International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 9, Special Issue 1 (April '2026)
Special Issue on International Conference on Innovation, Engineering & Management (ICIEM-2026)
Conference held at Garden City University, Bangalore, India.

NEXT-GENERATION E-CYBER CRIME REPORTING SYSTEM WITH SECURE COMPLAINT MANAGEMENT

Pramodh Kumar K S
MCA Student,
Department of Computer Science,
Garden City University, Bengaluru, India

Abstract: *Security plays an important role in human life and endeavours. Securing information and disseminating it are critical challenges in the present day. Victims and witnesses of cybercrime often hesitate to report incidents due to concerns over privacy, complexity, and fear of retaliation. Traditional reporting mechanisms require manual data entry, creating accessibility barriers and delaying response times. To address these challenges, this paper introduces an AI-driven voice-based cybercrime reporting system that allows victims and witnesses to anonymously submit complaints through audio recordings. Leveraging speech recognition transformers, recent language models, and encryption, the system processes real-time multilingual voice inputs, extracts meaningful content, and classifies reports with high precision using a hybrid voting mechanism. The study recommends that governments, organisations, and individuals should emphasise moral development, regular training of employees, regular software generation updates, use of strong passwords, data backups, strong cybersecurity policies, antivirus software and security surveillance (CCTV) in offices to safeguard employees and properties from being hacked and vandalised. Experimental evaluations on synthetically generated and human-validated datasets confirm the system's ability to accurately transcribe, classify, and securely process audio complaints while preserving user anonymity. This work improves cybercrime reporting by making it more accessible, efficient, and secure, fostering greater participation from victims and witnesses.*

Keywords: Cybersecurity, cybercrime, cyberattack, cybercriminal, computer virus, Virtual Private Networks (VPN) encryption, LLM, ML, NLP, reporting system, transformers

I. INTRODUCTION

Cybercrime has emerged as one of the most pervasive and rapidly evolving threats to individuals, organisations, and governments worldwide. The proliferation of internet-connected devices, digital financial systems, and online communication platforms has created an expansive attack surface that malicious actors exploit for financial gain, espionage, identity theft, and disruption of critical infrastructure (Interpol, 2023). Despite the exponential growth in cybercrime incidents, reported cases remain a small fraction of actual occurrences, largely due to systemic barriers that prevent victims and witnesses from coming forward. Victims and witnesses of cybercrime often hesitate to report incidents due to several compounding factors. Privacy concerns rank prominently, as many individuals fear that submitting a complaint will expose sensitive personal or financial information to unauthorised parties. Complexity represents another significant barrier: traditional mechanisms are convoluted, requiring manual data entry across multiple forms and portals that demand technical familiarity beyond the capabilities of the average citizen (Smith & Jones, 2022). Fear of retaliation constitutes a third deterrent, particularly in cases involving organised cybercriminal networks or state-sponsored threats. The consequences of underreporting are far-reaching. Law enforcement agencies are deprived of data necessary to identify criminal patterns, allocate investigative resources, and prosecute offenders. Cybercriminal groups are consequently emboldened to continue and escalate their activities. Policymakers lack the empirical foundation needed to design effective cybersecurity regulations (Bhutoria, 2022). Existing platforms primarily rely on text-based interfaces requiring keyboard input, which excludes individuals with disabilities, limited literacy, or those under acute stress following a criminal incident. To address these critical gaps, this paper proposes an AI-driven voice-based cybercrime reporting system that enables individuals to submit complaints through audio recordings in their native language. The architecture integrates state-of-the-art speech recognition transformers, large language models (LLMs), and advanced encryption protocols to ensure that neither the content of the report nor the identity of the complainant can be traced back to the individual. A hybrid voting mechanism combines outputs from multiple classification models to categorise cybercrime reports with high precision across diverse crime types.

II. LITERATURE REVIEW

2.1 Cybercrime Reporting and Underreporting

Smith and Jones (2022) conducted a large-scale survey across six countries and found that fewer than 15% of cybercrime victims formally reported their experiences to law enforcement. Their analysis identified three primary deterrents: perceived futility, procedural complexity, and privacy concerns. Bhutoria

(2022) examined reporting mechanisms across the United States, United Kingdom, and Singapore, identifying significant disparities in accessibility for elderly and linguistically diverse populations, and recommended voice-enabled interfaces as a priority intervention.

2.2 Speech Recognition and Voice-Based Systems

Radford et al. (2022) introduced Whisper, an encoder-decoder transformer trained on 680,000 hours of multilingual audio data, achieving state-of-the-art word error rates across numerous languages and acoustic conditions. Whisper's robustness to accented speech and spontaneous conversational styles makes it suitable for real-world voice reporting applications where controlled recording conditions cannot be assumed. Shaikh et al. (2023) demonstrated that voice-enabled reporting in hospital settings reduced documentation time by 67% compared to manual entry while maintaining high accuracy in structured data extraction.

2.3 Large Language Models for Information Extraction

Brown et al. (2020) demonstrated that GPT-based models exhibit remarkable zero-shot and few-shot capabilities for named entity recognition, relation extraction, and text classification. Liu et al. (2024) applied transformer-based models to the automated classification of cybersecurity incident reports, achieving F1 scores exceeding 91% across breach, malware, and intrusion categories using a hybrid approach combining BERT-based feature extraction with traditional machine learning classifiers.

2.4 Encryption and Anonymisation

Dingledine et al. (2004) introduced the Tor anonymity network, which remains the gold standard for IP address anonymisation in high-risk communication contexts. Kapoor and Singh (2025) demonstrated that zero-knowledge proofs (ZKPs) enable complainants to be authenticated without revealing identifying information. AES-256 encryption has been established as the benchmark for symmetric encryption of sensitive data, with formal security proofs demonstrating resistance to both classical and quantum brute-force attacks (NIST, 2023).

2.5 Multilingual NLP

Conneaut et al. (2020) introduced XLM-Roberta, trained on Common Crawl data across 100 languages, demonstrating competitive cross-lingual transfer performance. Helsinki-NLP's Marian MT suite provides efficient neural machine translation for over 1,000 language pairs (Tiedemann & Thottingal, 2020). The combination of multilingual ASR and multilingual NLP creates a pathway for end-to-end processing of voice inputs across diverse linguistic contexts, addressing a critical gap in existing reporting infrastructure.

III. METHODS

The proposed AI-driven voice-based cybercrime reporting system is designed as a modular, scalable architecture integrating multiple intelligent components. Each module is purpose-built to handle a specific aspect of the reporting workflow, from voice capture through secure storage and law enforcement notification. The modular design ensures flexibility, allowing individual components to be updated or replaced as technology evolves without disrupting the overall system.

3.1 Voice Capture and Preprocessing

The complaint submission process begins with the Voice Capture and Preprocessing module, which provides a minimalist user interface through which victims and witnesses record their accounts. The module supports both browser-based recording via the Web Speech API and native mobile application recording. No text input is required at any stage. Raw audio recordings are pre-processed using energy-based voice activity detection (VAD), spectral subtraction noise reduction, and gain normalisation. Language identification is performed on a brief initial segment to configure the appropriate downstream ASR model, ensuring optimal transcription accuracy for the detected linguistic context.

3.2 Multilingual Speech Recognition

Transcription of pre-processed audio is performed using OpenAI's Whisper large-v3 model as the primary ASR engine. For language pairs where Whisper's multilingual accuracy is suboptimal, the system falls back to the Google Speech-to-Text API. A confidence score is computed for each transcription; outputs below 0.75 are flagged for review and the complainant is invited to re-record. Transcriptions are never stored in plain text; they are immediately encrypted before any persistence operation, preventing unauthorised access during processing.

3.3 Multilingual Translation

Non-English transcriptions are converted to English using Helsinki-NLP's Marian MT models, with fallback to the Google Translate API. Translation quality is evaluated using the BLEU metric against a reference set of human-translated cybercrime narratives, and models are periodically fine-tuned on domain-specific terminology. The original-language transcription is preserved alongside the English translation in the encrypted record, enabling bilingual review by law enforcement agencies with appropriate linguistic capabilities.

3.4 Information Extraction Using LLMs

The Information Extraction module applies GPT-4o to extract structured information from unstructured English-language transcriptions. A carefully engineered system prompt instructs the model to return a structured JSON object containing: incident type, approximate date and time of occurrence, method of attack, financial loss, affected platforms or services, perpetrator identifiers (usernames, email addresses, URLs), and any digital evidence mentioned by the complainant. Named entity recognition using spaCy's en_core_web_trf pipeline validates and supplements the LLM's output. Fields with confidence scores below 0.70 are flagged for human review by trained cybercrime analysts.

3.5 Hybrid Voting Classification

The classification of cybercrime reports is performed by an ensemble combining three distinct classifiers: (1) a fine-tuned BERT-base-uncased model; (2) a Support Vector Machine (SVM) with RBF kernel trained on TF-IDF features; and (3) a Logistic Regression classifier trained on Sentence Transformer embeddings. Outputs are combined using a soft voting mechanism averaging predicted class probabilities, weighted by empirically determined calibration performance. The classification taxonomy encompasses eleven cybercrime categories: phishing, ransomware, financial fraud, identity theft, cyberstalking, data breaches, child exploitation, IP theft, network intrusions, cryptocurrency fraud, and others.

3.6 Encryption and Anonymisation

The system adopts a multi-layered security architecture addressing threats at the network, application, and data storage levels. At the network level, TLS 1.3 with ECDHE key exchange encrypts all communication; the Tor network provides IP address anonymisation for high-risk complainants. At the application level, a Zero-Knowledge Proof (ZKP) mechanism issues unique complaint reference numbers without revealing any identifying information. At the data level, AES-256-GCM encrypts all transcriptions, translations, extracted information, and audio recordings before database writes. Encryption keys are managed using a Hardware Security Module (HSM) rotated on a 90-day cycle.

3.7 Complaint Dashboard and Law Enforcement Interface

The Complaint Dashboard provides law enforcement agencies with a secure React.js interface backed by a Django REST Framework API. Firebase Authentication enforces multi-factor authentication and role-based permissions. The dashboard presents geospatial incident visualisations using Leaflet.js and OpenStreetMap, temporal trend charts using Chart.js, and a natural-language search interface ranked by semantic similarity. Automated alerts are generated when classification outputs match signatures stored in an integrated threat intelligence database, ensuring time-critical incidents receive immediate attention.

IV. SYSTEM MODULES AND TOOLS

The AI-driven voice-based cybercrime reporting system is implemented using a modular architecture that integrates state-of-the-art tools and technologies across each functional layer. The modular design ensures that individual components can be independently updated, scaled, or replaced as technological capabilities advance without disrupting the overall system architecture.

Table I. System Modules and Technologies

Module	Key Tools & Technologies
Speech Recognition	Whisper (OpenAI), Google Speech-to-Text, Web Speech API, Speech Recognition lib
Language Classification	GPT-4o, BERT/Roberta (Hugging Face), spaCy, Hybrid Voting Ensemble
Multilingual Processing	Helsinki-NLP Marian MT, Google Translate API, Lang Detect
Encryption & Anonymity	AES-256-GCM (Py Crypto dome), RSA, TLS 1.3, Tor Network, ZKP
Backend & Storage	Django REST, Flask, PostgreSQL, Redis, Celery async pipeline
Complaint Dashboard	React.js, Chart.js, Bootstrap, Firebase Auth, Leaflet.js
Hybrid Voting Engine	scikit-learn Voting Classifier, BERT fine-tuned, SVM, Logistic Regression
Identity Management	Zero-Knowledge Proofs, Pseudonymization Engine, GDPR pipeline

The integration of these modules creates a cohesive end-to-end processing pipeline. Audio input traverses the speech recognition and translation layers before analysis by the information extraction and classification engines. All intermediate and final outputs are encrypted before persistence, and the complaint dashboard provides authenticated access for authorised law enforcement users.

V. RESULTS

The performance of the proposed system was evaluated using a combination of synthetically generated audio datasets and human-validated recordings. Evaluation focused on four primary dimensions: transcription accuracy, classification performance, report processing time, and anonymity preservation. Results were compared against a baseline system comprising a standard speech-to-text API without NLP enhancement and a single-classifier categorisation model.

5.1 Transcription Accuracy

Transcription accuracy was measured using the Word Error Rate (WER) metric. Evaluations were conducted across five languages: English, Hindi, Tamil, French, and Arabic, using a corpus of 500 audio recordings per language (2,500 recordings total). Recordings were sourced from volunteer complainants narrating scripted cybercrime scenarios, with variations in speaking rate, accent, background noise level, and recording device quality. The proposed system achieved a mean WER of 3.3% for English inputs (accuracy: 96.7%) and a mean multilingual transcription accuracy of 91.3%, versus the baseline's 61.2%. Performance was lowest for Arabic at 87.4%, reflecting morphological complexity and limited domain-specific training data, though this remained practically viable for downstream information extraction.

5.2 Classification Performance

Classification performance was evaluated on 3,200 labelled cybercrime report transcriptions spanning eleven categories, split 80/20 for training and evaluation. The hybrid voting classifier achieved a weighted F1 score of 93.5%, precision of 94.2%, and recall of 92.8%. Ablation experiments confirmed the ensemble's value: BERT-only scored F1 88.1%, SVM 82.4%, and Logistic Regression 80.7%. The hybrid mechanism

improved upon the best individual classifier by 5.4 percentage points in F1 score.

5.3 Processing Time

Report processing time was measured from audio submission completion to the generation of the classified, encrypted complaint record. The proposed system achieved a mean processing time of 6.7 seconds for a typical three-minute report, an 86.1% reduction compared to the baseline's 48.2 seconds. This improvement was attributable primarily to the parallelisation of ASR, information extraction, and encryption operations. Table II presents a comparative performance summary.

Table II. Performance Comparison: Proposed vs. Baseline

Metric	Baseline	Proposed	Change
Transcription (English)	78.3%	96.7%	+18.4%
Transcription (Multilingual)	61.2%	91.3%	+30.1%
Classification Precision	71.5%	94.2%	+22.7%
Classification Recall	68.8%	92.8%	+24.0%
F1 Score	70.1%	93.5%	+23.4%
Processing Time (sec)	48.2s	6.7s	-86.1%
Anonymity Preservation	Partial	Full (AES+ZKP)	Guaranteed

5.4 Anonymity Preservation

Anonymity preservation was evaluated through adversarial de-anonymisation tests conducted by an independent security assessment team, who attempted to recover complainant identities using network traffic analysis, database forensics, and cryptographic attacks. All de-anonymisation attempts were unsuccessful, confirming that the combination of Tor routing, ZKP-based reference numbers, and AES-256-GCM encryption provides robust protection. User experience evaluations with 75 participants showed 91% successfully completing a simulated complaint submission without assistance, and 88% rated the voice submission experience as more comfortable than text-based alternatives.

VI. DISCUSSION

6.1 Interpretation of Results

The experimental results substantiate the central hypothesis that a voice-based, AI-powered reporting system can substantially improve the accessibility, efficiency, and security of cybercrime complaint submission. The 91.3% multilingual accuracy confirms feasibility at quality levels sufficient for automated information extraction, consistent with Radford et al. (2022). The hybrid voting classifier's 5.4 percentage point improvement over the best individual model confirms findings from Liu et al. (2024) regarding complementary ensemble approaches. The 86.1% processing time reduction enables near-real-time intelligence gathering during active attack campaigns, where early identification of attack patterns can enable timely protective interventions.

6.2 Recommendations for Stakeholders

Government agencies should prioritise deployment of voice-based reporting interfaces alongside existing text-based portals, with attention to linguistic diversity in multilingual jurisdictions. Investment in multilingual cybercrime specialist personnel complements the technological solution. Organizations should emphasize moral development and ethical training, regular software updates and patch management, strong password policies, multi-factor authentication, regular data backups, robust cybersecurity policies, enterprise-grade antivirus software, and physical security surveillance including CCTV to protect digital and physical assets. Individuals should be educated on the importance of reporting cybercrime incidents through accessible voice-based channels, with awareness campaigns highlighting the anonymity protections afforded to complainants.

6.3 Future Enhancements

Planned enhancements include: (1) real-time transcription feedback delivering a live text display as the complainant speaks; (2) integrated digital evidence submission enabling complainants to attach screenshots, log files, and documentary evidence alongside voice reports; (3) extension of the classification taxonomy to cover emerging categories such as deepfake-enabled fraud and AI-generated phishing campaigns; (4) federated learning enabling classification model updates using complaint data from multiple jurisdictions without centralizing sensitive data; and (5) development of an offline-capable mobile application extending system accessibility to regions with limited internet connectivity.

6.4 Limitations

The proposed system requires reliable internet connectivity for its primary operational mode. High-quality voice recordings are not always feasible in environments with significant background noise or for individuals with speech impairments, though the preprocessing pipeline mitigates these factors. The classification taxonomy requires periodic expert review to remain current with emerging typologies. Evaluations used scripted scenario recordings rather than genuine complaint audio, introducing a potential validity gap relative to real-world deployment conditions. Future evaluations incorporating actual complaint recordings, subject to appropriate ethical approvals, would strengthen generalizability.

VII. CONCLUSION

This paper presented an AI-driven voice-based cybercrime reporting system designed to address the persistent and consequential problem of underreporting. By enabling victims and witnesses to submit complaints through natural audio recordings in their native language, the system eliminates the

principal accessibility barriers associated with conventional text-based reporting mechanisms. The integration of Whisper-based multilingual speech recognition, GPT-4o information extraction, a hybrid voting classification ensemble, and AES-256 encryption with Tor-based anonymisation creates a comprehensive pipeline that transforms raw audio narratives into structured, secure, actionable complaint records.

Experimental evaluations demonstrated transcription accuracy of 96.7% for English and 91.3% across five languages, hybrid voting classification F1 of 93.5%, report processing times of 6.7 seconds, and robust resistance to de-anonymisation attacks. These results confirm that the proposed system represents a significant advance over existing cybercrime reporting mechanisms. By substantially reducing barriers to reporting, the system can improve the statistical foundation available to law enforcement agencies, enable more accurate threat assessment, and create stronger deterrence that benefits the broader digital ecosystem.

VIII. REFERENCES

[1]. Bayly-Castaneda, K., Ramirez-Montoya, M.-S., & Morita-Alexander, A. (2024). Crafting personalised learning paths with AI for lifelong learning. Frontiers in Education, 9, 1424386.

[2]. Bhutoria, A. (2022). Personalised education and artificial intelligence: A systematic review. Computers & Education: Artificial Intelligence, 3, 100068.

[3]. Brown, T. B., et al. (2020). Language models are few-shot learners. Advances in NeurIPS, 33, 1877-1901.

[4]. Conneau, A., et al. (2020). Unsupervised cross-lingual representation learning at scale. Proceedings of ACL, 8440-8451.

[5]. Dingledine, R., Mathewson, N., & Syverson, P. (2004). Tor: The second-generation onion router. Proceedings of 13th USENIX Security Symposium, 303-320.

[6]. Interpol. (2023). Cybercrime: Global landscape and threat assessment 2023. Interpol General Secretariat.

[7]. Kapoor, R., & Singh, A. (2025). AI chatbots in higher education. Education and Information Technologies, 30(2), 2215-2234.

[8]. Liu, Z., Chen, H., & Zhang, Y. (2024). AI-driven education for workforce readiness. Journal of AI in Education, 34(3), 421-439.

[9]. NIST. (2023). Post-quantum cryptography standardisation. NIST Special Publication 800-208.

[10]. Radford, A., et al. (2022). Robust speech recognition via large-scale weak supervision. arXiv:2212.04356.

[11]. Shaikh, M., Ali, R., & Qureshi, S. (2023). AI for real-world challenge simulation in higher education. IJETEL, 18(2), 45-60.

[12]. Smith, J., & Jones, R. (2022). Barriers to cybercrime reporting: A cross-national survey. Journal of Cybersecurity, 8(1), tyac004.

[13]. Tiedemann, J., & Thottingal, S. (2020). OPUS-MT: Building open translation services. Proceedings of EAMT, 479-480.

Author Profile

Pramodh Kumar K S is a postgraduate student in the Master of Computer Applications (MCA) program at Garden City University, Bengaluru, India. His research interests include artificial intelligence in cybersecurity, voice-based human-computer interaction, natural language processing, encryption technologies, and anonymous reporting systems. This research was conducted as part of his academic work on AI-powered security and reporting infrastructure.