Journal of Engineering and Applied Research (JEAR)

National University of Skills

Summer & Autumn 2024, Vol. 1, No. 2, p. 115-134

Journal Homepage: https://jear.tvu.ac.ir/

:10.48301/JEAR.2024.472780.1036

Process Mining for Situation Awareness: A Review of Current Practices and Future Prospects

Motahareh Dehghan[1*], Neda Shakib[2]

[1]Assistant Professor, Department of Industrial and Systems Engineering, Tarbiat Modares University, Tehran, Iran.

[2]MSc Student, Department of Industrial and Systems Engineering, Tarbiat Modares University, Tehran, Iran.

ARTICLE INFO

Article Type:
Original Research

Received: 08.13.2024
Revised: 09.01.2024
Accepted: 09.03.2024

Keyword:
Situation Awareness
Process Mining
Cyber Situation Awareness
Context Awareness
Discover
Conformance Checking
Enhancement

***Corresponding Author:**
Motahareh Dehghan
Email:
m_dehghan@modares.ac.ir

ABSTRACT

In the rapidly evolving landscape of modern organizations, maintaining robust situation awareness is crucial for agility, informed decision-making, and sustained competitive advantage. Traditional approaches often rely on documented processes, which, while useful, may fail to capture the dynamic and complex nature of actual workflows. Enter process mining—a powerful analytical tool that delves into real-time data, uncovering the true flow of tasks, identifying bottlenecks, and predicting future process behaviors. By transforming raw data into actionable insights, process mining offers an unparalleled level of transparency, enabling organizations to anticipate disruptions, optimize resource allocation, and enhance operational efficiency. This review explores the intersection of situation awareness and process mining, providing a comprehensive analysis of how these methodologies converge to offer a clearer understanding of organizational processes. The present research begins by examining the theoretical foundations of situation awareness and process mining. Then, it reviews existing research on the application of process mining in enhancing situation awareness, highlighting key advancements, use cases, and the transformative impact on decision-making processes. Despite its numerous benefits, the integration of process mining into situation awareness is not without challenges. This review identifies several open issues, including data quality concerns, the complexity of real-world processes, and the need for more sophisticated analytical techniques. To address these gaps, the authors recommend that future research should be directed toward the context of cyber situation awareness. By advancing the state of the art in process mining, this research aimed to pave the way for more resilient, adaptable, and aware organizations in the digital age.

E-ISSN: 3060-6357

Introduction

In today's fast-paced and complex business environment, organizations must possess a high level of situation awareness to maintain agility and make informed decisions. Situation awareness—the ability to perceive, comprehend, and project the current and future states of a process—plays a critical role in ensuring that organizations can respond swiftly and effectively to dynamic changes, disruptions, and opportunities. This heightened awareness enables decision-makers to navigate complexities, anticipate challenges, and optimize performance across various operational domains.

Traditionally, organizations have relied heavily on documented processes to guide their operations. These documents, while valuable, often present a static and sometimes outdated view of workflows. As a result, they may not fully capture the nuances, inefficiencies, and real-time dynamics that occur within the actual processes. This gap between documented processes and the reality of operations can lead to missed opportunities, unrecognized bottlenecks, and delayed responses to critical issues. The need for real-time insights into organizational processes has become increasingly evident as businesses strive to remain competitive in a rapidly changing world.

In the Endsley model, situation awareness is defined as the perception of elements in the environment within a specific time and space, the comprehension of their meaning, and the projection of their status into the near future [1]. Perception of Situation Awareness involves the sensory recognition of critical information regarding the system in operation and the environment in which it functions. Comprehension of Situation Awareness involves forming a comprehensive picture of the system to achieve a more integrated and complete understanding of what is happening. Projection, the highest level of situation awareness, involves predicting future states based on current information to see how they might affect the future state of the operational environment. This projection combines what one knows about the current situation with their mental model of the system to anticipate what is likely to happen next [2].

Cyber network attacks are often complex and might involve internal or external attackers operating at varying levels of sophistication. With the gradual increase and complexity of cyber threats, new solutions are needed to provide the information and processing required to support critical missions during cyber warfare. Before cyber operators can defend against these attacks, recover operations, or even retaliate, they must first gain and maintain a level of situation awareness that allows them to perceive, comprehend, and project evolving threats [2].

It is crucial to note that the proposed levels of situation awareness represent heightened levels of awareness rather than linear stages. A person who comprehends and understands the meaning of the current situation will have a higher level of situation awareness than someone who merely reads the data without grasping its significance. Similarly, someone capable of predicting future events and possible conditions will have a better understanding of the situation than someone who lacks this ability [3].

To counter the increasing security threats in large-scale networks, various types of security devices are employed. These devices generate numerous security events, which are stored as event logs. Process mining can significantly enhance situation awareness in cybersecurity by using event logs to discover patterns, identify anomalies, and optimize processes. The idea behind process mining is to discover, monitor, and improve actual processes by extracting knowledge from event logs that are readily available in today's systems [4]. By analyzing event logs, visual process models are produced that illustrate how processes operate, helping stakeholders understand process flows, identify inefficiencies, and make informed decisions. This enhancement of situation awareness through process analysis aids in identifying potential security risks and vulnerabilities, thereby strengthening security infrastructures [5].

This review paper aims to explore how process mining can serve as a powerful tool for enhancing situation awareness within organizations. Process mining is a data-driven technique that delves into actual event logs and other digital footprints to uncover the true flow of activities, identify inefficiencies, and predict future behaviors. By providing a transparent and accurate view of business processes, process mining enables organizations to bridge the gap between documented procedures and real-world operations.

The scope of this review includes an examination of the theoretical foundations of situation awareness and process mining, a comprehensive analysis of existing research on their intersection, and a discussion of the challenges and open issues that persist in this area. Furthermore, the paper will propose future research directions, particularly focusing on how process mining techniques can be further developed and applied to enhance cyber situation awareness. Through this exploration, the paper seeks to contribute to the growing body of knowledge on how organizations can better understand, monitor, and improve their processes in real-time, leading to more informed decision-making and greater overall efficiency.

Theoretical foundations

In this section, situation awareness and process mining are considered the theoretical foundations for this study.

Situation awareness

Situation awareness is a cognitive process that can perceive and comprehend the current situation and project the near future. Then, based on the obtained awareness, a plan, decision, and act can be performed [6]. There are different definitions for situation awareness. One of the most famous of which was provided by Mica Endsley [7]: " Situational awareness or situation awareness (SA) is the perception of environmental elements and events with respect to time or space, the comprehension of their meaning, and the projection of their future status." This definition subtly distinguishes between three levels of situation awareness, i.e., perception (including observation), comprehension, and projection (including prediction). Its lowest level is observation and perception, and the highest level is projection of the near future, i.e., the projection of the current situation into the future to predict the evolution of the tactical situation. The highest level in Endsley's situation awareness model is called projection when the status of elements in the environment in the near future is predicted [6].

Figure 1 illustrates the role of situational awareness (SA) in the decision-making process. According to the model, an individual's perception of relevant environmental elements—derived from system representations or direct sensations—forms the basis of their SA. Action selection and execution emerge as distinct phases from SA. Several factors influence this process, starting with individual variations in the ability to achieve SA from the same data input, which depends on information processing mechanisms, innate abilities, experience, and training. Additionally, biases and goals can shape how individuals filter and interpret their environment. The system design also impacts SA by determining how effectively it provides necessary information and its alignment with human information processing capabilities. Furthermore, characteristics of the work environment, such as workload, stress, and complexity, might affect SA. The influence of these individual and system factors on SA has been discussed [8].

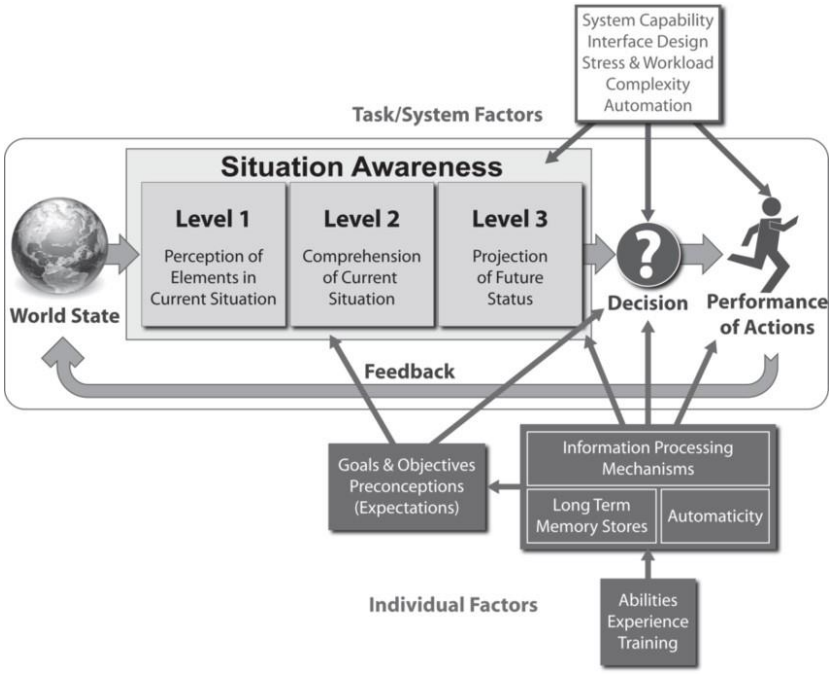

Figure 1. Model of situation awareness in dynamic decision-making [8].

Process Mining

Process mining is an analytical technique used to extract valuable insights from event logs produced by information systems. It provides a method to visualize, analyze, and improve business processes by using actual process data rather than relying solely on theoretical models or assumptions. Process mining plays a vital role in bridging the gap between theoretical process models and their practical execution. By examining the real data captured in event logs, process mining helps organizations understand how processes are performed, uncover hidden inefficiencies, and ensure alignment with business objectives [9].

Process mining is a relatively new research field that sits at the intersection of machine learning and data mining on one side and process modeling and analysis on the other. The concept of process mining involves discovering, monitoring, and improving actual processes (as opposed to hypothetical ones) by extracting knowledge from event logs that are readily available in modern systems. Figure 2 illustrates how process mining connects actual processes and their data with process models. Modern information systems record a vast number of events and provide detailed information of the activities that have been executed. Figure 2 refers to such data as event logs [4].

However, most information systems store this information in an unstructured format. For example, event data may be scattered across numerous tables or need to be collected from subsystems through message exchanges. In such cases, while event data exists, efforts are required to extract it. Data extraction is an integral part of any process mining activity [4].

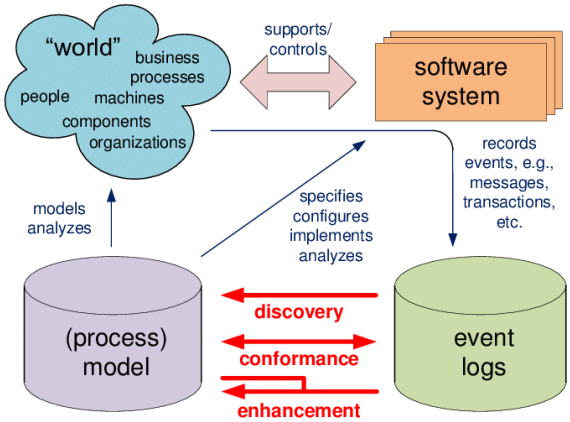

Figure 2. Positioning of the three main types of process mining: (a) discovery, (b) conformance checking, and (c) enhancement [4].

Process mining can provide insights into what truly happens within a process and offers a wide range of opportunities, from process discovery to advanced predictive algorithms that can be applied during process execution. Process discovery is particularly valuable when no process model exists or when an existing model is outdated or incomplete. Event data present in IT systems is used to create a bottom-up process model, ensuring that the generated model is based on activities that occurred and in the order they happened. If a process model already exists, events can be replayed against the data to verify whether the process model accurately represents the process. If the process model is validated, events can be replayed to check if any activities violated the process rules [10].

The applications of process mining are not limited to analyzing or creating a process model. With the right data, process mining can provide insights into the performance and relationships of resources within a process. The way people collaborate to complete a complex task can be visualized. In a semi-automated process, machines work alongside humans. Process mining can help generate performance statistics that are not restricted to a specific task. With simple business management tools, it is easy to identify who in a process can complete a particular task faster. This can be done very effectively with process mining, but

beyond that, it also enables the comparison of the performance of different process instances in which resources have participated [11]. Event logs can be used for three types of process mining: discovery, conformance, and enhancement, as shown in Figure 2 [4].

Application of process mining in situation awareness

In 2011, a study focused on the recognition of contextual states in pervasive environments to enhance situation awareness. This research emphasized the importance of tracking and identifying states to help pervasive systems concentrate on the essential information needed for a better understanding of the user's context. The critical aspect of identifying contextual states in pervasive environments to improve situation awareness has been widely explored. Pervasive computing environments, characterized by the widespread presence of sensors and smart devices, generate a large volume of data that requires effective interpretation to derive meaningful insights. In such environments, situation awareness depends on the system's ability to accurately understand and interpret the context. The conceptual architecture for situation-aware systems consists of five layers: sensing, fact extraction, reasoning, filtering, and situation recognition. Each layer plays a specific role in collecting raw data from sensors, extracting relevant facts, applying reasoning schemes, filtering information, and ultimately recognizing the overall situation. To create situation-aware systems in line with this conceptual architecture, the developer can intuitively break down the relevant situation into different states. Then, they can define the situation by imposing various constraints on a subset of these states [12].

The proposed model integrates various data from sensors and devices to create a comprehensive and dynamic understanding of the environment. The emphasis is on the importance of data fusion methods and machine learning algorithms for processing and analyzing contextual data. By identifying patterns and anomalies, the system can recognize different contextual states and respond appropriately to environmental changes. In the next section, data from the situation report generated by the reasoning layer is used to examine the application of process mining methods in a situation-aware system. In this system, the collected report data is compared and analyzed using conformance analysis. In process mining, the process model is derived from process instances, meaning the information obtained from the reasoning layer is cleansed and adjusted as needed; then, the model is extracted using process mining. For these activities, the ProM tool is utilized, and using heuristic algorithms, a process model is obtained for each instance. These models are then aggregated to create an overall model, which is evaluated for alignment with the actual situation

through conformance checking. Situation reports, which describe various activities performed by a resident over several days, are used to extract their daily processes and identify an interesting situation. Then, based on a set of labeled situation samples, the accuracy of identifying the interesting situation is measured by assessing the alignment between its model and the corresponding actual situations. The results show an accuracy of 91.30% for a threshold of 0.75.

This framework is particularly applicable in domains such as smart homes, healthcare, and industrial automation. For instance, in a smart home environment, the system can monitor residents' daily activities and detect unusual patterns that might indicate potential issues, such as health problems or security breaches. In the healthcare domain, the system can track patients' activities and conditions, providing timely alerts and interventions. Integrating context-aware computing with situation awareness enhances the system's ability to deliver timely and relevant responses to various situations, significantly improving performance and safety in these domains [12].

In 2012, a study was conducted to evaluate situation awareness in nuclear power plants by developing a method for measuring team situation awareness. The study emphasizes the critical role of team situation awareness in the safe and efficient operation of nuclear power plants, noting that understanding team situation awareness can provide valuable insights into team performance and cognitive processes. The proposed method focuses on establishing logical connections between team communication and team situation awareness, utilizing a speech act coding scheme to analyze these interactions. This method allows for the measurement of team situation awareness at various levels and provides a precise understanding of how team members perceive, comprehend, and anticipate future situations [13].

Additionally, the Global Situation Awareness Evaluation method is introduced as a robust approach for assessing team situation awareness in nuclear power plants. This method involves the random interruption of simulations to question the crew about their understanding of the current situation, thereby providing an objective measure of their situation awareness. The method is adaptable to various domains and offers valuable insights into both individual and team situation awareness, making it a critical tool for improving operational performance and safety in dynamic and complex environments like nuclear power plants. Based on the review of situation awareness measurement methods, several considerations should be taken into account when measuring team situation awareness. First, continuity should be considered. The method of measuring team situation awareness should not disrupt the primary task of a participant, as such interruptions could interfere with the measurement of

situation awareness. Second, objectivity is important. The measurement of situation awareness should not rely on a participant's memory. Third, sensitivity should be prioritized, as one of the reasons for focusing on situation awareness is its practical application in improving interface design. The method used must accurately detect changes in team situation awareness caused by different types of technology. Fourth, reliability must be ensured. The results of a method should be dependable. The findings of this study indicate that teams with higher levels of situation awareness also performed better, although the analysis did not reveal any significant correlation between different levels of situation awareness and team performance [13].

In 2016, a study examined the integration of process mining methods with the analysis of communication logs from the main control room crew in nuclear power plants to identify work processes and assess their quality. By extracting workflows, temporal and spatial information, and the flow of words that describe the crew's signals and knowledge, the research demonstrates that process mining methods are effective in identifying the essential information needed to evaluate work process quality. This approach reveals the sequence of actions performed by the crew and the spatial and temporal aspects of their workflows, providing them with a deeper understanding of decision-making processes after visualizing these workflows [14].

In this study, communication logs collected from a training scenario are analyzed to demonstrate the application of process mining methods in describing the work processes of the crew in a nuclear power plant. The process mining algorithm used to illustrate the workflows is an extension of the heuristic algorithm implemented by the Disco process mining tool. This algorithm calculates dependency metrics between two nodes from the footprint matrix and then draws a filtered directed graph based on a correct threshold. The use of process mining methods in addition to the analysis of communication logs provides a structured approach to understanding how the crew responds to simulated abnormal conditions, and it is noted that crew situation awareness can be accurately estimated through the analysis of communication logs. The information extracted from these logs not only helps improve the visualization of workflows but also contributes to a deeper understanding of the meaning behind crew members' responses to the current situation, ultimately leading to enhanced performance and decision-making abilities in complex and dynamic operational environments such as nuclear power plants.

In the field of situation awareness, combining process mining methods with communication log analysis offers an effective path for improving the crew’s cognitive processes. By providing structured insights into their workflows, this

integrated approach can help enhance the overall situation awareness of the crew, leading to more effective performance in complex and dynamic operational environments [14].

In 2016, a study aimed at developing an objective method for measuring team situation awareness was conducted. Situation awareness is typically measured by the degree of alignment between what is actually happening in a situation and the operator's understanding and perception of that situation. However, various studies have focused primarily on the situation awareness of individual operators. Yet, many complex systems are managed by teams. Complex systems usually require more than one operator, thus necessitating team situation awareness. The concept of team situation awareness is considered to be an integration of individual situation awareness, as the conceptualization of team situation awareness is derived from theories of individual situation awareness and team situation awareness is viewed as an intersection or overlap between the shared individual situation awareness [15].

The method used in the study is developed by establishing logical connections between team communication and team situation awareness. Additionally, a speech act coding scheme is implemented to analyze team communications. The concept of team situation awareness in this method is primarily based on the concept introduced by Endsley. It proposes a logical connection between team communications and team situation awareness by using an extended decision ladder model to identify the decision-making process. A decision ladder explains the steps of information processing and includes boxes corresponding to information processing activities and circles that match knowledge states. This method adopts insights from this model, meaning that information processing activities, considered as cognitive activities, can be observed from team communications. Consequently, the following cognitive activities are selected from the decision ladder model: activation, observation, identification, prediction, evaluation of options, definition, formulation, and execution. The method then uses a mapping process between the selected cognitive activities and each level of team situation awareness. After extracting the cognitive activities required for each level of team situation awareness, a speech act coding scheme is implemented to summarize and interpret process-tracking data, capture significant content in the data, and analyze the number and patterns in the transcripts.

To evaluate the feasibility of this method, a study was conducted. First, simulation data from nine operational teams working in a nuclear power plant was collected. A simulation was conducted on a full-scope simulator that included traditional alarms, indicators, trend recorders, and control devices. Additionally,

the loss of intermediate cooling system accident scenario was used. This scenario was designed to be challenging in terms of situation assessment. The objective was to create a situation where operational teams had to identify and isolate a leak in the residual heat removal system without explicit procedural guidance. An operator performance evaluation system was also used for the assessment, which included the results of task analysis and the extraction of ideal activities for the given tasks in the scenario. It was shown that this method has a high correlation between team situation awareness scores and task performance scores. Therefore, the proposed method can reasonably infer team situation awareness [15].

In 2017, a study was conducted that integrated process mining with context awareness. Process mining with context awareness in logistics addresses the complexity and dynamic nature of logistical processes. Traditional methods of documenting logistics processes are often inadequate as they struggle to keep pace with frequent changes and variations. Logistical processes exhibit significant variability and diversity, making standard process mining methods insufficient. To overcome these challenges, the integration of machine learning techniques with process mining was proposed. This involves classifying and categorizing event data based on various contextual factors such as time, location, and specific resources. The fields of logistics and manufacturing are ideal candidates for incorporating context-aware features as industrial activities take place in highly diverse environments where multiple pieces of information accompany the observed process. Environmental data can include the time, location, and frequency of events, relevant communications, tools, and devices [16].

In the proposed method of this study, an existing clustering algorithm is modified to incorporate contextual information about the frequency of process occurrences and consistency in terms of cycle time. Finally, clustering quality metrics are used to assess the improvement in process identification with the addition of contextual information. The proposed method enhances context-aware process mining by improving the accuracy and relevance of process models generated from event logs. Two types of contextual information are extracted from the data. First, the frequency of occurrence for each process is calculated. The basic assumption here is that the more frequently a process occurs, the more likely it is to be a standard process around which various process variations exist. Second, the stability of each process in terms of changes in cycle time is determined, based on the assumption that stable processes are standard processes. By adding contextual information, more accurate process models are provided that reflect the true nature of operations. This integration enables automated process documentation and ensures that documentation

remains up-to-date and accurate. Several case studies in the logistics sector demonstrate that context-aware process mining effectively manages the complexity and diversity of logistical processes, leading to improved process understanding and optimization. The implementation of this method in logistics has shown significant benefits in terms of process efficiency and accuracy, highlighting its potential for broader industrial applications [16].

In 2021, a study was conducted to explore ways to integrate situation awareness into business process management to better understand overly automated business processes. The importance of situation awareness in industrial environments, particularly the need to process and analyze real-time data, was emphasized. In this context, situation awareness involves the ability to collect, monitor, and interpret data simultaneously and act swiftly based on it. A comprehensive framework for situation awareness was designed, specifically tailored for industrial environments, which integrates various data sources and utilizes advanced analytics to provide actionable insights [17].

The proposed method in the study includes an ontology for modeling situations and event-handling mechanisms based on event calculus. The study creates a context for a business process with a focus on rules and entities to support contextual understanding. A system architecture is presented to illustrate the structure of the support system for smart and situation-aware business process management, and real-time event extraction and interpretation mechanisms are developed to understand the dynamics of the context and provide real-time responses. This framework is based on three core principles: real-time monitoring, data integration, and predictive analysis. Real-time monitoring involves the continuous observation of industrial processes to gather up-to-date information about operations. Data integration ensures that information from various sources is consolidated into a cohesive dataset, providing a comprehensive view of the industrial environment. Predictive analysis involves analyzing historical and real-time data to forecast future events and trends. Real-time sensor events and events from other sources are fed into a continuous event stream, and the system continuously queries this stream to detect whether events match a specific pattern. Detailed case studies demonstrate that the proposed framework is applicable in manufacturing and logistics. In manufacturing, this framework aids in monitoring production lines, identifying anomalies, and predicting equipment failures. In logistics, the framework is effective in optimizing supply chain operations by identifying potential bottlenecks and inefficiencies. These studies indicate that the implementation of situation awareness frameworks leads to significant improvements in operational efficiency, reliability, and decision-making. The

model was tested and implemented in a simulation of two mobile phone testing processes, showing significant improvements in process time and cost in the proposed model [17].

In 2022, an operational approach was presented for evaluating patient adherence to medical prescriptions, particularly for managing metabolic syndrome. This study utilizes process mining methods to model the medical prescription as a process model and to assess the rigor with which patients follow the prescribed activities. The objective is to measure their adherence and provide a computational intelligence model for situation awareness in healthcare [18].

The study applies process mining algorithms to analyze real event logs from home-based patients with metabolic syndrome. Three process mining algorithms—Alpha, Inductive, and Heuristic—are compared to identify the most suitable model for evaluating adherence. The evaluation criteria for adherence include fitness (replay accuracy), precision, generalization, and simplicity, all of which are used to assess how well patients adhere to their prescriptions. The real-world data used in this study include behavior logs from patients with metabolic syndrome. The dataset records patient information collected through home monitoring, leveraging IoT and medical devices, and documents various activities such as meals, medication intake, physical exercises, vital sign measurements, and weight tracking. These data were collected from a group of 19 patients under continuous monitoring, all of whom shared common characteristics and were located in the Apulia region of Italy. The data collection process spanned 30 days, capturing all the actions a patient performed throughout their daily routine via a set of medical devices that transferred the sensed data to a module. This module was responsible for gathering and formatting the data into an event log that aligns with process mining methodologies.

The fitness (replay accuracy) of the process mining models was over 79% across all algorithms, indicating that most patients followed the modeled behavior accurately. The precision measure showed significant variation, with the Alpha and Inductive algorithms exhibiting contrasting behaviors. The generalization metric, which aims to maximize the supported behaviors outside of the system that is not present in the event log, was low—an encouraging sign, as it indicates that patients adhered closely to the prescribed activities. The simplicity index for all the algorithms applied to the medical prescription event log indicated that the processed models were relatively straightforward. This research highlights the importance of situation awareness in healthcare, where AI-driven solutions can enhance awareness and help measure and predict the impact of patient behavior. By modeling the medical prescription as a process

model, the study demonstrates how conformance-checking methods can be used to assess patient adherence to treatment. The evaluation metrics provide insights into the level of adherence and offer information on the performance of process mining algorithms in accurately representing patient behaviors [18]. Table 1 demonstrates the summary of previous studies in the area of process mining and situation awareness.

Table 1. Summary of previous studies in the area of Process Mining with a Focus on Situation Awareness.

Reference	Main research concept	Key points, innovations, and contributions
Jaroucheh et al. [12]	Contextual situation detection in pervasive environments to enhance situation awareness	– Detection of contextual situation in pervasive environments to enhance situation awareness – Integration of diverse data from sensors and devices to create a comprehensive and dynamic understanding of the environment – Appropriate system response to environmental changes after detecting patterns and anomalies using contextual information Conformance result with an accuracy of 91.30% for a threshold of 0.75
Lee et al. [13]	Proposal of a method for measuring team situation awareness and its requirements	– Introduction of several indicators for team situation awareness: continuity, objectivity, sensitivity, and reliability Simulated environment for assessing team situation awareness of crew members – Positive impact of good team situation awareness on team performance
Park et al. [14]	Integration of process mining methods with analysis of communication reports from crew in nuclear power plants	– Analysis of communication reports collected during simulated abnormal conditions, describing work processes and enhancing human reliability analysis – Identification of key informational requirements for assessing work process quality – Use of process mining methods to extract valuable insights from communication data
Lee et al. [15]	Development of a method for measuring team situation awareness in nuclear power plants	– Development of a method for measuring team situation awareness – Analysis of team communications using a speech act coding scheme to measure each level of situation awareness

Reference	Main research concept	Key points, innovations, and contributions
		– Simulated environment for assessing team situation awareness of crew members
Becker and Intoyoad [16]	Integration of process mining and contextual awareness in logistics	– Integration of machine learning methods with process mining – Enhancement of process mining with contextual awareness to improve accuracy – Possibility of automatic process documentation using contextual information
Zhao et al. [17]	Integration of situation awareness in business process management	– Use of ontology to create a contextual modeling approach – Development of event-handling mechanisms based on event logs – Evaluation of the proposed method by analyzing cost savings from simulating several large business processes
Lofu et al. [18]	Analysis of event reports from home-based patients with metabolic syndrome	– Use of process mining to analyze event reports from patients with metabolic syndrome – Concurrent use of three process mining algorithms: Alpha, Heuristic, and Inductive to find the most suitable algorithm – Identification of four metrics: replay fitness, precision, generalization, and simplicity for evaluating algorithm conformance

Discussion

In this section, the challenges and open issues in the area of application of process mining in situation awareness are expounded on.

While process mining excels in analyzing structured and repeatable processes, its application to highly dynamic and non-linear workflows, often found in complex organizations, can be challenging. The variability in these processes can lead to incomplete or misleading models, thus impacting situation awareness. Although process mining provides valuable insights, real-time analysis at scale can be resource-intensive and may not always be feasible. This limits its applicability in environments where instantaneous situation awareness is crucial, such as in emergency response or cybersecurity.

Process mining primarily focuses on process flow and timing, but it cannot often fully capture and analyze contextual information, such as human decision-

making factors or external environmental variables, which are critical for comprehensive situation awareness.

The effectiveness of process mining is heavily dependent on the quality of the data being analyzed. Inaccurate, incomplete, or inconsistent data can lead to flawed insights, undermining the reliability of situation awareness. Issues such as event log completeness, timestamp accuracy, and data granularity are significant concerns.

Real-world business processes are often complex, involving numerous stakeholders, systems, and interactions. Capturing and analyzing such complexity requires sophisticated modeling techniques, which may not be fully supported by current process mining tools. This can result in oversimplified models that fail to capture critical aspects of the workflow.

Seamlessly integrating process mining tools with an organization's existing IT infrastructure can be a significant challenge. Compatibility issues and the need for custom solutions can hinder the deployment of process mining, limiting its impact on situation awareness.

Future research directions

Investigating how process mining can be leveraged to analyze cybersecurity event logs for real-time detection of threats, such as identifying anomalous patterns in network traffic or user behavior that may indicate a cyber attack. Research into the application of process mining to streamline and enhance incident response processes enables organizations to react more swiftly and effectively to cybersecurity threats, thereby improving overall cyber situation awareness. Exploring how process mining can be used to predict potential cyber threats by analyzing historical data and identifying trends or patterns that precede cyber incidents could lead to more proactive cybersecurity strategies.

Developing techniques that can be scaled to deal with the large volumes of data typical in cybersecurity environments while providing real-time insights, ensures that organizations can maintain a high level of situation awareness. Researching how process mining can be integrated with existing cybersecurity tools such as SIEM (Security Information and Event Management) systems enhances the granularity and accuracy of cyber situation awareness. Investigating the potential for process mining to support automated response systems that can detect and mitigate cyber threats without human intervention reduces response times and minimizes damage.

Exploring how AI and machine learning can be integrated with process mining to improve the accuracy of process models enables more sophisticated pattern recognition and enhances predictive capabilities. Research into the application of

cognitive computing technologies to process mining, enabling tools that can understand and adapt to complex, human-centered processes, provides deeper insights into organizational dynamics and improves situation awareness. Advancements in AI could lead to more automated and intelligent process discovery techniques, reducing the need for manual intervention and improving the efficiency of process mining in complex environments.

Researching the combination of process mining with simulation techniques to create more accurate and dynamic models of organizational processes enables better scenario analysis and decision-making. Investigating hybrid approaches that integrate process mining with other forms of analytics, such as predictive analytics, descriptive statistics, and network analysis, provides a more comprehensive view of organizational processes and enhances situation awareness. Exploring the application of process mining in conjunction with domain-specific analytical methods, such as those used in healthcare, manufacturing, or finance creates tailored solutions that address the unique challenges of these industries.

Conclusion

The combination of process mining with situation awareness methods offers a robust framework for improving the understanding and management of complex systems. The reviewed studies demonstrate the potential benefits of this combination across various fields including logistics, pervasive environments, and nuclear power plants. By integrating contextual information and developing advanced measurement techniques, these approaches enhance the accuracy and relevance of process models and situation assessments, thereby supporting better decision-making and performance, particularly in dynamic and high-risk environments. The application of these integrated methods can lead to significant improvements in efficiency and safety. For instance, in logistics, context-aware process mining can optimize supply chain processes and identify and rectify inefficiencies. In pervasive environments, real-time contextual awareness enhances system responsiveness and adaptation to changing conditions. In nuclear power plants, improved situational awareness through insights into cognitive processes and team dynamics supports safer and more effective team operations. Only one reviewed study used process mining directly to improve situational awareness, while others generally used situational awareness to enhance processes; no studies with this aim have been conducted in the cybersecurity domain.

The results of studies indicate that the combination of process mining and situational awareness can significantly improve the management of complex

systems. Future research could explore process mining methods within situational awareness and evaluate their effectiveness in enhancing the understanding and management of complex systems in the cybersecurity domain. By analyzing system event reports, it becomes possible to identify behavioral patterns, detect anomalies, and predict future behaviors. This information could help cybersecurity managers make better decisions, reduce risks, and improve responses to security threats. Additionally, process mining can be used to uncover dependency relationships between various organizational components such as infrastructure, threats, vulnerabilities, and organizational missions. By analyzing data related to security threats, system vulnerabilities, and organizational missions, relationships among these elements can be identified. This information could help organizations adjust their security strategies based on a better understanding of how these factors interact. For instance, if a particular vulnerability is associated with an increase in cyber attacks, the organization could focus on strengthening defenses against that vulnerability. Future research could also examine the impact of using process mining to improve situational awareness in addressing security challenges and bottlenecks. By using data collected from security systems, process mining could identify typical and anomalous behavioral patterns and propose measures to enhance security. This capability allows organizations to effectively address security threats and prevent security incidents.

Disclosure statement and funding

The authors declare no potential conflicts of interest. The present study received no financial support from any organization or institution.

Acknowledgment

We would like to give special thanks to all the participants in this study.

References

[1] Endsley, M. R. (1988). Design and Evaluation for Situation Awareness Enhancement. *Proceedings of the Human Factors Society Annual Meeting*, *32*(2), 97-101. https://doi.org/10.1177/154193128803200221

[2] Kott, A., Wang, C., & Erbacher, R. F. (2014). *Cyber defense and situational awareness*. Springer. https://doi.org/10.1007/978-3-319-11391-3

[3] Jiang, L., Jayatilaka, A., Nasim, M., Grobler, M., Zahedi, M., & Babar, M. A. (2022). Systematic Literature Review on Cyber Situational Awareness Visualizations. *Institute of Electrical and Electronics Engineers Access*, *10*, 57525-57554. https://doi.org/10.1109/ACCESS.2022.3178195

[4] Chapela-Campa, D., & Dumas, M. (2023). From process mining to augmented process execution. *Software and Systems Modeling*, *22*(6), 1977-1986. https://doi.org/10.1007/s10270-023-01132-2

[5] Tianfield, H. (2016, December 15-18). *Cyber Security Situational Awareness [Conference session].* 2016 IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data, Chengdu, China. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.165

[6] Dehghan, M., Sadeghiyan, B., Khosravian, E., Moghaddam, A. S., & Nooshi, F. (2022). Proapt: Projection of apt threats with deep reinforcement learning. *arXiv*, 1-16. https://doi.org/10.48550/arXiv.2209.07215

[7] Endsley, M. R. (1996). Automation and situation awareness. In R. Parasuraman & M. Mouloua (Eds.), *Automation and human performance: Theory and Applications* (pp. 163-181). Chemical Rubber Company Press. https://www.taylorfrancis.com/chapters/edit/10.1201/9781315137957-8/automation-situation-awareness-mica-endsley

[8] Endsley, M. R., & Jones, D. G. (2024). Situation Awareness Oriented Design: Review and Future Directions. *International Journal of Human–Computer Interaction*, *40*(7), 1487-1504. https://doi.org/10.1080/10447318.2024.2318884

[9] Milani, F., Lashkevich, K., Maggi, F. M., & Di Francescomarino, C. (2022). Process Mining: A Guide for Practitioners. In R. Guizzardi, J. Ralyté, & X. Franch (Eds.), *Research Challenges in Information Science* (pp. 265-282). Springer International Publishing. https://doi.org/10.1007/978-3-031-05760-1_16

[10] Karwehl, D. (2018). *Use case based introduction to process mining and current tools* [Bachelor, Haw-Hamburg]. Hamburg, Germany. https://reposit.haw-hamburg.de/handle/20.500.12738/8424

[11] Van Der Aalst, W. M. P. (2023). Object-Centric Process Mining: Unraveling the Fabric of Real Processes. *Mathematics*, *11*(12), 2691. https://doi.org/10.3390/math11122691

[12] Jaroucheh, Z., Liu, X., & Smith, S. (2011). Recognize contextual situation in pervasive environments using process mining techniques. *Journal of Ambient Intelligence and Humanized Computing*, *2*(1), 53-69. https://doi.org/10.1007/s12652-010-0038-7

[13] Lee, S. W., Park, J., Kim, A. R., & Seong, P. H. (2012). Measuring situation awareness of operation teams in NPPs using a verbal protocol analysis. *Annals of Nuclear Energy*, *43*(1), 167-175. https://doi.org/10.1016/j.anucene.2011.12.005

[14] Park, J., Jung, J-Y., & Jung, W. (2016). The use of a process mining technique to characterize the work process of main control room crews: A feasibility study. *Reliability Engineering & System Safety*, *154*, 31-41. https://doi.org/10.1016/j.ress.2016.05.004

[15] Lee, S. W., Kim, A. R., Park, J., Kang, H. G., & Seong, P. H. (2016). Measuring Situation Awareness of Operating Team in Different Main Control Room Environments of Nuclear Power Plants. *Nuclear Engineering and Technology*, *48*(1), 153-163. https://doi.org/10.1016/j.net.2015.09.008

[16] Becker, T., & Intoyoad, W. (2017). Context Aware Process Mining in Logistics. *Procedia CIRP*, *63*(2), 557-562. https://doi.org/10.1016/j.procir.2017.03.149

[17] Zhao, X., Yongchareon, S., & Cho, N-W. (2021). Enabling situational awareness of business processes. *Business Process Management Journal*, *27*(3), 779-795. https://doi.org/10.1108/BPMJ-07-2020-0331

[18] Lofù, D., Pazienza, A., Ardito, C., Noia, T. D., Sciascio, E. D., & Vitulano, F. (2022, June 6-10). *A Situation Awareness Computational Intelligent Model for Metabolic Syndrome Management* [Conference session]. 2022 Institute of Electrical and Electronics Engineers Conference on Cognitive and Computational Aspects of Situation Management, Salerno, Italy. https://doi.org/10.1109/CogSIMA54611.2022.9830673