Journal homepage: https://itce.vn.ua/en

Information Technologies and Computer Engineering **Vol. 23, No. 1. 2026**

Article's History: Received: 04.12.2025 Revised: 02.03.2026
Accepted: 26.03.2026 Published: 20.04.2026

ISSN 1999-9941; e-ISSN 2078-6387
UDC 004.85
DOI: 10.31649/vitce/1.2026.94

Algorithms and software architecture for automated user behaviour analysis in cyber threat detection systems

Denys Kovalchuk*
Postgraduate Student
International University
65009, 33 Fontanska Rd., Odesa, Ukraine
https://orcid.org/0009-0003-2302-8698

Abstract. The relevance of the present study is determined increasing complexity of cyber threats and the limited effectiveness of traditional detection methods, which necessitates the implementation of intelligent behavioural approaches using modern algorithmic and language models. The purpose of this study was to generalise and conceptually reinterpret approaches to automated user behaviour analysis in cyber threat detection systems from the perspective of algorithmic solutions and architectural principles of their construction. The study, based on theoretical analysis, a systemic approach, and comparative analysis, demonstrates that user behaviour analysis is an effective approach to cyber threat detection, capable of complementing and surpassing classical signature-based methods through the identification of context-dependent anomalies and multi-stage attacks. Comparative analysis of approaches to User and Entity Behaviour Analytics established a transition from a focus on individual actions to comprehensive analysis of interactions between users and technical components, which increases the accuracy of threat detection and reduces the number of false-positive alerts. Systemic analysis of the architecture of contemporary cybersecurity platforms showed that the integration of large language models ensures unified processing of structured, semi-structured, and unstructured data, modelling of long-term inter-event dependencies, and development of contextual behavioural models in real-time. Conceptual analysis and analytical evaluation indicated that combining behavioural analysis with large language models creates adaptive, scalable, and risk-oriented cybersecurity systems capable of early detection and proactive response to contemporary cyber threats while maintaining explainability, security, and regulatory compliance. The findings may support the design and implementation of intelligent cybersecurity systems in security operations and monitoring centres, security information and event management systems, and platforms for security orchestration, automation, and incident response

Keywords: User and Entity Behaviour Analytics; large language models; artificial intelligence; machine learning; data-driven approach

Introduction

The relevance of the study is determined by the rapid increase in the complexity of contemporary cyber threats, which increasingly exhibit multi-stage, adaptive, and covert characteristics and cannot be effectively detected through conventional signature-based and rule-based approaches. This situation emphasises the need for automated analysis of user behaviour as a key element of cybersecurity systems. The development of large language models creates new opportunities for contextual analysis of large volumes of structured and unstructured security data, correlation of events, and identification of latent patterns of malicious activity. Their practical application, however, requires scientifically grounded algorithmic and architectural solutions capable of ensuring scalability, real-time operation, accuracy of results, and compliance with information security requirements.

In contemporary cybersecurity research discourse, considerable attention is directed towards automated analysis of user and entity behaviour as a key mechanism for detecting complex and low-visibility threats. I. Sokyrka *et al.* (2025) examined behavioural analytics in authentication tasks, demonstrating that machine learning can support the development of dynamic user profiles based on behavioural patterns, thereby increasing system resilience to

Suggested Citation:
Kovalchuk, D. (2026). Algorithms and software architecture for automated user behaviour analysis in cyber threat detection systems. *Information Technologies and Computer Engineering*, 23(1), 94-109. doi: 10.31649/vitce/1.2026.94

*Corresponding author

credential compromise. The researchers emphasised that behavioural features, rather than static attributes, ensure the adaptability of protective mechanisms in a changing environment. A similar idea was developed by O. Suprun & N. Karpenko (2025), who focused on the analysis of user behaviour as an instrument for reducing the risks of insider threats. The researchers investigated the use of behavioural analysis for insider threat detection and emphasised the importance of constructing baseline models of "normal" activity for each user or role. The study indicated that even minor deviations from established behavioural patterns may signal malicious or compromised actions that remain unnoticed by signature-based systems.

In the international context, R.K. Mohanty (2025) systematised deep learning approaches to user and entity behaviour analytics and confirmed their effectiveness in the correlation of heterogeneous events and the construction of context-dependent models capable of generalising complex causal relationships. The researcher described neural network architectures in detail, including recurrent and graph-based models, which allowed effective consideration of temporal dependencies and relationships among events, users, and resources. A practical dimension of this issue was presented by M.I. Mihailescu *et al.* (2023), who implemented behavioural analysis in cybersecurity systems to detect hidden threats that evade conventional methods. The researchers observed that the correlation of user actions across time and space enabled the identification of multi-stage attacks that do not manifest through isolated events. The study presented examples of the integration of behavioural analysis into existing cybersecurity systems and indicated that this approach substantially reduces the number of false-negative detections. The research emphasised the practical value of behavioural analytics as a complement to conventional detection mechanisms. A. Wairagade & S. Ranjan (2025) conducted a comprehensive comparative analysis of conventional and modern machine learning algorithms for cyber threat detection based on behavioural user data. The researchers demonstrated that the effectiveness of detection depends not only on the selection of a model but also on the behavioural features and the method of their aggregation within a temporal context. The results indicated that models capable of accounting for event sequences and non-linear dependencies ensure a reduction in false-negative detections compared with conventional approaches, which makes them suitable for practical implementation in systems designed to detect complex attacks.

Another systemic approach was presented by G. Sharma *et al.* (2024), who proposed a comprehensive conceptual framework of User and Entity Behaviour Analytics (UEBA) oriented towards the integration of machine learning with contextual knowledge about users, entities, and execution environments. The researchers emphasised that isolated event analysis is insufficient for contemporary threat scenarios, whereas the combination of behavioural, role-oriented, and temporal contexts enables the development of more robust models of normal and anomalous activity. The study highlighted the importance of correlation among multi-level data sources and the adaptability of models to the evolution of behaviour, which directly connects UEBA with architectures of the new generation of Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) systems. A.G. Desetty (2024) examined the potential of the combined application of machine learning and UEBA for detecting hidden threats that are not susceptible to conventional signature-based detection. The researcher noted that integration of behavioural analysis with clustering algorithms and time-series modelling enables the construction of multidimensional profiles of normal entity activity, which ensures early detection of latent attacks and insider threats. In the report by A. Trivedi *et al.* (2025), emphasis was placed on the role of User Behaviour Analytics (UBA) in countering insider threats, and behavioural patterns were considered a critical indicator of deviations from normal employee activity. The researchers demonstrated that UBA, particularly in combination with modern machine learning methods, is capable of developing dynamic behavioural models that adapt to changes in user activity and identify early signs of sabotage, data leakage, or indirect system compromise. This emphasises the necessity of a comprehensive behaviour-oriented approach to the construction of security systems that extend beyond simple event monitoring.

Analysis of previous studies indicates that the majority of research in the field of User and Entity Behaviour Analytics focuses either on comparative evaluation of individual machine learning algorithms or on conceptual descriptions of UEBA and UBA architectures, without sufficient attention to their software integration into operational cyber threat detection systems. Several studies address behavioural analysis in isolation from streaming event processing and operational response mechanisms, which limits the practical applicability of the proposed approaches. Existing research also provides limited consideration of the combination of contextual analysis of user behaviour with temporal correlation of events in environments characterised by high dynamism and heterogeneous data sources, creating a gap between theoretical models and the requirements of contemporary Security Operations Centre (SOC)-oriented systems.

The purpose of this study was to theoretically generalise algorithmic and software-architectural approaches to automated analysis of user behaviour in cyber threat detection systems. The following tasks were formulated to achieve this purpose: analyse and systematise scientific approaches to modelling user and entity behaviour in the context of cybersecurity, considering the evolution of threats and the increasing complexity of information environments; and theoretically justify the relationship between behavioural analytics algorithms and software-architectural principles in the construction of cyber threat detection systems.

Materials and Methods

The study is theoretical and conceptual, grounded in a comprehensive analysis of contemporary approaches to behavioural analysis in cybersecurity and the integration of large language models into relevant analytical ecosystems. Research materials included studies from 2022-2025 addressing UBA, UEBA, and the operation of contemporary SIEM-, Security Orchestration, Automation and Response (SOAR)-, SOC-, and XDR-oriented systems. The methodological foundation of the study consisted of a set of interrelated theoretical methods applied sequentially according to the logic of the research tasks. Theoretical analysis served as an instrument for in-depth conceptual interpretation of key concepts and approaches in the behavioural analysis of cyber threats. Its application was determined by the need to distinguish clearly between behavioural and signature-based approaches and to provide theoretical justification of the capabilities of contemporary large language models (LLMs). The analysis addressed behavioural anomalies as context-dependent deviations from normal activity patterns and the architectural principles of LLMs, including mechanisms that model long-term dependencies among security events. Systematisation was applied to structure theoretical approaches to behavioural analysis in cybersecurity, enabling a coherent comparison of UBA and UEBA concepts within a unified analytical framework. It identified objects of analysis, levels of context, and functional capabilities of each approach, while examining relationships among users, technical entities, and services.

Comparative-analytical evaluation was employed to assess various approaches to behavioural analysis and the algorithms used for cyber threat detection. Its use was motivated by the need to identify conceptual and functional differences between UBA and UEBA, and between LLMs and classical machine learning or deep learning methods. Analysis considered characteristics such as scale of context, capacity for processing heterogeneous data, and potential integration of behavioural, network, and textual signals. The comparative assessment enabled the identification of key advantages and limitations of each approach and outlined trade-offs among accuracy, computational complexity, and explainability of decisions.

Conceptual generalisation provided a holistic interpretation of the role of behavioural analytics and LLMs within contemporary SOC ecosystems. Behavioural analysis and LLMs were treated as an intelligent analytical layer that ensures contextual interpretation of security events, correlation of heterogeneous signals, and reduction of false-positive alerts. Theoretical modelling was applied to describe algorithmic approaches to cyber threat detection using LLMs, including static and dynamic analysis of events. LLMs were interpreted as multi-level feature extraction mechanisms capable of forming semantic representations of logs, commands, and event sequences, integrating them into contextual models of user and system behaviour. They supported real-time streaming event processing, functioning as the core mechanism for contextual encoding and anomaly scoring, which enabled comprehensive detection of complex multi-stage attacks.

Analytical evaluation had a descriptive character and was applied to examine the Analytical evaluation had a descriptive character and was applied to examine the practical suitability of LLMs-based approaches, including system effectiveness and performance. Analysis addressed key criteria such as threat detection accuracy, processing latency, throughput, and adaptability to new attack scenarios. The study summarised deployment characteristics across edge, cloud, and hybrid infrastructures to identify optimal architectural approaches for real-time implementation. Limitations, risks, and ethical considerations were analysed, including explainability of LLMs' decisions, bias in training data, and potential misuse of models in defensive and offensive contexts. Systemic generalisation supported the analysis of privacy and regulatory compliance with reference to international standards and regulatory frameworks, including the General Data Protection Regulation (GDPR) (Regulation (EU) No. 2016/679, 2016) and ISO/IEC 27001:2022 (2022). Structural-logical modelling systematised relationships among architectural solutions, algorithmic approaches, risks, and mitigation measures. The study acknowledged limitations, including low explainability of LLMs decisions, possible bias in training data, the requirement to process confidential information, and the risk of misuse of models for cyber-attacks.

Results

User behaviour analysis as a component of contemporary cybersecurity systems

In cybersecurity, behavioural anomalies are considered deviations from established or expected patterns of actions of users, service accounts, or software agents within information systems. In contrast to signature indicators of attacks, which rely on previously known patterns of malicious activity, behavioural anomalies are contextual and dynamic, and they form based on statistical, temporal, semantic, and structural characteristics of interactions between actors and the system. Such anomalies may appear as atypical time intervals of access, unusual sequences of commands, changes in the frequency or volume of operations, or disruption of typical relationships among security events. A distinctive feature of behavioural anomalies is their relative character: an action may be normal for one user or role but suspicious for another. This requires constructing personalised or role-oriented behavioural models that incorporate historical data, business process context, and the system environment. Behavioural analysis extends beyond classical incident detection. It functions as a tool for identifying potential threats at the pre-compromise stage, when malicious activity has not yet produced explicit technical markers (Hakonen, 2022).

The concept of UBA emerged as a response to the limitations of conventional monitoring systems that primarily focus on network or system events without deep

consideration of the behavioural context of users. UBA involves developing profiles of normal user activity derived from authentication logs, resource access records, actions within application systems, and other telemetry data. Subsequent analysis focused on identifying deviations from these profiles that may indicate credential compromise, insider threats, or preparation for an attack. Further evolution of this approach led to the development of the UEBA concept, which expands the object of analysis beyond human users to include various entities of information infrastructure, including servers, virtual machines, container environments, Internet of Things (IoT) devices, and service accounts. UEBA treats the system as a complex socio-technical ecosystem in which interactions between users and technical components form multidimensional behavioural graphs. This approach enables the detection of anomalies not only at the level of individual actions but also within the structure of relationships among actors and events (Khan *et al.*, 2022). For clarity, the differences between UBA and UEBA are presented in Table 1.

Table 1. Comparative characteristics of UBA and UEBA

Characteristic	UBA	UEBA
Object of analysis	Users	Users and technical entities
Data types	Access logs, user actions	Access logs, network events, system telemetry
Level of context	Individual	System-wide and inter-entity
Primary objective	Detection of user anomalies	Detection of complex, multi-step attacks

Source: compiled by the author based on A.W. Mir & K.R. Kumar (2022), V. Malik *et al.* (2024)

Analysis of Table 1 demonstrates the evolution of approaches to behavioural analysis in cybersecurity and differences in the scale and complexity of threat assessment. UBA focuses on the individual user and immediate actions, which enables effective detection of simple anomalies such as unauthorised logins or unusual operations, yet its capabilities remain limited in cases of complex multi-stage attacks or interactions among multiple actors and system processes. UEBA expands the analytical focus by incorporating technical entities and system telemetry, which enables analysis of inter-entity dependencies, identification of correlations among events, and prediction of complex threats. Therefore, UEBA provides deeper contextual analysis and supports prioritisation of responses to complex attacks, which reflects the tendency of contemporary cybersecurity systems towards integration of behavioural and system analysis to increase detection effectiveness and minimise risks.

Behavioural models are effective in detecting threats that lack clearly defined signatures or rely on legitimate access mechanisms. Such threats cover insider misuse, in which a legitimate user or employee of an organisation performs actions beyond their functional responsibilities. Behavioural analysis enables identification of gradual changes in activity profiles that may indicate preparation for data exfiltration or sabotage. Another class of threats involves attacks using stolen credentials, such as credential stuffing or account takeover. In these scenarios, technical access parameters may appear legitimate, but behavioural characteristics such as login time, geographical origin of access, and sequence of actions differ from historically established norms. Behavioural models also detect lateral movement within corporate networks, where an attacker gradually expands access privileges while imitating legitimate administrative activity. Behavioural analysis plays a further role in detecting complex multi-stage attacks, including Advanced Persistent Threat (APT) campaigns, in which individual actions may appear harmless, yet their cumulative structure and correlation form a malicious scenario. In such cases, behavioural models act as an integrative mechanism, combining fragmented security signals into a unified semantic representation of the threat (Brandao, 2025).

Within cybersecurity centres, particularly SOC, automated analysis of user behaviour functions as a core element of the intelligent layer responsible for security event processing. Conventional SIEM systems aggregate, normalise, and correlate logs, but without behavioural context, they often generate significant numbers of false-positive alerts (Saraiva & Mateus-Coelho, 2022). Integration of UBA and UEBA modules reduces informational noise by prioritising events based on risk-oriented behavioural assessments. Within SOAR ecosystems, automated behavioural analysis triggers orchestration of incident response processes (Aljumaily *et al.*, 2025). Behavioural risk scoring may initiate automated response scenarios, including forced transition of a user into restricted access mode, additional authentication procedures, or initiation of deeper investigation. Behavioural analysis thus serves not only as a detection instrument but also as an active component of adaptive security management.

Analysis of operation principles and cybersecurity potential of large language models

Large language models rely on the Transformer architecture, which differs fundamentally from recurrent and convolutional approaches through the use of the self-attention mechanism as the principal instrument for sequence processing. Self-attention enables parallel modelling of dependencies among all elements of an input sequence regardless of positional distance, which is critically important for analysis of long-term and structurally complex contexts. In cybersecurity, this capability enables the integration of events distributed across time and space into a unified semantic model of an attack or user behaviour. A central component of the Transformer architecture is multi-head attention, which enables the model to focus on multiple aspects of input data simultaneously. In the context

of cyber threat analysis, the model may process temporal patterns of access, semantics of commands, network attributes, and role characteristics of users in parallel. Positional encoding compensates for the absence of recurrent structure and enables the model to preserve information about the order of events, which is essential for the reconstruction of multi-stage attack scenarios. The pre-training stage plays a decisive role in the development of generalised knowledge within the model. During this stage, LLMs are trained on extremely large corpora of data through self-supervised tasks such as prediction of the next token or reconstruction of missing fragments (Xu *et al.*, 2025). This process forms a latent space that encodes syntactic, semantic, and contextual dependencies. In cybersecurity applications, such representation enables the transfer of general linguistic and structural knowledge to specialised domains, including the analysis of logs, network protocols, and technical descriptions of attacks.

One advantage of large language models lies in their ability to operate uniformly with heterogeneous data types that have conventionally required separate analytical pipelines. In cybersecurity, structured data include event logs, system telemetry, network traffic flows, and access metadata, whereas unstructured data include textual messages, electronic correspondence, incident reports, technical documentation, and open-source threat intelligence. Large language models integrate these sources into a unified semantic space through transformation into token sequences followed by contextual analysis (Thelwall, 2025).

In contrast to conventional approaches that require separate models and feature mechanisms for structured and unstructured data, large language models provide a shared representation of information in which numerical, categorical, and textual attributes can be interpreted within a single architectural framework. This characteristic substantially simplifies correlation of security events, for example, the comparison of anomalous network activity with textual descriptions of suspicious messages or communications within support systems. Thus, Large language models function as a universal interface among different data layers within cybersecurity systems (Ali & Ghanem, 2025). For the generalisation of the characteristics of processing different data types in the context of LLMs, a comparative presentation is provided in Table 2.

Table 2. Comparison of data type processing in conventional methods and LLM in cybersecurity

Data type	Examples in cybersecurity	Conventional approaches	LLM approach
Structured	SIEM logs, NetFlow	Statistical models, rules (threshold rules, signature rules, SIEM correlation rules, expert-defined if-then rules in intrusion detection systems)	Contextual encoding
Semi-structured	JSON, XML, API logs	Feature engineering	Unified tokenisation
Unstructured	Email, reports, chats	NLP models separately	Shared semantic space

Note: JSON – JavaScript Object Notation, XML – eXtensible Markup Language, NLP – Natural Language Processing, API – Application Programming Interface

Source: compiled by the author based on F.N. Motlagh et al. (2024), W. Kasri *et al*. (2025)

The table demonstrates a fundamental transformation in approaches to data processing in cybersecurity due to the integration of large language models. Conventional analytical methods differ according to the structure of data: structured data are processed through statistical models or rule-based systems, semi-structured data require manual feature engineering, whereas unstructured data were previously analysed through isolated NLP models. This separation complicated the integration of results and created a gap between different information sources. The use of LLMs enables a unified analytical approach to all data types, forming a shared contextual and semantic space in which structured, semi-structured, and unstructured information are analysed simultaneously and in relation to one another. Such an approach enables correlation of behavioural and technical signals in real-time, increases the accuracy of detecting complex threats, and reduces the time required for the integration of heterogeneous data sources. Therefore, cyber defence systems become more flexible, scalable, and contextually adaptive.

Contextual modelling represents one of the key properties of large language models in tasks related to user behaviour analysis. Classical models usually operate with fixed observation windows or aggregated statistical features, whereas LLMs can construct long-term contexts that encompass sequences of user actions across different systems and time scales. This capability enables analysis of the evolution of behaviour rather than only instantaneous deviations. Within UEBA scenarios, contextual modelling means that each new action is interpreted with reference to previous events, the role of the user, the type of resource, and the current state of the system. Access to confidential data, for instance, may be legitimate within one business process but appear anomalous when combined with an unusual login time or earlier unsuccessful authentication attempts. LLMs allow such complex dependencies to be formalised without rigid rule specification, which increases the adaptability of the system to new and previously unknown threat scenarios (Fuentes *et al.*, 2025).

Comparison of large language models with classical machine learning and deep learning methods demonstrates fundamental differences in approaches to the construction of cyber defence systems. Classical machine learning (ML) models, such as support vector machine or Random Forest,

require careful feature selection and typically operate effectively within narrowly defined scenarios. Deep neural networks, including Long Short-Term Memory or Convolutional Neural Network, are capable of modelling complex dependencies, yet they are often limited by data type and contextual scale. Large language models provide universality and scalability of analysis by combining the capacity to process diverse data types with the modelling of long-term contextual dependencies. Such models are more suitable for detecting complex, multi-stage, and low-visibility attacks. Their application requires substantial computational resources and introduces new challenges related to explainability and quality control of results (Huang *et al.*, 2023).

Thus, the theoretical perspective indicates the necessity of hybrid approaches in which LLMs are integrated with classical analytical methods to maintain a balance between accuracy, performance, and interpretability. Large language models form a new paradigm in cybersecurity. They shift the analytical focus from isolated event analysis towards deep contextual understanding of user and system behaviour, which opens prospects for the development of adaptive and proactive cyber threat detection systems.

Algorithmic approaches to automated cyber threat analysis using LLMs

Static analysis of malicious software and security logs conventionally involves the evaluation of objects without their actual execution, focusing on internal structure, code features, or properties of events. Within the context of large language models, this approach acquires a new analytical dimension, since LLMs can transform bytecode, system logs, configuration files, and textual messages into a unified semantic space of tokens. The model can therefore identify latent indicators of malicious activity that are difficult to detect through conventional signature-based or statistical methods. Such indicators may include atypical combinations of API calls, anomalous sequences of events in access logs, or indirect signals of code injection into legitimate processes (da Costa *et al.*, 2022).

From an algorithmic perspective, LLMs perform functions of multi-level feature extraction, ranging from low-level analysis of command syntax and semantics to identification of global behavioural patterns of processes and users. Tokenisation of logs followed by contextual encoding enables the model to construct representations that incorporate temporal dependencies, object types, and relationships between them. Static analysis that uses LLMs is often combined with classical analytical approaches, including signature databases and heuristic techniques, which increases detection accuracy and reduces false-positive alerts (Wang *et al.*, 2024).

Dynamic analysis involves the examination of object behaviour during active operation, including process execution, user interaction with systems, and network activity. Integration with LLMs enables modelling of behavioural patterns in real-time and identification of deviations not only from historical user profiles but also from expected patterns of system activity. LLMs analyse sequences of actions, correlate them with semantically similar scenarios accumulated during pre-training, and can anticipate potentially malicious actions before they lead to system compromise. At the algorithmic level, dynamic analysis that incorporates LLMs relies on streaming analytics and incremental updating of the contextual model. Each new event modifies the latent representation of behaviour, which enables the model to adjust risk assessment immediately (Rahman, 2024). This approach supports effective detection of atypical patterns, including deviations in command sequences or interactions between users and systems that remain difficult to identify through static analysis (Fig. 1).

Figure 1. Stream processing of user events using LLMs in cybersecurity systems
Source: compiled by the author based on A.M. Mustafa (2024), A. Karras *et al.* (2025)

The diagram highlights the sequential integration of textual and behavioural analysis in real-time for the detection of cyber threats. The process begins with an event generated by a user or process that is recorded in logs or telemetry, after which the data undergoes tokenisation that transforms heterogeneous information (structured, semi-structured, and unstructured) into a unified representation. The next stage, contextual encoding by LLMs, forms multidimensional semantic representations that incorporate not only the current event but also the history of interactions, behavioural patterns, and system context. These representations support anomaly scoring, which enables assessment of the probability of malicious activity or deviations from normal behaviour. The final stage, threat ranking and the SOAR trigger, ensures prioritisation of response actions and automation of security measures. The diagram emphasises the integration of LLMs within the analytical workflow, which combines the precision of semantic analysis with the operational speed of behavioural monitoring and ensures scalability and adaptability of the system to new and unknown threats. The scheme illustrates how contemporary models integrate data of different structures and heterogeneous signals into a coherent representation of cyber threats in real-time (Ibrahim & Kashef, 2025).

LLMs provide the capacity to classify attacks not only through explicit technical indicators but also through complex analysis of behavioural and semantic characteristics. The model compares behavioural patterns of users and entities with historically recognised classes of attacks, including phishing, malware execution, privilege escalation, lateral movement, Distributed Denial of Service (DDoS), and other threats. Contextual understanding enables LLMs to differentiate legitimate deviations from malicious actions even when information is incomplete or logs are partially missing. Table 3 presents the classification effectiveness for illustrative purposes.

Table 3. Potential LLMs in detecting classes of cyberattacks based on behavioural indicators

Attack class	Typical behavioural indicators	LLMs potential
Phishing	Unusual communication sequences, atypical email structures	Semantic modelling of content and sequences
Malware execution	Abnormal process activity, atypical API calls	Contextual classification of commands and calls
Lateral movement	Unusual resource access, role changes	Correlation between events over time and entities
Privilege escalation	Sudden acquisition of elevated privileges	Detection of atypical scenarios from historical data
DDoS	Increased traffic from users or services	Analysis of temporal and network patterns

Source: compiled by the author based on G. Esposito (2025), H. Razavi *et al.* (2025)

Table 3 illustrates how large language models transform the approach to detecting different classes of cyber-attacks by shifting the analytical focus from simple observation of behavioural indicators towards contextual and semantic analysis. Conventional approaches rely on pattern recognition or anomaly detection within logs and network flows, which limits the capabilities of security systems in cases of complex or multi-stage attacks. The analytical potential of LLMs lies in the capacity to integrate heterogeneous signals, including textual, behavioural, and system data, into a unified contextual model. Such integration enables recognition of complex patterns, correlation of events across different entities, and forecasting of attack progression. This capability increases the accuracy of early detection of phishing campaigns, malicious processes, lateral movement, and privilege escalation, and supports analysis of network anomalies in real-time. Synthesis of these observations indicates that LLMs enable more flexible, adaptive, and context-oriented detection of cyber-attacks, which strengthens the ability of security systems to counter both known and emerging threats and represents a central factor in contemporary cyber defence.

Complex multi-stage attacks, including Advanced Persistent Threats (APT), represent a significant area of research interest. These attacks are characterised by long-term and concealed execution of malicious activity that frequently relies on legitimate user accounts and infrastructure mechanisms. Detection of such threats requires the construction of global contextual models that integrate information from multiple sources and time scales. In this context, LLMs function as an integrative algorithm that combines local signals, historical patterns, and semantic relationships between events into a unified representation of risk (Shakil *et al.*, 2023). Thus, algorithmic approaches that employ large language models integrate static and dynamic analysis, attack classification, and detection of complex multi-stage scenarios within a single analytical system. This integration considerably increases the effectiveness of identifying hidden threats and reduces incident response time.

Software architecture of automated behavioural analysis systems

The software architecture of automated behavioural analysis systems demonstrates a high level of modularity and orientation towards scalability, which supports efficient processing of large streams of security data from multiple sources. Conventional pipeline architectures process data sequentially from initial collection to final risk evaluation, which ensures clear traceability of each stage and supports integration of heterogeneous analytical algorithms. Each module within this architecture performs a strictly defined function, including pre-processing, tokenisation, contextual encoding, anomaly detection, and attack classification. This structure enables isolated optimisation of algorithms and effective monitoring of system performance. Microservice-based architectures increase flexibility in system deployment and maintenance because each service corresponds to a specific functional component, such as log interpretation, LLMs integration, or anomaly score generation. Microservices also support parallel scaling of critical components that process the largest volumes of data and facilitate integration of new analytical algorithms without restructuring the entire system (Guduru, 2025).

Events in complex multi-user and multi-platform environments are generally processed through an event-driven approach, in which each event (log entry, network packet, or system message) activates corresponding reactions within computational modules. This model reduces processing delays and ensures rapid response to atypical actions, which is particularly important for multi-stage attacks and dynamic scenarios of malicious activity. The conceptual scheme that combines these architectural patterns may be described as follows: the pipeline structure ensures sequential data processing,

microservices distribute computational tasks across modules, and the event-driven mechanism activates reactions in real-time (Vieira, 2025).

Integration of large language models into SIEM, SOAR, and XDR platforms requires careful design of data flows, interaction formats, and algorithms for prioritisation of analytical results. LLMs enrich events with additional semantic context, increase the accuracy of anomaly scoring, and support the identification of complex multi-stage attacks. Within SIEM modules, LLMs automatically correlate events from different sources and construct global graphs of user and entity behaviour. Within SOAR platforms, analytical outputs function as triggers for automated response scenarios, whereas within XDR environments, they integrate with analytical consoles and endpoint detection modules that maintain a unified threat context (Mareedu, 2025). Table 4 presents examples of the roles performed by LLMs within different platforms.

Table 4. Role of large language models across cybersecurity platform

Platform	LLMs role	Example functions
SIEM	Contextual event correlation	Detection of latent attack patterns, anomaly scoring
SOAR	Automated response	Triggers for scenarios, recommendations for access restriction, report generation
XDR	Endpoint and analytics integration	Synthesis of behavioural patterns from endpoint data, prediction of potential attacks

Source: compiled by the author based on R. Boddu & S. Lamppu (2024)

Table 4 emphasises that large language models strengthen the platform architecture of cybersecurity by integrating analytics, automation, and forecasting. They enable SIEM systems to detect hidden patterns of attacks, allow SOAR platforms to automate response actions and generate recommendations, and support XDR systems in synthesising data from endpoints and forecasting potential threats. Therefore, large language models transform protection systems into context-oriented, adaptive, and proactive cybersecurity instruments.

Within contemporary infrastructure, the volume of security data may reach hundreds of thousands of events per second, which requires the application of distributed computational solutions. System scalability is ensured through horizontal expansion of microservices, the use of cluster-based solutions for event stream processing, and parallel execution of LLMs on specialised computational nodes. Distributed processing involves not only parallelisation of computations but also effective management of contextual model states, replication of critical data, and synchronisation of anomaly scoring results. This architecture maintains high prediction accuracy even in geographically distributed infrastructures, multithreaded attack scenarios, and peak loads on SIEM, SOAR, and XDR platforms (Pitkar, 2025).

Phishing attacks and social engineering manipulation involve linguistic and semantic techniques designed to deceive users and obtain confidential information or unauthorised access to resources. Key indicators include atypical structures of electronic messages, including grammatical and stylistic deviations, recurring semantic patterns, use of emotional or terminological pressure, and substitution of domains or links. Conventional systems analyse such characteristics through signature verification, reputation databases, and simple rules based on the presence of specific keywords. These mechanisms frequently fail to detect complex adaptive campaigns. Large language models construct multi-level semantic representations of messages that include not only surface lexical information but also deeper contextual dependencies. The model therefore identifies unusual word combinations, metaphors, disguised calls to action, and hidden emotional signals that frequently occur in phishing and social engineering campaigns. Context modelling at the level of documents and dialogue histories enables LLMs to detect suspicious messages even when known signatures or reputation data are absent (Putra *et al.*, 2024).

Analysis of social engineering involves not only the identification of individual suspicious messages but also the detection of recurring manipulative patterns that form coherent influence scenarios targeting users. The complexity arises from the fact that attacks are distributed across several stages and interconnected communications that may initially appear as ordinary message flows. Large language models integrate temporal, semantic, and social contexts and construct multidimensional behavioural models of attackers. At the algorithmic level, this process involves analysis of sequences of tokenised messages, construction of interaction graphs between senders and recipients, and identification of patterns within the structure and frequency of communications. Large language models generate latent representations that encode hidden manipulation patterns and differentiate targeted campaigns from random anomalies within communication streams (Amer, 2025).

The effectiveness of phishing detection increases significantly through the correlation of textual analysis of messages with the behavioural patterns of users and security events within the information system. Atypical opening of attachments or navigation through links, combined with previously identified linguistic characteristics of a message, increases the accuracy of risk assessment. Within this analytical framework, LLMs function as an integrative analytical core that combines semantic information from texts, behavioural characteristics of users, and security metadata within a shared multidimensional space. The outcome consists of event ranking according

to risk level and generation of recommendations for automated response or preventive communication (Putra *et al.*, 2024; Amer, 2025).

Contextual analysis of communications functions as a central instrument in countering social engineering attacks. Large language models evaluate the meaning of messages within the context of communication history, user roles, interactions with systems, and characteristics of business processes. This approach enables the identification of hidden threats that cannot be detected through isolated analysis of texts or behaviour. The model may recognise implicit attempts of influence through gradual changes in message tone within long-term correspondence, combinations of formal and emotional signals, and indirect requests for confidential information. Large language models therefore function not merely as tools for detecting anomalies in textual content but as comprehensive mechanisms of semantic and behavioural analysis that detect complex, adaptive, and multi-stage social engineering scenarios. Table 5 demonstrates typical indicators of phishing messages and the corresponding role of LLMs in their analysis.

Table 5. Potential of LLMs in detecting phishing indicators

Phishing indicator	Description	LLMs role
Linguistic deviations	Grammatical errors, atypical style	Semantic recognition of atypical structures
Manipulative content	Use of emotional or terminological pressure	Detection of social engineering patterns
Hidden links	Masking of URLs or domains	Correlation with user behaviour and reputational data
Multi-stage scenarios	Series of messages with gradual influence	Contextual modelling of communication sequences

Note: URL – Uniform Resource Locator

Source: compiled by the author based on B. Naqvi *et al*. (2023), F.P.E. Putra *et al.* (2024)

Table 5 illustrates how large language models transform the approach to detection of phishing campaigns by shifting analytical focus from simple identification of surface indicators towards contextual and semantic analysis. Large language models integrate linguistic, behavioural, and socio-technical signals, which enables identification of unusual stylistic deviations, the detection of manipulative patterns, and the correlation of hidden links with user behaviour and reputation data. The models also represent multi-stage communication scenarios, which increases the accuracy of early detection of complex phishing attacks and supports proactive operation of cybersecurity systems rather than simple reaction to known threats. In synthesis, LLMs integrate semantic, behavioural, and contextual analysis and establish more adaptive and predictive mechanisms for countering phishing.

Analysis of the effectiveness and performance of LLMs in real-time environments

Evaluation of the effectiveness of large language models in real-time environments represents a critical component of their integration into automated behavioural analysis systems and cyber threat detection infrastructures. The principal criteria for assessing the performance of LLMs include threat detection accuracy, event processing latency, and system throughput. Detection accuracy reflects the capacity of the model to correctly classify behavioural anomalies and types of attacks while reducing the number of false-positive and false-negative alerts. Latency determines the speed with which the system responds to new events and generates warnings, which is particularly important for multi-stage attacks and complex Advanced Persistent Threat scenarios. Throughput characterises the volume of events that the system processes without performance degradation and directly influences scalability and the ability to support large corporate or distributed infrastructures. Adaptation of LLMs to new and previously unknown threats occurs through contextual modelling of user and entity behaviour, which enables the model to anticipate potentially malicious actions even when predefined signatures are absent. Mechanisms of incremental learning and online retraining perform an important role in this process because they integrate new data rapidly without complete re-initialisation of the model. System design must consider the trade-off between analytical depth and response speed: complex contextual models provide high accuracy but require greater computational resources and processing time, whereas simplified representations accelerate processing but may reduce analytical precision (Katreddy, 2023).

Resolution of this trade-off depends on the selected deployment architecture, which determines where and how data processing occurs. The edge approach provides local analysis at endpoints, reduces latency, and supports rapid response to critical events, although it remains limited by the computational capacity of devices. The cloud approach provides access to extensive computational resources and supports the use of full-scale LLMs for comprehensive analysis of large data volumes. Data transmission and processing delays may, however, affect real-time event analysis. The hybrid approach combines the advantages of both models by delegating initial evaluation and preliminary detection to edge nodes while transferring deeper and more resource-intensive contextual analysis to the cloud. This architecture maintains a balance between response speed and analytical accuracy (Donepudi *et al.*, 2025). Table 6 demonstrates the key performance criteria and trade-off aspects that require consideration during the deployment of LLMs in real-time environments.

Table 6. Key performance criteria of LLMs in real-time operation and associated trade-offs

Criterion	Definition	Impact on system	Trade-offs
Accuracy	Correct classification of threats and anomalies	Enhances the reliability of detection	Requires greater computational resources and time
Latency	Time between an event and the model signal	Affects responsiveness	May increase with deep contextual analysis
Throughput	Volume of events the system can process	Determines scalability	May decrease when using resource-intensive models
Adaptation	Ability to respond to new threats	Improves system flexibility and relevance	Requires mechanisms for online learning and model updates

Source: compiled by the author based on M. Zhang *et al.* (2025)

The table reflects the multidimensional character of evaluating the effectiveness of LLMs in cybersecurity, with each criterion interrelated with system performance and response efficiency. Synthesis indicates that achieving high accuracy and deep contextual analysis improves threat detection reliability while increasing latency and computational load. System throughput and scalability directly depend on the architectural approach and optimisation of data processing flows, which necessitates balancing response speed with analytical depth. Adaptation to new and previously unknown threats remains crucial for maintaining system relevance and flexibility, requiring mechanisms for online learning and regular model updates. Collectively, these criteria emphasise that real-time integration of LLMs represents a compromise between accuracy, speed, scalability, and adaptability, which defines the effectiveness of modern behavioural analysis systems.

Limitations, risks, and ethical considerations in the use of large language models

The deployment of LLMs in automated cyber threat analysis systems involves fundamental limitations and risks that require consideration throughout integration and operational processes. One critical challenge concerns model explainability, described as the "black box" problem. LLMs generate outputs from multidimensional latent representations formed during training on extensive corpora of textual and behavioural data. The complexity of internal attention mechanisms, transformer blocks, and multi-layered contextual links renders interpretation of why a model classifies an event as an anomaly or threat highly difficult. This creates challenges for justifying alerts to SOC operators and for compliance with regulatory requirements in critical sectors such as finance, healthcare, and energy. Another challenge involves the quality and bias of training data. LLMs train on large datasets that may contain structural, semantic, or social biases. In cybersecurity, these biases can lead to systematic underestimation or overestimation of particular user behaviours, specific event sources, or regional characteristics of cyber threats. Such biases negatively affect detection accuracy, increase false-positive signals, and generate uneven risk assessment. Mitigation requires implementation of data audit procedures, control over data representativeness, and application of decorrelation and class-balancing methods during training (Alang *et al.*, 2025).

Effective LLMs analysis requires access to user logs, network flows, messages, and other metadata containing sensitive information. Without robust anonymisation, encryption, and access control, the risk of data leakage or unauthorised use is high. LLMs integration in corporate and government information systems must comply with local and international regulatory frameworks, including GDPR (Regulation (EU) No. 2016/679, 2016), ISO/IEC 27001:2022 (2022), and other cybersecurity standards, which necessitates careful design of architecture and data-processing procedures. Separate attention is required for risks of model misuse by attackers. LLMs can be exploited to generate phishing messages, social-engineering scenarios, automate account-compromise attempts, or analyse structured and unstructured data to identify vulnerabilities (Semerikov *et al.*, 2025). This highlights the necessity of ethical and regulatory control over model access, restriction of potentially dangerous functionalities, and continuous monitoring of usage. Table 7 presents a structured overview of the relationships between limitations, risks, and their consequences.

Table 7. Key limitations and risks of using LLMs in cybersecurity and mitigation measures

Category	Nature of limitation/risk	Consequences	Potential mitigation measures
Explainability	Complexity of internal latent representations	Inability to justify decisions to SOC, regulatory risks	Interpretable models, LIME/SHAP, logging of intermediate outputs
Data bias	Uneven or structural biases	False positives/false negatives, systematic errors	Data audit, class balancing, pattern decorrelation
Confidentiality	Requirement for access to sensitive data	Information leakage, regulatory violations	Anonymisation, encryption, access control, compliance with GDPR/ISO
Misuse	Use of the model for attacks	Generation of phishing campaigns, social engineering scenarios	Functionality restrictions, usage audit, ethical policies, monitoring

Note: LIME – Local Interpretable Model-agnostic Explanations; SHAP – SHapley Additive exPlanations
Source: compiled by the author based on N.O. Jaffal *et al.* (2025)

The table demonstrates the multicomponent nature of risks associated with LLMs deployment in cybersecurity systems and underscores the need for comprehensive risk management. Explainability, data bias, confidentiality, and potential misuse are interrelated and affect both technical system performance and compliance with regulatory and ethical standards. Synthesis indicates that risks extend beyond technical aspects to include organisational, regulatory, and social factors. Effective LLMs utilisation requires an integrated approach that combines model interpretability, data auditing and cleansing, access control, encryption, and monitoring, maintaining a balance between analytical power and security. Such a comprehensive approach minimises adverse consequences and increases trust in real-time decisions generated by LLMs. Real-time integration of LLMs therefore demands a holistic approach that combines technical, organisational, and ethical measures to ensure reliability, security, and lawful use of models, while preserving system performance and analytical quality.

Discussion

The results obtained in the present study on behavioural analytics and the integration of large language models into cyber threat detection systems are fully consistent with the findings of other scholars. S. Subrahmanyam (2025) presented behavioural analysis as a core intellectual mechanism for detecting threats that lack explicit signatures, emphasising context, temporal dynamics, and profiling of normal activity. He concluded that the effectiveness of behavioural models increases when integrating heterogeneous data sources and employing adaptive algorithms. His findings correspond with observations regarding the central role of behavioural analysis as an intelligence layer within SOC ecosystems and its capacity to reduce false-positive alerts through event contextualisation. However, that study placed less emphasis on practical aspects of scaling and handling unstructured data, which the current study addressed through the deployment of large language models. R.R. Kethireddy (2022) applied behavioural analytics combined with LLMs to detect insider threats, where LLMs interpreted user action contexts and explained risky patterns. Scientists reported improved detection accuracy for insider threats compared with classical ML models, corresponding with findings on the universality and contextual power of LLMs. His study focused primarily on human users, whereas the present study demonstrates the advantage of a broader UEBA approach encompassing technical entities and inter-entity interactions.

T. Ali & P. Kostakos (2023) presented the HuntGPT system, applying a hybrid approach to anomaly detection by combining classical ML detectors with LLMs and elements of explainable AI. The researchers emphasised that LLMs do not fully replace conventional models, but act as an interpretative and correlation layer, enhancing clarity and practical value for SOC analysts. This conclusion partially differs from the findings of the current study, in which LLMs are considered the core of contextual encoding and behavioural scoring. In contrast, T. Arjunan (2024) examined the use of natural language processing methods for detecting anomalies and intrusions in unstructured cybersecurity data, including event logs, textual incident descriptions, and system messages. The researcher demonstrated that NLP approaches can identify latent semantic patterns not captured by conventional signature- or statistics-based methods, which aligns with the presented conclusion regarding the necessity of semantic interpretation of security events. However, the study relied primarily on classical NLP methods and shallow/deep learning models, whereas the present study shows that large language models provide substantially broader contextual analysis and unified processing of heterogeneous data. Therefore, the results of T. Arjunan correlate conceptually with the obtained findings but differ in contextual scope and the absence of full behavioural integration.

X. Jiang *et al.* (2025) investigated the detection of user behaviour anomalies in cloud environments using deep learning. The researchers confirmed the effectiveness of neural network models for early threat warning through analysis of behavioural features, time series, and access patterns. These findings align with the assertion regarding the high value of behavioural analysis for early attack detection. However, unlike the current study, X. Jiang *et al.* limited behavioural analysis primarily to the user level within cloud infrastructure and did not cover inter-entity interactions or heterogeneous data types. V. Önal *et al.* (2025) considered user behavioural analysis in SIEM data as a key AI application to reduce information noise and improve event correlation accuracy. The researchers showed that AI-driven UBA identifies anomalies in security event streams more effectively than conventional correlation rules. These findings directly correspond with the obtained findings regarding the role of behavioural analysis as an intelligence layer in SOC and SIEM platforms. However, the study emphasised classical AI and ML methods, whereas the present paper demonstrates that integrating large language models overcomes the limitations of SIEM-oriented analysis through deeper semantic correlation and support for multi-step attack scenarios.

M.J. Hussain (2024) reviewed behavioural analysis approaches using machine learning, particularly for detecting anomalies in user and system entity behaviour. The researcher highlighted the effectiveness of ML methods for early threat warning and reduction of false-positive alerts, which corresponds with the presented conclusion on the importance of behavioural analysis for improving detection accuracy. The study, however, is limited to classical ML methods and did not consider the potential of large language models for unifying heterogeneous data and contextually modelling complex multi-step attacks. S. Subrahmanyam (2025) emphasised the integration of user behavioural analysis into threat detection systems, including SOC platforms, and highlighted the role of AI in incident prioritisation and reducing informational noise. These findings confirm the presented conclusions regarding the effectiveness of UEBA as an intelligence layer within SOC and the value of risk-oriented scoring. The study, however,

predominantly employed classical AI/ML methods without deep involvement of LLMs, explaining partial discrepancies in contextual processing and unified handling of structured and unstructured data.

I. Hassanov *et al.* (2024) conducted a systematic review on the use of AI and LLMs for cyber intelligence and threat prediction. The researchers highlighted that LLMs can integrate heterogeneous information sources, model behavioural patterns, and detect complex anomalies, which supports key findings of the present study. The review has a broader strategic focus and provides less detail on practical integration of UEBA and real-time event streaming, explaining the differences in applied depth between the studies. L.A. Odozor *et al.* (2025) proposed an incident response approach combining malware behavioural analytics with adversarial modelling to improve detection accuracy and limit attack impact. The researchers emphasised the value of integrating multiple data sources and forming contextual models of malware behaviour, which aligns with the obtained findings on the importance of unifying structured and unstructured data and contextually modelling events to detect complex threats. Their study, however, focused mainly on malware analytics rather than user behavioural analysis and LLMs integration in SOC platforms, explaining differences in applied focus. I.H. Sarker (2024) explored the role of generative AI and large language models in cybersecurity, particularly regarding automation, intelligent decision-making, and explainability. The researcher demonstrated that LLMs can integrate heterogeneous data, form multi-level semantic representations, and enhance attack prediction, which corresponds with the present findings on contextual modelling and combining behavioural analysis with LLMs. I.H. Sarker's study did not detail practical integration into SIEM or SOAR platforms, which is a central emphasis of the present study.

Overall, comparative analysis indicates that the present study aligns with current studies on context-oriented, adaptive cybersecurity systems, moving beyond isolated detectors. Discrepancies among individual studies result from differences in scope, choice of analytical targets, and the role assigned to LLMs – either as auxiliary interpretation tools or as central components of behavioural analytics architecture. This confirms the scientific originality and practical relevance of the present study, which extends existing approaches through systematic integration of UEBA and LLMs in modern cybersecurity platforms.

Conclusions

User behavioural analysis is a key component of modern cybersecurity systems, capable of complementing and surpassing classical signature-based methods. The integration of behavioural models allows detecting anomalies and threats at early stages, predicting potentially harmful actions, and reducing false-positive alerts, which provides a more accurate and risk-oriented response. UBA and UEBA concepts demonstrate an evolution from analysis of individual actions to comprehensive evaluation of interactions between users and technical components, enabling effective detection of complex, multi-step attacks, including APT campaigns and lateral movement. Large language models establish a new paradigm in cybersecurity, as they can integrate heterogeneous data and construct contextual models of user and system behaviour. With the Transformer architecture and self-attention mechanism, LLMs can model long-term and complex dependencies between events, which is critical for reconstructing multi-step attacks and synthesising disparate signals into a coherent semantic picture. LLMs unify the processing of structured, semi-structured, and unstructured data, enhancing the accuracy of detecting complex threats in real-time and supporting system adaptability to novel and unpredictable attack scenarios.

The effectiveness of LLMs in real-time depends on detection accuracy, processing latency, throughput, and the ability to adapt to emerging threats. The balance between response speed and depth of contextual analysis is determined by deployment architecture: the edge approach accelerates processing at endpoints, the cloud approach enables large-scale analysis, and the hybrid approach combines the advantages of both models. Use of LLMs, however, carries several limitations and risks, including low interpretability of decisions, bias in training data, handling of sensitive information, and potential misuse of models for attacks. Ensuring reliability, security, and compliance requires a comprehensive approach that integrates model interpretability, data auditing and cleansing, access control, encryption, usage monitoring, and adherence to regulatory frameworks such as GDPR and ISO/IEC 27001. Overall, integrating behavioural analysis with large language models produces adaptive, context-oriented, and scalable cybersecurity systems capable of effectively detecting, assessing, and proactively responding to contemporary threats, thereby enhancing operational resilience and the efficiency of security infrastructure. Future studies should focus on enhancing model interpretability, developing hybrid edge–cloud architectures for real-time analysis, integrating behavioural, semantic, and contextual analytics, and addressing regulatory and ethical considerations of LLM use in cybersecurity.

Acknowledgements

None.

Funding

None.

Conflict of Interest

None.

References

[1] Alang, K., Hassan, S.Z., Katkam, V., & Hassan, S. (2025). Real-time ML and LLM optimization: Orchestrating Scalable workflows in distributed commerce environments. In *2025 international conference on computing technologies & data communication* (pp. 1-7). Hassan: IEEE. doi: 10.1109/ICCTDC64446.2025.11158822.

[2] Ali, A., & Ghanem, M.C. (2025). Beyond detection: Large language models and next-generation cybersecurity. *SHIFRA*, 2025, 81-97. doi: 10.70470/SHIFRA/2025/005.
[3] Ali, T., & Kostakos, P. (2023). Huntgpt: Integrating machine learning-based anomaly detection and explainable AI with large language models (LLMs). *ArXiv*. doi: 10.48550/arXiv.2309.16021.
[4] Aljumaily, M., Abd, H., & Majeed, E. (2025). Enhancing user and entity behavior analytics in SIEM systems using AI-powered anomaly detection: A data-driven simulation approach. *International Journal of Mechatronics, Robotics, and Artificial Intelligence*, 1(2), 82-93. doi: 10.33971/ijmrai.1.2.11.
[5] Amer, L. (2025). AI in cyber security: A dual perspective on hacker tactics and defensive strategies. *Cyber Security: A Peer-Reviewed Journal*, 8(3), 198-213. doi: 10.69554/CLXC9075.
[6] Arjunan, T. (2024). Detecting anomalies and intrusions in unstructured cybersecurity data using natural language processing. *International Journal for Research in Applied Science & Engineering Technology*, 12(2), 1023-1029. doi: 10.22214/ijraset.2024.58497.
[7] Boddu, R., & Lamppu, S. (2024). *Microsoft unified XDR and SIEM solution handbook: Modernize and build a unified SOC platform for future-proof security*. Birmingham: Packt Publishing Ltd.
[8] Brandao, P.R. (2025). Exploring the role of artificial intelligence in detecting advanced persistent threats. *Computers,* 14(7), article number 245. doi: 10.3390/computers14070245.
[9] da Costa, F.H., Medeiros, I., Menezes, T., da Silva, J.V., da Silva, I.L., Bonifácio, R., Narasimhan, K., & Ribeiro, M. (2022). Exploring the use of static and dynamic analysis to improve the performance of the mining sandbox approach for android malware identification. *Journal of Systems and Software*, 183, article number 111092. doi: 10.1016/j.jss.2021.111092.
[10] Desetty, A.G. (2024). Unveiling hidden threats with ML-powered user and entity behavior analytics (UEBA). *Turkish Journal of Computer and Mathematics Education*, 15(1), 44-50.
[11] Donepudi, S., Lakshmi, U.P., Kumar, N.P., Lalitha, S., Shaik, R., & Devi, D.A. (2025). Efficient LLM inference on mcp servers: A scalable architecture for edge-cloud ai deployment. *Journal of Theoretical and Applied Information Technology*, 103(13), 4885-4895.
[12] Esposito, G. (2025). *LLMs in the SIEM loop: A contract-based framework for threat detection with an evaluation on Windows telemetry and MITRE ATT&CK mapping*. Torino: Polytechnic University of Turin.
[13] Fuentes, J., Ortega-Fernandez, I., Villanueva, N.M., & Sestelo, M. (2025). Cybersecurity threat detection based on a UEBA framework using Deep Autoencoders. *AIMS Mathematics*, 10(10), 23496-23517. doi: 10.3934/math.20251043.
[14] Guduru, S. (2025). Autonomous cyber defense: LLM-Powered incident response with LangChain and SOAR integration. *International Journal of Computer Science and Information Technology Research*, 6(1), 72-82. doi: 10.63530/IJCSITR_2025_06_01_008.
[15] Hakonen, P. (2022). *Detecting insider threats using user and entity behavior analytics*. (Master's thesis, JAMK University of Applied Sciences, Jyväskylä, Finland).
[16] Hassanov, I., Virtanen, S., Hakkala, A., & Isoaho, J. (2024). Application of large language models in cybersecurity: A systematic literature review. *IEEE Access*, 12, 176751-176778. doi: 10.1109/ACCESS.2024.3505983.
[17] Huang, F., Xiong, H., Chen, S., Lv, Z., Huang, J., Chang, Z., & Catani, F. (2023). Slope stability prediction based on a long short-term memory neural network: comparisons with convolutional neural networks, support vector machines and random forest models. *International Journal of Coal Science & Technology*, 10(1), article number 18. doi: 10.1007/s40789-023-00579-4.
[18] Hussain, M.J. (2024). A survey based on behavior analysis of artificial intelligence using machine learning process. In *2024 4th international conference on sustainable expert systems* (pp. 1694-1701). Kaski: IEEE. doi: 10.1109/ICSES63445.2024.10763264.
[19] Ibrahim, N., & Kashef, R. (2025). Exploring the emerging role of large language models in smart grid cybersecurity: A survey of attacks, detection mechanisms, and mitigation strategies. *Frontiers in Energy Research*, 13, article number 1531655. doi: 10.3389/fenrg.2025.1531655.
[20] ISO/IEC 27001:2022. (2022). *Information security, cybersecurity and privacy protection – information security management systems – requirements*. Retrieved from https://www.iso.org/standard/27001.
[21] Jaffal, N.O., Alkhanafseh, M., & Mohaisen, D. (2025). Large language models in cybersecurity: A survey of applications, vulnerabilities, and defense techniques. *AI*, 6(9), article number 216. doi: 10.3390/ai6090216.
[22] Jiang, X., Jia, R., & Zhang, F. (2025). Deep learning-based user behavior anomaly detection and threat early warning in cloud computing environments. *Academia Nexus Journal*, 4(3).
[23] Karras, A., Theodorakopoulos, L., Karras, C., Theodoropoulou, A., Kalliampakou, I., & Kalogeratos, G. (2025). LLMs for cybersecurity in the big data era: A comprehensive review of applications, challenges, and future directions. *Information*, 16(11), article number 957. doi: 10.3390/info16110957.
[24] Kasri, W., Himeur, Y., Alkhazaleh, H.A., Tarapiah, S., Atalla, S., Mansoor, W., & Al-Ahmad, H. (2025). From vulnerability to defense: The role of large language models in enhancing cybersecurity. *Computation*, 13(2), article number 30. doi: 10.3390/computation13020030.

[25] Katreddy, S.S. (2023). Optimizing AI/ML workloads in cloud environments: A scalable approach. *International Journal of Intelligent Systems and Applications in Engineering*, 11(11), 710-719.
[26] Kethireddy, R.R. (2022). AI-powered insider threat detection with behavioral analytics with LLM. *International Journal of Science and Research*, 11(10), 1449-1453. doi: 10.21275/SR221013110718.
[27] Khan, M.Z.A., Khan, M.M., & Arshad, J. (2022). Anomaly detection and enterprise security using user and entity behavior analytics (UEBA). In *2022 3rd international conference on innovations in computer science & software engineering* (pp. 1-9). Karachi: IEEE. doi: 10.1109/ICONICS56716.2022.10100596.
[28] Malik, V., Khanna, A., Sharma, N., & Nalluri, S. (2024). Advanced persistent threats (APTs): Detection techniques and mitigation strategies. *International Journal of Global Innovations and Solutions*. doi: 10.21428/e90189c8.91e89a3e.
[29] Mareedu, A. (2025). Autonomous Security Operations Centers (SOC): AI agents for threat triage, response, and orchestration. *International Journal of Emerging Research in Engineering and Technology*, 6(2), 63-70. doi: 10.63282/3050-922X.IJERET-V6I2P108.
[30] Mihailescu, M.I., Nita, S.L., Rogobete, M., & Marascu, V. (2023). Unveiling threats: Leveraging user behavior analysis for enhanced cybersecurity. In *2023 15th international conference on electronics, computers and artificial intelligence* (pp. 1-6). Bucharest: IEEE. doi: 10.1109/ECAI58194.2023.10194039.
[31] Mir, A.W., & Kumar, K.R. (2022). An enhanced implementation of security management system (SSMS) using UEBA in Smart Grid based SCADA systems. In J.K. Mandal, S. Misra, J.S. Banerjee & S. Nayak (Eds.), *Proceedings of 2nd global conference on artificial intelligence and applications: Applications of machine intelligence in engineering* (pp. 1-11). Boca Raton: CRC Press. doi: 10.1201/9781003269793.
[32] Mohanty, R.K. (2025). Deep learning for analyzing user and entity behaviors: Techniques and applications. In N. Marriwala, S. Jain, V. Shukla & D. Kumar (Eds.), *Hybrid soft computing techniques for machine learning and optimization* (pp. 121-148). Hershey: IGI Global Scientific Publishing. doi: 10.4018/979-8-3693-6864-0.ch006.
[33] Motlagh, F.N., Hajizadeh, M., Majd, M., Najafi, P., Cheng, F., & Meinel, C. (2024). Large language models in cybersecurity: State-of-the-art. *ArXiv*. doi: 10.48550/arXiv.2402.00891.
[34] Mustafa, A.M. (2024). *Leveraging AI for confident classification and prioritization of intrusion detection system alerts*. (Master's thesis, American University of Beirut, Beirut, Lebanon).
[35] Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S., & Porras, J. (2023). Mitigation strategies against the phishing attacks: A systematic literature review. *Computers & Security*, 132, article number 103387. doi: 10.1016/j.cose.2023.103387.
[36] Odozor, L.A., Ransome-Kuti, O.S., Odeniran, Q., Olisa, A.O., Berko, S.N., & Abaya, J.T. (2025). Data-driven incident response: Enhancing detection and containment through adversarial reasoning and malware behavior analytics. *International Journal of Innovative Science and Research Technology*, 10(9), 218-230. doi: 10.38124/ijisrt/25sep154.
[37] Önal, V., Arslan, H., & Canay, Ö. (2025). Anomaly detection in SIEM data: User behavior analysis with artificial intelligence. In P. Bhambri & A.J. Anand (Eds.), *Handbook of AI-driven threat detection and prevention: A holistic approach to security* (pp. 269-289). Boca Raton: CRC Press. doi: 10.1201/9781003521020.
[38] Pitkar, H. (2025). Cloud security automation through symmetry: Threat detection and response. *Symmetry*, 17(6), article number 859. doi: 10.3390/sym17060859.
[39] Putra, F.P.E., Ubaidi, Zulfikri, A., Arifin, G., & Ilhamsyah, R.M. (2024). Analysis of phishing attack trends, impacts and prevention methods: literature study. *Brilliance: Research of Artificial Intelligence*, 4(1), 413-421.
[40] Rahman, N. (2024). *Leveraging large language models for network traffic analysis: Design, implementation, and evaluation of an LLM-powered system for cyber incident reconstruction*. (Master's thesis, University of Turku, Turku, Finland).
[41] Razavi, H., Ouaissa, M., Ouaissa, M., Nakouri, H., & Abdelgawad, A. (2025). *AI-driven cybersecurity: Revolutionizing threat detection and defence systems*. Boca Raton: CRC Press. doi: 10.1201/9781003631507.
[42] Regulation (EU) No. 2016/679 of the European Parliament and of the Council "On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)". (2016, April). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.
[43] Saraiva, M., & Mateus-Coelho, N. (2022). CyberSoc framework a systematic review of the state-of-art. *Procedia Computer Science*, 204, 961-972. doi: 10.1016/j.procs.2022.08.117.
[44] Sarker, I.H. (2024). Generative AI and large language modeling in cybersecurity. In *AI-driven cybersecurity and threat intelligence: Cyber automation, intelligent decision-making and explainability* (pp. 79-99). Cham: Springer. doi: 10.1007/978-3-031-54497-2_5.
[45] Semerikov, S.O., Vakaliuk,T.A., Kanevska, O.B., Moiseienko, M.V., Donchev, I.I., & Kolhatin, A.O. (2025). LLM on the edge: The new frontier. In *Proceedings of the 5th edge computing workshop* (pp. 137-161). Zhytomyr: CEUR-WS.
[46] Shakil, N.A.F., Mia, R., & Ahmed, I. (2023). Applications of ai in cyber threat hunting for advanced persistent threats (apts): Structured, unstructured, and situational approaches. *Journal of Applied Big Data Analytics, Decision-Making, and Predictive Modelling Systems*, 7(12), 19-36.

[47] Sharma, G., Thakur, A., & Tiwari, C. (2024). Developing a comprehensive framework for user and entity behavior analytics (UEBA): Integrating advanced machine learning and contextual insights. *Journal of Communication Engineering & Systems*, 14(2), 20-31.

[48] Sokyrka, I., Kukulevskyi, I., & Tolbatov, A. (2025). Authentication methods using behavioral analytics and machine learning for internet of things devices. *Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique",* 2(30), 35-49. doi: 10.28925/2663-4023.2025.30.941.

[49] Subrahmanyam, S. (2025). Behavioral analysis for threat detection. In P. Bhambri & A.J. Anand (Eds.), *Handbook of AI-driven threat detection and prevention: A holistic approach to security* (pp. 95-115). Boca Raton: CRC Press. doi: 10.1201/9781003521020.

[50] Suprun, O., & Karpenko, N. (2025). Information security in the context of user behavior analysis. In *International scientific-practical conference "Problems of computer sciences, software modeling and security of digital systems"* (pp. 104-107). Lutsk: Lesya Ukrainka Volyn National University.

[51] Thelwall, M. (2025). Research quality evaluation by AI in the era of large language models: Advantages, disadvantages, and systemic effects – an opinion paper. *Scientometrics*, 130(10), 5309-5321. doi: 10.1007/s11192-025-05361-8.

[52] Trivedi, A., Gupta, R., & Jangal, K. (2025). Research paper on cybersecurity and insider threat detection: The role of user behavior analytics (UBA) in modern defense strategies. *International Journal for Research in Applied Science & Engineering Technology,* 13(1), 455-466. doi: 10.22214/ijraset.2025.66298.

[53] Vieira, L.D.S.L. (2025). *Development of a web application for real-time inference in AI models for autonomous driving*. (Master thesis, University of Porto, Porto, Portugal).

[54] Wairagade, A., & Ranjan, S. (2025). User behavior analysis for cyber threat detection: A comparative study of machine learning algorithms. In *2025 13th international symposium on digital forensics and security* (pp. 1-6). Boston: IEEE. doi: 10.1109/ISDFS65363.2025.11011949.

[55] Wang, F., Zhu, G., Yuan, C., & Huang, Y. (2024). LLM-enhanced cascaded multi-level learning on temporal heterogeneous graphs. In *Proceedings of the 47th international ACM SIGIR conference on research and development in information retrieval* (pp. 512-521). New York: ACM. doi: 10.1145/3626772.3657731.

[56] Xu, H., Wang, S., Li, N., Wang, K., Zhao, Y., Chen, K., Yu, T., Liu, Y., & Wang, H. (2025). Large language models for cyber security: A systematic literature review. *ACM Transactions on Software Engineering and Methodology*. doi: 10.1145/3769676.

[57] Zhang, M., Shen, X., Cao, J., Cui, Z., & Jiang, S. (2025). Edgeshard: Efficient LLM inference via collaborative edge computing. *IEEE Internet of Things Journal,* 12(10), 13119-13131. doi: 10.1109/JIOT.2024.3524255.

Алгоритми та програмна архітектура автоматизованого аналізу поведінки користувачів у системах виявлення кіберзагроз

Денис Ковальчук
Аспірант
Міжнародний університет
65009, дор. Фонтанська, 33, м. Одеса, Україна
https://orcid.org/0009-0003-2302-8698

Анотація. Актуальність представленої роботи зумовлена зростаючою складністю кіберзагроз і обмеженою ефективністю традиційних методів їх виявлення, що потребує впровадження інтелектуальних поведінкових підходів із використанням сучасних алгоритмічних і мовних моделей. Метою цього дослідження було узагальнення та концептуальне переосмислення підходів до автоматизованого аналізу поведінки користувачів у системах виявлення кіберзагроз з позицій алгоритмічних рішень і архітектурних принципів їх побудови. У результаті дослідження, виконаного з використанням теоретичного аналізу, системного підходу та порівняльно-аналітичного методу, встановлено, що поведінковий аналіз користувачів є ефективним інструментом виявлення кіберзагроз, здатним доповнювати та перевершувати класичні сигнатурні методи за рахунок ідентифікації контекстно-залежних аномалій і багатокрокових атак. Порівняльний аналіз підходів аналізу поведінки користувачів і об'єктів системи продемонстрував перехід від фокусування на індивідуальних діях до комплексного аналізу взаємодій між користувачами та технічними компонентами, що підвищує точність виявлення загроз і зменшує кількість хибнопозитивних сповіщень. Системний аналіз архітектур сучасних платформ кіберзахисту показав, що інтеграція великих мовних моделей забезпечує уніфіковану обробку структурованих, напівструктурованих і неструктурованих даних, моделювання довготривалих міжподієвих залежностей та формування контекстуальних поведінкових моделей у режимі реального часу. Концептуальне узагальнення й аналітична оцінка підтвердили, що поєднання поведінкового аналізу з великими мовними моделями створює адаптивні, масштабовані та ризик-орієнтовані системи кіберзахисту, здатні забезпечувати раннє виявлення й проактивне реагування на сучасні кіберзагрози за умови дотримання вимог пояснюваності, безпеки та нормативної відповідності. Отримані результати можуть бути корисними для розроблення та впровадження інтелектуальних систем кіберзахисту в центрах управління та моніторингу інформаційної безпеки, системах управління інформацією та подіями безпеки, платформах оркестрації, автоматизації та реагування на інциденти

Ключові слова: User and Entity Behaviour Analytics; великі мовні моделі; штучний інтелект; машинне навчання; data-driven підхід