracy is 97%, and the reliability index is approximately 0.89. The results obtained demonstrate the method's ability to provide a consistent and logically coherent chronology of events in the absence of clock synchronization between subsystems.

The proposed method significantly extends existing approaches to event correlation, which typically rely on timestamp alignment or assume the availability of synchronized clocks. In contrast, the developed approach enables reconstruction under conditions of temporal distortion, asynchronous logging, and incomplete temporal consistency, which are characteristic of real-world information systems.

From a practical perspective, the method can be integrated into security information and event management (SIEM) systems, digital forensics tools, and incident response platforms, enhancing their ability to correctly identify causal chains of cyber incidents. This, in turn, improves the accuracy of attack scenario reconstruction and supports more reliable decision-making in cybersecurity operations.

Furthermore, the use of reference and stabilizing relationships between events introduces an additional structural layer of analysis, allowing the system to operate not only with temporal attributes but also with semantic dependencies between events. This creates prerequisites for increasing robustness against noise, missing data, and adversarial manipulation of timestamps.

Overall, the developed method contributes to improving the cyber resilience of information and communication systems by enabling accurate reconstruction of event chronology under conditions of temporal uncertainty and system heterogeneity.

Declaration on Generative AI

During the preparation of this work, the author(s) used ChatGPT in order to: Grammar and spelling check, Paraphrase and reword.

References

[1] I. Subach, V. Kubrak, A. Mykytiuk, V. Korotaev, Rule-oriented method of cyber incidents detection by SIEM based on fuzzy logical inference, CEUR Workshop Proceedings (CEURWS.org) Vol. 2859 (2020) 210–219. doi:10.5281/zenodo.7123656.

[2] I. Subach, D. Mogylevych, A. Mykytiuk, V. Kubrak, V. Fesokha, Simulation Model of a Fuzzy Cyber Attack Detection System, CEUR Workshop Proceedings (CEUR-WS.org) Vol. 3421 (2021) 92–101. doi: 10.5281/zenodo.7247964.

[3] Akidau T., Bradshaw R., Chambers C., Chernyak S., Fernández-Moctezuma R. J., Lax R., McVeety S., Mills D. et al. The Dataflow Model: A Practical Approach to Balancing Correctness, Latency, and Cost in Massive-Scale, Unbounded, Out-of-Order Data Processing // Proceedings of the VLDB Endowment. 2015. V. 8, № 12. P. 1792–1803. DOI: 10.14778/2824032.2824076.

[4] Sheeraz M., Durad M. H., Paracha M. A., Mohsin S. M., Kazmi S. N., Maple C. Revolutionizing SIEM Security: An Innovative Correlation Engine Design for Multi-Layered Attack Detection // Sensors. 2024. V. 24, № 15. P. 4901. DOI: 10.3390/s24154901.

[5] Lamport L. Time, Clocks, and the Ordering of Events in a Distributed System // Communications of the ACM. 1978. V. 21, № 7. P. 558–565. URL: https://lamport.azurewebsites.net/pubs/time-clocks.pdf.

[6] Mattern F. Virtual Time and Global States of Distributed Systems // Parallel and Distributed Algorithms. North-Holland, 1989. P. 215–226. URL: https://homes.cs.washington.edu/~arvind/cs425/doc/mattern89virtual.pdf.

[7] Allen J. F. Maintaining Knowledge about Temporal Intervals // Communications of the ACM. 1983. V. 26, № 11. P. 832–843. URL: https://cse.unl.edu/~choueiry/Documents/Allen-CACM1983.pdf.

[8] Snodgrass R. T. Temporal Databases // IEEE Computer. 1986. V. 19, № 9. P. 35–42. URL: https://www2.cs.arizona.edu/~rts/pubs/EDC.pdf.

[9] Akidau T., Bradshaw R., Chambers C., Chernyak S., Dimov D. et al. The Dataflow Model: A Practical Approach to Balancing Correctness, Latency, and Cost in Massive-Scale, Unbounded, Out-of-Order Data Processing // Proc. of the VLDB Endowment. 2015. V. 8, № 12. P. 2188–2203. URL: https://static.googleusercontent.com/media/research.google.com/uk//pubs/archive/43864.pdf.

[10] Breitinger F., Studiawan H., Hargreaves C. SoK: Timeline based event reconstruction for digital forensics: Terminology, methodology, and current challenges // arXiv preprint arXiv:2504.18131. 2025. URL: https://arxiv.org/abs/2504.18131.

[11] Olegård J. Tracking event causality for improved forensic analysis and logging sufficiency // Forensic Science International: Digital Investigation. 2025. DOI: 10.1016/j.fdi.2025.09.012.

[12] Loumachi F. Y., Ghanem M. C., Ferrag M. A. Advancing Cyber Incident Timeline Analysis Through Retrieval-Augmented Generation and Large Language Models // Computers. 2025. V. 14, № 2. P. 67. URL: https://doi.org/10.3390/computers14020067.

[13] Fesokha V., Subach I. Conceptual framework for enhancing cyber resilience of information and communication systems in the context of evolution of cyber threats // Cybersecurity: Education, Science, Technique. 2025. V. 4, № 28. P. 511–528. DOI: 10.28925/2663-4023.2025.28.856.

[14] Fesokha V., Subach I., Kravchyk R. Method of chronological reconstruction of events in information communication systems for cyber security purposes based on the coordination of local time spaces // Communication, Informatization and Cybersecurity Systems and Technologies. 2025. № 8. P. 236–243. DOI: 10.58254/viti.8.2025.18.236.

[15] Dos Santos J. B., Heuser C. A., Moreira V., Wives L. K. Automatic Threshold Estimation for Data Matching Applications // Information Sciences. 2011. V. 181. P. 3665–3688. URL: https://www.sciencedirect.com/science/article/pii/S0020025510002380.

[16] Rekabsaz N., Lupu M., Hanbury A., Zuccon G. Exploration of a Threshold for Similarity Based on Uncertainty in Word Embedding // Advances in Information Retrieval: 39th European Conference on IR Research (ECIR 2017), Aberdeen, UK, April 8–13, 2017. Lecture Notes in Computer Science. V. 10193. Springer, Cham, 2017. P. 396–409. DOI: 10.1007/978-3-319-56608-5_31. URL: https://doi.org/10.1007/978-3-319-56608-5_31.

[17] Ilemobayo J. A., Durodola O. I., Alade O., Awotunde O. J., Olanrewaju A. T., Falana O., Ogungbire A., Osinuga A., Ogunbiyi D., Ifeanyi A., Odezuligbo I. E., Edu O. E. Hyperparameter Tuning in Machine Learning: A Comprehensive Review // Journal of Engineering Research and Reports. 2024. V. 26, № 6. P. 388–395. DOI: 10.9734/jerr/2024/v26i61188.

[18] Mercadier Y. Kendall Tau Distance // distancia 0.0.1 documentation. 2024. URL: https://distancia.readthedocs.io/en/latest/KendallTau.html#kendall-tau-distance.

[19] Fagin R., Kumar R., Sivakumar D. Comparing top-k lists // SIAM Journal on Discrete Mathematics. 2003.

[20] MITRE ATT&CK® Updates // MITRE ATT&CK®. 2025. URL: https://attack.mitre.org/resources/updates/.