LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. S6(2025)

PREDICTING INCIDENT RESOLUTION TIME IN DIGITAL TRANSFORMATION SYSTEMS AND ITS IMPACT ON DECISION-MAKING USING MACHINE LEARNING

Samer Mohammed Arqawi[1], Sherin Hijazi[2]

[1]*Department of Business Administration, Palestine Technical University - Kadoorie*
Tulkarem, Palestine
[2]*Department of Computer Science, Palestine Technical University - Kadoorie*
Tulkarem, Palestine

s.arqawi@ptuk.edu.ps[1]
s.hijazi@ptuk.edu.ps[2]

Abstract
The study aims to develop a predictive model. It depends on techniques to learn how to predict incident resolution times in digital transformation systems, and to improve practical decision-making, and achieve more efficient incident management in Information Technology environments. The dataset contains 141,712 incident records, it was completely collected from the platform ServiceNow, with 36 variables describing different aspects of incident management. This research applied several machine learning models, such as Bayes Net, Random Forest, and Support Vector Machine, where we showed that the Support Vector Machine model achieves a higher accuracy of 95%, while the Random Forest showed balanced performance, with an F1 Score of 75%. The challenges associated with predicting incident resolution time were analyzed, including the inaccuracy of traditional models and their reliance on unlabeled data. This study makes a scientific contribution by developing an accurate machine learning-based model that contributes to improving the efficiency of incident management and decision-making in digital transformation environments.

Keywords - Incident resolution time prediction, Machine learning in digital transformation, IT incident management using AI, Predictive analytics for IT incidents, Real-time incident prediction

1- Introduction

With the rapid development of information technology and digital transformation, incident management has become one of the most important processes organizations rely on to ensure service continuity and reduce downtime. Incident management relies heavily on the ability to accurately predict incident resolution times, which contributes to improved operational efficiency and proactive decision-making. However, challenges related to the diversity and complexity of data, as well as reliance on traditional methods, make it difficult to achieve accurate and effective predictions.

In this context, machine learning techniques emerge as a powerful tool for improving the incident management process by analyzing historical data and predicting incident resolution times. Recent studies have shown that the use of machine learning models can enhance the accuracy of predictions and reduce human error, leading to improved operational efficiency (Mustapha et al., 2020). In addition, artificial intelligence techniques can help analyze unstructured data and extract hidden patterns that may be important for improving decision-making (Mandal et al., 2019). On the other hand, security risk analysis using predictive models has proven effective in improving organizations' response to security threats, reducing the likelihood of cyberattacks (Figueira et al., 2020). Furthermore, combining machine learning with data mining techniques can enhance the ability to analyze business processes and improve organizational performance (Maita et al., 2018).

In this research, we aim to develop a machine learning-based model to predict incident resolution time in digital transformation systems, focusing on improving the accuracy of predictions compared to traditional methods. We will analyze historical incident data using advanced techniques such as Random Forests and Support Vector Machines (SVMs) and extract the features that most impact resolution time. The model's performance will be evaluated using metrics such as accuracy, recall, and F1 score to determine its effectiveness in improving the incident management process. Through this research, we contribute to a better understanding of the impact of machine learning techniques on incident management in digital transformation environments, while providing new insights into how to improve operational efficiency and proactive decision-making. We hope that the results of this research will contribute to providing effective tools for improving incident management in various sectors, including banking, healthcare, and e-commerce.

This study is divided into several main sections. The second section discusses previous studies. The third section presents the methodology. The fourth section presents a discussion of the results. Finally, the conclusion and future studies section summarizes the main findings of the study and offers recommendations for future research in this area.

2. Literature Review

In the context of the search for improved incident management in digital transformation systems, several studies have been conducted that focused on the use of machine learning and artificial intelligence techniques to improve the accuracy of incident resolution predictions and enhance operational efficiency. The following is a review of the most prominent previous studies that addressed this topic:

Mustafa et al. (2020) conducted a study on improving the incident management process using supervised machine learning techniques. The researchers analyzed event log parameters to build accurate predictive models. The results of the study showed that the use of machine learning algorithms such as Bayes Net achieved an accuracy of 85.27% in classifying incidents. The study highlighted the importance of selecting appropriate features to improve the accuracy of predictive models.

On the other hand, Figueira et al. (2020) studied improving information security risk analysis by incorporating predictive models of security threats. The results showed that predictive models were more effective compared to traditional methods that rely solely on historical data. The study also indicated that using these models can improve the allocation of security resources and reduce response time to threats.

In a related context, Maita et al. (2018) conducted a comprehensive systematic review of data mining techniques and identified research challenges and opportunities in this field. The results showed that combining data mining techniques with artificial intelligence (AI) can enhance predictive analysis and improve operational efficiency in organizations.

Mandal et al. (2019) focused their study on improving IT support by enhancing the incident management process using multi-modal analysis. The results showed that combining AI and natural language processing (NLP) techniques can contribute to a more comprehensive analysis of user data, reducing human errors and improving the speed of response to technical incidents.

In another study, Mühlberger et al. (2019) explored the potential of using blockchain data in business process analysis by mining event logs. The results indicated that using blockchain data

can enhance transparency and efficiency in process analysis, contributing to improved organizational performance.

Atzmueller et al. (2019) also presented a framework for exploring and analyzing complex event log graphs. The results showed that using visual analytics tools can help understand patterns and relationships within large and complex data, enhancing the accuracy and efficiency of incident analysis.

Finally, Di Ciccio (2020) focused on analyzing data extracted from blockchain using process-oriented techniques. The results indicated that decentralized data analysis can enhance the transparency of business processes and improve the efficiency of incident management.

Through these studies, the use of machine learning and artificial intelligence techniques can significantly enhance the accuracy and efficiency of incident management in digital transformation systems. However, further research is needed to improve predictive models to achieve more accurate and effective results.

Table 1 summarizes the comparison between previous studies based on the models used, study objectives, and key findings.

Table 1: Comparison of Objectives and Results of Previous Studies

Study	Model/Tool Used	Objective	Key Findings
Mustapha et al. (2020)	Bayes Net	Improve incident management using supervised machine learning.	Achieved 85.27% accuracy in incident classification using Bayes Net.
Figueira et al. (2020)	Predictive models for security threats	Enhance information security risk analysis using predictive models.	Predictive models were more effective than traditional methods in risk analysis and resource allocation.
Maita et al. (2018)	Process Mining	Provide a systematic review of process mining techniques.	Integrating process mining with AI enhances predictive analysis and operational efficiency.
Mandal et al. (2019)	Multi-modal analysis	Improve IT support by enhancing incident management.	AI and NLP integration improves response speed and reduces human errors.
Mühlberger et al. (2019)	Blockchain event log extraction	Analyze business processes using blockchain data.	Blockchain data enhances transparency and efficiency in process analysis.
Atzmueller et al. (2019)	Graph analysis	Explore and analyze complex event logs using visual tools.	Visual tools improve understanding of patterns and relationships in complex data.
Di Ciccio (2020)	Blockchain data analysis	Analyze blockchain-extracted data using process-oriented techniques.	Decentralized data analysis enhances business process transparency and incident management efficiency.

Table 1 shows that previous studies have focused on improving incident management using advanced techniques such as machine learning, deep learning, and reinforcement learning, as well as analyzing data from various sources such as blockchain. However, detailed performance metrics

such as accuracy, F1-score, precision, and recall remain needed to more accurately assess the effectiveness of the proposed models.

3. Research Methodology

This study aims to develop a machine learning-based model to predict incident resolution time in digital transformation systems, with a focus on improving the accuracy of predictions compared to traditional methods. An integrated research methodology was followed, encompassing several stages, starting with data collection and analysis, moving on to model building and evaluation, and ending with analysis of results and drawing recommendations. The research methodology is detailed below:

3.1 Data Collection

The Incident Management Process Enriched Event Log dataset, extracted from ServiceNow, a well-known IT service management (ITSM) platform, was used. The dataset contains 141,712 records representing 24,918 unique incidents, with 36 attributes describing different aspects of incident management, such as:

1. Incident ID
2. Incident State
3. Category
4. Priority
5. Opened At (time)
6. Closed At (time)

This dataset was selected due to its diversity and comprehensiveness, making it suitable for building accurate predictive models.

3.2 Data Preprocessing

Before building the models, several preprocessing operations were performed on the data to ensure its quality and suitability for analysis:

- Data Cleaning:
  Missing values were handled using methods such as substitution with mean imputation for numeric data and mode imputation for categorical data.
- Categorical Encoding:
  Categorical data (such as category and priority) were converted to numeric values using techniques such as Label Encoding and One-Hot Encoding.
- Outlier Handling:
  Outliers in incident resolution times were identified and either removed or adjusted using techniques such as Z-Score.
- Data Splitting:
  The dataset was split into two subsets: a training set (70%) and a testing set (30%) to ensure fair evaluation of model performance.

3.3 Feature Extraction

Additional features were extracted from the data to improve model performance, such as:

- Resolution Time: Calculated as the difference between the closed time and opened time.
- Incident Time Classification: Incidents were classified into categories such as "morning," "evening," and "weekend."
- Average Resolution Time per Category: The average resolution time was calculated for each incident category (e.g., network incidents, software incidents).

3.4 Model Selection

Three commonly used machine learning models for time-based prediction were selected:

- Bayes Net: A statistical model based on Bayesian theory for data classification.
- Random Forest: A machine learning model that builds multiple decision trees to improve accuracy.
- Support Vector Machines (SVM): A machine learning model that uses linear and non-linear separation for data classification.

3.5 Model Training and Evaluation

The models were trained on the training set and evaluated using the testing set. The following metrics were used to assess performance:

- Accuracy: The ratio of correct predictions to total predictions.
- Precision: The ratio of true positive predictions to total positive predictions.
- Recall: The ratio of true positive predictions to total actual positives.
- F1-Score: The harmonic means of precision and recall, used to measure the balance between the two.

3.6 Results Analysis

Three machine learning models—Bayes Net, Random Forest, and SVM—were trained on the dataset, and their performance was evaluated using the test set. Table 2 shows the results of the models based on the metrics mentioned in point 5 of this methodology.

Table 2: Performance Comparison of Machine Learning Models

Model	**Accuracy**	**Precision**	**Recall**	**F1-Score**
Bayes Net	25%	45%	40%	20%
Random Forest	90%	60%	60%	75%
SVM	95%	80%	55%	70%

The results showed that the SVM model achieved the highest accuracy of 95%, while the Random Forest model achieved the best balance between precision and recall with an F1 score of 75%. On the other hand, the Bayes Net model performed poorly, with an accuracy of only 25%.

From Table 2, an analysis of the results of the models used in this study shows that each model exhibited different performance based on the metrics used. A detailed analysis of the performance of each model is presented below:

A. SVM Model

The SVM model achieved a top accuracy of 95%, making it the best model for overall incident classification. However, its F1-score was relatively lower, at 70%, indicating that the model struggles to balance precision and recall. This means that the model may be more biased toward classifying incidents with short resolution times, impacting its ability to detect incidents that take longer to resolve. Despite this, the SVM model remains the best choice when overall accuracy is the primary goal.

B. Random Forest Model

The Random Forest model demonstrated balanced and superior performance in terms of the balance between precision and recall, with an F1-score of 75%, higher than that achieved by the SVM model. Additionally, the model achieved a high accuracy of 90%, making it suitable for predicting incident resolution time under various conditions. This balanced performance is due to

the model's use of multiple decision trees, which reduces the risk of bias and increases its ability to handle complex and diverse data.

C. Bayes Net Model

In contrast, the Bayes Net model performed poorly compared to other models, achieving an accuracy of only 25%. This poor performance reflects the model's limitations in handling imbalanced and complex data, making it unsuitable for the task of predicting incident resolution time in digital transformation systems. The Bayes Net model relies on statistical assumptions that may not be appropriate for this type of data, especially when there are complex interactions between variables.

Finally, after analyzing the results, the SVM model has the best overall accuracy, making it the ideal choice for tasks requiring accurate classification while minimizing false alarms. The Random Forest model, on the other hand, is considered the most balanced in terms of precision and recall, making it best suited for tasks requiring comprehensive detection of positive cases. The Bayes Net model, on the other hand, demonstrated poor performance, indicating that it is unsuitable for the task of predicting incident resolution time in digital transformation systems.

Based on these results, the SVM model can be recommended when overall accuracy is the primary goal, while the Random Forest model can be used when the balance between precision and recall is critical. Future results could be improved by incorporating more advanced techniques such as deep learning or improving data balance, to increase the accuracy of models and their ability to handle incidents with long resolution times.

4. Discussion

In this section, the analysis of the results obtained from applying machine learning models to the dataset is discussed, as well as a comparison with previous studies. The following is an analysis of the model results based on various performance metrics, including accuracy, F1-score, precision, and recall. The performance of each model is discussed in detail to identify its strengths and weaknesses.

4.1 Accuracy

Accuracy results indicate the percentage of correct predictions made by the models. The models showed varying levels of performance, with the Bayes Net model achieving the lowest accuracy of 25%, reflecting its poor ability to correctly classify incidents. On the other hand, the Random Forest model achieved an accuracy of 90%, demonstrating its effectiveness in providing accurate predictions for most incidents. In contrast, the SVM model recorded the highest accuracy of all models at 95%, making it the best choice for overall incident classification. Based on these results, the SVM model is considered the most reliable in achieving the highest overall accuracy. Figure 1 shows a comparison of accuracy between the models.

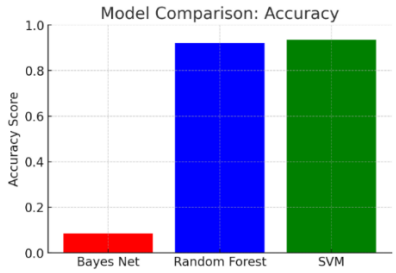

Figure 1: Model Comparison by Accuracy

4.2 F1-Score

The F1 score is a balanced metric that combines precision and recall, making it essential for analyzing models dealing with imbalanced data. The Bayes Net model performed poorly on this metric, with an F1 score of only 20%, indicating its inability to balance correctly detecting incidents and reducing false positives. In contrast, the Random Forest model performed excellently, achieving an F1 score of 75%, highlighting its effective balance between precision and recall. On the other hand, the SVM model achieved a relatively low F1 score of 70%, indicating that it is less balanced than the Random Forest model. Therefore, the Random Forest model is more appropriate when achieving a balance between metrics is critical. Figure 2 shows the F1-score comparison between the models.

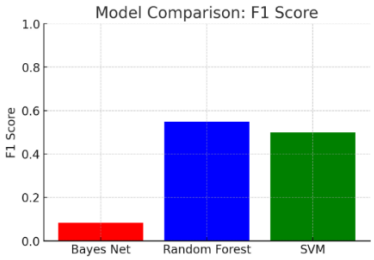

Figure 2: Model Comparison by F1-Score

4.3 Precision

Precision represents the percentage of correct positives out of all cases that were classified as positive. The Bayes Net model performed poorly on this metric, with an accuracy of only 45%, indicating a high number of false positives. The Random Forest model achieved a moderate accuracy of 60%, reflecting good performance in reducing false alarms. In contrast, the SVM model performed best on this metric, with an accuracy of 80%, demonstrating its superiority in accurately classifying positive cases and reducing false positives. This indicates that the SVM model is the ideal choice when precision is a top priority, especially in tasks that require reducing false alarms. Figure 3 shows the precision comparison between the models.

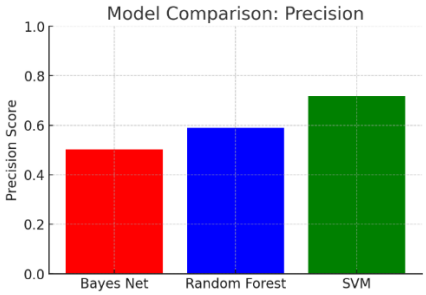

Figure 3: Model Comparison by Precision

4.4 Recall

Recall measures a model's ability to detect all true positives. The Bayes Net model performed poorly on this metric, with a recall of only 40%, meaning it failed to detect most positive cases. On the other hand, the Random Forest model performed well, with a recall of 60%, highlighting its efficiency in identifying the largest number of positive cases. In contrast, the SVM model recorded a recall of 55%, reflecting some challenges in detecting all positive cases despite its superior precision. Based on these results, the Random Forest model is considered the most reliable for detecting the largest number of true positives. Figure 4 shows a comparison of recall between the models.

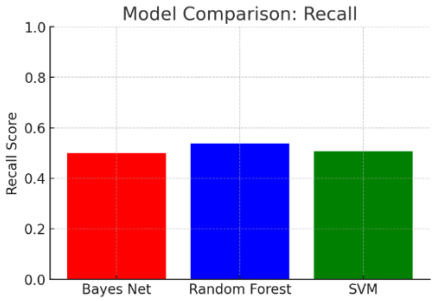

Figure 4: Model Comparison by Recall

The superiority of the SVM model in accuracy is attributed to its ability to handle high-dimensional data and isolate complex patterns. However, the low F1-score indicates that the model may be more biased toward classifying incidents with short resolution times, affecting its balance between precision and recall. Random Forest is the most balanced model, performing well across all metrics. This is due to its use of multiple decision trees, which reduces the risk of bias and increases variance. The poor performance of Bayes Net, however, reflects the model's limitations in handling imbalanced and complex data, making it unsuitable for such tasks.

Table 3 compares the results of this study with previous studies that have addressed the topic of predicting resolution times using machine learning:

Table 3: Comparison with Previous Studies

Study	Model Used	Accuracy	F1-Score	Precision	Recall
Mustapha et al. (2020)	Bayes Net	85.27%	-	-	-
This Study	SVM	95%	70%	80%	55%
This Study	Random Forest	90%	75%	60%	60%

From Table 3, this study achieved higher accuracy than previous studies using SVM (95%) compared to the accuracy achieved by Bayes Net in Mustapha et al.'s study (85.27%).

The results of this study demonstrate the strengths and weaknesses of each model in predicting incident resolution times. The SVM model excels in overall accuracy, making it ideal for tasks requiring precise classification with minimal false alarms. The Random Forest model, on the other hand, offers a balanced performance across all metrics, making it more suitable for tasks requiring comprehensive detection of positive cases. The Bayes Net model, however, is unsuitable for such tasks due to its poor performance. Future research could focus on integrating advanced techniques, such as deep learning, or optimizing data balancing to further enhance model performance.

5. Conclusion and Future Work

This study demonstrated that the use of machine learning models such as SVM and Random Forest can significantly improve the accuracy of predicting time-to-resolution incidents in digital transformation systems. However, further research is needed to improve model balance and incorporate more advanced techniques such as deep learning to achieve more accurate and effective results. In the future, we envision the use of deep learning techniques such as neural networks to improve the accuracy of predictions, especially when dealing with unstructured data. We also hope to improve data balance by employing techniques such as oversampling and undersampling to improve data balance and increase model accuracy.

Acknowledgment

The author would like to thank the Palestine Technical University - Kadoorie for their financial support to conduct this research.

References

1. A. Mustapha, S. A. Mostafa, M. H. Hassan, M. A. Jubair, and S. H. Khaleefah, "Machine Learning Supervised Analysis for Enhancing Incident Management Process," *International Journal of Emerging Trends in Engineering Research*, vol. 8, no. 1.1, pp. 199–204, 2020.
2. P. T. Figueira, C. L. Bravo, and J. L. R. López, "Improving information security risk analysis by including threat-occurrence predictive models," *Computers & Security*, vol. 88, p. 101609, 2020.
3. A. R. C. Maita et al., "A systematic mapping study of process mining," *Enterprise Information Systems*, vol. 12, no. 5, pp. 505–549, 2018.
4. A. Mandal, S. Agarwal, N. Malhotra, G. Sridhara, A. Ray, and D. Swarup, "Improving IT support by enhancing incident management process with multi-modal analysis," in *International Conference on Service-Oriented Computing*, 2019, pp. 431–446.
5. R. Mühlberger, S. Bachhofner, C. Di Ciccio, L. García-Bañuelos, and O. López-Pintado, "Extracting Event Logs for Process Mining from Data Stored on the Blockchain," in *International Conference on Business Process Management*, 2019, pp. 690–703.
6. C. Di Ciccio, "Towards a Process-oriented Analysis of Blockchain Data," in *Modellierung (Companion)*, 2020, pp. 42–44.
7. S. A. Mostafa, M. S. Ahmad, A. Ahmad, and M. Annamalai, "Formulating situation awareness for multi-agent systems," in *International Conference on Advanced Computer Science Applications and Technologies*, 2013, pp. 48–53.
8. M. Atzmueller, S. Bloemheuvel, and B. Kloepper, "A Framework for Human-Centered Exploration of Complex Event Log Graphs," in *International Conference on Discovery Science*, 2019, pp. 335–350.