HackAware: Cybersecurity, Privacy Awareness and a Personalized Multilingual Chatbot

Dr. Aye Nyein Mon, Wai Yan Tun, Thi Han Soe, Phyo Zaw Lin, Hein Htet San, Lynn Myat Bhone

Natural Language Processing Lab
University of Computer Studies, Yangon (UCSY), Myanmar

Background

- Cybersecurity and privacy risks threaten to undermine the benefits of ICT-driven development.
- Cyberattacks occur globally every 39 seconds, and 95% of breaches involve human error, often through phishing or mishandling malicious files.
- These incidents disrupt essential services, cause financial loss, and erode trust in digital infrastructure, limiting the potential of ICT to contribute to the Sustainable Development Goals (SDGs).
- Traditional security tools remain overly technical, costly, and inaccessible to many users.

HackAware: Cybersecurity, Privacy Awareness and a Personalized Multilingual Chatbot

- ASEAN’s digital transformation is challenged by rising cybersecurity and privacy risks, with human error driving most attacks.
- Existing tools are often too technical and inaccessible, leaving citizens and Small and Medium-sized Enterprises (SMEs) vulnerable while also lacking personalization and language support for ASEAN users, delivering one-size-fits-all solutions that fail to meet local needs.

HackAware: Cybersecurity, Privacy Awareness and a Personalized Multilingual Chatbot

Targets:

- HackAware introduces an AI-powered, multilingual cybersecurity assistant that combines real-time threat detection, privacy risk awareness, and personalized, conversational guidance.
- Pilots in ASEAN universities and SMEs will evaluate improvements in awareness and safer practices, with plans for regional expansion through localized datasets, browser extensions, and gamified learning.
- By making cybersecurity accessible and inclusive, HackAware will strengthen digital resilience and support progress toward the Sustainable Development Goals across ASEAN.

Proposed Method

- HackAware is developed as a hybrid ICT solution integrating AI personalization with cybersecurity scanning tools.

  Core functions include:

  - Conversational AI Chatbot for personalized guidance.
  - Threat Scanning Tools (URLs, files) with categorization of risks.
  - Privacy Risk Detection for hidden permissions, trackers, and weak practices.
  - User-Friendly Interface with interactive results, history, and progress tracking.
  - Browser Extension: Real-time scanning during browsing.
  - Gamified Learning: Quizzes, badges, and challenges to engage users.

- Community Hub: Platform for shared experiences, threat reporting, and peer learning.
- Integration with Security APIs: Link to ASEAN and global threat-intel databases.
- Regional Deployment: Collaborations with universities, SMEs, and NGOs for ASEAN-wide adoption.

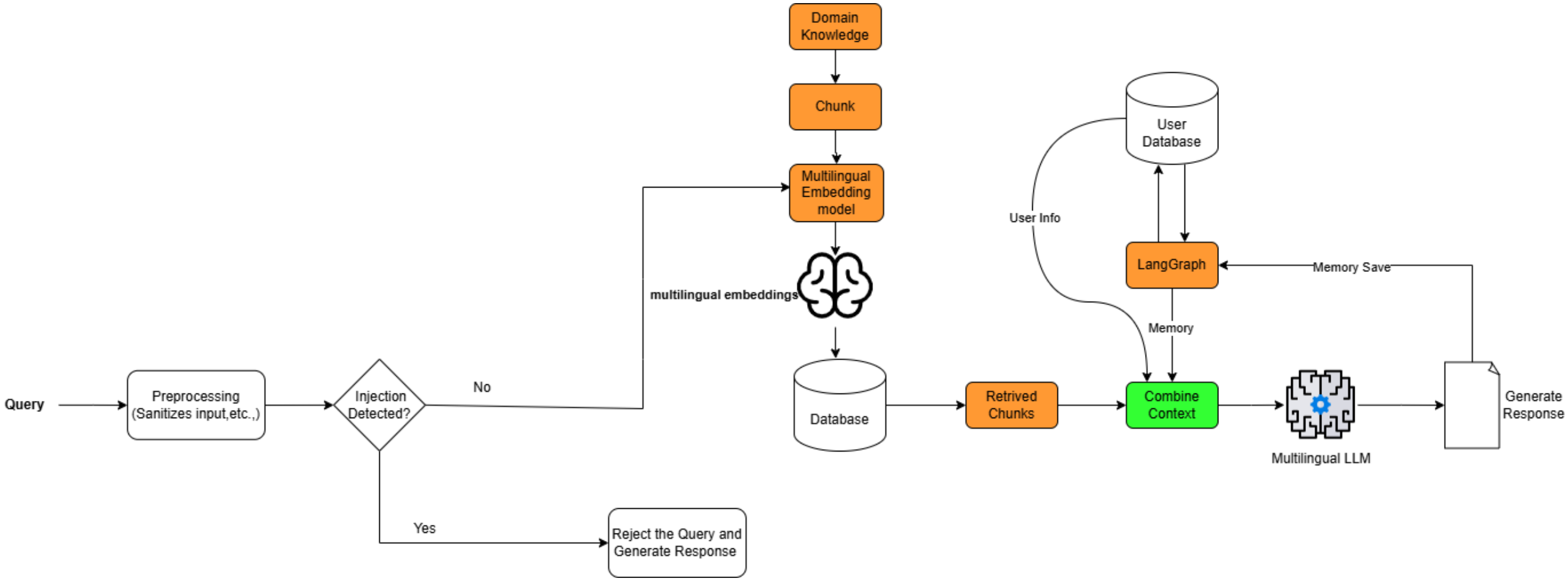

Figure 1: Model Architecture for General Chat

Impact

Scientific and Technological Impact

- **Enhanced AI Training Models:** The method supports the development of smarter AI models that can detect, interpret, and respond to cyber threats in various languages
- **Cyber Threat Detection:** By interacting with users in their native language, the chatbot can more effectively raise awareness about phishing, malware, and social engineering attacks.
- **Scalability and Adaptability:** The chatbot can be integrated across various platforms (web, mobile, messaging apps), making it a flexible tool for cyber hygiene education globally.

Impact

Societal Impact

- **Increased Cybersecurity Awareness:** Educates individuals in their native languages, bridging the digital literacy gap and helping users make safer online choices.
- **Privacy Empowerment:** Users become more aware of how to protect personal data, leading to better individual and societal resilience against identity theft and fraud.
- **Inclusion of Diverse Communities:** Multilingual support ensures non-English speakers and marginalized communities have equal access to vital cybersecurity knowledge.
- **Digital Trust Building:** Encourages trust in digital systems by promoting responsible online behavior and risk awareness.

Impact

Collaborative Impact

- **Global Collaboration:** The chatbot can be a shared open-source or community-enhanced tool, encouraging contributions from international researchers, linguists, and cybersecurity experts.
- **Cross-Sectoral Use:** Can be adopted by governments, educational institutions, NGOs, and private sectors to promote cybersecurity training and awareness.

Output/Outcome:

Scientific Output

- **New Applications in AI and Cybersecurity**: Demonstrates cross-domain applications—combining NLP, cybersecurity education, and user engagement technologies.
- **Benchmark Data Sets**: Creation of annotated multilingual datasets related to cybersecurity awareness, helpful for training and evaluating other AI systems.

Societal Output

- **Open Access Educational Tool:** A freely accessible chatbot that can be used by the public for cybersecurity and privacy education.

- **Multilingual Data Sets:** Language-specific cybersecurity phrasebooks or threat-related terminology databases can be shared with the public or research community.

Collaborative Output

- **New Partnerships:** Collaboration opportunities with universities, cybersecurity organizations, language technology researchers, and international NGOs
- **Interdisciplinary Teams:** Formation of teams with expertise in AI, linguistics, cyber law, and education

Conclusion:

HackAware contributes to:

- improve cyber literacy through adaptive learning
- strengthen secure ICT ecosystems
- build trust and resilience in digital systems
- provide multilingual, personalized, and locally relevant tools, supporting ASEAN regions for a Secure and Smart Community, reducing harm from cyberattacks and enabling safer, more inclusive digital participation

Thank You!!