Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14307
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Predicting IT Incident Duration using Machine Learning: A Case Study in IT Service Management

Resha Meiranadi Caturkusuma[1], Farrikh Alzami [2)*], Aris Nurhindarto [3], MY Teguh Sulistiyono[4], Candra Irawan[5], Yupie Kusumawati[6]

[1,2,,3,4,5,6]Information Systems, Universitas Dian Nuswantoro, Semarang, Indonesia

[1]reshameiranadi@gmail.com, [2]alzami@dsn.dinus.ac.id, [3]arisnurhindarto@dsn.dinus.ac.id, [4]teguh.sulistyono@dsn.dinus.ac.id, [5]candra@dsn.dinus.ac.id, [6]yupie@dsn.dinus.ac.id

Submitted :Dec 8, 2024 | **Accepted** : Dec 31, 2024 | **Published** : Jan 8, 2025

Abstract: In the digital era, ensuring customer satisfaction with IT services is crucial for business success. However, the complexity of IT infrastructure makes it difficult to manage services, requiring companies to focus on improving efficiency and reducing operational costs. One of the strategies used is Information Technology Service Management (ITSM), the main component of which is incident management, which aims to minimize service disruptions. While various studies on ITSM exist, research focused on Machine Learning models for predicting incident resolution times is relatively limited. This research aims to develop an incident resolution duration prediction model using a Random Forest Regressor-based regression approach. The dataset used is an event log from the ServiceNow system containing data on 24,918 incidents. This modeling step also includes the process of handling missing values, handling highly correlated features, and handling dependent features to ensure model robustness. The model was evaluated using the Mean Absolute Error (MAE), Root Mean Squared Error (RMSE), and R2 metrics, where the model achieved a MAE of 14.33 hours, RMSE of 69.8 hours, and R2 of 0.98. These results show that the model can provide accurate predictions and support better decision-making in IT incident handling. Time-related features, such as sys_update_month and closed_month, proved to be the most influential factors in predicting incident resolution duration.

Keywords: IT Service Management (ITSM); Incident Management; Duration Prediction; Random Forest Regressor; Machine Learning

INTRODUCTION

Customer satisfaction with IT services is essential for business success in today's digital era (Ntobongwana & Telukdarie, 2024). High-quality and responsive IT services can maintain customer loyalty and maintain company revenue (Agarwal & Dhingra, 2023; Khalid, 2024; Salamah et al., 2022). In the digital era, customers expect seamless service, and any disruptions or delays in IT services can lead to dissatisfaction and potential loss of business. However, the rapid evolution of IT infrastructure has introduced new challenges in managing IT services, as they have become more complex and diverse. This is particularly true in sectors such as B2B, where digital services are increasingly becoming essential components of business operations (Terpoorten et al., 2024). This condition requires companies to focus on maintaining the quality of their IT services through improving service efficiency while reducing operational costs.

In response to these challenges, one of the strategies that can be used to maintain the stability of corporate IT services is to adopt Information Technology Service Management (ITSM) (Widianto & Subriadi, 2022). ITSM provides a set of processes and best practices for planning, providing, and supporting efficient and effective IT services by its quality standards (Gunawan et al., 2024; Sarwar et al., 2023). As an example of its implementation, companies can use platforms such as ServiceNow that facilitate companies in planning, providing, and managing IT services more efficiently. The platform, developed in 2004, adheres to a platform-as-a-service (PaaS) system with the main focus on features related to IT service management that can be customized according to their IT services. This platform can help companies improve the quality of IT service management services by increasing the productivity and efficiency of their daily services (Santos & Rodrigues, 2024).

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14307
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Incident management is one of the main focuses of ITSM, which is to manage disruptions and minimize the impact of incidents on business services (Baptista & Barata, 2024). This management activity includes the process of incident detection, analysis, logging, resolution search, and incident closure (Palma et al., 2024). Incident management is not only limited to the duration of resolution but also includes the process of analyzing the leading cause to the process of preventing the recurrence of future disruptions. This indicates the critical role of incident management in ensuring the continuity of operations, maintaining user satisfaction, and minimizing potential losses due to incidents.

However, as IT infrastructure becomes more complex, the increasing complexity of incidents can be a significant challenge. If not handled properly, the incident resolution process can take a long time (Ali et al., 2021). In this case, it is essential to predict incident resolution time because it affects company decisions to Service Level Agreement (SLA) (Ahmed et al., 2023). Several companies still rely on traditional methods to predict the length of incident resolution, which is often inaccurate due to the many factors that influence it (Ahmed et al., 2023). For this reason, data-based approaches such as Machine Learning can be applied to obtain better solutions (Nikulin et al., 2021).

Several studies on incident management and ITSM have been conducted previously. One example is research related to implementing a compliance assessment system in the incident management process that helps auditors evaluate the level of process compliance with reference standards and prioritize incident resolution based on deviations that occur (Palma et al., 2024). However, research on developing Machine Learning models to predict IT incident resolution time is still relatively limited. Therefore, a regression approach will be used in this study to develop a prediction model for incident resolution duration in IT Service Management.

Regression approaches have been applied in various studies to predict the duration of traffic incidents, utilizing different machine learning algorithms. Among these, Random Forest has consistently demonstrated superior prediction accuracy to other models, such as Decision Trees and Linear Regression, due to its ability to handle large datasets and capture complex relationships between features (Ulu et al., 2024). Based on the results of that study, the Random Forest Regressor model is also used in this study to predict the duration of incident resolution. The dataset consists of event log data from an IT company, retrieved through the ServiceNow system, comprising 24,918 incident records with various time and incident-related attributes (Claudio Amaral, 2018). This research is expected to help companies accurately estimate the duration of incident resolution and improve operational efficiency. Additionally, the insights generated from this research can be used to support decision-making processes and foster more proactive incident management strategies.

LITERATURE REVIEW

Incident management is a crucial aspect of IT service management (ITSM), focusing on the systematic handling of incidents to restore normal service operation as swiftly as possible while minimizing disruption to business activities. The significance of effective incident management is underscored by its impact on service quality and customer satisfaction, which are vital for organizational success in today's competitive landscape.

A foundational element of incident management is the classification and prioritization of incidents. Ahmed et al. emphasize that traditional manual processes in incident management can lead to inefficiencies, such as misassigned tickets and prolonged resolution times, primarily due to human errors (Ahmed et al., 2023). This inefficiency highlights the need for improved methodologies and technologies to streamline incident management processes. The integration of automated systems, particularly those utilizing machine learning, has been shown to enhance the classification and routing of incidents. Nikulin et al. demonstrate that machine learning methods can significantly reduce response times and minimize errors associated with human intervention, thereby improving the overall efficiency of incident management systems (Nikulin et al., 2021).

One of the primary advantages of machine learning in incident management is its predictive capability. Kuleshov et al. highlight the potential of machine learning to predict incidents and reduce occupational risks in workplaces, particularly in high-risk industries such as oil and gas (Kuleshov et al., 2023). This is echoed by Ain (Zahrothul Ain & Safitri, 2023), who discusses innovative ML approaches for incident prioritization and resolution within ITIL frameworks, emphasizing the need for efficient decision-making support systems. Furthermore, research by Kurian et al. (Kurian et al., 2020) demonstrates the use of machine learning and keyword analysis to analyze incidents in oil sands operations, showcasing how predictive analytics can lead to a reduction in risks associated with operational hazards.

Furthermore, the adoption of ITSM frameworks, such as ITIL (Information Technology Infrastructure Library), provides a structured approach to incident management. Sarwar et al. discuss how a well-implemented ITSM delivery system can yield substantial benefits, particularly in the context of digital transformation within public sector organizations (Sarwar et al., 2023). By aligning incident management practices with ITIL guidelines, organizations can ensure that their processes are not only efficient but also responsive to the evolving needs of the business environment.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14307
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Moreover, the evaluation of IT service management practices is essential for continuous improvement. Widianto and Subriadi propose a comprehensive evaluation method based on content, context, and process approaches, which can help organizations assess their incident management effectiveness (Widianto & Subriadi, 2022). This evaluation is critical for identifying areas for improvement and ensuring that incident management processes align with organizational goals and customer expectations.

METHOD

Research Stages

The research flow used in this research includes the stages of problem understanding, data collection, Data Exploration, Feature Engineering, Exploratory Data Analysis (EDA), Data Preprocessing, Modeling, and Model Evaluation. The flow can be seen in the following flow diagram.

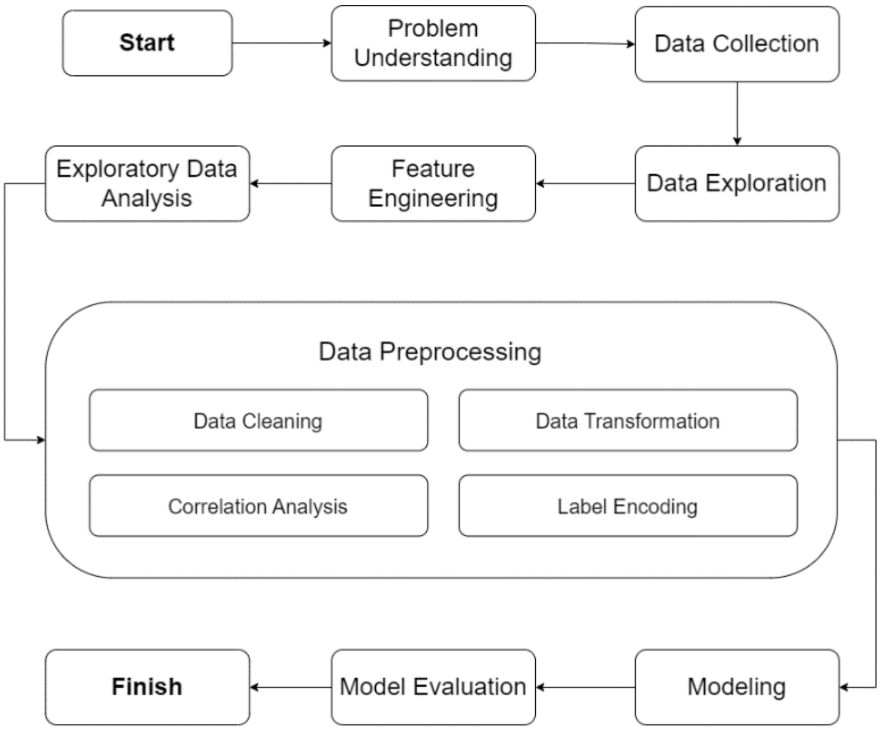

Fig. 1 Research Flow Diagram

Problem Undestanding

The first step in this study is problem understanding, which involves an in-depth understanding of the problem to be solved. This stage includes understanding the specifics of the problem, defining boundaries, and analyzing relevant data issues.

Data Collection

The next stage is data collection. In this study, the data used is taken from the UCI Machine Learning Repository public data site. The dataset is entitled Incident Management Process Enriched Event Log (Claudio Amaral, 2018).

Data Exploration

After data collection, the next step is data exploration to understand the dataset's characteristics. At this stage, an initial analysis is performed by displaying the data summary, the number of rows and columns, the type of data type, and the unique values of each column. This stage also includes identifying missing values to determine the completeness of the data to be used (Sadeghi et al., 2024).

Feature Engineering

After understanding the characteristics of the data, the next step is feature engineering to create new features or modify features to make them more relevant. This stage includes transforming attributes with time data type and creating incident resolution duration features (Verdonck et al., 2024).

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14307
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Exploratory Data Analysis (EDA)

The Exploratory Data Analysis (EDA) stage is conducted to further explore data patterns and distributions. At this stage, data visualizations such as histograms, boxplots, and scatterplots are used to analyze the relationship between specific variables (Sadeghi et al., 2024).

Data Preprocessing

The next stage is data preprocessing, which prepares the data before modeling. This stage includes data cleaning, data transformation, feature selection with correlation analysis, and label encoding (Luftensteiner et al., 2024).

a. Data Cleaning

Data cleaning is done to handle missing values in the data. One of the methods used by the author to address missing values is mode imputation, which enables the retention of all existing data points and prevents the loss of important information that could result from removing entire rows with missing entries (Erian et al., 2021).

b. Data Transformation

After the data is cleaned, a data transformation process is performed to change the data type still in objects to the actual data type such as datetime.

c. Correlation Analysis

Once the data has been transformed, it moves on to the correlation analysis process to select the features to be used in modeling. Utilizing a correlation matrix helps provide a clearer understanding of the relationships between features, facilitating the identification of critical features that are most relevant to the model (Das et al., 2022).

d. Label Encoding

The last step in the data preprocessing stage is converting categorical data to numerical data using a label encoder. The advantages of label encoders are in their simplicity and ability to retain information in the data well so that the model can be more effective in recognizing patterns and improving prediction accuracy. Label encoding improves regression accuracy by enabling binary classification algorithms, enhancing error correction, and supporting end-to-end training across various regression tasks and network architectures (Shah et al., 2022).

Modeling

The next stage is modeling the data. In this research, the method used is a regression with the Random Forest Regressor algorithm. Random Forest regressor is an ensemble learning algorithm combining decision trees to obtain higher accuracy. Random Forest works to vote classification and average regression (Zhang, 2024). The ensemble method itself is a technique that utilizes the training results of several models to improve accuracy and predictive ability (Polaganga & Liang, 2024). In the process of forming a decision tree, Random Forest has several Random Forest equation formulas, including:

1. Bootsrap sampling (1):

   D = {(x1,y1),(x2,y2),...,(xn,yn)} with n samples (1)

2. Random feature selection

   m ≪ M (for regression) for M is the number of features and m random features

3. Split function

   In regression, impurity is calculated using Mean Square Error with the following formula (2):

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2 \qquad (2)$$

where
n = number of samples in the tree
y_i = actual value of the target
$\hat{y}_i$ = predicted value of the target

The best feature selection is done by calculating the change in MSE value before and after division. The feature that provides the largest MSE reduction will be selected to split the data at that node.

The process ends with merging all the trained trees to obtain the average prediction of all the trees. The figure is obtained through the following equation (3) (Adewale et al., 2024):

$$\hat{y} = \frac{1}{t}\sum_{i=1}^{t}\hat{y}_i \qquad (3)$$

where
t = number of Random Forest trees formed
$\hat{y}_i$ = i-th tree prediction.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14307
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Model Evalutaion

The evaluation stage is interpreting the modeling results to see the model's performance (Kebede et al., 2024). The evaluation metrics used are Mean Absolute Error (MAE), Root Mean Square Error (RMSE), and R^2. MAE is used because it can provide an average description of the magnitude of the prediction error directly in original units, making it easy to interpret. RMSE was chosen because it is more sensitive to significant errors, which allows the model to be more penalized for highly skewed predictions. R^2 measures how well the model explains the variability of the data, indicating how well the model fits the observed data. MAE and RMSE are both used to measure the performance of a regression model through the following formula:

1. MAE Formula (4):

$$\text{MAE} = \frac{1}{n}\sum_{i=1}^{n}|y_i - \hat{y}_i| \qquad (4)$$

where
n = the number of data
y_i = the actual value
$\hat{y}_i$ = the predicted value
$|y_i - \hat{y}_i|$ = the absolute value of the difference between the predicted value and the true value.

2. RMSE Formula (5):

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2} \qquad (5)$$

where
n = the number of data
y_i = the actual value
$\hat{y}_i$ = the predicted value
$(y_i - \hat{y}_i)^2$ = the difference between the predicted value and the squared true value.

3. R-squared Formula (R^2) (6):

$$R^2 = 1 - \frac{SSres}{SStot} \qquad (6)$$

Where Ssres (Residual Sum of Squares) is the sum of the squares of the difference between the actual value and the predicted value (7):

$$SSres = \sum_{i=1}^{n}(y_i - \hat{y}_i)^2 \qquad (7)$$

Moreover, Sstot (Total Sum of Squares) is the sum of the squares of the difference between the true value and the average true value (8):

$$SStot = \sum_{i=1}^{n}(y_i - \bar{y})^2 \qquad (8)$$

where
y_i = the actual value of the dependent variable for the ith observation.
$\hat{y}_i$ = the predicted value of the dependent variable for the ith observation.
$\bar{y}$ = the average true value.
n = the number of data.
While the R value2 measures how well the regression model explains variations in actual data.
R2 = 1 this model is perfect (100% accurate prediction).
R2 = 0 model explains no variation at all.

RESULT

Data collection is done by taking a public dataset from the UCI Machine Learning Repository with the title Incident Management Process Enriched Event Log. This data is the result of an audit of a ServiceNow platform in an IT Company in the form of an event log. The dataset consists of 141,712 rows representing 24,918 different incidents. It includes 36 attributes with information related to incident handling, such as time of occurrence, incident category, priority, resolution status, etc. Each attribute in this dataset has been anonymized to maintain data confidentiality and privacy.

In this dataset, each row represents a unique incident with an identifier feature labeled as 'number,' which serves as a key to track individual incidents. Additionally, the dataset includes 1 feature related to the status of the incident named 'incident_state'. Thirty-two descriptive features provide further details about each incident, and 2 dependent features, namely 'closed_at' and 'resolved_at,' indicate when the incident was officially resolved and closed. During the exploration stage, it was observed that the dataset contains several missing values. These missing values were represented by the symbol '?', which is commonly used as a placeholder. To handle this issue, the '?' symbols were

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14307
e-ISSN : 2541-2019
p-ISSN : 2541-044X

converted into NaN (Not a Number) to facilitate proper handling during the data cleaning process. The following is a description of each feature that can be seen in the table 1.

Table 1 Attributes incident management

No	Column Name	Data Type	Description
1	number	object	incident identifier
2	incident_state	object	eight levels controlling the incident management process transitions from opening until closing the case
3	active	bool	boolean attribute that shows whether the record is active or closed/canceled
4	reassignment_count	int64	number of times the incident has the group or the support analysts changed
5	reopen_count	int64	number of times the incident resolution was rejected by the caller
6	sys_mod_count	int64	number of incident updates until that moment
7	made_sla	bool	boolean attribute that shows whether the incident exceeded the target SLA
8	*caller_id*	object	identifier of the user affected
9	*opened_by*	object	identifier of the user who reported the incident
10	opened_at	object	incident user opening date and time
11	*sys_created_by*	object	identifier of the user who registered the incident
12	*sys_created_at*	object	incident system creation date and time
13	sys_updated_by	object	identifier of the user who updated the incident and generated the current log record
14	sys_updated_at	object	incident system update date and time
15	contact_type	object	categorical attribute that shows by what means the incident was reported
16	*location*	object	identifier of the location of the place affected
17	*category*	object	first-level description of the affected service
18	*subcategory*	object	second-level description of the affected service
19	*u_symptom*	object	description of the user perception about service availability
20	*cmdb_ci*	object	identifier used to report the affected item
21	impact	object	description of the impact caused by the incident
22	urgency	object	description of the urgency informed by the user for the incident resolution
23	priority	object	calculated by the system based on 'impact' and 'urgency'
24	*assignment_group*	object	identifier of the support group in charge of the incident
25	*assigned_to*	object	identifier of the user in charge of the incident
26	knowledge	bool	boolean attribute that shows whether a knowledge base document was used to resolve the incident
27	u_priority_confirmation	bool	boolean attribute that shows whether the priority field has been double-checked
28	notify	object	categorical attribute that shows whether notifications were generated for the incident
29	problem_id	object	identifier of the problem associated with the incident
30	rfc	object	identifier of the change request associated with the incident
31	*vendor*	object	identifier of the vendor in charge of the incident
32	*caused_by*	object	identifier of the RFC responsible by the incident
33	*close_code*	object	identifier of the resolution of the incident
34	*resolved_by*	object	identifier of the user who resolved the incident
35	*resolved_at*	object	incident user resolution date and time
36	closed_at	object	incident user close date and time

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14307
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Each incident has several events with different incident states. The following table is sample data from incident number INC0000045 which can be seen in table 2.

Table 2 Incident Status

Number	Incident-state	....	Resolved-at	Closed-at
INC0000045	New	....	29/2/2016 11:29	5/3/2016 12:00
INC0000045	Resolved	....	29/2/2016 11:29	5/3/2016 12:00
INC0000045	Resolved	....	29/2/2016 11:29	5/3/2016 12:00
INC0000045	Closed	....	29/2/2016 11:29	5/3/2016 12:00

This modeling aims to determine the completion duration of each incident, so the data is simplified by selecting one event row with a certain status that represents each incident. This approach is intended so that the development of the model can be balanced without any bias or imbalance of data on specific incidents. The selected event row has an incident state of closed, indicating that this incident has been handled. This selection is also based on the fact that all incidents in this dataset have a closed status so that all incidents can be included in the modeling process.

After the closed dataset is prepared, the next step is to perform feature engineering on the duration feature. This feature is created by taking the difference between the 'closed_at' column value and the 'opened_at' column value. For this purpose, the 'closed_at' and 'opened_at' columns must first be converted to a datetime data type. The following is a sample duration of 5 incidents that can be seen in the table 3.

Table 3 Sample duration of 5 incidents

Number	Duration
INC0000045	5 days 10:44:00
INC0000047	6 days 05:20:00
INC0000057	5 days 20:50:00
INC0000060	7 days 06:22:00
INC0000062	5 days 09:02:00

The stage continues to Exploratory Data Analysis (EDA) by visualizing key features to extract meaningful insights and better understand the features and the target variable. In this study, a histogram illustrates the distribution of the target variable, incident duration, in hours. The following is a histogram visualization of the target duration distribution in hours.

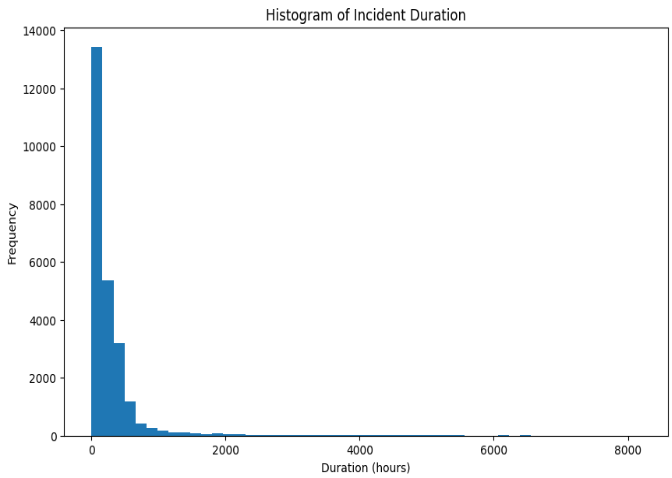

Fig. 2 Distribution of target duration

Figure 2 shows that the duration of IT incidents ranges from 0 hours to 8,000 hours, with most incidents being resolved within 1 hour. Specifically, the shortest incident duration recorded is 2 minutes, while the longest spans 341 days. This wide range indicates significant variability in incidents' complexity and resolution time, which several factors can influence. Additionally, there are nine incidents with a recorded duration of 0 hours, indicating errors or inconsistencies in data recording. These entries will be removed to ensure the accuracy and reliability of the model.

*name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

Besides analyzing the target feature (incident duration), visualizations were created for other key features, such as made_sla, impact, and priority, based on the assumption that these features will likely significantly influence the incident resolution process. These features were chosen as they are expected to provide valuable insights into the factors affecting resolution times, helping to guide the development of a more accurate and robust machine learning model. The following Figure 3 is a bar chart of the three features.

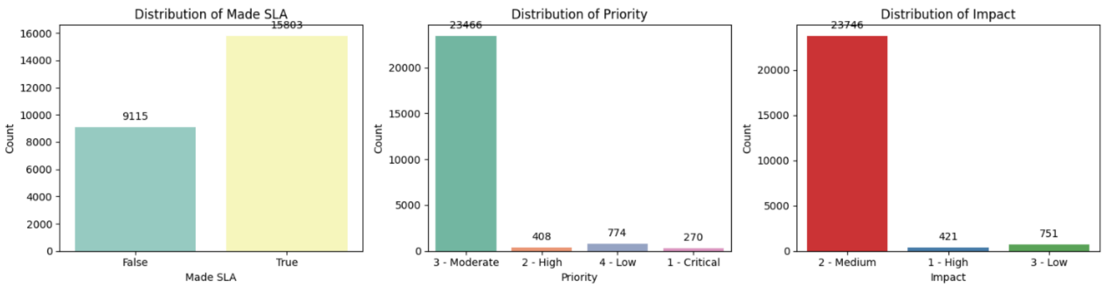

Fig. 2 Bar chart of the three features

The figure 3 indicates an imbalanced distribution across the three features. For the made_sla feature, most incidents have a True value, indicating that most incidents met the Service Level Agreement (SLA), while a smaller portion did not (False). In the priority feature, the distribution is heavily skewed towards the Moderate category, accounting for 23,466 incidents, followed by Low, High, and Critical priorities. Similarly, in the impact feature, the Medium category dominates with 23,746 incidents, followed by Low and High. These imbalances suggest that incidents are predominantly moderate in both priority and impact, which could reflect the general nature of the incidents being managed.

The dataset is then prepared for modeling through the data preprocessing stage. The data cleaning process starts by checking for missing values in the dataset. In this dataset, 18 features have missing values, including caller_id (3 records), opened_by (417 records), sys_created_by (11495 records), sys_created_at (11495 records), location (6 records), category (7 records), subcategory (8 records), u_symptom (5839 records), cmdb_ci (24864 records), assignment_group (2157 records), assigned_to (725 records), problem_id (24538 records), rfc (24742 records), vendor (24903 records), caused_by (24915 records), closed_code (107 records), resolved_by (99 records), and resolved_at (99 records). Features with missing values such as 'cmdb_ci', 'problem_id', 'rfc', 'vendor', 'caused_by' were removed. Categorical features such as 'caller_id', 'closed_code', 'location', and similar features were handled by mode filling. Time-related features are filled with values in similar columns such as 'opened_at' and 'closed_at'. The rest are filled with unknown values.

The next step in the process was transforming the dataset by splitting all features with a datetime data type into more granular components. All features such as 'sys_created_at', 'opened_at', 'sys_updated_at', 'resolved_at', and 'closed_at' were decomposed into year, month, day, weekday, and hour components, respectively. This is followed by removing features not used in the modeling process such as 'number', 'sys_mod_count', 'incident_state', 'active'. The data preprocessing stage concluded with label encoding on categorical variables using a label encoder to ensure the data was properly formatted for machine learning algorithms.

The modeling begins by splitting the dataset into training and testing sets using an 80% training and 20% testing split. The model training process uses the Random Forest Regressor with the random_state parameter = 42. The evaluation matrix used in this training is MAE and RMSE, where the model produces a MAE of 14.33 hours (0.63 days) and a RMSE of 69.8 hours (2.84 days). The model also produced an R2 of 0.98. Table 4 provides evidence that the model has a very strong predictive ability.

Table 4 Predictive evalutation

Evaluation Matrix	Value
MAE	14.33 hours
RMSE	69.8 hours
R2	0.98

DISCUSSIONS

To find out what features affect the model, Random Forest Regressor provides the features_importance function to print the importance of each feature to the model. In this study, as seen in Figure 4, the most influential feature in the regression model is the sys_updated_month feature, followed by the closed_month, made_sla, sys_created_month, opened_month, resolved_month features, and followed by other features. These results show that time variables such as month play an essential role in the prediction process of incident resolution duration.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14307

e-ISSN : 2541-2019
p-ISSN : 2541-044X

The dominance of these variables indicates that incident processing time is strongly influenced by monthly trends, which organizational work patterns can cause monthly SLA policies.

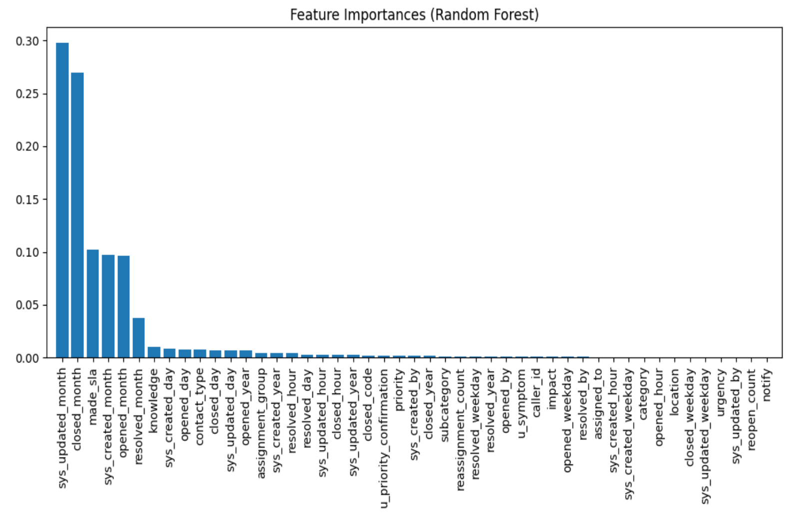

Fig. 4 Feature importances

Model Performance Analysis

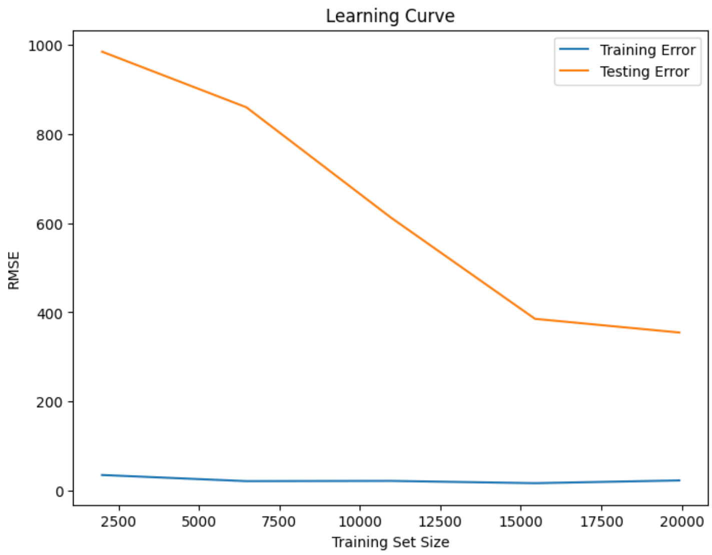

Fig. 5 Learning curves

The learning curve graph in Figure 5 shows that the Random Forest Regressor model has performed well. The training error decreases as the size of the training data increases, indicating that the model is able to learn the patterns in the data well. The testing error also stabilizes after a specific training data size, indicating that the model does not experience significant overfitting.

The Random Forest Regressor model demonstrated exceptional predictive capability with an R^2 score of 0.98, indicating that it explains 98% of the variance in incident duration. The MAE of 14.33 hours suggests that, on average, predictions deviate by less than one day from actual resolution times. While the RMSE of 69.8 hours is higher than the MAE, this difference indicates the presence of some outlier predictions, possibly for complex incidents with unusually long resolution times. This robust performance can be attributed to Random Forest's ability to handle non-linear relationships and capture complex interactions between features.

Temporal Feature Dominance

The feature importance analysis revealed a significant finding: temporal features, particularly monthly indicators, are the most crucial predictors of incident resolution duration. This dominance of temporal features can be explained by several factors:

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14307
e-ISSN : 2541-2019
p-ISSN : 2541-044X

1. Organizational Patterns: Monthly trends in incident resolution may reflect organizational work cycles, resource allocation patterns, and service delivery schedules.
2. SLA Compliance: The high importance of 'made_sla' suggests that organizational SLA policies significantly influence resolution times.
3. Seasonal Effects: Monthly variables might capture seasonal variations in incident volumes and complexity, affecting resolution durations.

Operational Implications

The findings have several important implications for IT service management:

1. **Resource Planning**: The strong influence of temporal features suggests the need for dynamic resource allocation based on monthly patterns.; Organizations can better predict staffing requirements by understanding these temporal patterns.
2. **SLA Management**: The significant impact of 'made_sla' on prediction accuracy indicates the effectiveness of current SLA policies.; Organizations can use this insight to refine their SLA definitions and monitoring processes.
3. **Process Optimization**: The model's ability to predict resolution times accurately can help in Proactive incident management, better communication with stakeholders, more efficient resource allocation; The identification of key predictive features can guide process improvement efforts

Model Learning Behavior Analysis

The learning curve characteristics provide valuable insights into the model's behavior and reliability:

1. **Training-Testing Convergence**: The decreasing training error with stable testing error indicates optimal model complexity; The convergence pattern suggests that the model has Sufficient training data, Good generalization capability, Balanced bias-variance trade-off; The stability of testing error demonstrates the model's robustness across different data subsets
2. **Data Volume Implications**: The learning curve stabilization suggests that The current dataset size is adequate for reliable predictions; Additional data might yield diminishing returns in model performance; The model has captured the underlying patterns effectively.

Business Value and Practical Applications

In matter of Predictive Capabilities, the model's high accuracy ($R^2 = 0.98$) enables Reliable estimation of incident resolution times, better management of customer expectations, more effective prioritization of incidents. Then, the 14.33-hour MAE provides a practical margin for operational planning.

In matter of Strategic Benefits, the model provides enhanced resource management which is more accurate capacity planning, improved workforce scheduling, better allocation of technical expertise. The Model also provides Customer Experience Improvement which is more accurate communication of resolution times, proactive management of high-risk incidents, better alignment with service level agreements.

Model Limitations and Challenges

Here, we provide the challenges as follows:

1. Data Representation Challenges in Categorical Feature Encoding: The use of label encoding might not fully capture the ordinal relationships between categories, and Complex interactions between categorical variables might be partially lost.
2. Data Representation Challenges in Time-Based Feature Engineering: The current monthly aggregation might miss finer temporal patterns, and Daily or hourly patterns could provide additional predictive value.
3. Operational Considerations in Real-Time Implementation: The model's performance in real-time scenarios needs further validation, and Dynamic feature updates might affect prediction accuracy
4. Operational Considerations in System Integration: Integration with existing ITSM tools requires additional development, and Real-time feature extraction might pose technical challenges.

Future Reseach directions could follows several approaches:

1. Advanced Feature Engineering, such as Investigation of interaction effects between features, Development of more sophisticated temporal features, Incorporation of text analysis from incident descriptions
2. Algorithm Exploration, such as Comparison with deep learning approaches, Implementation of hybrid models combining different algorithms
3. Automated Decision Support, such as Real-time SLA risk assessment, Integration with resource allocation systems
4. Predictive Analytics Extension, such as Early warning systems for potential delays, Prevention of SLA violations and Incident complexity assessment

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14307
e-ISSN : 2541-2019
p-ISSN : 2541-044X

CONCLUSION

Based on the time duration prediction model developed in this study, it can be concluded that the Random Forest Regressor model has achieved excellent prediction performance in predicting the duration of incident resolution in IT service management. The evaluation results indicate a MAE of 14.33 hours, a RMSE of 69.8 hours, and an R2 score of 0.98, reflecting the model's ability to make highly accurate predictions. These accurate time predictions support decision-making processes, especially in managing service-level agreements (SLAs) and improving operational efficiency. The feature importance analysis further highlights that time-related variables, such as sys_updated_month, closed_month, sys_created_month, and resolved_month, significantly influence the duration of incident resolution. This finding underscores the criticality of temporal factors in determining how quickly incidents are resolved.

This study offers valuable practical insights for organizations aiming to enhance their IT Service Management through the integration of predictive models into their IT systems. By utilizing these models, companies can streamline decision-making processes by prioritizing incident resolutions based on predicted resolution durations. This approach enables organizations to allocate resources more efficiently while maintaining adherence to Service Level Agreements (SLAs).

However, this study does have some limitations. The dataset used comes from a single IT company's event logs, which may restrict the model's generalizability to other industries or IT environments with different incident management processes. Future research should consider incorporating datasets from various companies and IT infrastructures to enhance the model's robustness and applicability. Additionally, exploring other advanced machine learning algorithms, such as Gradient Boosting or deep learning models, could improve predictive accuracy and adaptability to more complex IT environments.

REFERENCES

Adewale, M. D., Ebem, D. U., Awodele, O., Sambo-Magaji, A., Aggrey, E. M., Okechalu, E. A., Donatus, R. E., Olayanju, K. A., Owolabi, A. F., Oju, J. U., Ubadike, O. C., Otu, G. A., Muhammed, U. I., Danjuma, O. R., & Oluyide, O. P. (2024). Predicting gross domestic product using the ensemble machine learning method. *Systems and Soft Computing*, *6*, 200132. https://doi.org/10.1016/j.sasc.2024.200132

Agarwal, R., & Dhingra, S. (2023). Factors influencing cloud service quality and their relationship with customer satisfaction and loyalty. *Heliyon*, *9*(4), e15177. https://doi.org/10.1016/j.heliyon.2023.e15177

Ahmed, S., Singh, M., Doherty, B., Ramlan, E., Harkin, K., Bucholc, M., & Coyle, D. (2023). An Empirical Analysis of State-of-Art Classification Models in an IT Incident Severity Prediction Framework. *Applied Sciences*, *13*(6), 3843. https://doi.org/10.3390/app13063843

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance. *Applied Sciences*, *11*(8), 3383. https://doi.org/10.3390/app11083383

Baptista, B., & Barata, J. (2024). Continuously Improving IT Service Management in the Pharmaceutical Industry. *Procedia Computer Science*, *239*, 923–930. https://doi.org/10.1016/j.procs.2024.06.253

Claudio Amaral, M. F. (2018). *Incident* management *process enriched event log* [Dataset]. UCI Machine Learning Repository. https://doi.org/10.24432/C57S4H

Das, R., Kasieczka, G., & Shih, D. (2022). *Feature Selection with Distance Correlation* (No. arXiv:2212.00046). arXiv. http://arxiv.org/abs/2212.00046

Erian, K. H., Regalado, P. H., & Conrad, J. M. (2021). Missing data handling for machine learning models. *IAES International Journal of Robotics and Automation (IJRA)*, *10*(2), 123. https://doi.org/10.11591/ijra.v10i2.pp123-132

Gunawan, H., Irianto, A. B. P., & Negara, J. G. P. (2024). IMPLEMENTATION OF SUSTAINABLE SERVICE IMPROVEMENT IN ORGANIZATIONS USING FRAMEWORK INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL). *Procedia Computer Science*, *234*, 748–755. https://doi.org/10.1016/j.procs.2024.03.061

Kebede, Y. B., Yang, M.-D., & Huang, C.-W. (2024). Real-time pavement temperature prediction through ensemble machine learning. *Engineering Applications of Artificial Intelligence*, *135*, 108870. https://doi.org/10.1016/j.engappai.2024.108870

Khalid, B. (2024). Evaluating customer perspectives on omnichannel shopping satisfaction in the fashion retail sector. *Heliyon*, *10*(16), e36027. https://doi.org/10.1016/j.heliyon.2024.e36027

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14307
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Kuleshov, V. V., Aygumov, T. G., Zolkin, A. L., Tychkov, A. S., & Bityutskiy, A. S. (2023). Use of machine learning for prevention of incidents and reduction of occupational risks at the workplace. In A. Gibadullin & G. Khalmatjanova (Eds.), *International Conference on Digital Transformation: Informatics, Economics, and Education (DTIEE2023)* (p. 6). SPIE. https://doi.org/10.1117/12.2680682

Kurian, D., Sattari, F., Lefsrud, L., & Ma, Y. (2020). Using machine learning and keyword analysis to analyze incidents and reduce risk in oil sands operations. *Safety Science*, *130*, 104873. https://doi.org/10.1016/j.ssci.2020.104873

Luftensteiner, S., Chasparis, G. C., & Küng, J. (2024). PAS - A Feature Selection Process Definition for Industrial Settings. *Procedia Computer* Science, *232*, 308–316. https://doi.org/10.1016/j.procs.2024.01.030

Nikulin, V., Shibaikin, S. D., & Vishnyakov, A. N. (2021). Application of machine learning methods for automated classification and routing in ITIL. *Journal of Physics: Conference Series*, *2091*(1), 012041. https://doi.org/10.1088/1742-6596/2091/1/012041

Ntobongwana, L., & Telukdarie, A. (2024). A critical review of global best practices elements in digital technologies: Advancing a theoretical architecture for quality engineering. *Journal of Industrial Information Integration*, *41*, 100665. https://doi.org/10.1016/j.jii.2024.100665

Palma, A., Acitelli, G., Marrella, A., Bonomi, S., & Angelini, M. (2024). A compliance assessment system for Incident Management process. *Computers & Security*, *146*, 104070. https://doi.org/10.1016/j.cose.2024.104070

Polaganga, R. K., & Liang, Q. (2024). Ensemble prediction of RRC session duration in real-world NR/LTE networks. *Machine Learning with Applications*, *17*, 100564. https://doi.org/10.1016/j.mlwa.2024.100564

Sadeghi, B., Molayemat, H., & Pawlowsky-Glahn, V. (2024). How to choose a proper representation of compositional data for mineral exploration? *Journal of Geochemical Exploration*, *259*, 107425. https://doi.org/10.1016/j.gexplo.2024.107425

Salamah, A. A., Hassan, S., Aljaafreh, A., Zabadi, W. A., AlQudah, M. A., Hayat, N., Al Mamun, A., & Kanesan, T. (2022). Customer retention through service quality and satisfaction: Using hybrid SEM-neural network analysis approach. *Heliyon*, *8*(9), e10570. https://doi.org/10.1016/j.heliyon.2022.e10570

Santos, S. B. M. G., & Rodrigues, N. J. P. (2024). ServiceNow: Implications and Practice within the Business Environment. *Procedia Computer Science*, *239*, 11–18. https://doi.org/10.1016/j.procs.2024.06.140

Sarwar, M. I., Abbas, Q., Alyas, T., Alzahrani, A., Alghamdi, T., & Alsaawy, Y. (2023). Digital Transformation of Public Sector Governance With IT Service Management–A Pilot Study. *IEEE Access*, *11*, 6490–6512. https://doi.org/10.1109/ACCESS.2023.3237550

Shah, D., Xue, Z. Y., & Aamodt, T. M. (2022). *Label Encoding for Regression Networks* (No. arXiv:2212.01927). arXiv. http://arxiv.org/abs/2212.01927

Terpoorten, C., Klein, J. F., & Merfeld, K. (2024). Understanding B2B customer journeys for complex digital services: The case of cloud computing. *Industrial Marketing Management*, *119*, 178–192. https://doi.org/10.1016/j.indmarman.2024.04.011

Ulu, M., Türkan, Y. S., Mengüç, K., Namlı, E., & Küçükdeniz, T. (2024). Dynamic Forecasting of Traffic Event Duration in Istanbul: A Classification Approach with Real-Time Data Integration. *Computers, Materials & Continua*, *80*(2), 2259–2281. https://doi.org/10.32604/cmc.2024.052323

Verdonck, T., Baesens, B., Óskarsdóttir, M., & Vanden Broucke, S. (2024). Special issue on feature engineering editorial. *Machine Learning*, *113*(7), 3917–3928. https://doi.org/10.1007/s10994-021-06042-2

Widianto, A., & Subriadi, A. P. (2022). IT service management evaluation method based on content, context, and process approach: A literature review. *Procedia Computer Science*, *197*, 410–419. https://doi.org/10.1016/j.procs.2021.12.157

Zahrothul Ain, A. A., & Safitri, C. (2023). Enhancing ITIL Incident Management: Innovative Machine Learning Approaches for Efficient Incident Prioritization and Resolution. *JURNAL TEKNIK INFORMATIKA*, *16*(2), 204–214. https://doi.org/10.15408/jti.v16i2.31439

Zhang, J. (2024). Impact of an improved random forest-based financial management model on the effectiveness of corporate sustainability decisions. *Systems and Soft Computing*, *6*, 200102. https://doi.org/10.1016/j.sasc.2024.200102

*name of corresponding author