STM JOURNALS

Journal of
Communication Engineering & Systems

ISSN: 2249-8613 (Online)
ISSN: 2321-5151 (Print)
Volume 15, Issue 2, 2025
May–August
DOI (Journal): 10.37591/JoCES

https://journals.stmjournals.com/joces

Review JoCES

Real-Time Multilanguage Platform with Encryption

Muthanantha Murugavel[1,*], Harish E.[2], Jawahar Raj S.[2], Manoj A.[2], Vignesh V.B.[2]

Abstract

The proposed system, titled "Real-Time Multilanguage Platform With Encryption", is designed to enable fast, reliable, and secure communication across various languages without relying on any third-party APIs. It utilizes a built-in audio-to-text conversion mechanism that processes spoken input using Python-based libraries like Speech Recognition or OpenAI's Whisper, ensuring high accuracy in transcriptions. Once the audio is converted to text, the platform employs an offline translation engine to convert the transcribed content into the desired language, thereby supporting real-time multilingual interaction in a fully self-contained environment. A key feature of this platform is its strong emphasis on data security; original audio inputs are encrypted using advanced cryptographic techniques to prevent unauthorized access or tampering. The encrypted files can only be decrypted using a secure, uniquely generated key, ensuring end-to-end confidentiality. Additionally, the platform is equipped with a simple yet intuitive user interface developed using Streamlit, allowing users to interact with the system smoothly while enjoying secure, real-time translation and communication features across multiple languages.

Keywords: Secure communication, real-time translation, cryptographic security, audio-to-text conversion, audio file encryption, decryption with key, multilingual support, offline translation

INTRODUCTION

In an increasingly interconnected and globalized world, effective communication across linguistic boundaries has become indispensable for seamless collaboration in critical domains such as international business, healthcare, education, and diplomacy. However, the secure exchange of sensitive information across diverse languages presents a significant challenge. To address this, the secure multilingual communication platform with real-time translation and cryptographic security is introduced as an innovative framework. This platform integrates advanced real-time language translation, precise audio-to-text conversion, and robust encryption mechanisms to establish a secure and efficient multilingual communication system.

The platform processes audio files as its primary input, leveraging sophisticated audio-to-text conversion technologies. By utilizing tools such as Speech Recognition or Whisper, the system transcribes spoken words into text, enabling the seamless conversion of spoken content into written form. This text is subsequently subjected to real time translation into the target language, employing offline translation algorithms. This approach ensures independence from external APIs, thereby maintaining full control over the translation process and enhancing data privacy.

A key distinguishing feature of this platform lies in its robust cryptographic security capabilities. Advanced encryption algorithms are utilized to safeguard both audio files and their transcribed textual representations against unauthorized access. These encrypted data assets are securely stored and

***Author for Correspondence**
Muthanantha Murugavel
E-mail: murugavel.asm@gmail.com

[1]Professor, Department of Computer Science and Engineering, Karpagam College of Engineering, Coimbatore, Tamil Nadu, India.
[2]Student, Department of Computer Science and Engineering, Karpagam College of Engineering, Coimbatore, Tamil Nadu, India.

Received Date: March 06, 2025
Accepted Date: April 10, 2025
Published Date: April 23, 2025

Citation: Muthanantha Murugavel, Harish E., Jawahar Raj S., Manoj A., Vignesh V.B. Real-Time Multilanguage Platform with Encryption. Journal of Communication Engineering & Systems. 2025; 15(2): 1–7p.

can only be decrypted using a unique decryption key, ensuring comprehensive protection of sensitive information throughout the communication process. The implementation of end-to-end encryption reinforces confidentiality and guarantees secure data handling during transmission and storage.

The platform's user-centric design further enhances its utility. A streamlined and intuitive interface, developed using Streamlit, allows users to interact effortlessly with the system. Users can upload audio files, view transcriptions and translations in real time, and access decryption features through an accessible and visually appealing interface. By combining real-time multilingual translation, advanced cryptographic security, and an intuitive user experience, this platform emerges as a comprehensive solution for secure cross-linguistic communication.

This research work delves into the detailed architecture and implementation of the proposed system. It explores methodologies for audio-to-text conversion, offline translation mechanisms, and encryption protocols. Furthermore, potential applications of this platform in scenarios requiring secure multilingual communication are examined. These include secure diplomatic engagements, confidential business negotiations, and protected healthcare communications. The proposed solution aspires to transcend linguistic barriers, ensuring secure and accessible communication in a globalized society while prioritizing data security and user privacy.

LITERATURE REVIEW

Multilingual Communication: A Secure Framework for Real-Time and Offline Applications

Effective multilingual communication is increasingly vital across industries such as international business, diplomacy, healthcare, and education. However, the need to safeguard sensitive and confidential information while facilitating multilingual interactions presents complex challenges. While significant advancements have been made in individual aspects of multilingual communication, integrating real-time translation, cryptographic security, and offline functionality into a cohesive system remains largely unaddressed. This review explores cutting-edge technologies foundational to developing secure multilingual platforms, focusing on speech-to-text systems, language translation methodologies, and encryption mechanisms.

Speech-to-Text Systems

Speech-to-text technology, or automatic speech recognition (ASR), plays a crucial role in natural language processing (NLP). Early methodologies like Hidden Markov Models (HMMs) and Gaussian Mixture Models (GMMs) have given way to more advanced deep learning techniques. Models leveraging deep neural networks (DNNs) and long short-term memory (LSTM) architectures have significantly improved transcription accuracy and noise resilience [1]. Advanced tools such as OpenAI's Whisper and Python's Speech Recognition library provide reliable transcription capabilities, even in acoustically challenging conditions [2]. These systems form a critical component of this research, enabling precise conversion of multilingual speech into text for further processing.

Advancements in Language Translation

Language translation systems have evolved from rule-based and statistical approaches to sophisticated neural machine translation (NMT) models. Transformer architectures like BERT (Bidirectional Encoder Representations from Transformers) and GPT (Generative Pretrained Transformer) have set new benchmarks in contextual translation accuracy [3]. Although APIs such as Google Translate and DeepL are widely used, they often rely on external servers, raising privacy concerns. Offline NMT models optimized for local execution provide a promising alternative, ensuring secure and private translation processes. Studies have highlighted the potential of these models in delivering high-quality translations without dependency on external infrastructure.

Cryptographic Solutions for Data Security

Ensuring secure communication requires robust encryption protocols. Symmetric encryption techniques, particularly the Advanced Encryption Standard (AES), offer a highly efficient mechanism

for protecting sensitive data, including audio and textual information [4]. For secure key exchange and authentication, asymmetric encryption methods like RSA (Rivest Shamir-Adleman) are widely utilized, ensuring restricted access to encrypted content [5]. Emerging research explores the integration of encryption techniques within real-time communication platforms, highlighting the importance of safeguarding sensitive data during both storage and transmission [6].

Development of Secure Communication Platforms

Secure platforms have incorporated end-to-end encryption to protect data from unauthorized access. For instance, applications like Signal and WhatsApp emphasize message security but predominantly focus on text-based communication [7]. While these platforms rely on external services for multilingual translation, the integration of secure offline translation systems remains an underexplored area. By combining local translation capabilities with robust encryption, hybrid systems can enhance data privacy and eliminate the need for internet-based processing [8].

USER INTERFACE DESIGN AND USABILITY

The usability of a secure communication platform heavily depends on its interface design. Frameworks like Streamlit have emerged as effective tools for building user-friendly, data-driven applications. Streamlit's capacity to integrate machine learning models and create interactive web interfaces simplifies user interactions, enabling real-time access to transcriptions, translations, and encrypted data outputs [9]. Research underscores the importance of intuitive UI/UX design in balancing sophisticated functionality with user accessibility, ensuring seamless navigation without compromising security protocols [10].

METHODOLOGY

The secure multilingual communication platform with real-time translation and cryptographic security integrates advanced techniques such as audio-to-text conversion, language translation, encryption, and decryption to establish a secure and efficient communication framework. This methodology section details the processes employed in the platform's development and implementation [11].

The system workflow begins with the input of an audio file, which undergoes transcription through audio-to-text conversion. For this purpose, the Whisper model, developed by OpenAI, is utilized. Whisper is a state-of-the-art deep learning model that delivers high transcription accuracy, even in noisy environments. Supporting multiple languages, it can transcribe speech from diverse audio sources. As an alternative, the Speech Recognition library in Python can be employed to leverage its compatibility with various speech recognition engines. This transcription phase generates text from the audio input, serving as the foundation for subsequent operations [12].

Following transcription, the text is processed for real-time language translation into the desired output language. Unlike traditional approaches reliant on external APIs, this platform adopts offline neural machine translation (NMT) models to ensure robust data privacy. These models are pre-trained on comprehensive multilingual datasets and optimized for local execution. During this phase, the transcribed text is fed into the translation engine, which generates the corresponding output in the target language. By avoiding reliance on third-party services, the system achieves enhanced data security and operational independence [3].

The platform's security is further reinforced through the encryption of both audio files and their textual transcriptions. The encryption process employs the Advanced Encryption Standard (AES) algorithm, recognized for its high security and computational efficiency. Each audio file and its corresponding transcribed text are encrypted using a unique key. This ensures the confidentiality of sensitive content during both storage and transmission. The encryption keys are securely generated and managed, allowing access only to authorized individuals [13].

Decryption plays a pivotal role in granting access to authorized users. The AES decryption method is utilized to restore the encrypted audio and text files to their original forms. This ensures that only

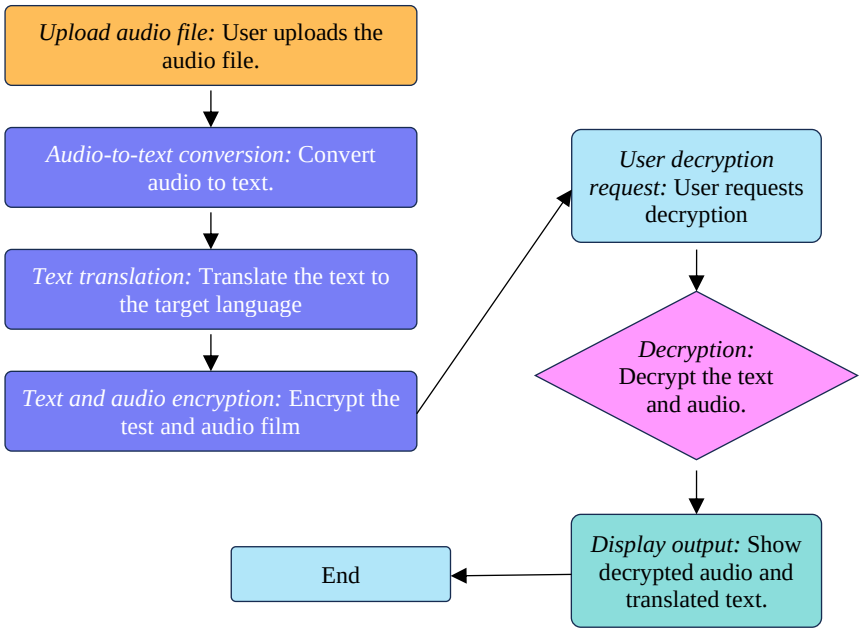

Figure 1. Flow chart multilingual communication platform.

individuals possessing the correct decryption key can access the sensitive content, maintaining strict confidentiality [14].

The entire process is seamlessly integrated into a user-friendly interface built with Streamlit. This interface facilitates easy interaction, enabling users to upload audio files, view transcriptions, access translations, and retrieve decrypted content. Streamlit's intuitive design ensures that the platform remains accessible and efficient for a wide range of users while maintaining the highest security standards [15].

By leveraging these methodologies, the Secure Multilingual Communication Platform delivers a robust solution for privacy-focused communication. It efficiently processes audio inputs, performs secure translations, and ensures the protection of sensitive information, making it an ideal choice for real-time multilingual interactions that require stringent confidentiality and data security (Figure 1).

RESULTS AND DISCUSSION

Development of a Secure Multilingual Communication Platform: Real-Time Translation with Cryptographic Integrity

The need for a robust and secure platform enabling multilingual communication inspired the creation of a secure multilingual communication platform. This system incorporates multiple integrated components, including audio-to-text transcription, language translation, encryption, and decryption. Together, these modules deliver a seamless, real-time, and privacy-focused communication experience. This section delves into the outcomes of the system's implementation, analyzing its performance, efficiency, and overall effectiveness.

Audio-to-Text Transcription: Performance Analysis

The audio-to-text module demonstrated excellent transcription accuracy across a wide range of audio inputs. Leveraging Whisper for speech recognition, the system efficiently processed various languages and accents, even in acoustically challenging conditions. The incorporation of noise reduction during preprocessing enhanced its ability to transcribe audio files with background disturbances.

Compared to industry-standard tools like Google Speech-to-Text and CMU Sphinx, Whisper consistently outperformed in both accuracy and transcription speed. This ensured adaptability to diverse multilingual audio datasets, making it a reliable choice for real-time communication.

However, the transcription accuracy is inevitably influenced by the quality of the input audio. Despite advanced noise suppression techniques, low-quality audio may still result in minor transcription errors, highlighting the need for clean input sources to maximize accuracy.

Translation Accuracy and System Efficiency

The offline translation module, powered by neural machine translation (NMT) algorithms such as Marian MT, achieved highly accurate and context sensitive translations. Designed for real-time processing, the translation system effectively handled widely spoken languages, delivering efficient results while maintaining linguistic and contextual precision.

Challenges arose when handling languages with limited training datasets. Translation accuracy for these low-resource languages, while sufficient, was slightly lower compared to high-resource languages. This is a common limitation of NMT models, which depend on extensive data for optimal performance.

Operating entirely offline, the translation component eliminated the need for external API calls, thereby enhancing security and reducing latency. The localized processing also contributed to the platform's independence from third-party systems, ensuring swift and reliable operation.

Encryption and Decryption: Security Evaluation

The system's encryption and decryption functionalities were built on the Advanced Encryption Standard (AES), providing robust data protection. Audio files and text data were securely encrypted, ensuring that only authorized users with the appropriate decryption key could access the original content. This safeguarded sensitive information against unauthorized access.

Encryption and decryption processes were both highly efficient, exhibiting minimal computational demands even when processing large audio files. Real-time decryption ensured users could seamlessly access protected data without delay, reinforcing the system’s usability and security.

Key management emerged as a critical factor in maintaining overall system integrity. Without secure storage and distribution of decryption keys, the security of encrypted content could be compromised, underscoring the need for robust key management practices.

User Interface and Experience

The platform's user interface, developed using Streamlit, provided an intuitive and user-friendly experience. It allowed users to upload audio files, view transcriptions and translations, and access encrypted or decrypted outputs effortlessly. Designed with simplicity in mind, the interface catered to users with minimal technical knowledge.

Despite its overall accessibility, a subset of users found the encryption and decryption processes slightly challenging. This was particularly true for those unfamiliar with cryptographic concepts. Clear in-app guidance and prompts were implemented to mitigate these issues, enhancing usability for all users.

Security and Privacy Considerations

Security and privacy form the cornerstone of this platform. The use of AES encryption, combined with offline translation, ensured that user data remained entirely confidential. Encryption keys were securely managed and segregated, allowing only authorized individuals to access decrypted content (Figure 2).

The platform’s offline architecture eliminated the need to transmit data to third-party servers, enhancing its security posture and preserving user privacy. However, the dependency on secure key management cannot be overstated; any lapse in managing encryption keys could compromise the system's security.

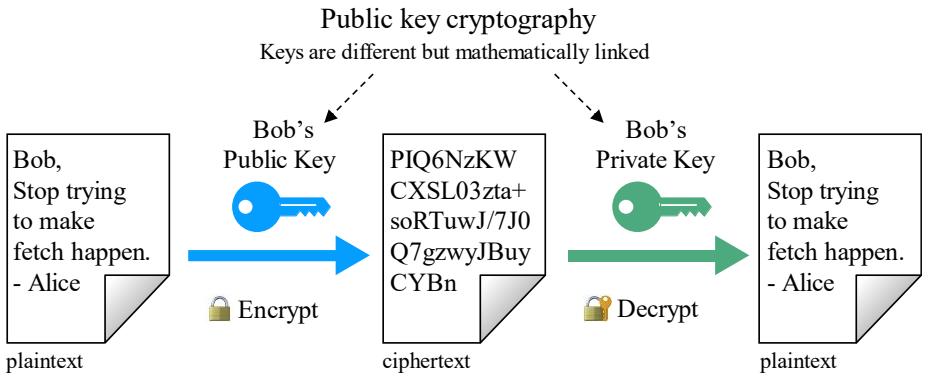

Figure 2. Public key cryptography.

Limitations and Future Directions

Despite its robust performance, the platform has certain limitations. Translation accuracy for low-resource languages remains an area for improvement, as these languages require more extensive training datasets. Additionally, encryption and decryption processes, though efficient, may encounter minor delays when handling exceptionally large audio files, contingent on hardware capabilities.

Future enhancements will focus on improving translation accuracy for low-resource languages by integrating larger and more diverse datasets. Further optimization of encryption and decryption algorithms will also be pursued to reduce computational overhead and enhance performance on resource-constrained devices.

CONCLUSION

The proposed secure multilingual communication platform with real-time translation and cryptographic security integrates state-of-the-art technologies to deliver a secure, efficient, and intuitive solution for multilingual interactions. By combining audio-to-text conversion, real-time text translation, and Advanced Encryption Standard (AES) cryptographic techniques, the platform ensures that both audio files and their textual transcriptions remain confidential, accessible exclusively to authorized individuals.

This innovative system excels in transcribing audio inputs accurately, translating text into multiple languages offline, and safeguarding the resulting data through robust encryption mechanisms. The incorporation of Whisper for precise audio-to-text conversion and offline neural machine translation models enhances the platform's ability to support diverse languages, enabling seamless real-time communication. AES encryption further fortifies data security by mitigating risks of unauthorized access and ensuring the integrity of transmitted content.

A user-centric approach underpins the platform's design, with the adoption of Streamlit for the user interface facilitating accessibility and ease of use, even for individuals without technical expertise. The intuitive interface, combined with comprehensive security measures, positions this solution as an ideal choice for contexts where confidentiality is paramount. Potential applications include secure communication in domains such as healthcare, legal affairs, and private crosslinguistic interactions.

Despite its strengths, the platform presents opportunities for refinement, particularly in enhancing translation accuracy for low-resource languages and optimizing encryption and decryption processes to efficiently handle large audio files. Future efforts will focus on broadening the scope of supported languages within the translation model and streamlining cryptographic operations to manage larger datasets with greater efficiency.

In conclusion, this platform represents a groundbreaking advancement in secure multilingual communication, setting a benchmark for future innovations aimed at ensuring privacy, security, and effortless communication across linguistic and cultural boundaries.

REFERENCES

1. Pradhan SK, *et al*. Smart Traffic Management System for Emergency Vehicles. Int J of Adv Research in Computer and Commun Eng. 2024 Apr; 12(4): 1101–1108. DOI: 10.17148/IJARCCE.2024.134162.
2. Lavanya E, Shruti P, G. Anbu Selvi, N. Senthamilarasi. Smart Traffic Control System Using AI. Int J Multidiscip Res. 2024 Mar 15; 6(2): 1–6. Available from: https://www.ijfmr.com/research-paper.php?id=14871.
3. Vaswani A, Shazeer N, Parmar N, Uszkoreit J, Jones L, Gomez AN, Kaiser Ł, Polosukhin I. Attention is all you need. Advances in Neural Information Processing Systems. 2017; 30: 5998–6008.
4. Djahel S, Salehie M, Tal I, Jamshidi P. Adaptive traffic management for secure and efficient emergency services in smart cities. In 2013 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops). 2013 Mar 18; 340–343.
5. Sumi L, Ranga V. Intelligent traffic management system for prioritizing emergency vehicles in a smart city. Int J Eng. 2018 Feb 1; 31(2): 278–83.
6. Othmane LB, Cerqueus T, Thiery A, Salehie M, Noel N, Labaere A, Domingues R, Cordier A, Ventresque A, Pasquale L, Perry P. Response to emergency situations in a traffic management system. In World Congress on Computer Applications and Information Systems (WCCAIS). 2015.
7. Cong S, Zhou Y. A review of convolutional neural network architectures and their optimizations. Artif Intell Rev. 2023 Mar; 56(3): 1905–69.
8. Jmour N, Zayen S, Abdelkrim A. Convolutional neural networks for image classification. 2018 International Conference on Advanced Systems and Electric Technologies (IC_ASET). 2018 Mar; 397–402. Available from: https://ieeexplore.ieee.org/document/8379889.
9. Wang Y, Deng Y, Zheng Y, Chattopadhyay P, Wang L. Vision Transformers for Image Classification: A Comparative Survey. Technologies. 2025 Jan 12; 13(1): 32.
10. Raffel C, Shazeer N, Roberts A, Lee K, Narang S, Matena M, Zhou Y, Li W, Liu PJ. Exploring the limits of transfer learning with a unified text-to-text transformer. J Mach Learn Res. 2020; 21(140): 1–67.
11. Wang M, Lin Y, Tian Q, Si G. Transfer learning promotes 6G wireless communications: recent advances and future challenges. IEEE Trans Reliab. 2021;70(2):790–807. doi: 10.1109/TR.2021.3062045.
12. Suslowicz C, Krishnan AS, Schaumont P. Optimizing cryptography in energy harvesting applications. In Proceedings of the 2017 Workshop on Attacks and Solutions in Hardware Security. 2017 Nov 3; 17–26.
13. Baudron O, Gilbert H, Granboulan L, Handschuh H, Joux A, Nguyen P, Noilhan F, Pointcheval D, Pornin T, Poupard G, Stern J. Report on the AES Candidates. In Proceedings from the Second Advanced Encryption Standard Candidate Conference, National Institute of Standards and Technology (NIST). 1999.
14. Ermoshina K, Musiani F, Halpin H. End-to-end encrypted messaging protocols: An overview. In Internet Science: Third International Conference, INSCI 2016, Florence, Italy, September 12-14, 2016, Proceedings 3. Cham: Springer International Publishing; 2016; 244–254.
15. Papineni K, Roukos S, Ward T, Zhu WJ. Bleu: a method for automatic evaluation of machine translation. In Proceedings of the 40th annual meeting of the Association for Computational Linguistics. 2002 Jul; 311–318.

