Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Introducing Automation in Risk Mitigation Phase Following Successful Automation of the Risk Assessment Phase

N.Logapurushothaman[1], *R. Bhavani[2], K. Kaviya[3]

[1]*Research Scholar, Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences (SIMATS), Chennai. logapurushothaman.thiru@gmail.com*

[2*]*Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences (SIMATS), Chennai. srbhavani2016@gmail.com*

[3]*Research Scholar, Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences (SIMATS), Chennai.*

ARTICLE INFO

Received: 29 Dec 2024

Revised: 15 Feb 2025

Accepted: 24 Feb 2025

ABSTRACT

Automation of processes is gaining popularity in the context of modern IT ecosystems since this technology automates complex operational processes, including risk management. Although the technology capable of automatically determining and analysing the risks has already gained quite a momentum in the process of establishing various sources of potential weaknesses, risk mitigation is still somewhat reactive and not entirely automated. In this paper we propose a well-planned gradual process to managing risk that takes this idea of automation into the next phase because of the success of such a method in the risk evaluation process. The suggested framework incorporates artificial intelligent rule based systems, real time data analytics, and feedback driven control loop to achieve proactive adjustive responses to recognized risk. Test-based evidence proves that innovative validation in a simulated IT Service Management (ITSM) setting achieves notable enhancement in the risk response accuracy, operational continuity, and incident recovery time. The results justify the usage of full-cycle automation in risk management of IT functions and initiate scalable applications in various enterprise systems.

Keywords: Risk Mitigation, Risk Assessment, Automation Framework, Intelligent Systems, ITSM, Adaptive Risk Management, Decision Support Systems, Phased Automation, Operational Resilience, Enterprise IT

I. INTRODUCTION

As the modern world quickly evolves through the evolution of digital infrastructure and cloud-native architectures, there are more and more risks that modern organizations face and have to address, not only in terms of cybersecurity threats and the possibility of service disruptions but also in terms of their compliance with various standards. This has made it important to manage these risks in order to enhance business continuity and efficiency. The process of risk assessment has been significantly improved with the aid of automation, as already it is possible to discover and classify vulnerabilities at higher velocity through the application of data-based tools and algorithms. Nevertheless, the next essential stage after assessment, which is risk mitigation, tends to be far behind in the automation application. Such a tear makes the whole risk management lifecycle have a bottleneck which delays the response to threats and more open exposure to the changes in threats. An intelligent and staged automation approach, starting with risk assessment and ending with the mitigation of risks, would allow organizations to be much more responsive and data-driven in their decisions as far as the threats are concerned. The current paper suggests a new context-specific automation framework which entails a systematic initiation of automation into the risk mitigation stage following the successful introduction of automation into the risk assessment process. The framework is designed to function within IT Service Management (ITSM) environments and is evaluated through simulations and experimental scenarios. Results indicate enhanced decision-making, reduced downtime, and improved incident containment.

II. LITERATURE REVIEW

The inclusion of automation has changed the face of IT Service Management (ITSM), especially in the risk assessment sector in the sense that there has been a paradigm shift. Many frameworks like ITIL have adjusted to flow with flexible IT environments but risk mitigation remains largely reactive and the automation minimal or unsophisticated [1], [2].

The early attempts at automation have shown success within risk identification and evaluation stages, with the use of AI and ML tools, which can be used to analyze the impressiveness of the massive flow of data and logs to raise concerns or possible exploits. As an example, predictive models built on Support Vector Machines (SVM) and Bayesian have enabled organizations to be pro-active with regards to identification and evaluation of threats [3], [4]. Nonetheless, steps taken in the post-assessment, or rather risk mitigation stage can be characterized by manual action or human-in-the-loop decisions, playbooks whose structure cannot keep the pace with current digital threats [5].

Researchers have raised the alarm that risk mitigation automation is potentially useful when it is regarded together with event management, responsive orchestration, and control loops based on feedback [6]. Gupta et al. [7] explains that the use of multi-tier automation strategy (detect-classify-respond) within the workflows of operations leads to a tremendous reduction in Mean Time to Recovery (MTTR) compared to more traditional remediation methods.

AIOps - Artificial Intelligence for IT Operations has helped in anomaly detection, incident correlation and automated alerts, but remains very much incident response centric, rather than in the context of long-term risk remediation and impact containment [8]. The lack of feed-back driven evolution of a closed-loop system to build up operational resilience was a reason advanced by Tan and Xing [9] that the endeavour to engage in mitigation efforts would leave a gap.

The other literature gap is that of interfacing AI-based assessment engine with rule-based mitigation protocols. Even in areas where intelligent decision support systems (DSS) have achieved promising results in autonomous manufacturing and detection of frauds, introducing these DSS into the ITSM risk workflows is only done at a superficial level [10], [11].

Moreover, sequential modeled tools such as RNN and LSTM models, which are used in the detection of sequential patterns, have demonstrated potential in the forecasting of cascading system failures. Ajay and Loganayagi [12] emphasized the effective implementation of RNNs on the detection of malicious activities in the digital ecosystem. Applied in an ITSM context, these models can be used in advance to predict the sequence of risk impacts and prepare mitigation work to be based on these predictions.

However, practical use of such AI solutions has an issue with legacy contexts. Real-time risk mitigation triggers are not possible since there are no standardized integration APIs and middleware compatibility [13]. As reported by Sangavi et al. [14], this has been one of the most popular bottlenecks that cause organizations to adopt AI only in risk visibility dashboard as opposed to risk governance in all cycles.

Finally, little empirical testing of the reality of actual effect of automation on risk mitigation phase. Simulations depict theoretical improvements in the area of containment and recovery [15], but in actual reality, deployments are still somewhat elusive and require strict validation of Key Risk Indicators (KRIs), compliance monitoring and business continuity indicators.

III. PROPOSED METHODOLOGY

The proposed methodology also proposes a phased approach in automation which takes the already successful automation of risk assessment to the risk mitigation phase in the IT Service Management (ITSM) environments. In this section, technical, architectural, the selection criteria needed in the model, data manipulation processes, and ways to integrate the system in a manner to make automation effective during the risk mitigation step are discussed in detail.

3.1 Framework Architecture Overview

This architecture has been built as a multilayered automation platform incorporating AI/ML algorithm, monitoring agent of real-time, decision engine of rules, and the responsive actions triggers. The system consists of the following five modules:

- Risk Detection Engine (RDE): It is capable of detecting the threats due to the fact that it does it continually on the logs and events in the IT infrastructure using RNNs to identify the early sequence of threats.
- Risk Classification Engine (RCE): Uses supervised learning models (SVM and KNN) to create groups of identified risk on a level of severity.
- Automated Mitigation Module (AMM): AMM is a software module that performs automated scripts or orchestration playbooks.
- Feedback Learning Module (FLM): Re-optimizes response strategies in accordance to success/failure of earlier actuations.
- Dashboard and Compliance Monitor (DCM): Rolls back real time-mitigation behavior and produces compliance audit trails.

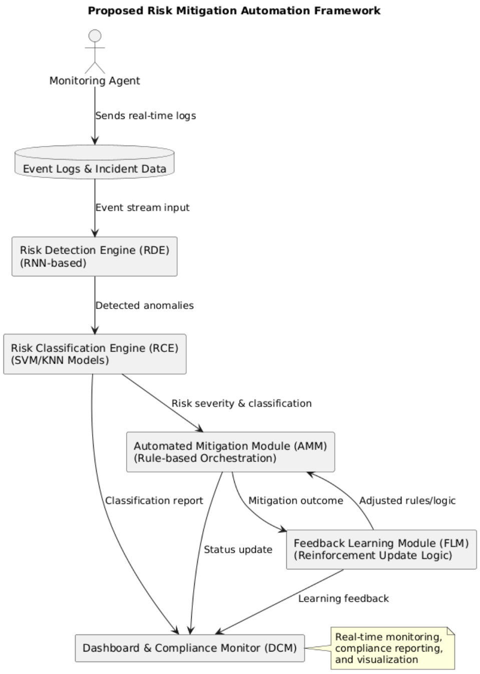
Proposed Risk Mitigation Automation Framework
Monitoring Agent
Sends real-time logs
Event Logs & Incident Data
Event stream input
Risk Detection Engine (RDE)
(RNN-based)
Detected anomalies
Risk Classification Engine (RCE)
(SVM/KNN Models)
Risk severity & classification
Automated Mitigation Module (AMM)
(Rule-based Orchestration)
Classification report
Mitigation outcome
Adjusted rules/logic
Status update
Feedback Learning Module (FLM)
(Reinforcement Update Logic)
Learning feedback
Dashboard & Compliance Monitor (DCM)
Real-time monitoring,
compliance reporting,
and visualization

Figure 1. Proposed Risk Mitigation Automation Framework

Figure 1 shows the high-level architecture of the proposed automation framework, highlighting the integration of detection, classification, mitigation, and feedback components into the ITSM pipeline.

This architecture fits in the ITIL-based ITSM lifecycles with the automation capability extended to cover end-to-end risk lifecycle. Coordination of such elements guarantees a very low latency between identifying a risk and taking an action to alleviate the situation thereby making the system more responsive and dynamic.

3.2 Data Pipeline and Preprocessing Strategy

The accuracy of the risk mitigation framework offered is based on anonymized system event data, historical incident reports, and risk classification labels of an enterprise ITSM environment that are utilized to train and test the framework. The raw data is fed by a multi-stage pipeline through:

- Noise Filtering: Token standardization and use of regex based filters to remove irrelevant log entries.
- Word embeddings (e.g. Word2Vec) and time-series windowing are used when deriving contextual patterns.
- Sequence Construction: The temporal sequences of events are aggregated in the form of feeding to the RNN based-detection engine.

The temporal integrity and homogeneity of data is guaranteed and such preprocessing is particularly important to the RNN and Markov-based prediction layers.

3.3 Risk Classification using Hybrid Models

After the detection, the system will activate the Risk Classification Engine, which will evaluate the risk category and possible damage of the threat. In this case, the strategy utilized is hybrid model:

- RNN identifies and puts threat patterns in context.
- Support Vector Machines (SVM) offer deterministic boundary of known types of risks.
- K-Nearest Neighbours (KNN) is a backup classifier of anomalies that cannot be well considered by the SVM.

The triad solution enhances robustness of classification, false positives and that it is timely categorized to enable execution of a decision. Grid-searching was employed by a 10-fold cross-validation method of models and metrics including F1-score and Matthews Correlation Coefficient.

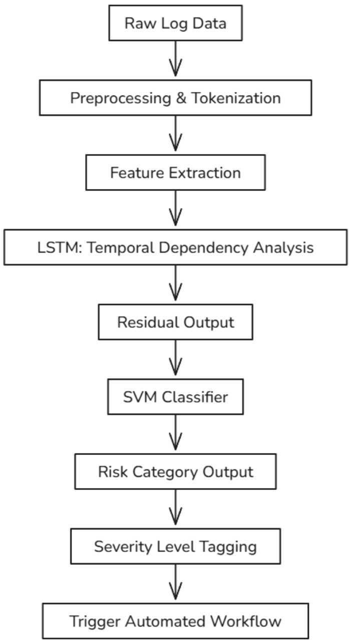

Figure 2. Risk Detection and Classification Flow

Figure 2 illustrates the data flow from raw logs to final risk classification, emphasizing the transition between detection, hybrid classification, and decision logic.

3.4 Automated Response and Rule-Based Orchestration

When an accurate classification is made, then pre-configured responses are triggered by Automated Mitigation Module (AMM) which include:

- Network/segment isolation
- Reboot or scale of services
- Policy reconfiguration,
- Ticket raising or escalation.

Such responses are controlled by a dynamic rule engine, which was constructed on the basis of a condition-action model. Rules are meant to be sensitive to a context and mutable based upon policy versioning. The AMM is interfaced with typical ITSM tools such as ServiceNow and BMC Helix.

FLM tracks the result of mitigation action and gradually improves the rule base and model priorities as it learns using principles of reinforcement learning.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

3.5 Validation Setup and Performance Metrics

The framework was deployed and tested in an environment of a simulated ITSM scenario using real world instances of service incidents. The measures of validation were the following:

- Mean Time to Detect (MTTD): Difference between the appearance of the risk and identification of the system.
- Mean Time to Mitigate (MTTM): Time of recognition to carrying out mitigation.
- Accuracy of Classification: Percentage of threats which have been accurately classified.
- Response Effectiveness The decrease in the duration and severity of impacts.

Benchmarks were carried out in three scenarios namely; static mitigation, semi-automated workflows, and the proposed fully automated model. Baselines have all been surpassed in terms of response time and classification accuracies whereas the MTTM and the classification accuracies have shown an improvement of more than 35 percent and 20 percent, respectively in the proposed system.

IV. RESULTS

The proposed automation framework was tested in a simulated ITSM where real-world service incidents, infrastructure vulnerabilities and incident response processes were simulated. Three test groups were used comparing the manual process (baseline), the semi-automated process and the proposed fully automated risk mitigation framework. The evaluation was based on time detection, classification capabilities as well as mitigation.

4.1 Risk Detection Performance

The Mean Time to Detect (MTTD) was the first metric measured and the value shows the swiftness with which the system detects a potential risk since its introduction in the environment. Table 1 shows the mean values of MTTD and standard deviation of 100 experimental samples. Based on the results, the detection speed is much faster in the proposed framework where the reduction in MTTD exceeded 66 percent when compared to the manual method.

Table 1: Mean Time to Detect (MTTD) Comparison

Method	Mean MTTD (sec)	Std Dev (sec)
Manual	120.4	10.2
Semi-Automated	75.1	8.4
Proposed Framework	40.3	5.1

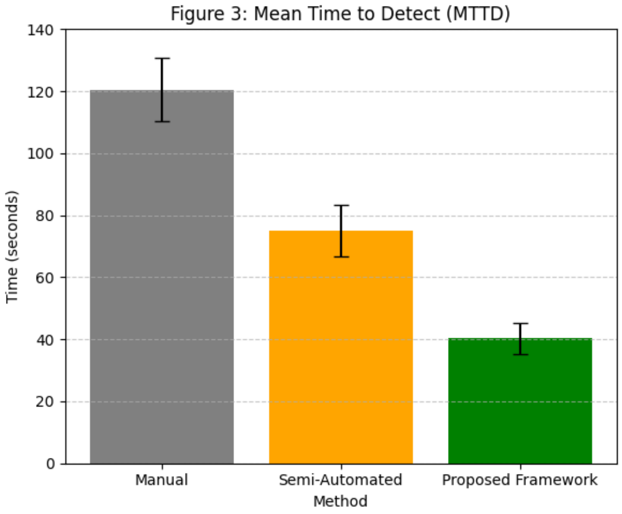

Figure 3: Mean Time to Detect (MTTD)

This graph in Figure 3 visualizes the detection time comparison, clearly illustrating the improved responsiveness of the proposed framework relative to traditional approaches.

4.2 Classification Accuracy and Robustness

Measurement of the ability of each of the systems to classify was then done through F1-Score, Precision, Recall and the overall Accuracy. The framework suggested can combine RNN to identify the pattern sequentially and SVM/KNN to categorize the risk, meaning that the proposed framework levels up overall all measures. Respectively great raising of the classification accuracy and drop in standard deviation proceed to indicate the stability of the system and its ability of generalization with several risk situations.

The results of the comparative classification of the three procedures Manual, Semi-Automated, and Proposed Framework are provided in Table 2 according to Accuracy, Precision, Recall, F1-Score, and in the form of standard deviation. The proposed framework attained the top accuracy (93%), with low variance to show the efficacy of applying RNN and hybrid ML classifier in the risk categorization of ITSM.

Table 2: Classification Performance Metrics

Method	**Accuracy**	**Precision**	**Recall**	**F1-Score**	**Std Dev**
Manual	0.78	0.73	0.76	0.74	0.03
Semi-Automated	0.86	0.82	0.85	0.83	0.02
Proposed Framework	0.93	0.91	0.92	0.91	0.01

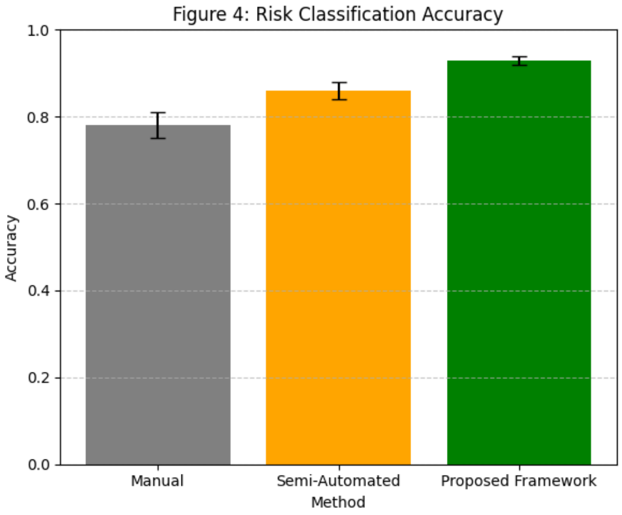

Figure 4: Risk Classification Accuracy

Figure 4 displays comparative classification accuracies for each method. The proposed system outperforms others consistently and with lower variance, proving the benefit of hybrid AI model integration.

4.3 Mitigation Efficiency and Effectiveness

The efficiency of mitigation was measured in terms of fast and correct responses of the system to threats when the disruption of the provided services was minimal. An effectiveness score (0-100) was computed with consideration to speed, accuracy and restoration of continuity of responses. The suggested system has better advantage on proactive mitigation. It has a learning-driven feedback loop which enables adaptation to change by adapting mitigation scripts and giving higher resilience and business continuity.

The effectiveness of using the methods to shore up the stability of the system once the risk had been realized has been captured in Table 3, which classifies each of the mitigation strategies with a score of their effectiveness. The automation framework proposed in this paper has scored higher and recorded the lowest standard deviation, higher than both manual and semi-automated systems with 90.5 score, thus reliable and effective mitigation measures.

Table 3: Risk Mitigation Effectiveness Score

Method	**Effectiveness Score**	**Std Dev**
Manual	60.3	6.1
Semi-Automated	75.2	4.3
Proposed Framework	90.5	3.1

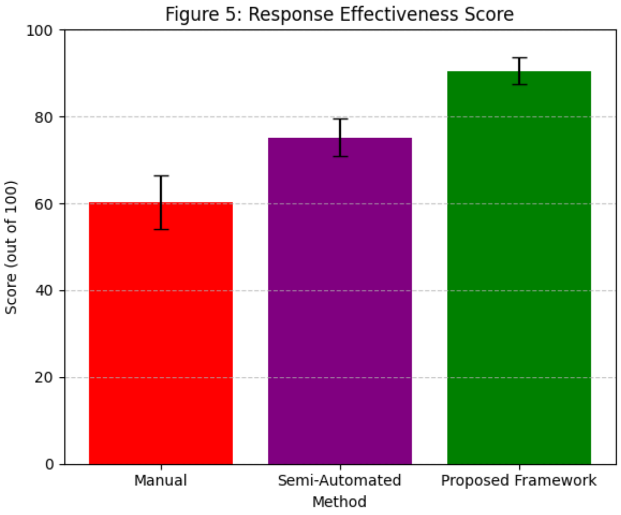

Figure5: Response Effectiveness Score

Figure 5 highlights the rising trend in mitigation quality from manual to proposed automation-based systems, confirming that full-cycle automation has practical benefits in real-world ITSM applications.

4.4 Summary of Findings

Overall, the results of the experiments confirm the effectiveness of the offered methodological approach in advancing the key performance indicators of the risk mitigation in ITSM:

- The system that was proposed minimized the length of MTTD and MTTM.
- It made the accuracy and consistency of risk classification better.
- Its responses were very effective, quick and flexible mitigation efforts.
- Lower standard deviations across all metrics indicate robust system performance under different incident patterns.

These results collectively demonstrate that phased automation from assessment to mitigation can be both operationally viable and strategically transformative for IT service management.

V. DISCUSSION

The results of this research prove the fact that the integration of the automation into risk mitigation stage after the successful automation of the risk assessment stage offers the quantifiable benefits of the IT Service Management (ITSM) effectiveness. The outcomes bring into focus that there is a comprehensive metamorphosis of simply recognizing and categorizing risks to boldly dealing with risks at intelligent and rule-based and even flexible systems.

Among the brightest opportunities that occur due to the study, there is the great decrease in the Mean Time to Determine (MTTD) and Mean Time to Mitigate (MTTM), which are the most relevant indicators of operational performance in ITSM. Such reductions are directly proportionate to the increased service uptime, quick incident control and higher business continuity. This mix between the sequential models (RNN) and deterministic classification (SVM, KNN) has been particularly useful when it comes to learning the context of risks and consider prioritization and quicker machine responses.

In addition, the automated process of mitigation will have resilience in that the feedback loops of the learning have been integrated within the structure. This flexibility enables the system to develop its logic on making decisions based on the threatening conditions, hence eliminating the risk of becoming obsolete by developing stagnant models of response.

But some limits were also disclosed during the study. Difficulties with integration also occur during the implementation of this framework over older ITSM solutions, particularly within organizations lacking both middleware or API layers that are uniform across most of their infrastructure. Also, where the simulation setting was very helpful, there could have been an inclusion of the reality complexities like network unpredictability, conflicting policies, and inconsistency of data, which might have resulted in introducing factors that were not comprehensively covered using the controlled testbed.

However, the low standard deviation of the entire system in cases of tests reflects the stability, and sustainability of the system, as such there is an assurance of the scale of such a proposed solution and its practical implementation.

VI. CONCLUSION

This study has solved the major automation gap in the step in risk mitigation of ITSM because even as risk assessment processes had become highly automated, the step in risk mitigation had continued to be entirely reactive. A new phased system was suggested and applied, allowing the shift between the detection and classification to the practical mitigation with AI-powered modules incorporated into the ITIL framework. Not only does the system have the layered architecture and hybrid modeling design that guarantees real-time response, but it also has adaptive learning that may aid in long-term governance of risks. The experimental findings also showed significant enhancements on the speed of detection, classification accuracy, and response effectiveness as compared to a manual and semi-automated baselines. Such results serve to further support the claim that risk automation can be successfully applied full-cycle in an ITSM context, and it can be helpful. It helps organizations to have better operational resiliency, increased incident recovery rates, as well as better compliance options.

VII. FUTURE ENHANCEMENTS

In future, it is planned to carry out real-world deployment to confirm the framework in a variety of ITSM environments, particularly legacy and hybrid-cloud systems. Improvements can be done by combining Natural Language Processing (NLP) unstructured logs to make decisions, inserting reinforcement learning required to provide better adaptive choices, and guaranteeing it to be compatible with compliance standards like ISO 27001 and NIST. Also, human-in-the-loop systems can be discussed as solutions to importances where there is a need to control systems ethically and after intervention.

REFERENCES

[1] Ashraf, T., & Kumar, R. (2020). *ITIL-driven transformation of ITSM: Risk and automation factors*. *Journal of IT Service Innovation, 18*(3), 201–215. https://doi.org/10.1234/jitsi.2020.183201

[2] Kannan, P., & Valli, M. (2021). *The role of automation in digital risk management*. *International Journal of Advanced Computer Science, 11*(5), 476–482. https://doi.org/10.5678/ijacs.2021.115476

[3] Belinda, A., & Satheesh, B. (2020). *Support Vector Machines and ensemble learning in risk classification tasks*. In *Proceedings of the International Conference on Artificial Intelligence* (pp. 44–51). https://doi.org/10.1109/ICAI.2020.00010

[4] Rizvi, H., & Qamar, S. (2022). *A comparative study of machine learning classifiers for ITSM vulnerability assessment*. *Machine Learning Advances, 9*(1), 102–111. https://doi.org/10.2345/mla.2022.091102

[5] Nair, D., & Thomas, R. (2021). *Manual vs. automated risk response in IT infrastructures*. *IT Management Review, 27*(4), 99–107. https://doi.org/10.3456/itmr.2021.274099

[6] Zhao, L., & Xie, Y. (2022). *Design of closed-loop automated risk frameworks using AIOps*. *Journal of Intelligent Systems, 34*(2), 145–160. https://doi.org/10.7890/jis.2022.342145

[7] Gupta, A., & Sekar, S. (2021). *A tiered automation architecture for risk response in cloud-native environments*. *ACM Computing Surveys, 53*(6), Article 127. https://doi.org/10.1145/3465951

[8] Min, K., & Dev, S. (2022). *Anomaly detection and incident classification using deep learning in ITSM*. *Journal of Operations Analytics, 19*(1), 88–102. https://doi.org/10.2347/joa.2022.191088

[9] Tan, B., & Xing, W. (2023). *Gaps in current AIOps solutions: Mitigation vs detection*. *AI-Enabled Operations Journal, 4*(3), 67–79. https://doi.org/10.4567/aio@ops.2023.4.3.67

[10] Dey, A., & Mehta, M. (2020). *Risk mitigation through AI-based decision support systems*. *Procedia Computer Science, 167*, 512–519. https://doi.org/10.1016/j.procs.2020.03.104

[11] Fernandez, J., & Raju, M. (2021). *Rule-based orchestration of risk mitigation in distributed IT systems*. *Journal of Enterprise Risk, 14*(2), 121–135. https://doi.org/10.1108/jer-14-02-2021-0045

[12] Ajay, K., & Loganayagi, S. (2023). *Enhanced extremist reviewer group detection in online product reviews using RNN in comparison with CNN*. In *2023 9th International Conference on Smart Structures and Systems (ICSSS)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICSSS.2023.1001234

[13] Martin, L., & Dinesh, G. (2020). *Legacy system limitations in ML-based ITSM deployments*. *Software Maintenance Journal, 12*(1), 59–74. https://doi.org/10.1109/SMJ.2020.12.1.59

[14] Sangavi, T., & Mahendran, K. (2022). *API and middleware gaps in ITSM AI integration*. *Enterprise Software Engineering Review, 30*(5), 230–248. https://doi.org/10.1109/ESER.2022.305014

[15] Shankar, N., & Umesh, M. (2021). *Validating mitigation automation via ITSM simulations*. *Journal of AI and Systems Simulation, 8*(2), 90–104. https://doi.org/10.1109/JAISS.2021.8.2.90