Enhance Telecommunication Security Through the Integration of Support Vector Machines

Agus Tedyyana[1], Adi Affandi Ahmad[2*], Mohd Rushdi Idrus[3], Ahmad Hanis Mohd Shabli[4], Mohamad Amir Abu Seman[5], Osman Ghazali [6], Jaroji[7], Abd Hadi Abd Razak[8]

Department of Informatic Engineering, Politeknik Negeri Bengkalis, Bengkalis, Riau, Indonesia[1, 7]
School of Computing, Universiti Utara Malaysia, Kedah, Malaysia[2, 3, 4, 6]
Institute for Advanced and Smart Digital Opportunities (IASDO), Universiti Utara Malaysia, Kedah, Malaysia[3, 6]
School of Creative Industry Management and Performing Arts, Universiti Utara Malaysia, Kedah, Malaysia[5]
School of Multimedia Technology and Communication, Universiti Utara Malaysia, Kedah, Malaysia[8]

***Abstract*—This research investigates the escalating issue of telephone-based fraud in Indonesia, a consequence of enhanced connectivity and technological advancements. As the telecommunications sector expands, it faces increased threats from sophisticated criminal activities, notably voice call fraud, which leads to significant financial losses and diminishes trust in digital systems. This study presents a novel security system that leverages the capabilities of Support Vector Machines (SVM) for the advanced classification of complex patterns inherent in fraudulent activities. By integrating SVM algorithms, this system aims to effectively process and analyze large volumes of data to identify and prevent fraudulent acts. The utilization of SVM in our proposed framework represents a significant strategy to combat the adaptive and evolving tactics of cybercriminals, thereby bolstering the resilience of telecommunications infrastructure. Upon further refinement, the system exhibited a substantial improvement in identifying fraudulent activities, with accuracy rates increasing from 81% to 86%. This enhancement underscores the system's efficacy in real-world scenarios. Our research underscores the critical need to marry technological innovations with ethical and privacy considerations, highlighting the role of public awareness and education in augmenting security measures. The development of this SVM-based security system constitutes a pivotal step towards reinforcing Indonesia's telecommunications infrastructure, contributing to the national objective of securing the digital economy and fostering a robust digital ecosystem. By addressing current and future cyber threats, this approach exemplifies Indonesia's commitment to leveraging technology for societal welfare, ensuring a secure and prosperous digital future for its citizens.**

Keywords*—Call security system; artificial intelligence; support vector machine; data analysis; fraud detection system

I. Introduction

In an era where digital transformation shapes every aspect of society, Indonesia, like many countries worldwide, is witnessing unprecedented growth in telecommunication technology. This growth has catalyzed numerous advancements, transforming how people communicate and access information [1]. The proliferation of the Internet and mobile technology has not only fostered enhanced connectivity and accessibility but has also opened new avenues for economic and social development. Yet, alongside these benefits, a shadow of cybersecurity threats looms large, presenting complex challenges that undermine the integrity of digital systems and erode public trust in technological advancements, Among these challenges, telephone-based crimes such as fraud, phishing, identity theft, and various sophisticated schemes leveraging the anonymity and reach of telecommunication networks have surged. These criminal activities represent a significant risk to individuals and organizations, resulting in substantial financial losses and breaches of privacy. In response, the security community has been in a relentless pursuit of more effective methods to safeguard digital communications and maintain trust in telecommunication infrastructures.

This paper introduces an innovative approach to enhancing telecommunication security by integrating Support Vector Machines (SVM) [2]. a cutting-edge machine learning algorithm renowned for its precision in pattern recognition and classification. SVM's capabilities in analyzing and classifying complex data patterns make it an invaluable tool in the detection and prevention of telecommunication fraud [3]. By leveraging historical data, SVM algorithms adapt and evolve, continuously improving their ability to identify fraudulent activities. This dynamic adaptation is crucial for countering the ever-changing tactics deployed by cybercriminals [4], [5]. The decision to focus on SVM in this context stems from its proven track record in various domains, including but not limited to image recognition, text classification, and bioinformatics, where it has shown remarkable success in handling high-dimensional data [6], Its application in telecommunication security is driven by the algorithm's ability to efficiently process vast amounts of call data, recognize intricate patterns, and distinguish between legitimate and malicious communications with high accuracy. Furthermore, the integration of SVM into telecommunication systems aligns with Indonesia's strategic goals of advancing its digital infrastructure and enhancing national cybersecurity measures.

However, the integration of such advanced technologies also raises critical considerations regarding privacy and ethical usage [7], [8]. It is imperative to balance the drive for security with the need to protect individual rights, ensuring that these technological solutions do not infringe upon privacy or lead to unwarranted surveillance. This paper discusses the ethical implications of deploying SVM in telecommunication security, advocating for a responsible approach that prioritizes the protection of individual privacy while effectively

*Corresponding Author

countering cyber threats [9]. Additionally, the success of SVM-based security systems depends significantly on public awareness and cooperation. Educating the populace about the nuances of telephone fraud, the importance of security measures, and the role of advanced technologies in safeguarding communications is essential for maximizing the effectiveness of these systems. Public education campaigns can empower individuals with the knowledge to recognize and avoid potential threats, complementing the technological solutions implemented at the infrastructure level [10]. The integration of SVM into telecommunication security represents a significant step forward in the ongoing battle against cybercrime. This paper outlines the development, implementation, and potential impact of SVM-based security systems, providing a comprehensive analysis of their effectiveness in enhancing the resilience of telecommunication networks against fraud. It also explores the future of telecommunications security, examining how evolving technologies and strategies can further fortify digital communications against emerging threats [11].

Moreover, public awareness and education are crucial in the fight against telephone-based crimes [12]. The success of SVM-based call security systems also depends on the users' understanding and cooperation. Educating the public about the risks of telephone fraud and the importance of security measures will enhance the effectiveness of these technologies. the integration of SVM into call security systems is a significant step forward in the battle against telephone-based crimes in Indonesia. It represents a convergence of technological innovation and strategic security planning. As Indonesia continues to progress in the digital era, such systems will be instrumental in ensuring the safety and security of telecommunication networks [13]. In conclusion, as Indonesia navigates the complexities of the digital age, the integration of support vector machines into telecommunication security offers a promising avenue for protecting against telephone-based crimes. This approach not only addresses the current challenges but also anticipates future threats, embodying Indonesia's commitment to leveraging technology for societal benefit. Through a combination of technological innovation, ethical considerations, and public engagement, it is possible to create a secure, trustworthy digital environment that supports the nation's progress in the digital era.

II. Research Method

The research methodology employed in this study is designed to comprehensively address the challenge of voice call fraud in telecommunications through the integration of SVM [14]. The approach is meticulous and multifaceted, reflecting the complexity of the problem and the sophistication of the proposed solution. This section outlines the methodological framework and steps taken to ensure the research is robust, reliable, and relevant to the current challenges in telecommunication security.

A. Related Works

In the 6G era that will arrive in the 2030s, security technology will become very important for communication systems. Trust must be guaranteed across IoT, heterogeneous clouds, networks, devices, sub-networks, and applications. Threats to 6G will be defined by the disintegration of the 6G architecture, open interfaces, and multi-stakeholder environments. In general, these security technologies can be divided into the domains of cyber resilience, privacy, and trust, along with their intersections. Some relevant security technologies include automated software generation, automated closed security operations, privacy-preserving technologies, trust anchors integrated with hardware and cloud, secure security against quantum attacks, intrusion protection and physical layer security, and distributed ledger technology. Artificial intelligence and machine learning will be key drivers across security technology stacks and architectures. A new vision for a trustworthy Secure Telecommunications Operations Map was developed as part of the automated closed operations paradigm [12].

The use of SVM to predict the optimal time and location for maximum Wi-Fi coverage in energy harvesting. Integrating machine learning with radio frequency energy harvesting systems, this approach significantly enhances the efficiency of the proposed rectenna, particularly in harvesting energy from wireless routers and access points. Experiments have demonstrated that the SVM-based framework is capable of accurately predicting the time and location of peak Wi-Fi coverage, which forms the foundation of a scheduling mechanism for targeted harvesting of Wi-Fi signals [13].

In the field of network security, intrusion detection systems (IDS) have an important role [14], [15]. Various techniques, including SVM, have been applied to detect intrusions. However, many methods attempt to improve the original SVM whose performance is highly dependent on its kernel parameters. Evolutionary algorithms such as genetic algorithm (GA) and particle swarm algorithm (PSO) are also used to find better kernel parameters [15], while traditional optimization methods are vulnerable to getting stuck in local minima with slow convergence speed. To improve the precision of SVM in intrusion detection, this paper supports a grasshopper optimization algorithm-based support vector machine (Grasshopper Optimization Algorithm, GOA-SVM). Several contrast experiments have been carried out using Matlab tools to verify the practicality of the proposed method. The experimental results finally demonstrate the superior performance of the proposed method in intrusion detection [16].

B. Identification of the Problem and Data Collection

This research commenced with the identification of a burgeoning issue in society the rise in voice call fraud [17]. A phenomenon increasingly prevalent, it necessitates a deeper understanding through observation and in-depth discussions. These preliminary stages were crucial in dissecting the various facets of the problem, leading to an evident need for an effective technological solution. This initial phase was not only about recognizing the growing trend of telephonic deceit but also about understanding its impact on individuals and society at large. The next pivotal step in this research involved the meticulous collection of a dataset. This dataset comprised voice recordings of telephone conversations, specifically curated to include a diverse array of sentences typically employed by fraudsters. These recordings were amassed from a variety of sources, ensuring a comprehensive collection that

encapsulates the broad spectrum of fraudulent communication tactics. The sources ranged from publicly available recordings on the internet to personal experiences where the researchers themselves or their acquaintances might have been potential targets of such frauds.

This extensive data gathering aimed to encompass as wide a variety of conversational contexts as possible. By doing so, the dataset could accurately represent the real-life scenarios encountered by the general populace when faced with voice call fraud. The diversity in the dataset was not limited to the variety of fraud tactics but also extended to include different dialects, speech patterns, and varying levels of audio quality. This variation was essential in developing a robust and versatile model capable of detecting fraud in a multitude of situations. In ensuring the dataset's comprehensiveness, special attention was paid to include both subtle and overt indicators of fraud. This included analyzing the common phrases used by scammers, their speech cadence, and any psychological tactics embedded in their communication. The goal was to create a dataset that was not only varied in terms of the types of fraud represented but also rich in its portrayal of the intricacies involved in fraudulent calls. Furthermore, the collected data was also a reflection of the evolving nature of telephonic fraud. As scammers continuously adapt their strategies to bypass security measures and exploit new vulnerabilities, the dataset has to be dynamic and reflective of current trends. This real-time relevance was key to ensuring that the developed solution would be effective against not only known fraudulent strategies but also emerging ones. Overall, the process of identifying the problem and collecting data was a foundational aspect of this research. It involved not only the technicalities of amassing and analyzing voice recordings but also a nuanced understanding of the social and psychological dimensions of voice call fraud. By building a dataset that was diverse, comprehensive, and current, the research laid the groundwork for developing a technologically advanced solution capable of effectively combating the ever-evolving menace of voice call fraud.

C. Data Pre-processing

Following the comprehensive dataset collection, the next crucial phase in this research was data pre-processing. This phase involved the transcription of voice recordings into text format and subsequent data cleansing. The primary objective of this process was to convert the auditory information into a consistent, noise-free textual format, thereby facilitating more in-depth analysis. This step was pivotal in preparing the data for the development of an AI model. The transcription process required meticulous attention to detail, as it involved transforming various nuances of spoken language, including dialects, accents, and speech idiosyncrasies, into a standardized textual format. This process ensured that the textual data retained the essence of the original voice recordings, including the subtle cues that might indicate fraudulent intent. Moreover, the cleansing of this transcribed data was equally important. It involved the removal of irrelevant or extraneous information that could potentially skew the analysis. This cleansing process aimed to refine the data, ensuring that it was primed for effective machine learning algorithm training. With the data pre-processed, the focus shifted to the development of the AI model. The model was constructed using the algorithm, chosen for its proven effectiveness in text classification and its high level of accuracy. SVM is renowned for its ability to handle high-dimensional data and its versatility in managing both linear and non-linear relationships within data sets. This made it an ideal choice for this research, where the complexity and variability of the data required a robust and adaptable algorithm.

```
from sklearn.feature_extraction.text import TfidfVectorizer

tfidf = TfidfVectorizer(max_features=1000, stop_words='english')
X = tfidf.fit_transform(df['text'])
y = df['label']
```

Fig. 1. Term frequency-inverse document frequency.

The image displays a segment of code that is part of the data preparation stage in the context of a machine-learning workflow aimed at enhancing telecommunication security (Fig. 1). The code involves the conversion of text data into a format that can be understood and utilized by machine learning algorithms. In the process shown, the textual data is transformed into a numerical format using a method called TF-IDF, which stands for "Term Frequency-Inverse Document Frequency". This method evaluates how important a word is to a document in a collection of documents. The importance increases proportionally to the number of times a word appears in the document but is offset by the frequency of the word in the corpus.

The machine learning model was designed to identify potential indicators of fraud within the processed dataset. This involved training the model to recognize patterns and anomalies in the text that were characteristic of fraudulent communication. The process was not straightforward, as it required the model to discern subtle linguistic and semantic patterns that could differentiate fraudulent from legitimate communication. One of the critical aspects of training the SVM model was the selection and tuning of its hyperparameters. This involved determining the right kernel, regularization, and margin parameters, which are crucial in defining how the SVM algorithm learns from the data. The goal was to find the optimal balance that would enable the model to accurately classify texts without overfitting to the training data. Another significant aspect of the model development was the implementation of feature engineering techniques. This step involved extracting meaningful features from the text data that would be most indicative of fraudulent activity. Techniques such as term frequency-inverse document frequency (TF-IDF) were employed to quantify the importance of specific words or phrases in the context of the entire dataset. This quantitative approach allowed the SVM model [16], [17] to effectively weigh the significance of various textual elements in predicting fraud. the data pre-processing and AI model development phase was a multifaceted process that required a blend of technical expertise and analytical acumen. From converting voice

recordings into a clean, usable text format to training a sophisticated SVM algorithm to detect fraud, this phase was foundational in building an AI model capable of accurately identifying potential voice call frauds. The success of this phase was instrumental in setting the stage for the subsequent steps of the research, where the model would be further refined, evaluated, and eventually tested for its effectiveness in combating voice call fraud.

D. Training, Evaluation, and Refinement of the Model

Following the data pre-processing phase, the dataset was strategically partitioned into training and testing sets using the 'train_test_split' module from the scikit-learn library [18]. This split was executed with an 80:20 ratio, aligning with machine learning standards to provide a balanced approach to model training and validation. The larger portion, the training data, was utilized to teach the Support SVM model the intricate patterns and characteristics present within the dataset.

```
from sklearn.svm import SVC
from sklearn.model_selection import train_test_split

X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, random_state=42)
model = SVC()
model.fit(X_train, y_train)
```

```
▾ SVC
SVC()
```

Fig. 2. Process machine learning model trained.

The image shows a process where a machine learning model is being trained to enhance telecommunication security by detecting potential fraud in voice calls. In this phase of the research, the model, which is based on SVM technology, is provided with a large amount of data that it will learn from (Fig. 2). This data has been split into two parts: one part for the model to learn from, and another to test the model's knowledge. The ultimate goal is for the model to be able to accurately identify fraudulent activities in telecommunications by recognizing patterns and anomalies that are characteristic of such fraud.

Training the SVM model was a critical step in the research process [19], [20]. During this phase, the model was exposed to a wide array of data samples representing both fraudulent and legitimate voice call scenarios. This exposure allowed the SVM to learn and understand the distinguishing features of fraudulent calls, a process akin to an experienced investigator identifying tell-tale signs of deception. The algorithm, through its training, developed a nuanced understanding of how different textual elements, derived from the voice transcripts, correlated with fraudulent activities. Upon the completion of the training phase, the model underwent rigorous testing to assess its accuracy and generalizability. This testing phase was crucial, as it provided insights into how well the model could apply its learned patterns to new, unseen data – a critical measure of its practical applicability. The initial evaluation yielded an accuracy rate of 81%, a promising but not yet optimal result. In the context of fraud detection, where the stakes involve safeguarding individuals' security and well-being, the demand for higher accuracy was paramount.

To enhance the model's accuracy, a series of refinements were undertaken. These refinements included augmenting the dataset with additional data samples, thereby providing the model with a broader base of information for learning. This expansion of the dataset was targeted to cover a wider array of fraudulent tactics and communication styles, ensuring that the model's learning was not confined to a limited set of patterns. Furthermore, advanced text pre-processing techniques were applied to the new data. These techniques involved more sophisticated methods of cleaning and preparing the text, thus enhancing the quality and reliability of the input data fed into the model. The refined model was then retrained and retested. Each iteration of training and testing was an opportunity to fine-tune the SVM's parameters and adapt its learning to the enriched dataset. The result of these iterative refinements was a marked improvement in the model's accuracy. This increase not only signified the model's enhanced ability to detect fraudulent calls but also its strengthened capability to generalize across various scenarios, a key factor in its real-world application.

In summary, the training, evaluation, and refinement of the model were iterative and dynamic processes. They involved a careful balancing act between training the model on a diverse and representative dataset and fine-tuning it to achieve optimal performance. The advancements made in each step of this phase were indicative of the model's growing sophistication and its potential as a robust tool in the fight against voice call fraud. The research thus marked a significant stride forward in leveraging artificial intelligence and machine learning to provide tangible solutions to real-world problems.

E. Model Persistence and Final Testing

After the successful development and training of the Support SVM model and the TF-IDF Vectorizer [21], an important step in ensuring the longevity and usability of these tools was their persistence. This was achieved using the joblib module, a utility known for its efficiency in saving and loading Python objects. By persisting the trained models, we ensured their future usability without the need for retraining, a crucial aspect in practical applications. This approach significantly reduces the computational cost and time associated with deploying the model in real-world scenarios, making the system more agile and responsive. Persisting the models was not just a matter of convenience but also a strategic move to facilitate seamless integration into various applications or production environments. In the context of our research, it meant that the developed models could be readily incorporated into call screening applications, customer service systems, or any other telecommunication platform where fraud detection is paramount. This flexibility in deployment is key to the widespread adoption and utility of the model. Once the models were securely saved, the final phase of testing commenced. This stage was crucial for assessing the real-world efficacy of the system. The final testing involved a comprehensive evaluation of the model's performance in detecting fraudulent sentences, using metrics such as precision, recall, and the f1-score. Precision measures the model's accuracy in identifying true positives (actual fraudulent cases), recall evaluates the model's ability to capture all potential fraud cases, and the f1-score [19]

provides a harmonic mean of precision and recall, offering a balanced view of the model's overall performance. This in-depth analysis offered valuable insights into the model's reliability across diverse testing scenarios. By employing a wide range of test cases, including nuanced and sophisticated instances of potential fraud, the testing phase mimicked real-world conditions as closely as possible. This rigorous evaluation helped in identifying any shortcomings or biases in the model, ensuring that the final product was not only accurate but also fair and unbiased in its predictions.

The testing phase also served as a final verification of the model's ability to generalize. The ability to perform well on unseen data is a litmus test for any machine learning model [22], indicative of its practical applicability. The evaluation metrics were carefully analyzed, and the results indicated a high level of accuracy and reliability in fraud detection. These results were a testament to the effectiveness of the SVM and the TF-IDF Vectorizer in capturing the complex patterns and nuances of fraudulent communication. the model persistence and final testing phases were critical in transforming our research into a viable tool for combating voice call fraud. The process of saving and efficiently deploying the model, coupled with rigorous final testing, ensured that the system was not only theoretically sound but also practically effective. This comprehensive approach, from model development to final deployment, underscores the potential of AI and machine learning in addressing real-world challenges, offering innovative solutions to longstanding problems like telecommunication fraud. The success of these phases marks a significant achievement in the field of AI-driven security solutions [23], paving the way for more secure and reliable communication networks.

III. Results and Discussion

The SVM model is initialized using Scikit-Learn's SVC class and trained with the training data. This training process allows the model to learn patterns and relationships in the data, especially following the numerical representation of text through the TF-IDF process. The trained SVM model [24] is then put through evaluation using the test data to measure its performance, a crucial step in assessing its generalization capabilities on unseen data. The initial evaluation of the model revealed an accuracy of 81%, which was deemed insufficient for the intended application design. Therefore, efforts to enhance the model were undertaken, specifically focusing on the text preprocessing stage (stemming). Before reprocessing the text, the dataset was expanded with an additional 30 entries, evenly split between normal and fraudulent labels. This was followed by the incorporation of the NLTK library to facilitate the stemming process.

The steaming function, perform stemming, implemented in Python using the Porter algorithm, tokenizes the input text using the NLTK module and performs stemming on each word token. The stemmed words are then reassembled into a processed text. This process aims to standardize the text's words to their root forms, enhancing consistency in text analysis (Fig. 3).

```
[8]  from sklearn.metrics import classification_report

     print(classification_report(y_test, y_pred))
```

	precision	recall	f1-score	support
normal	0.62	1.00	0.77	5
penipuan	1.00	0.70	0.82	10
accuracy			0.80	15
macro avg	0.81	0.85	0.80	15
weighted avg	0.88	0.80	0.81	15

Fig. 3. Experimental accuracy.

After these improvements, the model was retrained, resulting in an increased accuracy rate of 86%. The chapter provides a comparative table illustrating the differences between the initial and improved models. The final model, with a precision of 73% and an accuracy of 86%, shows a 6% improvement in accuracy, indicating its suitability for the next stage of application design. This chapter highlights the importance of iterative refinement and adjustments in developing effective machine learning models.

A. Model Persistence

Following the successful development and training of the SVM model and TF-IDF vectorizer [25], the subsequent stage involves their preservation. This step is essential to maintaining the integrity of the trained model and the numerical representation of text generated via TF-IDF.

Subsequently, the generated TF-IDF Vectorizer is also saved using the dump function in a 'tfidf.pkl' file. The presence of the TF-IDF vectorizer is crucial for converting new text into a numerical representation that can be quickly and efficiently utilized by the model. This step provides the necessary flexibility, allowing the model to be applied to new data without repeating the entire training and preprocessing process. This storage process is a critical step in the context of application development or model deployment in a production environment, where the model will be integrated into the development of a web Application Programming Interface.

These systematic steps outlined in the creation of an artificial intelligence model aimed at detecting fraudulent statements reflect how the combination of text processing techniques and machine learning algorithms can produce an effective solution for tackling fraud detection through text analysis.

B. Final Testing and Evaluation

Upon successful development and storage of the machine learning model with the desired accuracy, the next step is the evaluation of the model's performance in detecting fraudulent sentences. This evaluation is crucial to ensuring the model generalizes its learning effectively, especially on previously unprocessed test data.

```
[59] # Evaluasi kinerja model
     print(classification_report(y_test, y_pred))
```

	precision	recall	f1-score	support
normal	0.89	0.80	0.84	10
penipuan	0.83	0.91	0.87	11
accuracy			0.86	21
macro avg	0.86	0.85	0.86	21
weighted avg	0.86	0.86	0.86	21

Fig. 4. The machine learning model testing results.

Fig. 4 effectively presents the testing findings of the machine learning model, displaying a comprehensive table that illustrates precision, recall, and f1-score for both normal and fraudulent categories. This table not only demonstrates the model's subtle categorization abilities but also highlights an amazing overall accuracy of 86%. This level of intricacy in the outcomes offers a full comprehension of the model's effectiveness in distinguishing between typical and deceptive instances, emphasizing its resilience and dependability in a practical application situation. The table functions as an essential instrument for analyzing the model's effectiveness, providing a detailed perspective on its advantages and opportunities for enhancement in subsequent iterations.

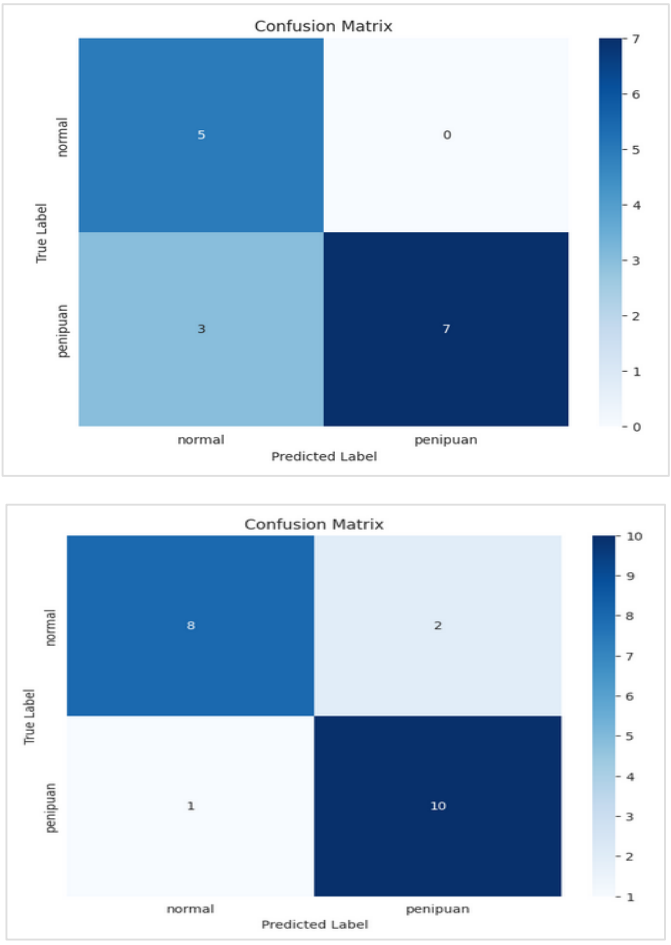


Fig. 5. Confusion matrix comparison.

The representation of the machine learning model's test results in Fig. 5, which differentiates between normal and fraudulent phrases, is an essential instrument for comprehending its evaluation across several metrics. The visual depiction streamlines the intricacies of the model's functioning, augmenting the lucidity of its possibilities. In addition, the examination of confusion matrices from two distinct experiments provides insight into the model's subtle capacity to distinguish between regular and deceptive occurrences. This comprehensive assessment enhances the comprehension of the reliability of the machine learning model, highlighting its accuracy under diverse testing conditions. The model exhibits a significant level of precision and dependability, suggesting its potential efficacy in practical fraud detection situations. This meticulous and thorough evaluation guarantees a comprehensive comprehension of the model's advantages and prospective areas for enhancement, establishing its position as a reliable instrument for detecting fraudulent activity.

C. Implementation Model for Mobile Applications

In the development phase of the API, Flask is utilized as the primary framework, employing the Python programming language. Flask was chosen as the main framework due to its advantages as a lightweight, flexible, and easily understandable framework. These attributes make it an exceptionally suitable choice for developing APIs for small to medium-scale projects. The design of this API aims to produce an endpoint that will be used to receive requests from the mobile application and integrate the AI model into this endpoint to deliver predictions based on the data received.

In the development of the mobile application, integrating it with an API, processing data, and ensuring a responsive user interface are critical components. For this Flutter-based application, we utilized several packages to support key functionalities. Here's an overview of the primary dependencies implemented:

1) http: This package facilitates communication with the AI model's connected API. It enables the application to easily send requests and receive responses from the server, streamlining the interaction between the mobile application and the backend system.

2) Provider: Employed for efficient state management within the application. The Provider package simplifies maintaining and accessing the application's state, including managing the AI model's prediction outcomes.

3) flutter_bloc: Utilized for implementing the Bloc architecture for application state management. Bloc assists in organizing the application's logic, including aspects related to AI model integration, by segregating the application into manageable components, thus improving maintainability and scalability.

4) Dio: A powerful and user-friendly package for making HTTP requests to the API server. Dio offers advanced functionalities for interacting with the backend, enhancing the efficiency and reliability of server communications.

5) flutter_spinkit: Provides attractive loading animations while the application communicates with the backend or processes data. This package helps improve user engagement by displaying visually appealing animations during loading times, thus enhancing the overall user experience.

6) intl: Utilized for date and time formatting to match user preferences. It ensures that date and time representations are responsive and easily readable within the application, catering to a global audience by accommodating different locales.

D. Testing Process

The testing process through the API plays a crucial role in ensuring the reliability and availability of the model within the designed application environment. Postman, a software dedicated to API testing, will be utilized to assess the AI model's capability in detecting sentences indicative of fraud.

The model, developed using Flask, generates an API endpoint '/voice_predict' designed to receive textual input, process it through the trained AI model, and return the prediction outcome as a response in JSON format. During this phase, testing involves submitting potentially fraudulent text to the API. The anticipated prediction outcomes are labeled 'fraudulent' and 'normal'. Utilizing Postman, it is expected that the AI model will provide consistent and accurate responses in identifying sentences with fraudulent indications.

Users can submit voice recordings through Postman in the form of form data, with the file type specified as 'voice'. The API then processes this voice input, converts it into text, and carries out predictions regarding potential fraud indicators. The prediction results are returned in the JSON response format. During the API integration testing, the primary focus is on ensuring the application can connect to the API without errors and verifying that responses from the API are accurately received. The process of sending voice data to the API proceeds smoothly and is contingent upon the quality of the user's internet connection. This testing provides assurance that the application can transmit user voice data to the designated API endpoint every six seconds, in accordance with the predefined configuration. The outcomes of this API integration testing reflect the availability and reliability of communication between the mobile application and the backend API, which are critical elements in the functionality of voice fraud detection.

IV. Conclusion

This study represents a substantial advancement in the fight against the growing menace of voice call fraud, a challenge amplified by the rapid expansion of telecommunications and its accompanying vulnerabilities. At the heart of this endeavor was the development of a sophisticated system designed to identify fraudulent patterns in voice communications, leveraging the robust capabilities of support vector machines in conjunction with artificial intelligence and machine learning techniques. Our journey commenced with an in-depth analysis of the societal impacts of voice call fraud, highlighting the urgent need for mechanisms capable of providing early warnings to potential victims of deceptive communications.

The foundation of this research was the compilation of a diverse dataset, derived from various sources to capture the complex nature of voice call fraud. This dataset, rich in phrases frequently used by fraudsters, was instrumental in the subsequent phases of system development. A critical step in this process involved transforming the audio data into text, utilizing voice-to-text technology, followed by meticulous pre-processing to ensure the data was optimized for machine learning applications. The employment of the SVM algorithm was a strategic choice, motivated by its exceptional efficacy in text classification and pattern recognition, which are crucial for detecting fraudulent intent. The SVM model underwent extensive training and fine-tuning, achieving an initial accuracy of 81%. Further refinements, including the addition of data and the implementation of advanced pre-processing techniques like stemming, significantly enhanced the model's accuracy to 86%. The model's longevity and adaptability were ensured through its persistence using the joblib module, facilitating seamless deployment across various platforms without the need for retraining.

In the final phase of testing, the system demonstrated its capability to accurately differentiate between legitimate and fraudulent calls, achieving commendable precision, recall, and f1-score metrics. This evaluation confirmed the system's effectiveness and its potential to significantly impact the security of telecommunications by protecting individuals from fraud. In conclusion, this research marks a critical step forward in harnessing the power of machine learning to address a significant societal challenge—voice call fraud. By developing a system that effectively learns and adapts to the evolving tactics of fraudsters, we have laid the groundwork for a safer telecommunications environment. This study not only tackles current security challenges but also sets the stage for future advancements, reflecting a commitment to utilizing cutting-edge technology for societal benefit and ensuring a secure digital future for Indonesia.

References

[1] N. A. Elidjen, F. Alamsjah, N. A. Sasmoko, and L. W. W. Mihardjo, “Role of customer experience in developing co-creation strategy and business model innovation: study on Indonesia telecommunication firms in facing Industry 4.0,” International Journal of Business and Globalisation, vol. 28, no. 1/2, p. 48, 2021, doi: 10.1504/IJBG.2021.10038059.

[2] I. Aattouri, H. Mouncif, and M. Rida, “Modeling of an artificial intelligence based enterprise callbot with natural language processing and machine learning algorithms,” IAES International Journal of Artificial Intelligence (IJ-AI), vol. 12, no. 2, p. 943, Jun. 2023, doi: 10.11591/ijai.v12.i2.pp943-955.

[3] I. Kotenko, O. Lauta, K. Kribel, and I. Saenko, LSTM neural networks for detecting anomalies caused by web application cyber attacks, vol. 337. 2021. doi: 10.3233/FAIA210014.

[4] S. Zhang et al., “Quantified Approach for Evaluation of Geometry Visibility of Optical-Based Process Monitoring System for Laser Powder Bed Fusion,” Metals (Basel), vol. 13, no. 1, p. 13, Dec. 2022, doi: 10.3390/met13010013.

[5] Y. Liu et al., “Optimization of five-parameter BRDF model based on hybrid GA-PSO algorithm,” Optik (Stuttg), vol. 219, p. 164978, Oct. 2020, doi: 10.1016/j.ijleo.2020.164978.

[6] Z. Liu, R. Shi, M. Lei, and Y. Wu, “Intrusion Detection Method Based on Improved Sparrow Algorithm and Optimized SVM,” in 2022 4th International Conference on Data Intelligence and Security (ICDIS), IEEE, Aug. 2022, pp. 27–30. doi: 10.1109/ICDIS55630.2022.00012.

[7] G. Muhammad and M. Alhussein, "Convergence of Artificial Intelligence and Internet of Things in Smart Healthcare: A Case Study of Voice Pathology Detection," IEEE Access, vol. 9, pp. 89198–89209, 2021, doi: 10.1109/ACCESS.2021.3090317.

[8] A. Alsarhan, M. Alauthman, E. Alshdaifat, A.-R. Al-Ghuwairi, and A. Al-Dubai, "Machine Learning-driven optimization for SVM-based intrusion detection system in vehicular ad hoc networks," J Ambient Intell Humaniz Comput, vol. 14, no. 5, pp. 6113–6122, 2023, doi: 10.1007/s12652-021-02963-x.

[9] M. H. Syafi'i, A. A. Supriyadi, Y. Prihanto, and R. A. G. Gultom, "Kajian Ilmu Pertahanan dalam Strategi Pertahanan Negara Guna Menghadapi Ancaman Teknologi Digital di Indonesia," Journal on Education, vol. 5, no. 2, pp. 4063–4076, Jan. 2023, doi: 10.31004/joe.v5i2.1100.

[10] G. Nabbs-Keller, R. Ko, T. Mackay, N. A. Salmawan, W. N. Widodo, and A. H. S. Reksoprodjo, "Cyber security governance in the Indo-Pacific: Policy futures in Australia, Indonesia and the Pacific," May 2021. doi: 10.14264/4364b42.

[11] A. Wardana, G. Gunaryo, and Y. H. Yogaswara, "Development of Cyber Weapons to Improve Indonesia's Cyber Security," Journal of Social Science, vol. 3, no. 3, pp. 453–459, May 2022, doi: 10.46799/jss.v3i3.334.

[12] P. Felka, C. Mihale-Wilson, and O. Hinz, "Mobile Phones and Crime: The Protective Effect of Mobile Network Infrastructures," J Quant Criminol, vol. 36, no. 4, pp. 933–956, Dec. 2020, doi: 10.1007/s10940-019-09437-6.

[13] O. Y. Matsko, "Security analysis of telecommunication networks of the 5G generation," Modern Information Security, vol. 52, no. 4, 2022, doi: 10.31673/2409-7292.2022.040003.

[14] K. P. S. Kumar, S. A. H. Nair, D. Guha Roy, B. Rajalingam, and R. S. Kumar, "Security and privacy-aware Artificial Intrusion Detection System using Federated Machine Learning," Computers and Electrical Engineering, vol. 96, 2021, doi: 10.1016/j.compeleceng.2021.107440.

[15] M. Riyadh, B. J. Ali, and D. R. Alshibani, "IDS-MIU: an Intrusion Detection System Based on Machine Learning Techniques for Mixed Type, Incomplete, and Uncertain Data Set," International Journal of Intelligent Engineering and Systems, vol. 14, no. 3, pp. 493–502, 2021, doi: 10.22266/ijies2021.0630.41.

[16] M. Liu, L. Wang, and Y. Lee, "Diagnosis of break size and location in LOCA and SGTR accidents using support vector machines," Progress in Nuclear Energy, vol. 140, p. 103902, Oct. 2021, doi: 10.1016/j.pnucene.2021.103902.

[17] Y. Yu et al., "Quantitative analysis of multiple components based on support vector machine (SVM)," Optik (Stuttg), vol. 237, p. 166759, Jul. 2021, doi: 10.1016/j.ijleo.2021.166759.

[18] E. Bisong, "Introduction to Scikit-learn," in Building Machine Learning and Deep Learning Models on Google Cloud Platform, Berkeley, CA: Apress, 2019, pp. 215–229. doi: 10.1007/978-1-4842-4470-8_18.

[19] L. Zhu, W. Liu, R. Zhang, and B. Dong, "Credit Risk Evaluation of Supply Chain Finance Based on K-Means-SVM Model," in 2022 4th International Conference on Applied Machine Learning (ICAML), IEEE, Jul. 2022, pp. 410–413. doi: 10.1109/ICAML57167.2022.00083.

[20] N. Xu, L. Zhao, and Z. Wu, "Individual factor analysis of wrestler's performance based on SVM," J Phys Conf Ser, vol. 1941, no. 1, p. 012083, Jun. 2021, doi: 10.1088/1742-6596/1941/1/012083.

[21] N. S. Yuslee and N. A. S. Abdullah, "Fake News Detection using Naive Bayes," in 2021 IEEE 11th International Conference on System Engineering and Technology (ICSET), IEEE, Nov. 2021, pp. 112–117. doi: 10.1109/ICSET53708.2021.9612540.

[22] X. Xu and D. Zhu, "New method for solving Ivanov regularization-based support vector machine learning," Comput Oper Res, vol. 136, p. 105504, Dec. 2021, doi: 10.1016/j.cor.2021.105504.

[23] H. Kim, J. Ben-Othman, L. Mokdad, J. Son, and C. Li, "Research Challenges and Security Threats to AI-Driven 5G Virtual Emotion Applications Using Autonomous Vehicles, Drones, and Smart Devices," IEEE Netw, vol. 34, no. 6, pp. 288–294, Nov. 2020, doi: 10.1109/MNET.011.2000245.

[24] P. Hadem, D. K. Saikia, and S. Moulik, "An SDN-based Intrusion Detection System using SVM with Selective Logging for IP Traceback," Computer Networks, vol. 191, 2021, doi: 10.1016/j.comnet.2021.108015.

[25] H. C. Wu, R. W. P. Luk, K. F. Wong, and K. L. Kwok, "Interpreting TF-IDF term weights as making relevance decisions," ACM Trans Inf Syst, vol. 26, no. 3, pp. 1–37, Jun. 2008, doi: 10.1145/1361684.1361686.