World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Real-time incident reporting and intelligence framework: Data architecture strategies for secure and compliant decision support

Shamnad Mohamed Shaffi [1,*] and Jezeena Nikarthil Sidhick [2]

[1] *Amazon Web Services, Seattle, Washington, United States.*
[2] *Egencia, Bellevue, Washington, United States.*

World Journal of Advanced Research and Reviews, 2025, 26(03), 110–118

Publication history: Received on 23 April 2025; revised on 30 May 2025; accepted on 02 June 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.3.2160

Abstract

The growing complexity and frequency of incidents across many fields, particularly cybersecurity, healthcare, critical infrastructure, and emergency response, highlight the pressing need for automated, intelligent, and effective frameworks for incident reporting. Traditional manual methods often face constraints regarding latency, vulnerability to errors, and lack of analytical insights that are vital to supporting timely decision-making. This research explores the conceptual model and implementation of an Automated Incident Reporting and Intelligence Framework that enhances the speed, accuracy, and strategic value of incident management processes. The system proposed in this research leverages cutting-edge technologies like machine learning, natural language processing, decision support systems, real-time analytics, and Artificial Intelligence to support the detection, classification, and reporting of incidents. It also includes predictive intelligence and contextual analysis to develop actionable insights to aid stakeholders in prioritization of interventions and prevention of future incidents. The system architecture presented in this paper emphasizes scalability, interoperability, and modularity to cater to a diversity of organizational types while ensuring protection, confidentiality, and compliance with local and international regulations and standards. By integrating literature, technological innovations, and empirical case studies, this paper outlines fundamental design principles, deployment strategies, and assessment metrics essential to the effectiveness of an automated incident reporting system.

Keywords: Automated Incident Reporting; Incident Management; Intelligence Framework; Artificial Intelligence; Real-Time Data Analytics; Predictive Intelligence; Decision Support Systems; Cybersecurity Automation

1. Introduction

In today's fast-changing operational environments involving cybersecurity, emergency management, industry safety, and healthcare, incident reporting is a core element enabling swift responses, ensuring accountability, and consistent improvement. Incident reporting systems are designed as systematic mechanisms that collect, document, and analyze events that can potentially impair operations, pose risks, or identify vulnerabilities. Traditionally, the systems were manual in nature, requiring extensive human effort for identification, documentation, and escalation of events. However, conventional manual reporting systems are often plagued by the issues of sluggish responses, inconsistent or partial information, and inaccuracies on the part of the users, all of which compound comprehensive analysis and speedy resolution.

Over the past two decades, advances in technology have enabled a significant shift from manual reporting processes to automated reporting systems. The integration of real-time data feeds, electronic logging devices, Internet of Things (IoT) sensors, and smart user interfaces has improved the ability of modern systems to automatically detect, classify, and report incidents [10]. However, exclusive dependence on automation is not sufficient. The integration of advanced

* Corresponding author: Shamnad Mohamed Shaffi

technologies—such as artificial intelligence (AI), machine learning (ML), and natural language processing (NLP)—has spurred a transition from reactive incident reporting to a proactive and predictive approach in incident management. Intelligent systems can analyze large datasets, both structured and unstructured, detect patterns, assess risk factors, and suggest optimal response methods in real-time. Despite these developments, many organizations still do not have a comprehensive system that properly aligns automated reporting capabilities with intelligence-led insight. This lack of proper integration causes opportunities for early interventions to be lost, significant periods of inactivity, and less-than-optimal organizational learning. Of special interest to this study is the lack of a comprehensive, smart, and automated system for reporting incidents that can support real-time decision-making, minimize the risk of human error, and drive continuous optimization of various functional domains [10]. Though fragmented systems exist, a complete model that unifies detection, documentation, contextual analysis, and strategic intelligence is often insufficiently developed or poorly implemented in the majority of organizations.

The main purpose of this work is to design and validate a Framework for Automated Incident Reporting and Intelligence using artificial intelligence technologies to provide support for effective detection of incidents, real-time reporting, data-driven strategic prioritization, and responses. The suggested framework pursues a convergence of automation and intelligence by proposing a flexible and modularity-enabled system structure suitable for diverse application domains like cybersecurity, healthcare safety, industrial safety, and disaster response. Apart from that, this study investigates the core enabling technologies, hurdles to their application, real-world applications, and potential means of enhancing the responsiveness and accuracy of incident management systems.

2. Limitations of Traditional Reporting Mechanisms

Traditional incident reporting mechanisms, despite their historical value, are increasingly inadequate in addressing the complexities of modern operational environments. One of the foremost limitations is their dependence on manual inputs, which inherently introduces human error, subjectivity, and inconsistency. Incidents may go unreported due to fear of blame, lack of awareness, or a belief that the issue is too minor [8]. This results in underreporting, which compromises the integrity of data sets and prevents organizations from recognizing systemic patterns or emerging risks.

Another major shortcoming lies in the latency of reporting and response. In traditional systems, incidents are often reported long after they have occurred, usually when someone has the time to fill out a form or send an email. This delay can prove costly in environments like cybersecurity, emergency medicine, or industrial production, where every second matters [9]. Traditional reporting also tends to be descriptive rather than analytical, capturing what happened without offering insights into why it happened or how to prevent recurrence.

Data silos present another challenge. Information captured by one department often remains inaccessible to others due to incompatible systems, organizational boundaries, or privacy concerns. This fragmentation limits the potential for a holistic organizational response and weakens the ability to conduct cross-functional investigations.

Moreover, traditional systems typically lack real-time analytical capabilities and predictive power. Without integration with real-time data sources or advanced analytics, organizations are unable to identify high-risk scenarios proactively. These systems also struggle with handling unstructured data, such as verbal reports, handwritten notes, or text messages—valuable sources of information often lost in translation.

2.1. Gaps in Existing Frameworks

Despite advances in automation, analytics, and intelligent system integration, modern incident reporting schemes still face significant shortcomings that undermine their effectiveness across different domains. One of the key limitations is the lack of interoperability between different systems. Many organizations use incident management solutions that are department- or function-specific, leading to siloed data stores and limited sharing across functions. These conditions make it difficult to establish a unified operating view in the course of significant events.

A chronic shortfall in capability involves the lack of contextual understanding and semantic reasoning. Even though platforms that leverage machine learning and artificial intelligence exhibit skill in pattern recognition, many systems lack the deep contextual awareness needed to distinguish between normal anomalies and true threats. For instance, increased login behavior can be detected as a potential anomaly in a bank environment, while similar behavior in the course of system maintenance is wholly routine. Failure to involve organizational context in automated decision-making leads to alert fatigue and can generate false positives.

The deployment of smart incident reporting systems is also complicated by legislative and ethical considerations. Data privacy issues, potential over-surveillance, and algorithmic biases are concerns that are often insufficiently addressed, especially in the healthcare and law enforcement sectors. Furthermore, current systems tend to disregard the human factor, failing to provide intuitive interfaces, extensive training, or feedback loops that ensure continuous improvement.

The focus on flexibility and resilience is severely limited. Present frameworks are normally built upon a pre-defined threat model, leading to decreased performance in countering unexpected and ambiguous scenarios, which encompass cyber-physical attacks, hybrid warfare, or disruption due to pandemics [4]. In addition, these frameworks lack self-adaptive aspects that are needed to transform their operation according to changing environments.

In the end, most frameworks are inherently reactive rather than strategically proactive. They focus predominantly on responding to events rather than on proactive prevention and future-proofing. Individually and collectively, these failings point toward the need for a rigorous, automated, and intelligence-led system of incident reporting—founded in contextual data, real-time analysis, human supervision, and learning adaptation.

Table 1 Identifying Gaps in Current Frameworks: Challenges and Opportunities

Description of Gap	Impact on Current Frameworks	Potential Solution/Opportunity
Lack of seamless integration between systems and data sources.	Leads to fragmented data and inaccurate insights.	Implement advanced data integration tools and AI to standardize data pipelines.
Existing frameworks struggle to handle large-scale operations.	Limits the ability to process big data effectively, causing performance issues.	Develop scalable cloud-based solutions to manage high-volume data efficiently.
Inadequate support for real-time data processing.	Delays in decision-making and reduced operational efficiency.	Utilize edge computing and real-time analytics tools to improve responsiveness.
Frameworks are often rigid and difficult to adapt to new requirements or changing environments.	Limits the ability to innovate and adapt quickly to market changes.	Build modular frameworks with plug-and-play capabilities for easier customization.
Insufficient focus on security protocols and regulatory compliance.	Increases vulnerability to cyber threats and non-compliance risks.	Integrate robust cybersecurity measures and automated compliance checks.
Existing frameworks lack user-friendly interfaces and adaptability for diverse user needs.	Leads to poor user adoption and suboptimal utilization of the framework.	Design frameworks with intuitive, customizable user interfaces to enhance user experience.
Limited compatibility with other systems, technologies, or platforms.	Reduces the effectiveness of multi-system environments and collaboration.	Standardize APIs and improve interoperability across different platforms.

3. Advancements in Automation and AI

The last decade has witnessed groundbreaking advancements in automation and artificial intelligence (AI), fundamentally transforming how incidents are reported, analyzed, and addressed. Automation has made it possible to shift from human-dependent, reactive systems to proactive platforms that can detect, classify, and escalate incidents without requiring manual input [2]. This transformation is largely driven by the emergence of sensors, intelligent monitoring systems, and data stream analytics that provide 24/7 surveillance over critical infrastructure, digital ecosystems, and operational environments.

At the heart of this shift is the application of machine learning (ML), which enables systems to recognize patterns of normal and abnormal behavior by learning from historical data. For example, in a networked environment, automated systems can detect unusual spikes in traffic, unauthorized access attempts, or service outages and flag them as potential incidents [3]. These detections are immediate and can be tied to automated response protocols, significantly reducing downtime and human workload.

Furthermore, Natural Language Processing (NLP) plays a critical role in extracting insights from textual data, such as emails, chat logs, or free-text reports. This allows organizations to convert unstructured inputs into structured intelligence that can be analyzed and acted upon. Robotic Process Automation (RPA) complements these technologies by handling repetitive tasks—such as sending alerts, filing reports, or triggering workflows—thereby accelerating the entire incident management lifecycle.

Advanced AI systems can also perform risk scoring, impact assessment, and root cause analysis in real time, enabling strategic decision-making. These tools not only enhance the efficiency and accuracy of incident reporting but also support predictive capabilities, allowing organizations to anticipate and mitigate threats before they escalate. By embedding AI into the core of incident reporting systems, organizations are transitioning from passive record-keeping to active, intelligent governance models that drive resilience, safety, and performance.

3.1. Intelligence Frameworks in Cybersecurity and Healthcare Contexts

The implementation of intelligence frameworks has revolutionized incident management across various critical domains, notably cybersecurity, healthcare, and military operations. In cybersecurity, intelligence frameworks aggregate data from internal logs, threat feeds, and user behaviors to identify and respond to emerging threats in real time [3]. Systems such as Security Information and Event Management (SIEM) and Threat Intelligence Platforms (TIPs) employ machine learning and behavioral analytics to detect anomalies, assign risk scores, and suggest mitigation steps. These tools allow organizations to manage vast streams of data, prioritize responses, and enhance their defensive postures.

In healthcare, intelligence frameworks are vital for patient safety and operational continuity. Systems like Clinical Decision Support Systems (CDSS) integrate incident reporting with patient records to detect adverse drug reactions, surgical errors, or procedural deviations. By analyzing structured data from Electronic Health Records (EHRs) and unstructured clinical notes, healthcare institutions can respond swiftly to prevent harm. Additionally, these systems enable organizations to fulfill regulatory requirements such as those from the Joint Commission or FDA, while also improving the quality of care through continuous learning from past incidents [13].

Across all sectors, these intelligence frameworks highlight a paradigm shift from documentation to dynamic decision-making. However, while each domain demonstrates success within its silo, there remains a lack of unified frameworks that transcend these boundaries. This underscores the need for a cross-sectorial model—an adaptable, automated intelligence framework that integrates the best practices of each domain to enhance incident reporting and response on a broader scale.

3.2. Integration of Data Analytics and Real-Time Systems

The combination of real-time systems and data analytics is the biggest leap forward in the field of incident reporting systems [5]. Traditionally, data was reviewed retrospectively, which means that events were analyzed after the fact. Today, real-time analytics allow for instant detection, analysis, and, in certain cases, even resolution of events in real-time. These capabilities are made possible through the methodical use of data ingestion platforms, stream analytics engines, and machine learning routines that are capable of processing data in milliseconds.

Real-time systems like Internet of Things (IoT) devices, closed-circuit television (CCTV), network monitoring applications, and mobile apps are continual sources of data. They generate both unstructured and structured data that then flows to central processing units or data lakes [12]. Advanced data analysis platforms like Apache Kafka, Spark Streaming, and Flink are used to screen this data for anomalies, patterns, and thresholds that can indicate impending events.

When combined with predictive analytics and model-driven technologies based on artificial intelligence (AI), these systems are equipped not only to spot incidents but also predict their occurrence by analyzing historic data in conjunction with contextual indicators. For example, in production environments, real-time sensors can recognize unusual machinery vibrations, then trigger alerts before any possible failures. In cybersecurity, systems can recognize early indicators of Distributed Denial of Service (DDoS) attacks by noticing traffic anomalies.

In addition, visualization tools, heat maps, and dashboards enhance situational awareness by transforming raw data into actionable insights. These platforms enable resources to be allocated efficiently, understand the flow of incidents, and allow for swift response actions. The overall ability to process data in real-time stems from how well it enhances the bridge between detection and response, thus creating a dynamic, self-reinforcing incident management system [10].

This unified consolidation is the basis of modern automated intelligence and incident reporting systems, which allow organizations to react with unmatched speed, specificity, and understanding.

4. Core Components of the Automated Incident Reporting and Intelligence Framework

4.1. Incident Detection and Categorization

The identification and classifying processes are the building blocks and core components of automated incident reporting and intelligence. The capability of the system to quickly identify anomalies and correctly classify them allows for fast-response interventions, hence preventing further damage. Incident detection refers to automated identification of unusual activities or events that diverge from the predetermined system operating norms. Some of these anomalies may include security breaches (e.g., attempted intrusion), system failures (e.g., hardware malfunctions), or user errors (e.g., data entry errors).

In the world of efficient incident identification, the system utilizes cutting-edge technologies, which involve machine learning (ML), artificial intelligence (AI), and statistical models, to examine data derived from different sources [6]. Data is collected from network traffic, application logs, security infrastructure, and physical sensors, thus enabling continual observation for any variations from predefined parameters [11]. For instance, in the cybersecurity field, ML models can be used to identify unusual patterns of user actions that might reflect a probable breach or insider risk. In industry, sensors built into machinery can identify anomalies like vibrations or variations in temperature, which may reflect a heightened probability of equipment failure.

Upon identifying an anomaly, it is important to classify it precisely. It involves grouping the incident according to its level of severity, nature, and possible implications. Efficient categorization allows organizations to prioritize their actions based on the level of severity of the incident, ensuring that critical cases are dealt with immediately. Typically, the classification process involves using predetermined rules or machine learning-based artificial intelligence models that learn and change according to the new needs of the organization, categorizing the incidents as critical, high, medium, or low severity level. It allows the automation of response prioritization and triage, leading to a more efficient incident management process.

4.2. Data Collection and Processing Modules

A successful system of incident reporting and intelligence relies primarily on the functionality of its data collection and processing functions. These functions are charged with the continuous collection, protection, and analysis of assorted types of data that support the functions of incident identification, classification, and the creation of decision-making procedures. Proper data collection ensures that the system possesses a complete and up-to-date picture of the environment, while the processing functions are responsible for converting the data into actionable intelligence.

Traditionally, data comes in a wide range of forms, including sensor readings, activity logs, user interaction data, network traffic, security systems, and external feeds. Both structured data (e.g., system logs and sensor readings) and unstructured data (e.g., text reports, social media posts, and voice recordings) are produced by these sources. The challenge comes in coordinating this wide range of data types in operational form while ensuring that all relevant details are included.

In managing the large amount of data, the system utilizes data aggregation platforms and data lakes that collect different forms of data and aggregate them to one infrastructure. After collecting the data, the system undertakes data processing routines that scan, cleanse, and normalize the data sets. Often, ETL (Extract, Transform, Load) processes are applied to ensure that only relevant data is kept and processed according to what other system components require. Data processing involves the use of real-time analytical engines that operate on incoming streams of data. The engines analyze the data as it comes in, looking for patterns, anomalies, or specific triggers that could indicate an event. Data processing is improved by the integration of machine learning models, which get better and better as they continually learn and adjust from past events, thus enabling the system to attain greater accuracy and efficiency with extended use [9].

The successful integration of these data acquisition and processing elements forms a crucial factor in ensuring that the system is able to respond to incidents swiftly and accurately, hence allowing instant analysis and knowledgeable decision making.

4.3. Real-Time Intelligence and Decision-Making Engine

The Real-Time Intelligence and Decision-Making Engine operates as the central processing center in an automated environment that is committed to intelligence and incident reporting. It interprets the data gathered by the system and utilizes machine learning models in addition to artificial intelligence algorithms to enable fast and well-informed decision-making, thus improving the effectiveness and accuracy of incident response.

This module processes data obtained by the detection and classification modules to gauge circumstances and decide upon responsive actions in the scope of incident response. Unlike traditional systems based upon manual analysis, this real-time engine operates by itself, using advanced predictive models and anomaly detection methods to gauge risk, predict probable outcomes, and make recommendations. As an example in the cybersecurity sphere, the engine can gauge the likelihood of an existing attack escalating and decide whether automated countermeasures like segmenting off a compromised server or blocking malicious traffic need to be initiated.

A core aspect of decision-making is its ability to prioritize events by their severity, intensity, and available resources. Decision trees in addition to dynamic scoring parameters are utilized in this operation to allocate appropriate resources to events accordingly, ensuring critical events are treated in a timely manner. It is critical in scenarios where speed of response directly translates to minimizing damage or loss, which is common in cases of cyberattacks, factory accidents, or healthcare emergencies.

Also, the ability of the engine to learn from previous events ensures continued refinement of its decision-making ability. Through analyzing outcomes of previous actions and continuously perfecting the procedures, the system can better tailor resolutions for similar events in the future, thus ensuring heightened operating efficiency and supporting organizational resiliency.

4.4. Reporting and Documentation Automation

The final key aspect of an automated system for incident reporting and intelligence involves automating both reporting and documentation. Such a feature affords organizations the ability to maintain exact and up-to-date records related to incidents and their resolutions. Having such a feature ensures that all relevant information is properly recorded and formally documented, enabling organizations to meet regulatory requirements, perform post-incident analysis, and maintain an audit trail for future reference.

After the discovery and correction of an occurrence, the system automatically generates detailed reports that synopsize the event, outlining the type of occurrence, level of severity, corrective steps taken, and resulting impact. Automation of the reports ensures accuracy and also eliminates the need for manual entry of data. Such a feature is of paramount importance in industries that require strict application of standards, such as healthcare, finance, and cybersecurity, where maintenance of detailed records is legally mandated.

In addition, automated reporting makes it easier to prepare post-incident analyses that allow organizations to learn lessons from each incident. These reports generally include analysis of the root causes of the failure, rectification measures taken to address the issue, and the precautionary steps that can be taken to prevent similar cases in the future. In addition to that, the system can also generate longitudinal trend reports that provide organizations with detailed insight of recurring issues or system vulnerabilities, thus enabling organizations to be proactive in managing risks.

The use of automated documentation greatly enhances the accuracy and timeliness of information. It is particularly beneficial in dynamic environments where manual intervention can bring in delays. Through the maintenance of accurate and automated records, organizations are well-equipped to facilitate well-informed decision-making, continuous improvement, and respect for both internal rules and external laws. In the end, automated reporting and documentation enable efficient collection and retention of incident data, hence providing critical insights for future strategic direction and continuous optimization

5. System architecture and design principles

5.1. Layered Architecture (Data Layer, Intelligence Layer, Response Layer)

A multi-tier architecture is essential to support a well-organized flow of data as well as defining roles in the automated generation of events and in the intelligence sphere. It divides the system into three basic tiers: the data tier, the intelligence tier, and the response tier, each playing separate functions that ensure the efficient, secure, and responsive operation of the system.

- **Data Layer**: As the core of the system, the data layer is responsible for the processes of data collection, storing, and preliminary processing. It collects data from diverse sources, including sensors, logs, user behavior, and external systems, and compiles it in a single, unified repository. Its main roles include implementing data cleansing, filtering, and transformation processes that ensure passing on of only relevant and actionable data to the next layers. Also, it utilizes data storage technologies like relational databases or data lakes in order to facilitate easy query and direct access to historical data.
- **Intelligence Layer**: It acts as the system's core processing unit, using high-level algorithms like machine learning (ML), artificial intelligence (AI), and data analysis to assess the gathered data. It processes raw, unprocessed data obtained from the data layer, determines patterns, detects anomalies, and creates forecasts or recommendations. Its tasks include the recognition and identification of events, as well as the creation of decisions that inform decision-making processes. It utilizes AI models to support instant decision-making while also ranking actions according to the priority of events.
- **Response Tier**: It focuses on the efficacy of decision-making outcomes that are made in the intelligence tier. It triggers appropriate response actions that can encompass notification dissemination, automated operation initiation, or alerting of concerned stakeholders. Its function involves execution of predefined workflows and automation of functions like dispatch of incident reports, initiation of mitigation actions, or assignment of resources to deal with the incidents.

The division of the framework into three layers enables improved scalability, modularity, and maintainability, while at the same time simplifying the troubleshooting and debugging processes.

Table 2 Three-Layered Architecture for Real-Time Decision-Making Systems

Layer	Description	Components	Functions
Data Layer	The foundational layer that handles data collection, storage, and management.	Data Sources (e.g., IoT devices, databases, APIs)	Data ingestion and collection
		Data Storage (e.g., Data Lakes, Databases)	Data storage and retrieval
		Data Preprocessing Tools (e.g., ETL pipelines)	Data cleaning, normalization, and aggregation
Intelligence Layer	The layer responsible for advanced analytics, machine learning, and decision-making algorithms.	Analytics Engines (e.g., AI, ML models)	Data analysis, pattern recognition, and prediction
		Decision Support Systems (e.g., optimization models, rule engines)	Real-time decision-making, anomaly detection, recommendation
		Data Science Tools (e.g., Python, R, Tensor Flow)	Forecasting and predictive insights
Response Layer	The final layer where insights are acted upon, displayed, or communicated.	Dashboards and Visualizations (e.g., Power BI, Tableau)	Deliver actionable insights and recommendations
		Actionable Interfaces (e.g., Automated systems, Alerts, Notifications)	Trigger automated actions based on insights (e.g., alerts)
		Feedback Loops (e.g., user interaction, system adjustments)	Continuous improvement of decision-making models

5.2. Interoperability and Modularity

The modularity and interoperability fundamentals are necessary to create a robust automated system for incident reporting and intelligence gathering. These concepts enable the system to easily integrate with a heterogeneous set of external systems, devices, and technologies, while fostering flexibility, scalability, and ease of maintenance.

- Interoperability refers to the ability of a system to interact and enable data sharing across various platforms, technologies, and services. Since organizations increasingly rely on complex IT infrastructures, it is essential that a system integrate well with external platforms, hardware, and software, which includes Enterprise Resource Planning (ERP) systems, Customer Relationship Management (CRM) systems, and Security

Information and Event Management (SIEM) systems. Interoperability needs to be implemented in order to provide a unified view of the events across various departments and increase organizations' responsiveness.

- Modularity ensures that the system is built as a collection of separate and interchangeable components. Each module performs a specific function in the overall system, ranging from tasks of incident detection, classification, reporting, or handling notifications. The modularity of the system ensures that the addition of new functionalities or changes does not affect the overall system's integrity. Additionally, the design promotes improved troubleshooting efficiency, where faults can usually be attributed to a specific component, hence ensuring reduced downtime and improved system reliability.

In addition, a modular and interoperable system allows for the easy integration of new technologies. Modular architecture makes it possible for organizations to replace or upgrade individual components as necessary, without the need for full system overhauls and keeping the system adaptable to new technologies and changing operating requirements.

5.3. Security and Access Management

Given the sensitive nature of data related to incidents, particularly in domains like healthcare, finance, and critical infrastructure, security and access controls should take precedence in developing an automated incident reporting and intelligence system. It is necessary to ensure that only authorized personnel are allowed to access critical systems and data, as this is crucial for ensuring confidentiality, integrity, and availability.

Security is achieved by employing different defensive mechanisms that include encryption methods to secure data in transit and in storage, firewalls to keep unauthorized entities away, and intrusion detection systems (IDS) that catch aberrations in activities [7]. In addition, strong communication methods like HTTPS and TLS are used to secure data transfers in the system, which ensures that reported incidents and Intel data are kept secure from possible interception or tampering.

Access controls are a mechanism that ensures restricted access to the platform by authorized users or systems. Historically, this is achieved through role-based access control (RBAC), where the user is assigned a specific role (e.g., administrator, analyst, or technician) and is given access to different levels of data and functionality based on the assigned role [12]. Secondly, the use of multi-factor authentication (MFA) seeks to restrict access by allowing it only after the verification of the user's identification through various layers of authentication.

In ensuring continuous security, the system integrates systematic security audits, vulnerability scanning, and patch management practices that help identify and deal with potential threats to security ahead of their exploitation. Through the use of strict access controls and stringent security procedures, the system minimizes the risk of data breaches, unauthorized access, and cyberattacks.

6. Conclusion

Implementation of an Automated Incident Reporting and Intelligence System is drawing near to enhancing incident reporting systems to become better, faster, and more accurate in various industries. The research examined the key components, issues, advantages, and future concepts for applying automation, artificial intelligence, and data-based intelligence in incident reporting systems. With automation and real-time data analysis, organizations can significantly reduce response time, minimize human errors, and ensure critical incidents get reported and resolved in an accurate and timely manner.

The advantages of automation frameworks are apparent, yet research also indicates areas to consider. Some of those include integration with existing systems, resistance to automation use, and concerns about false positives and system reliability. These should be key areas in future research, particularly enhancing automation processes and better integration of systems. In using such frameworks, consideration should be given to company culture, readiness of infrastructure, and regulations to achieve success in setup as well as long-term success.

There is a necessity to conduct further research in critical areas at an urgent level. This entails research into making quick decisions using automatic systems, developing tools for anticipating events using AI, and implementing universal rules for reporting events. Collaboration among various communities and cooperation in partnerships across the globe is necessary to manage matters related to applying AI, machine learning, and blockchain in reporting events in ways that maintain privacy, security, and trust in them. In summation, the Automated Incident Reporting and Intelligence Framework displays significant advancements in improved and adaptable mechanisms to manage today's era of

complexity in incident events in sectors such as cybersecurity, healthcare, and IoT in industry. Constantly evolving mechanisms make companies stronger, assist in making better-informed decisions, and provide optimum security, resulting in accelerated incident response in today's evolving digital era

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Alharbi, A., Atkins, A., and Wills, G. (2016). Security incident response: A systematic literature review. Computers and Security, 56, 35–45. https://doi.org/10.1016/j.cose.2015.10.003

[2] Arora, S., and Sood, S. K. (2021). A comprehensive review of artificial intelligence techniques used for incident detection in cybersecurity. Computers and Security, 104, 102183. https://doi.org/10.1016/j.cose.2021.102183

[3] Denecke, K., and Nejdl, W. (2019). Automated processing of incident reports in healthcare using natural language processing. Journal of Biomedical Informatics, 96, 103247. https://doi.org/10.1016/j.jbi.2019.103247

[4] ENISA. (2021). Incident Reporting in the EU: Evaluation and Recommendations. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

[5] Gartner. (2022). Automation in Incident Response: Best Practices for Enterprise Resilience. Gartner Research.

[6] Google Cloud. (2023). Incident Response and Automation: A Cloud-Native Approach. https://cloud.google.com/security

[7] ISO/IEC 27035-1:2016. Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management. International Organization for Standardization.

[8] Kwon, J., Johnson, M. E., and D'Arcy, J. (2022). The impact of data breaches on organizational reputation and the role of incident response systems. Information and Management, 59(3), 103532. https://doi.org/10.1016/j.im.2021.103532

[9] Liu, Y., and Zhang, C. (2020). AI-based intelligent incident classification and prioritization in IT operations. Expert Systems with Applications, 148, 113263. https://doi.org/10.1016/j.eswa.2020.113263

[10] Microsoft. (2022). Securing your environment with AI-powered Incident Management. Microsoft Security Blog.

[11] National Institute of Standards and Technology (NIST). (2018). Computer Security Incident Handling Guide (SP 800-61 Rev. 2). https://csrc.nist.gov/publications

[12] Nguyen, T. T., Ngo, T. D., and Choi, D. (2021). A real-time incident detection framework for smart cities using IoT and deep learning. Journal of Information Security and Applications, 59, 102831. https://doi.org/10.1016/j.jisa.2021.102831

[13] Office of the National Coordinator for Health IT. (2020). Health IT and Patient Safety: Building Safer Systems for Better Care. U.S. Department of Health and Human Services.