BOOK OF ABSTRACTS

2ND UNDERGRADUATE RESEARCH COLLOQUIUM - 2026

"Digital Technologies for the Future: Innovation, Integration, and Impact."

20th- 22nd April 2026

DEPARTMENT OF INFORMATION & COMMUNICATION TECHNOLOGY
FACULTY OF TECHNOLOGY
SOUTH EASTERN UNIVERSITY OF SRI LANKA

URCDICT 2026

Book of Abstracts

2nd Undergraduate Research Colloquium of DICT 2026

April 20th - 22nd, 2026

"DIGITAL TECHNOLOGIES FOR THE FUTURE: INNOVATION, INTEGRATION, AND IMPACT."

Department of Information and Communication Technology
Faculty of Technology
South Eastern University of Sri Lanka
Sri Lanka

URCDICT 2026

2ND UNDERGRADUATE RESEARCH COLLOQUIUM OF DICT

SOUTH EASTERN UNIVERSITY OF SRI LANKA - APRIL 20TH-22ND, 2026

Title : *URCDICT 2026, Book of Abstracts*

Published by : *Department of ICT, Faculty of Technology*
South Eastern University of Sri Lanka
Sri Lanka

Pages : *(XVII+82) Pages*

Layout : Mr. K.K.Y.M. Alawathugoda
Ms. A.R. Fathima Shafana

Cover Design : Mr. R.M.N. Rathnayaka
Ms. A. Fathima Musfira

e-ISBN : 978-955-627-501-8

Colloquium Secretariat
2nd Undergraduate Research Colloquium of DICT - 2026
Department of ICT, Faculty of Technology,
South Eastern University of Sri Lanka
University Park
Oluvil #32360
Sri Lanka.

COLLOQUIUM EDITORIAL TEAM

CHIEF EDITOR

Mr. S.L. Abdul Haleem

EDITORIAL TEAM MEMBERS

Mr. R.K.A.R. Kariapper

Dr. I.M. Kalith

Ms. A.R. Fathima Shafana

Mr. M.S.S. Razeeth

e-ISBN 978-955-627-501-8

URCDICT 2026

CHAIRMAN

Mr. M.J. Ahamed Sabani
Head, Department of ICT
Faculty of Technology
South Eastern University of Sri Lanka

KEYNOTE SPEAKER

Prof. Roshan G. Ragel, PhD
Professor in Computer Engineering
University of Peradeniya, Sri Lanka
Senior Member, IEEE

COORDINATOR

Ms. A. Fathima Musfira
Senior Lecturer
Department of ICT
South Eastern University of Sri Lanka

SECRETARY

Ms. A.F. Masroofa
Lecturer (Prob.)
Department of ICT
South Eastern University of Sri Lanka

e-ISBN 978-955-627-501-8

COLLOQUIUM STEERING COMMITTEE

Mr. M.J. Ahamed Sabani	**CHAIRMAN**
Ms. Fathima Musfira Ameer	**COORDINATOR**
Ms. A.F. Masroofa	**SECRETARY**
Mr. A. Mohamed Aslam Sujah	**TREASURER**

TRACK COORDINATORS

Mr. R.K.A.R. Kariapper	Artificial Intelligence Technologies (AIT)
Ms. A.R. Fathima Shafana	Multimedia and Gaming Technologies (MGT) Software Technologies (SWT)
Dr. I.M. Kalith	Network and Security Technologies (NST)
Mr. M.S.S. Razeeth	Ubiquitous Computing Technologies (UCT)

COLLOQUIUM WORKING COMMITTEE

Mr. R.M.N. Rathnayaka
Ms. M.V.D.P.D. Malawana
Mr. K.K.Y.M. Alawathugoda
Ms. U.A.F. Munaffara
Mr. J.A. Aathil

e-ISBN 978-955-627-501-8

LIST OF REVIEWERS

Dr. I. M. Kalith, *Dept. of ICT, SEUSL*

Dr. M. M. Mohamed Mufassirin, *Dept. of Computer Science, SEUSL*

Mr. M. J. Ahamed Sabani, *Dept. of ICT, SEUSL*

Mr. R. K. A. R. Kariapper, *Dept. of ICT, SEUSL*

Mr. S. L. Abdul Haleem, *Dept. of ICT, SEUSL*

Mrs. A. Fathima Musfira, *Dept. of ICT, SEUSL*

Mrs. A. R. Fathima Shafana, *Dept. of ICT, SEUSL*

Mrs. M.S. Faathima Fayaza, *Dept. of IT, SEUSL*

e-ISBN 978-955-627-501-8

MESSAGE FROM THE VICE CHANCELLOR

It gives me a great pleasure to convey my greetings to all participants of the Second Undergraduate Research Colloquium (URCDICT 2026) organized by the Department of Information and Communication Technology (DICT), Faculty of Technology.

The continuation of this colloquium marks a significant step forward in embedding a research culture within our undergraduate academic environment. Showcasing the work of the 2019/2020 final-year ICT students, this event reflects the university's growing emphasis on inquiry-driven learning and innovation.

This year's theme, "Digital Technologies for the Future: Innovation, Integration, and Impact," is both timely and forward-looking. As digital technologies increasingly influence every dimension of society, it is essential for students to not only understand these changes but also actively contribute to shaping them. This platform enables them to present ideas that go beyond the classroom, addressing real-world needs through creative and integrated technological solutions.

I appreciate the dedicated efforts of the Department of Information and Communication Technology in consistently advancing academic initiatives that promote research, critical thinking, and collaboration. Their commitment plays a vital role in nurturing graduates to respond effectively to evolving global challenges. My sincere appreciation goes to the organizing committee and all those who have contributed to making this event a success.

To our students, I encourage you to approach this experience as an opportunity to refine your perspectives, strengthen your confidence, and further your engagement with research and innovation. The knowledge and skills you develop through such platforms will remain valuable throughout your professional journey.

I wish URCDICT 2026 a productive and inspiring colloquium, and I look forward to the meaningful contributions it will bring forth.

Prof. S.M. Junaideen
The Vice Chancellor,
South Eastern University of Sri Lanka
Sri Lanka.

e-ISBN 978-955-627-501-8

MESSAGE FROM THE DEAN

I It gives me immense pleasure to extend my warmest congratulations to the Department of ICT on the successful organization of the Undergraduate Research Colloquium (URCDICT 2026). This annual event has become a cornerstone in nurturing the spirit of inquiry, creativity, and scholarly excellence among our undergraduate community. The impressive submission of 76 research papers this year is a testament to the growing enthusiasm and commitment of our students toward advancing knowledge and contributing meaningfully to society.

The theme of URCDICT 2026, "Digital Technologies for the Future: Innovation, Integration, and Impact", is both timely and inspiring. We live in an era where digital technologies are reshaping every aspect of human life—from education and healthcare to governance and industry. Innovation drives progress, integration bridges disciplines, and impact ensures that our efforts resonate beyond academic boundaries to create tangible benefits for communities and the nation at large. By engaging with these dimensions, our undergraduate researchers are not only preparing themselves for professional success but also positioning themselves as agents of positive change in a rapidly evolving world.

As Dean of the Faculty of Technology, I am proud to witness the dedication of our ICT students, the guidance and the support of our academic community converging to make URCDICT 2026 a reality. I encourage all participants to embrace this opportunity to share ideas, challenge perspectives, and build collaborations that will extend far beyond this colloquium. May this event inspire you to continue your journey of discovery with passion, integrity, and purpose.

I wish URCDICT 2026 every success and look forward to seeing the remarkable contributions of our undergraduate researchers shaping the future of digital technologies.

RK. Ahmadh Rifai Kariapper
Dean, Faculty of Technology
South Eastern University of Sri Lanka
Sri Lanka.

e-ISBN 978-955-627-501-8

MESSAGE FROM THE CHAIRMAN

It is with great pleasure and pride that I extend my warmest greetings to all participants of the Second Undergraduate Research Colloquium of the Department of Information and Communication Technology (URCDICT 2026), Faculty of Technology, South Eastern University of Sri Lanka, held under the theme *"Digital Technologies for the Future: Innovation, Integration, and Impact".*

Building upon the success of the inaugural colloquium, this second edition marks a significant milestone in our continued efforts to cultivate a strong research culture among undergraduate students. The Department of ICT has, within a short span, demonstrated commendable progress in promoting innovation, critical thinking, and academic excellence. This achievement reflects the collective dedication of academic staff, the enthusiasm of our students, and the shared vision of embedding research as a fundamental component of undergraduate education.

This colloquium provides a valuable platform for final-year students of the 2019/2020 ICT batch to present their research findings, exchange ideas, and engage in constructive academic discourse with peers, faculty members, and industry representatives. Such interactions not only strengthen research capabilities but also foster collaboration, critical inquiry, and intellectual growth. To our young researchers, I encourage you to approach this opportunity with curiosity, confidence, and a commitment to excellence. Your contributions extend beyond academic requirements - they play an important role in shaping your professional identity and contributing to the broader digital transformation of society.

I take this opportunity to express my sincere appreciation to the coordinator, secretary and the organizing committee for their dedication and commitment in successfully planning and executing this colloquium. I also extend my gratitude to the editorial team for their meticulous efforts in compiling and maintaining the quality of the research proceedings.

I am confident that URCDICT 2026 will further strengthen the department's commitment to research excellence and contribute to building a sustained culture of innovation and scholarly achievement.

I wish all participants a highly productive and inspiring colloquium.

Mr. M.J. Ahamed Sabani
Chairman / URCDICT2026
Head, Department of ICT
Faculty of Technology
South Eastern University of Sri Lanka
Sri Lanka.

e-ISBN 978-955-627-501-8

MESSAGE FROM THE COORDINATOR

It is with great pleasure that I welcome you to the Second Undergraduate Research Colloquium (URCDICT 2026) organized by the Department of Information and Communication Technology, Faculty of Technology.

This year's colloquium showcases the research efforts of the 2019/2020 final year ICT students, reflecting their dedication, creativity, and commitment to addressing real-world challenges through technology. The continuation of this event marks an important step in strengthening a sustainable research culture within our undergraduate community.

The theme, "Digital Technologies for the Future: Innovation, Integration, and Impact," highlights the transformative role of digital advancements in shaping our society. The projects presented in this colloquium demonstrate not only technical competence but also the ability of our students to integrate knowledge and create meaningful impact through innovative solutions.

As the coordinator, I take great pride in witnessing the growth and achievements of our students throughout their research journey. This platform serves as an opportunity for them to present their ideas, receive constructive feedback, and engage in academic dialogue that will further enhance their learning experience.

I would like to express my sincere gratitude to the Vice Chancellor, Dean, Head of the Department, academic staff, supervisors, and examiners for their continuous support and guidance. My appreciation also extends to the organizing committee and all those who have contributed to the successful organization of this colloquium. To our students, I encourage you to take this experience forward as a foundation for your future academic and professional endeavors.

Wishing URCDICT 2026 every success.

Ms. Fathima Musfira Ameer
Coordinator / URCDICT2026
Department of ICT
Faculty of Technology
South Eastern University of Sri Lanka
Sri Lanka.

e-ISBN 978-955-627-501-8

MESSAGE FROM THE KEYNOTE SPEAKER

It is a pleasure to be part of URCDICT 2026 and to witness the research enthusiasm and creativity of undergraduate students. Events such as this are important not only because they provide a platform to present ideas, but also because they help nurture the mindset needed to explore, question, build, and contribute.

The theme, "Digital Technologies for the Future: Innovation, Integration, and Impact," is timely and relevant. Today, digital technologies are shaping how we live, learn, work, and solve problems. Yet, the true value of these technologies does not come from innovation alone. It comes from how well we integrate them into real contexts and how meaningfully they create impact for people, institutions, and society.

As young researchers and future professionals, students play an important role in this journey. The future will be shaped not simply by those who use technology, but by those who can apply it thoughtfully, responsibly, and creatively to address real-world challenges.

I congratulate the organizers, staff, and students involved in URCDICT 2026, and I wish the colloquium every success.

Warm regards,

Prof. Roshan G. Ragel, PhD
Professor in Computer Engineering
University of Peradeniya, Sri Lanka
Senior Member, IEEE

e-ISBN 978-955-627-501-8

Second Undergraduate Research Colloquium of DICT 2026

DEPARTMENT OF ICT | FACULTY OF TECHNOLOGY | SEUSL

"Digital Technologies for the Future: Innovation, Integration, and Impact"

The Undergraduate Research Colloquium of DICT- 2026, organized for the second time by the Department of Information and Communication Technology (ICT), Faculty of Technology, South Eastern University of Sri Lanka (SEUSL), marks a significant milestone in promoting research and innovation among undergraduates. This inaugural event provides an inspiring platform for students to present their work, exchange ideas, and contribute to shaping a society strengthened by technological progress and digital empowerment.

This year's colloquium features 76 abstracts, representing diverse and forward-looking studies across five thematic tracks: *Artificial Intelligence Technologies, Multimedia and Gaming Technologies, Network and Security Technologies, Software Technologies, and Ubiquitous Computing Technologies*. Each track highlights emerging and globally relevant research directions within ICT.

The Artificial Intelligence (AI) Technologies track presents 25 papers focusing on machine learning, intelligent systems, and data-driven solutions addressing real-world challenges. The Multimedia and Gaming Technologies (MGT) track, comprising 8 papers, emphasizes Human–Computer Interaction (HCI), user experience, game development, and interactive design. The Network and Security Technologies (NST) track includes 24 papers dealing with cybersecurity, secure communication, and network performance enhancement. The Software Technologies (SWT) track, with 5 papers, explores innovative software design, development methodologies, and practical system implementations. Finally, the Ubiquitous Computing Technologies (UCT) track, featuring 14 papers, investigates emerging trends in pervasive systems, smart devices, and context-aware computing environments.

Collectively, these research contributions demonstrate the creativity, analytical ability, and dedication of young scholars in advancing technological solutions for societal benefit. The 2nd Undergraduate Research Colloquium of DICT (URCDICT 2026) stands as a platform that nurtures innovation, encourages collaboration, and empowers the next generation of ICT professionals to lead transformative change for a sustainable future.

e-ISBN 978-955-627-501-8

TABLE OF CONTENTS

e-ISBN 978-955-627-501-8

e-ISBN 978-955-627-501-8

e-ISBN 978-955-627-501-8

e-ISBN 978-955-627-501-8

e-ISBN 978-955-627-501-8

e-ISBN 978-955-627-501-8

e-ISBN 978-955-627-501-8

ABSTRACT OF KEYNOTE SPEECH

Digital Technologies for the Future: Innovation, Integration, and Impact

Roshan G. Ragel

Professor in Computer Engineering, University of Peradeniya, Sri Lanka

Artificial Intelligence is becoming a major force in digital transformation across nearly every sector. From education, healthcare, and agriculture to industry, finance, and public services, AI is no longer used only as a standalone tool for prediction, automation, or content generation. Its real potential is realized when it is integrated with data systems, connectivity, cloud platforms, domain knowledge, and human decision-making to create solutions that are practical, scalable, and socially relevant.

This keynote will examine how AI is reshaping the future of digital technologies by moving beyond isolated applications toward integrated systems that create measurable impact. It will discuss how innovation today increasingly depends not only on advances in algorithms, but also on the ability to connect technologies, people, and processes in meaningful ways. The talk will also highlight the importance of responsible and context-aware deployment, especially in environments where resources, needs, and priorities vary widely.

For students and young researchers, this shift presents both an opportunity and a responsibility. The future will be shaped by those who can combine technical skill with creativity, systems thinking, and an understanding of real-world challenges. In that sense, AI-driven digital transformation is not only about smarter technologies, but also about building solutions that truly matter.

e-ISBN 978-955-627-501-8

TRACK – AI TECHNOLOGIES

e-ISBN 978-955-627-501-8

Real Time Suspicious Activity Detection in Banking Environments using Edge AI CCTV Cameras with Model Optimization and Mobile Alerting

J.M. Lahiru Buddhika Jayasundara[1] and A. Mohamed Aslam Sujah[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]2001lahiru123@gmail.com, [2]ameersujah@seu.ac.lk

Abstract

Intelligent surveillance systems have been necessary in the security systems to achieve safety in risky areas like banks and Automated Teller Machine areas. Conventional CCTV systems are extensively employed to provide surveillance services, but they are quite dependent on human operators and are usually restricted in capacity to detect and act on any suspicious activities in real time. This leaves a significant gap in anticipatory identification of threats and decision-making. This research developed a system of the suspicious activity detection in a real-time based on Edge AI and deep learning. The system is based on connecting an IP camera and a Raspberry Pi edge device that will allow local processing of video streams. It uses YOLO based object detection model to detect important objects like weapons, helmets, masks, and human presence. Optimization methods such as quantization and conversion to TensorFlow Lite were used to increase the performance of the system with resource-constrained hardware. In addition, the system includes the behavioral analysis based on time tracking that helps identify loitering in sensitive zones. Through the examination of the movement patterns and the length of time of individuals the system would be able to detect the possible suspicious behavior more efficiently. When this is identified, the system sends real-time alerts, such as voice warnings and mobile messages, in this way, supporting proactive and reactionary measures. Performance metrics used to evaluate the system include detection accuracy and latency with Precision of about 0.92-0.94, Recall of 0.86-0.88, and a maximum F1-score of 0.89 with confidence threshold of about 0.37, which is a good real-time system with low computational cost. The edge computing approach lowers the reliance on cloud computing infrastructures, minimizes latency, and improves data privacy.

Keywords: *Edge AI, Intelligent Surveillance, Loitering Detection, Object Detection, Real Time Monitoring, Suspicious Activity Detection, YOLO*

A Comparative Study of Hybrid and On-Device Explainable Deep Learning for Chest X-ray Abnormality Screening with User-friendly Text Voice Explanations in a Mobile Application

M.H.A. Hafas[1] and M.S. Suhail Razeeth[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]ahmedhafas105@gmail.com, [2]razeethsuhail@seu.ac.lk

Abstract

Despite being highly accurate at analyzing medical images, the translation of deep learning (DL) models into clinical practice is hinder by three significant issues: the inability of neural network models to provide reliable alerts on the uncertainty of their prediction, the impossibility of accessing these models on a mobile device due to the large amounts of computation required, and the lack of transparency in the decision-making process of the models. This research proposes a mobile decision support system designed to track abnormalities on chest x-rays, prioritizing clinical safety and transparency. Using the NIH ChestX-ray14 dataset, the study initially evaluated a hybrid Tri-Ensemble featuring Vision Transformers (ViT) and CNNs. However, empirical results revealed significant overfitting in Transformer-based models (96.8% training vs. 66.54% validation accuracy), leading to the development of a highly optimized pure CNN ensemble DenseNet121, EfficientNetB0, and ConvNeXtTiny. To ensure clinical reliability, a new Selective Classification (Triage) algorithm was implemented to detect model uncertainty; Predictions within a probability range of 0.35 to 0.65 are automatically redirected to human experts via a webhook pipeline. Transparency is addressed through Score-CAM Explainable AI (XAI), which generates noise-free visual heatmaps converted into humancentric, multimodal audio summaries. Finally, a comparative study of deployment architectures – from Python/Flask cloud backends to TensorFlow Lite quantized models for offline inference at the edge – was conducted using a Flutter mobile app. Experimental data demonstrates that by eliminating epistemic uncertainty through the screening safety net, the CNN ensemble achieved 86.14% accuracy and a clinical confidence Area Under the Curve of 0.88. This study provides a viable roadmap for implementing reliable, interpretable, and resource-efficient AI in contemporary mobile health (mHealth) ecosystems.

Keywords: *Deep Learning, Chest X-ray, Explainable AI (XAI), Selective Classification, Mobile Health (mHealth), CNN Ensemble, Triage Mechanism, Mobile App Framework, Automation*

e-ISBN 978-955-627-501-8

Customer Churn Prediction for Sri Lankan Restaurant Chains Using Machine Learning

F.S. Ahamed[1] and A.R.F. Shafana[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]shafeeahamed494@gmail.com, [2]arfshafana@seu.ac.lk

Abstract

The restaurant industry is highly competitive, with customers able to discontinue their engagement at any time, leading to revenue loss and reduced customer retention. Identifying customers at risk of churn is therefore essential for sustaining business performance. This research develops a machine learning–based approach to predict customer churn using real-world transaction data collected from two popular restaurants comprising 42485 transaction entries . The dataset includes transaction-level information such as order dates, bill amounts, purchased items, and payment details. These data were aggregated to the customer level to enable effective modeling. Feature engineering was conducted using the Recency, Frequency, and Monetary (RFM) framework, and churn was defined based on customer inactivity over a 60 days. Three machine learning models namely, Logistic Regression, Random Forest, and XGBoost were evaluated using accuracy, precision, recall, and F1-score. Logistic Regression consistently outperformed the other models across both datasets, achieving accuracy between 0.873 and 0.913, precision between 0.914 and 1.000, recall between 0.510 and 0.815, and F1-scores between 0.675 and 0.861. Feature importance analysis revealed that frequency is the most significant predictor of customer churn, while the monetary feature indicates that customers with lower overall expenditure are more likely to churn. These findings are consistent with the principles of the RFM model, emphasizing the importance of customer activity and purchasing behavior in retention prediction. The results demonstrate the effectiveness of machine learning techniques in identifying churn-prone customers. The proposed approach enables restaurants to implement targeted retention strategies, thereby improving customer loyalty and overall profitability.

Keywords: *Customer Churn Prediction, Machine Learning, Restaurant Analytics, RFM Model, Customer Behavior Analysis, Predictive Modeling*

e-ISBN 978-955-627-501-8

Multilingual LLMs for Promoting Regional Tourism in Sri Lanka

P.W.D.M.K. Thushari[1] and A. Mohamed Aslam Sujah[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]dilmimadumalka67@gmail.com, [2]ameersujah@seu.ac.lk

Abstract

Tourists frequently encounter challenges in accessing accurate, comprehensive, and contextually relevant information about historical attractions. Existing tourism information systems are predominantly based on static content, offering limited interactivity and minimal personalization, which constrains user engagement and the overall quality of the visitor experience. However, recent advancements in Artificial Intelligence (AI) present significant opportunities to transform how tourism information is delivered and consumed. In this context, the development of AI powered, multilingual chatbot system offers a promising solution. By leveraging Retrieval Augmented Generation (RAG), such a system can dynamically integrate reliable data sources to generate precise, up-to-date, and context-aware information about historical sites across Sri Lanka. The methodology to achieve this begins with data collection by scraping data from reliable online sources, followed by data cleaning and structuring, with the result being JSON-formatted data. The data is then processed using a chunking approach, so that embeddings can be generated through Azure OpenAI embedding models. In order to enable fast and accurate data retrieval through a user query, the embeddings used in one step are now used in another step, where the actual embeddings generated in the previous step are retrieved using vector databases like Pinecone. The system will retrieve the required information by embedding the user query and comparing it to all request-related stored embeddings; therefore, the system will extract accurate data with the proper context. GPT model combines retrieved contexts and user queries to produce informative answers. A custom dataset is used to fine-tune the response and provide a better domain-specific understanding. FastAPI for backend and React for frontend technologies are used to implement this work and create an interactive user interface. It is anticipated that this research project will improve tourist experience, access to historical information, and support the development of regional tourism in Sri Lanka.

Keywords: *Artificial Intelligence, Azure OpenAI, Large Language Model, Pinecone, Retrieval Augmented Generation, Sri Lanka Tourism, Tourism Chatbot, Vector Database*

Design and Development of AI & Machine Learning-Based Diabetes Disease Evaluation System [REEF-DDES]

M.A.M. Thashreef[1] and R.K.A.R. Kariapper[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]reef.2trameen@gamil.com, [2]rk@seu.ac.lk

Abstract

In the Sri Lankan healthcare context, diabetes remains one of the most prevalent chronic diseases, contributing significantly to mortality and long-term health complications. The increasing number of diabetes patients has created a need for efficient and automated solutions to support early detection, continuous monitoring, and timely intervention for effective disease management. However, conventional healthcare systems often depend on the manual analysis of medical records, which is time-consuming and prone to human error. Thus, a Sri Lanka–focused diabetes prevention and evaluation system is proposed, designed with both doctor (admin) and patient dashboards to improve interaction and data accessibility. The system integrates machine learning and artificial intelligence techniques to enhance diagnostic accuracy and patient care, utilizing supervised learning algorithms such as Decision Trees, Random Forests, and Support Vector Machines to analyze key clinical parameters and patient risk factors, enabling accurate classification of diabetes stages. Furthermore, the system incorporates a medical glucose report image processing capability that uses machine learning techniques to extract and interpret data from uploaded laboratory reports, reducing manual effort and errors. An AI-based advisory module is also included to provide personalized health recommendations based on individual patient profiles and risk levels. The system supports remote monitoring, secure data management, and real-time interaction between healthcare providers and patients through dedicated dashboards, ultimately aiming to improve early diagnosis, optimize resource utilization, and enhance long-term patient outcomes through automated screening, risk-based evaluation, and continuous follow-up.

Keywords: *Healthcare, Diabetes Classification, Risk Factor Diabetes Prediction, AI Recommender System, Diabetes Remote Screening*

An AI Model Developed for Vehicle Emission Testing, False Detection and Suggesting Conclusions and Answers

M.G.V. Abeykoon[1] and I.M. Kalith[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]19ict019@seu.ac.lk, [2]imkalith@seu.ac.lk

Abstract

This project focuses on making vehicle emission testing smarter and more accurate by using Artificial Intelligence (AI). In traditional systems, emission results depend only on sensor readings. However, these sensors can sometimes produce incorrect data due to issues such as poor calibration, environmental conditions, or human error. Because of this, vehicles may be wrongly marked as failing or passing the test. The proposed AI model improves this process by learning from past emission test data. It understands what normal and abnormal emission patterns look like by analyzing values such as carbon monoxide (CO), nitrogen oxides (NOx), and engine conditions. When a new test is performed, the system compares the results with what it has learned. If something unusual is detected, it flags the result as suspicious instead of making an immediate decision. In addition to detecting errors, the system also provides simple explanations. For example, it can suggest whether a problem is caused by a faulty sensor, incorrect testing conditions, or an actual vehicle issue. It can also recommend possible reasons for real emission problems, helping technicians fix them faster. Overall, this system turns emission testing into a more intelligent and reliable process. It reduces mistakes, improves decision-making, and helps ensure that only vehicles that truly meet environmental standards are approved.

Keywords: *Anomaly Detection, Data Patterns, False Detection, Sensor Errors, Predictive Analytics, Vehicle Emission Testing*

e-ISBN 978-955-627-501-8

Generate Functional Test Cases from Software Requirements using NLP Techniques

M.S. Fathima Afrin[1] and A. Mohamed Aslam Sujah[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]fathimaafrin8283@gmail.com, [2]ameersujah@seu.ac.lk

Abstract

The creation of test cases from Software Requirement Specifications (SRS) requires significant human effort and is essential for ensuring software quality. Manual test case generation often leads to inconsistencies, incomplete system coverage, and extended development time. Existing automated tools provide limited support and lack the capability to accurately interpret natural language requirements. Therefore, there is a need for an intelligent system that can automatically analyze requirements and generate structured functional test cases efficiently. This study presents an Artificial Intelligence system called Test Case Generator, which converts textual requirements into functional test cases using Natural Language Processing and Large Language Models. The developed approach follows a modular pipeline consisting of requirement extraction, validation, classification, and test case generation. A pre-trained BERT model was fine tuned to classify requirements into functional, non-functional, and invalid categories. Subsequently, functional requirements were processed using a Large Language Model (Gemma via Ollama) to generate structured test cases. These test cases include fields such as test case ID, title, preconditions, steps, and expected results. The system was implemented using Python and integrated with a user-friendly interface developed using Streamlit, allowing users to input requirements manually or upload SRS documents. The classification model was evaluated and achieving effective performance in requirement classification. The generated test cases were exported in structured formats such as JSON and CSV for practical use. Experimental results indicate that the proposed system reduces manual effort, improves test coverage, and produces consistent results. This study demonstrates that machine learning and large language models can effectively support automated software testing and enhance overall software quality.

Keywords: *BERT, Large Language Models, Natural Language Processing, Software Testing, Test Case Generation*

Explainable Aspect-Based Product Recommendation System Integrating Aspect-Level Sentiment Analysis, Semantic Embeddings, and Hybrid Retrieval for Personalized and Transparent Suggestions

G.V.N. Nilupul[1] and A. Mohamed Aslam Sujah[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]nilupulnishitha6@gmail.com, [2]ameersujah@seu.ac.lk

Abstract

This research addresses the limitations of traditional product recommendation systems, particularly their inability to understand user intent and provide explainable results. Existing approaches often rely on keyword matching or user interaction data, which restricts their effectiveness in handling natural language queries and unstructured review data. To overcome these challenges, this study presents an intelligent product recommendation system that integrates semantic search and aspect-based sentiment analysis (ABSA) to improve both the relevance and interpretability of recommendations. The system uses Sentence-BERT (SBERT) to generate semantically meaningful embeddings for user queries and product related text, enabling accurate similarity matching. FAISS (Facebook AI Similarity Search) is employed for efficient vector-based retrieval of candidate products. Aspect-based sentiment analysis is applied to extract fine grained sentiment information for specific product features, allowing the system to identify strengths and weaknesses based on user reviews. A cross-encoder model is further used to re-rank the retrieved results, improving the accuracy of final recommendations. The system is implemented as a complete end-to-end application with a React based web interface and a FastAPI backend, enabling users to submit natural language queries and receive recommendations with aspect-level explanations. Additionally, user feedback is incorporated through dynamic score adjustment, allowing the system to refine recommendations without requiring model retraining. Evaluation is conducted using qualitative analysis and Precision@5, where the system achieved an average precision score ranging between 0.80 and 1.00 across tested queries. The results demonstrate that the system effectively retrieves relevant products while providing clear, explainable insights into product strengths and weaknesses.

Keywords: *Aspect Based Sentiment Analysis, Cross Encoder, Explainable AI, FAISS, Natural Language Processing, Recommendation System, Semantic Search, Sentence-BERT*

LANKATRAFFIX: LLM Powered Multilingual RAG System for Sri Lankan Traffic Law Question and Answering

Y. Hanusjan[1] and A. Mohamed Aslam Sujah[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]kanukanushi@gmail.com, [2]ameersujah@seu.ac.lk

Abstract

Access to legal information is a fundamental requirement for fairness, transparency, and accountability, yet citizens in multilingual societies like Sri Lanka frequently struggle to interpret complex traffic regulations due to formal legal language, technical jargon, and linguistic barriers. With Sinhala, Tamil, and English as official languages, the Motor Traffic Act and its amendments remain largely inaccessible to the general public, professional drivers, and even law enforcement officers, particularly in rural areas where legal expertise is limited. General purpose Large Language Models (LLMs) exacerbate the problem through hallucination, generating plausible but inaccurate responses while most existing legal AI solutions are English-centric and cloud-dependent, creating privacy, cost, and connectivity issues in low-resource settings. This research presents LANKATRAFFIX, an LLM powered multilingual Retrieval Augmented Generation (RAG) system specifically designed for Sri Lankan traffic law question and answering. The system integrates the Llama 3.2 model with LangChain and Ollama for fully local execution, ensuring data sovereignty and operational efficiency on modest hardware. A curated knowledge base was constructed from the official Motor Traffic Act (Chapter 203) and recent gazette notifications detailing revised spot fines. Documents were processed using PyPDFLoader, chunked via Recursive Character Text Splitter, and embedded with the multilingual-e5-large model. These embeddings are stored in ChromaDB, enabling high-speed, cross-lingual semantic retrieval. When a query is received in any of the three languages, the RAG pipeline retrieves the most relevant legal clauses and augments the prompt, allowing the LLM to generate accurate, contextually grounded, and citable responses. LANKATRAFFIX features a responsive web interface that supports real-time conversational interaction for citizens seeking rule clarifications, drivers checking penalties, and officers verifying statutes in the field. By grounding every answer directly in verified legal sources, the system eliminates hallucination risks while promoting legal literacy and road safety compliance.

Keywords: *Artificial Intelligence, Large Language Models, Legal Question Answering, Low Resource Legal AI, Motor Traffic Act, Retrieval Augmented Generation, Sri Lankan Traffic Law*

e-ISBN 978-955-627-501-8

Real-Time Multi Hazard Detection System for Motorbikes: An Integrated Embedded Vision and Community Mapping Approach

P.L.A.J. Liyanage[1] and M.S.Suhail Razeeth[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]asithjayasahan31@gmail.com, [2]razeethsuhail@seu.ac.lk

Abstract

Hazards on road surfaces like potholes, speed bumps, debris, and crosswalks also have a disproportionate number of victims among motorcycle riders that do not have the onboard safety features that are common in other vehicles. Conventional hazard detection systems are manual inspection or accelerometer-based rudimentary sensors, which do not give early warnings to the rider. The study focuses on the design and deployment of a motorbike-specific, multi-hazard detection and community mapping system that is based on the YOLO engine and is developed in real-time. A YOLOv2-6s object detector model is a recently released and highly capable entry in the YOLO (You Only Look Once) line of object detectors that was trained on a custom balanced dataset of 2,344 annotated images of four hazard categories and then exported to the TensorFlow Lite INT8 quantized format to be deployed on a Raspberry Pi 4 Model B. The embedded platform has a Sony IMX219 camera, a u-blox NEO-7M GPS module, and an active buzzer to provide instant audible feedback on detection. The hazards located are also geo-tagged and uploaded to a Firebase Realtime Database, which is then visualized in a companion native Android application as color-coded labels displayed on a live Google Maps interface. A proximity alert system also alerts the rider 60 meters before any danger had ever been noted in the community database and creates a closed safety loop with each detection, making the road permanently safer to all future riders on the same road. The system shows that a relatively inexpensive edge-deployed computer vision can bridge the divide in having personal real-time warnings and shared crowdsourced hazard maps, a cost-effective and scalable answer to motorcycle road safety that does not require specialized infrastructure.

Keywords: *Road Hazard Detection, Yolov26, Embedded Computer Vision, Raspberry Pi, Real-Time Object Detection, GPS Hazard Tagging, Firebase, Android Mobile Application, Motorcycle Safety, Edge AI*

e-ISBN 978-955-627-501-8

AI-Powered Tutoring System for Enhancing Cybersecurity Skills through Command-Line Tools Analysis

Manmatharaja Mangala[1] and M. J. Ahamed Sabani[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]mathugeethan18@gmail.com, [2]mjasabani@seu.ac.lk

Abstract

In cybersecurity education, students should understand how to use the command-line commands Nmap and Netcat. But lots of students have a hard time deciphering raw terminal outputs and learning what they imply as to security. This makes them not learn effective, practical cybersecurity concepts. Despite the vast opportunities of artificial intelligence in education and cybersecurity, not a single tutoring system that integrates command-line analysis, security reasoning, and understandable explanations is available. This work provides the architecture and design of an AI-guided tutoring system to improve cybersecurity education by systematically exploring command-line applications. The system concentrates on Nmap and Netcat and utilises a hybrid approach which combines deterministic parsing, feature extraction, and AI-generated explanations. Common cybersecurity tasks (service detection, operating system identification, vulnerability scanning, connectivity testing, banner grabbing, and network behaviour analysis) are represented with simulated datasets (in place of real-world attack scenarios to ensure safe training). These datasets are augmented with security knowledge, such as risk rating, CVEs, and recommendations. The system comprises command parsing, output analysis, vulnerability detection, risk scoring, anomaly detection and natural language explanation generation modules. Each and every output will be organised into a single JSON format and will be displayed using a dashboard created with Gradio, allowing the students to have an intuitive and interactive learning experience. The findings indicate that the system is effective in converting the unstructured command line outputs into structured, meaningful feedback that can be used in learning. This article presents the promise of hybrid AI systems to enhance cybersecurity education by making the interpretation of complex technical outputs easier and providing better learning outcomes for students through interactive and explainable feedback mechanisms.

Keywords: *AI-guided system, Command-Line Analysis, Cybersecurity Education, Intelligent Tutoring System, Netcat, Nmap*

e-ISBN 978-955-627-501-8

GlucoDietix: An ML-Based and AR-Based Smart System for Personalized Diabetes Dietary Management for Sri Lanka

V.F. Kishor[1] and F. Musfira Ameer[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]kishofathima814@gmail.com, [2]ameermusfi@seu.ac.lk

Abstract

The effective management of diabetes heavily depends on precise dietary tracking; however, manual logging methods present significant challenges, including frequent inaccuracies, high user burden, and a critical lack of integration with regional food variations. To address these limitations, this study introduces GlucoDietix, a novel mobile-integrated system that automates dietary monitoring by combining advanced Computer Vision with Augmented Reality (AR) portion visualization. A cross-platform mobile application was developed using the Flutter framework, supported by a robust Supabase cloud infrastructure for secure user authentication, profile management, and dietary database routing. Real-time food recognition is facilitated through a YOLOv11-based computer vision model supported by on-device ML Kit and Google Vision fallbacks enabling the automatic identification of localized food categories without manual entry. Upon detection, the system cross-references the identified foods with the user's profile and recent blood glucose readings to dynamically generate personalized meal alternatives and exercise recommendations. Furthermore, AR overlays are incorporated to assist users in visually estimating exact portion sizes directly on their physical plates. The system underwent comprehensive usability and technical evaluation. The results demonstrated that the YOLOv11 model achieved a high detection precision of 86.5% and a Mean Average Precision (mAP) of 84.4% on local cuisine, significantly reducing the errors typically associated with manual data entry. Furthermore, user studies yielded a System Usability Scale (SUS) score of 78.5, confirming that the AR-based portion estimation and automated logging successfully reduced cognitive load and improved informed dietary decision-making. Ultimately, the integration of Computer Vision and AR in GlucoDietix provides a highly accessible, culturally tailored, and practical solution for digital healthcare and diabetes self-management.

Keywords: *Augmented Reality, Machine Learning, Computer Vision, Diabetes Management, Personalized Nutrition, Mobile Application*

Efficient Response to Village Grievances via Emotion-Based NLP on Sinhala Complaint Letters

K.R.H.R. Kahathuduwa[1] and A.R.F. Shafana[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]hiruniransika218@gmail.com, [2]arfshafana@seu.ac.lk

Abstract

In Sri Lanka, village-level government offices receive a substantial volume of complaint letters addressing community issues such as public health, infrastructure deficiencies, and social welfare needs. These complaints are predominantly handled through manual procedures, resulting in delays, inefficiencies, and limited responsiveness in public service delivery. This study proposes an automated framework for processing and assigning priority levels to Sinhala-language complaint letters using advanced Natural Language Processing (NLP) techniques. The system used a fine-tuned XLM-RoBERTa model for emotion detection and prioritization. Domain-specific fine-tuning using complaint data improves the model's accuracy and specificity in identifying critical emotional states, including urgency, frustration, and distress. Based on the detected emotional context and associated confidence scores, complaints are systematically classified into three priority levels: high, medium, and low. The system is implemented as a dynamic web application that supports the submission of complaint letters in PDF or image formats. Optical Character Recognition (OCR) was used to extract textual content, which is subsequently processed in real time. The system outputs include detected emotion, confidence level, and assigned priority, enabling administrative personnel to respond to critical issues more effectively. Post-evaluation results demonstrate that the proposed framework successfully achieved the objective of automating complaint prioritization for Sinhala-language submissions. Emotion-driven classification provided more accurate and meaningful prioritization than conventional methods, with urgent complaints consistently assigned higher priority. This reduced manual workload, improved response times, and enhanced administrative efficiency. The findings highlight the potential of AI-driven local language processing in advancing digital governance and improving public service delivery in Sri Lanka.

Keywords: *Natural Language Processing, Sinhala Letters, Text Emotion Analysis, Priority Classification, Web Application*

Phishing URL Detector Extension using Machine Learning for Web Browsers

A.M. Hansamal[1] and M.J. Ahamed Sabani[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]malinduhansamal99@gmail.com, [2]mjasabani@seu.ac.lk

Abstract

Phishing is still a major web-based cybersecurity threat, and most of the available detection techniques are based on submitting visited URLs to remote servers to analyse them, which poses serious privacy issues. In order to overcome this limitation, this project proposes a privacy-aware Chrome browser extension that classifies phishing URLs on-device and does not send any user information to the outside world. The system uses a Random Forest classifier that has been trained on 19,696 URLs using a hybrid feature set of TF-IDF-based 26-character n-grams and 23 handcrafted structural features such as domain entropy, suspicious top-level domain indicators, brand keyword patterns and digit-letter substitution characteristics. The trained model is made available as a 300-decision-tree JSON file and is put into service by the service worker of the browser extension with a pure JavaScript inference engine, which is compatible with Chrome Manifest V3 limits, which restrict the use of WebAssembly and external inference runtimes. There is a whitelist of known genuine domains that is applied before model inference to enhance reliability and minimise false positives. The test on 3,940 unknown test URLs was scored at 94% accuracy overall, and phishing precision of 0.97 and a recall of 0.90. Cross-validation (5-fold) generated a standard deviation of 0.002 and an average F1-score of 0.937, indicating performance consistency in generalisation. A real-time deployment test with 20 known URLs had 100% correct classification. The suggested system is entirely offline, lightweight and can be deployed in modern browsers; thus is highly suited for real-time user protection. Eliminating the reliance on external servers, the framework increases user privacy and does not decrease the detection performance. The paper shows that efficient on-device machine learning can be feasible to detect phishing in the web environment safely and without violating privacy.

Keywords: *Browser Extension, Chrome MV3, Phishing Detection, Privacy Preserving, TF-IDF, URL Classification*

e-ISBN 978-955-627-501-8

Machine Learning-Based Phishing Email Detection: Algorithm Comparison and Prototype Implementation

S. Hajistha Begum[1] and F.M. Ameer[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]sl.hajistha@gmail.com, [2]ameermusfi@seu.ac.lk

Abstract

Phishing email attacks continue to be a highly resilient cybersecurity threat in the online environment due to the continued exploitation of emails in terms of their content, hyperlinks, and formatting techniques by attackers in order to trick users into providing their sensitive information. However, traditional methods of phishing email attack detection, such as the use of blacklisting techniques and rule-based approaches, have proved ineffective in detecting increasingly complex phishing tactics. Therefore, this research proposes the employment of machine learning algorithms for detecting phishing emails by comparing various machine learning models and developing prototypes. A quantitative experimental approach was used, with data being collected from a dataset comprising emails classified as phishing and non-phishing.Five different supervised machine learning classifiers, including Random Forest, SVM, Naive Bayes, Decision Tree, and Logistic Regression, were trained and tested within the same experimental environment. Performance evaluation measures such as Accuracy, Precision, Recall, and F1 score were used to select the optimal classifier. It is found that machine learning approaches can efficiently classify phishing emails from authentic emails if adequate data pre-processing and feature selection techniques are used. Also, the optimal classifier is integrated into the prototype application through Streamlit, where the user enters the contents of the email, and instant classification outputs are provided together with hints of any detected URLs and key words.

Keywords: *Phishing Email Detection, Machine Learning, TF-IDF, Text Classification, Cybersecurity, Streamlit Prototype*

e-ISBN 978-955-627-501-8

Real-Time Detection of Chicken Eye Diseases Using CNNs: A Mobile-Based Deep Learning Approach

M.Athistakumar[1] and M.S.S. Razeeth[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]athistakumar1804@gmail.com, [2]razeethsuhail@seu.ac.lk

Abstract

Early and precise diagnoses of poultry diseases are needed to keep the flocks healthy, reduce losses indefinitely, and have a sustainable production of poultry. Chicken eye diseases in particular pose a challenge to diagnose at an early stage because of the insidious visual issues, and the conventional manual examination technique tends to be the most subjective with time-consuming and ineffective to use in mass surveillance. This paper aims at solving this problem with a proposal of a real-time deep learning-based system to detect the chicken eye disease in a computer vision. The methodology encompasses the image data collection and processing of the chicken eye data, development and assessment of three neural networks. First, an object detector YOLOv8 was applied to detect and localise the eye region and differentiate between healthy and sick scenarios. After that, the YOLO11n-seg segmentation model was used to hone down the identified areas and further isolate the eye region more specifically, without losing disease-related signal. Lastly, a YOLO11n-cls model of the processed eye image was developed that used the model to classify the image as either healthy or diseased. The given experimental results demonstrate that the object detection model received an accuracy of 71.17, recall of 71.92 and mAP of 0.5 of 75.74 and the segmentation model a mAP of 0.5 of 43.92. The model with the best performance was the classification model with the Top-1 accuracy of 96.20% and Top-5 accuracy of 100%. These results suggest that the framework offered can be successfully used as a tool of real-time screening poultry eye disease and it has a promising future in its usage as a tool in precision poultry farming.

Keywords: *Chicken Eye Disease Detection, Deep Learning, Convolutional Neural Network, YOLOv8, YOLO11n-seg, YOLO11n-cls, Mobile-Based Detection, Precision Poultry Farming*

e-ISBN 978-955-627-501-8

Smart Glove for Real-Time Translation of Tamil Sign Language using Machine Learning

K. R. Rashad Ahamed[1] and M.S.S. Razeeth[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]nameisrashad@gmail.com, [2]razeethsuhail@seu.ac.lk

Abstract

Real-time fluid communication remains a major challenge for the Tamil-speaking Deaf and Hard of Hearing (DHH) community. The existing translation systems rely mostly on cloud computing or a camera, which has high latency and significantly disrupts the usual flow of conversation. To overcome this barrier, there is a critical need for a decentralized, system capable of providing continuous, real-time translation. This research proposes developing an IoT-enabled, edge-computing smart glove capable of translating the dynamic Tamil Sign Language (TSL) both in real time and offline. It records spatiotemporal kinematics using flex sensors and an MPU-6050 IMU connected directly to an ESP32-S3 microcontroller, which is stabilized by a DC power supply to eliminate analog noise. Telemetry data is captured on the device and transmitted via Bluetooth Low Energy (BLE) to the Flutter-based mobile app. For the prediction, the device was trained with a structurally unrolled Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM). A Consecutive Voting State Machine and a rest position null class were also introduced to reduce transitional conversational noise. The optimized CNN-LSTM was tested against a 1280-sequence dataset and achieved a classification accuracy of 94% across 16 gesture categories. The end-to-end edge inference latency was less than 250 milliseconds, and it was smoothly triggered to generate localized bilingual text-to-speech output. The results reveal that the prototype can combine sensor-based kinematic tracking, asynchronous BLE communication, and offline AI prediction in a single implementation with zero-latency application to enable accessible digital communication, which is extremely practical.

Keywords: *Tamil Sign Language, Wearable Smart Glove, Edge Computing, CNN-LSTM, Sensor Fusion, Assistive Technology, Real-Time Translation*

Personalized Resume Generation and Job Matching System using NLP

A.K.F. Rustha[1] and A.R.F. Shafana[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]akf.rustha@gmail.com, [2]arfshafana@seu.ac.lk

Abstract

Modern recruitment processes increasingly rely on Applicant Tracking Systems (ATS), which introduce algorithmic constraints that may disadvantage qualified candidates whose resumes do not conform to required structural and semantic patterns. Conventional static resumes lack adaptability to diverse job descriptions, while unrestricted use of Large Language Models (LLMs) for resume generation risks producing factually inaccurate content. This study presents the design and evaluation of a localized artificial intelligence–driven platform for automated generation of ATS-compliant curriculum vitae. The system adopts a decoupled architecture comprising a React-based client interface, a FastAPI backend serving as a service coordination layer, and a SQLite database for persistent storage, with SQLAlchemy employed for database abstraction. To ensure factual integrity, the proposed method utilizes context-injected prompting, constraining the GPT-4o model to a predefined, user-validated master profile and thereby restricting generation to verifiable information. The platform further incorporates GPT-4o Vision for multimodal text extraction, enabling automated interpretation of job requirements from image-based vacancy postings. System performance was quantitatively evaluated using Term Frequency–Inverse Document Frequency (TF-IDF) vectorization and cosine similarity to measure alignment between generated resumes and target job descriptions. In all test cases, baseline similarity scores remained below 45%, indicating a lack of required semantic markers and keywords. Following the execution of the proposed AI-driven tailoring pipeline, similarity scores consistently exceeded 84%, demonstrating substantial improvement in both lexical and semantic alignment compared to baseline resumes. The findings indicate that constraining generative models with structured personal data enables accurate, context-aware resume generation, thereby improving compatibility with ATS-based screening mechanisms.

Keywords: *Applicant Tracking Systems (ATS), Context-Injected Prompting, Generative AI, TF-IDF Vectorization, Cosine Similarity*

AI Driven Real Time CV Ranking and Feedback Generating Platform for Transparent Candidate Evaluation

A.D.N. Kumarasiri[1] and A. Mohamed Aslam Sujah[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]adnayanathara@gmail.com, [2]ameersujah@seu.ac.lk

Abstract

Recruitment is a critical function in organizations. Traditional CV screening processes are often time-consuming, inefficient, and susceptible to bias. Existing automated recruitment systems rely on static keyword matching and rule-based approaches, which lack adaptability and may fail to identify candidates who are meaningfully aligned with job requirements. Furthermore, candidates frequently receive limited or no constructive feedback on how to improve their CVs, thereby reducing transparency and fairness in the hiring process. This research proposes an AI driven platform for real-time CV ranking and feedback generation, aimed at enhancing recruitment efficiency and ensuring equitable candidate evaluation. The system evaluates and ranks CVs by comparing them with job descriptions using three primary techniques. First, graph-based similarity is employed to assess the alignment between CV keywords and job requirements. Second, semantic similarity is computed using a pre-trained Sentence-BERT model, enabling contextual understanding beyond exact keyword matching. Third, temporal weighting is applied to prioritize recent professional experience, assigning greater importance to more current career information. These approaches are integrated into a composite weighted scoring mechanism to produce an accurate ranking of candidates. The system is implemented using FastAPI, PostgreSQL, and React. Users can upload job descriptions and multiple CVs in PDF format, after which the system automatically performs text extraction, data processing, similarity computation, and generates ranked candidate lists along with feedback suggestions. The proposed approach is evaluated using CV datasets from diverse job domains to assess its accuracy and reliability. The results indicate that the integration of semantic similarity with graph-based methods and temporal weighting significantly improves candidate job matching compared to traditional rule-based screening techniques. This system provides effective tool to reduce screening time while promoting fairness and consistency in candidate evaluation.

Keywords: *CV Ranking, Recruitment Automation, Semantic Similarity, Sentence-BERT, Temporal Weighting*

Real Time Pre-harvest Tomato Ripeness Detection and Weight Estimation using Computer Vision and Deep Learning

S. Hana Hasmath[1] and A. Mohamed Aslam Sujah[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]hanashams10.20@gmail.com, [2]ameersujah@seu.ac.lk

Abstract

Accurate pre-harvest assessment of tomato ripeness and weight plays a crucial role in optimizing harvest timing, improving yield estimation, and reducing post-harvest losses in agricultural practices. Traditional manual methods of evaluation are labour-intensive, time-consuming, and often subjective, leading to inconsistencies in decision-making. This research developed real-time mobile system for tomato ripeness detection and weight estimation. The system uses the YOLOv8 object detector model to identify tomatoes and categorize them into three degrees of ripeness: unripe, semi-ripe, and fully ripe. The custom dataset was created and processed, with annotation and balancing of classes, to improve the performance of the model and decrease bias between the classes. TensorFlow Lite is used to integrate the trained model into an android mobile application, allowing it to efficiently perform inference on device without having to use the internet, making it an appropriate choice to be deployed in the field. Also, the system estimates tomato weight with image geometric computations with a reference marker to create scale normalization and enhance measurement consistency. The system offers a range of weights instead of a single exact value to improve its robustness in a different environmental condition e.g., lighting, perspective, and shape of objects. Furthermore, Firebase Realtime Database is integrated to store, manage, and retrieve scan results, enabling users to track historical data and analyze trends over time. It has been demonstrated that the proposed model gives a precision of 85.2%, recall of 73.5%, and mean Average Precision (mAP@0.5) of 79.5%, which is good detectors and consistent classification accuracy during the various ripeness levels. The system offers a powerful, portable, and user-friendly tool that helps in making decisions in smart agriculture and precision farming settings.

Keywords: *Computer Vision, Deep Learning, Tomato Ripeness Detection, Weight Estimation, YOLO*

CalTracker: A Real -Time Food Recognition System For Calorie Tracking In Sri Lanka

M. Fathima Reeshma[1] and F.M. Ameer[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]fathimareesh527@gmail.com, [2]ameermusfi@seu.ac.lk

Abstract

The increasing prevalence of diet-related diseases such as obesity, diabetes and cardiovascular disease, accurate dietary assessment and monitoring of food intake is imperative for chronic disease prevention. Manual food diaries and self-reported estimation of diet can be cumbersome, time-consuming, biased and subject to human error when the collection of data is performed. To overcome those challenges, this study presents a real-time food recognition and calorie tracking system called CalTracker for Sri Lankan food, developed using computer vision, deep learning, mobile app development, and cloud-based nutrient database, to provide an efficient and easy-to-use dietary planning tool for Sri Lankans. A lightweight YOLOv26n object detection model was trained on a labeled dataset, created from the selected food classes to recognize Sri Lankan food captured from the camera or users' photo gallery. The model was converted to TensorFlow Lite (TFLite) format so that it can be used in an Android app for on-device inference. The app uses Firebase Realtime Database to get the nutritional information about the calories, carbohydrates, proteins, fats, vitamins, and minerals of each of the detected food items. For each detected food item, the nutritional information stored on Firebase Realtime Database is displayed based on a 100g portion. Development and evaluation were conducted in terms of dataset preparation, model training, application development, and actual performance evaluation. The work achieved a high level of recognition accuracy, real-time detection performance, and improved usability for actual dietary records. Adapting the system could provide a culturally relevant, user-friendly approach to recommending dietary and lifestyle improvements.

Keywords: *Calorie Tracking, Computer Vision, Deep Learning, Firebase, Mobile Application, Sri Lankan Cuisine, YOLOv26n*

e-ISBN 978-955-627-501-8

A Secure and Privacy-preserving Framework for AI-powered Student Mental Health Chatbots

P.M.K.B. Nisansala[1] and I.M. Kalith[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]19ict083@seu.ac.lk, [2]imkalith@seu.ac.lk

Abstract

University students commonly experience stress, anxiety, and other psychological challenges, yet many hesitate to seek professional support due to stigma, lack of awareness, or privacy concerns. AI-powered mental health chatbots have emerged as accessible tools for students to express their concerns and receive timely guidance. However, the sensitive nature of mental health data requires robust security and privacy mechanisms to ensure confidentiality, integrity, and ethical use. This research presents a secure and privacy-preserving framework for an AI-powered student mental health chatbot platform. The study identifies significant vulnerabilities in the existing system, including weak authentication, inadequate access control, unsecured data storage, and a lack of encryption. To address these issues, the proposed framework incorporates Bearer Token authentication, Role-Based Access Control (RBAC), end-to-end encryption, secure API communication, and real-time WebSocket-based interaction. Additionally, the platform integrates an emotion detection model to provide context-aware recommendations and improve the overall support experience. Security assessments and penetration testing confirm that the enhanced system effectively mitigates the identified vulnerabilities and provides a safer, more trustworthy environment for handling sensitive mental health information. The results demonstrate that the proposed framework significantly improves data protection, system reliability, and overall user trust. This research contributes a secure, scalable, and ethically aligned approach that universities can adopt to support student well-being responsibly.

Keywords: *Emotion Detection, Mental Health Chatbot, Privacy Preservation, Role-Based Access Control, REST API, WebSockets*

Fingerprint Ridge Pattern Analysis for Automated Gender Prediction Using Deep Transfer Learning in Forensic Applications

J.G.A. Vibhooshitha[1] and A.R.F. Shafana[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]abhishekvibhooshitha@gmail.com, [2]arfshafana@seu.ac.lk

Abstract

Gender prediction from biometric data has gained increasing attention in forensic and security applications as a means of narrowing suspect identification. Among various modalities, fingerprint images have been explored for gender prediction based on secondary biometric traits such as ridge density and pattern characteristics. However, despite its practical relevance, fingerprint-based gender prediction exhibits relatively low accuracy when used in isolation. Traditional approaches, including manual ridge counting and conventional machine learning techniques, are time-consuming, error-prone, and often produce inconsistent results due to variations in image quality and overlapping biometric features between genders. To address these limitations, this study presents an automated gender prediction system based on Deep Transfer Learning. A baseline Convolutional Neural Network (CNN) is developed and compared with fine-tuned transfer learning models, namely VGG16 and ResNet50, pre-trained on ImageNet and adapted for binary classification using frozen convolutional layers and custom classification heads. To mitigate class imbalance, three strategies are investigated: random undersampling, data augmentation using geometric transformations, and a hybrid approach combining augmentation with inverse-frequency class weighting. The models are trained and evaluated on the SOCOFing benchmark dataset, comprising approximately 6,000 fingerprint images, supplemented with self-collected samples acquired through a custom hardware setup using an Arduino Uno and an optical fingerprint sensor. A web-based data collection platform with automated image quality assessment was also developed to support efficient data acquisition and labeling. Model performance is evaluated using accuracy, precision, recall, F1-score, and confusion matrices. Experimental results demonstrate that transfer learning models, combined with balanced training strategies, achieve classification accuracy exceeding 85%, significantly outperforming the baseline CNN. These findings indicate that while fingerprint-based gender prediction alone has inherent limitations, the application of Deep Transfer Learning can substantially improve classification performance, enhancing its applicability in forensic investigations.

Keywords: *Fingerprint Ridge Patterns, Gender Prediction, Deep Transfer Learning, Forensic Biometrics, Arduino Fingerprint Sensor*

e-ISBN 978-955-627-501-8

Stock Management and Data Extraction for Sales Prediction using Point of Sales System

A.S.F. Farha[1] and A. Mohamed Aslam Sujah[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]farhasaleem933@gmail.com, [2]ameersujah@seu.ac.lk

Abstract

Sales forecasting is a fundamental component of supply chain management, serving as a critical link between retailers and manufacturers. However, the retail sector continues to face significant challenges in stock management and demand prediction due to reliance on outdated and manual processes. Accurate sales forecasting is essential for effective decision-making across multiple domains, including customer service, inventory control, and marketing strategies. This research aims to develop a machine learning model capable of predicting sales and providing an optimized stock management approach, with results presented in a clear and interpretable format through visualizations such as graphs and charts. The proposed approach utilizes point-of-sale (POS) data, which includes transactional information such as product details, purchase quantities, customer information, and timestamps. Analyzing such data enables businesses to gain deeper insights into customer behavior and purchasing patterns. The dataset used in this research was obtained from the Kaggle platform and is based on POS system records. Multiple machine learning algorithms including Linear Regression, Random Forest, Lasso Regression, and Decision Tree were developed and evaluated, with particular emphasis on handling multi-attribute variables and capturing seasonal variations to enhance inventory optimization and minimize issues such as stock shortages and overstocking. Experimental results indicate that the Random Forest Regression model outperforms the other models, achieving a Root Mean Square Error (RMSE) of 0.0027 and a Mean Absolute Error (MAE) of 0.0129. These findings demonstrate the effectiveness of the proposed approach in improving forecasting accuracy. Overall, the system provides a comprehensive understanding of customer behavior and purchasing trends, thereby supporting more efficient stock management and informed decision-making in the retail sector.

Keywords: *Decision Tree, Linear Regression, Random Forest, Sales Forecasting, Time Series Analysis*

An Intelligent Real-Time Framework for Human-Verified Medicine Availability using Proximity-Based Ranking and Demand Forecasting

I.G.S. Pravishka[1] and R.K.A.R. Kariapper[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]19ict037@seu.ac.lk, [2]rk@seu.ac.lk

Abstract

Over the past years, the healthcare industry has increasingly adopted digital technologies to enhance service delivery and accessibility; however, challenges such as inaccurate medicine availability information, lack of real-time updates, and inefficient communication between patients and pharmacies continue to affect timely access to essential medications. This study presents an intelligent real-time framework designed to improve medicine availability using human-verified data, proximity-based ranking, and demand forecasting techniques. The proposed system is implemented as a mobile and web-based application that connects patients with nearby pharmacies and enables real-time verification of medicine availability. Patients can search for required medicines and send requests through the application, while pharmacists manually confirm availability based on actual stock conditions, ensuring higher accuracy and reliability. A proximity-based filtering mechanism is used to identify pharmacies within a defined geographic range, providing location-specific results. In addition, an intelligent ranking system prioritizes pharmacy responses based on distance, response speed, and reliability, allowing patients to select the most suitable option efficiently. The system also incorporates demand analysis and basic forecasting techniques to identify frequently requested medicines and predict future demand trends, supporting effective inventory management. The framework is developed using Flutter for cross-platform applications and Firebase for real-time database management, authentication, and cloud services, with Google Maps API integration for location-based functionalities. Experimental results demonstrate that the system improves efficiency in medicine searching, reduces time and effort for patients, and provides accurate real-time information. The integration of human verification, intelligent ranking, and demand forecasting enhances overall system performance and usability, contributing to modern digital healthcare solutions.

Keywords: *Medicine Availability, Proximity Based Ranking, Demand Forecasting, Cloud Computing, Healthcare Technology*

TRACK – MULTIMEDIA AND GAMING TECHNOLOGIES

e-ISBN 978-955-627-501-8

An Empirical Investigation on the Effect of Consistency Design Principle for Enhancing Usability and User Experience: A Study with Prototypes and Leading Websites

R.R. Jahan[1] and A.R.F. Shafana[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]rakfiya2001@gmail.com, [2]arfshafana@seu.ac.lk

Abstract

Consistency is a fundamental design principle in user experience (UX) design. University websites are essential digital platforms for delivering academic and administrative information. However, many suffer from usability issues caused by inconsistent navigation, non-uniform layouts, varying terminology, irregular visual elements, and poor page continuity. These issues increase user confusion, reduce task efficiency, and negatively affect the overall user experience. To investigate the impact of design consistency on usability and user experience, this study adopts a comparative, prototype-based approach focusing on selected Sri Lankan university websites. Initially, five university websites were evaluated by experts using a structured questionnaire and heuristic analysis to assess their level of design consistency and perceived usability. The findings revealed clear variations among the websites and identified one official university website as the weakest in terms of consistency and overall usability, confirming a strong relationship between the two. Based on these findings, a revised prototype of the selected website was developed using Laravel, incorporating improvements in navigation structure, layout consistency, terminology, visual hierarchy, component uniformity, and overall page organization. To evaluate the effectiveness of the redesigned prototype, a within-subject user study was conducted with 40 participants using the System Usability Scale (SUS). The results demonstrated a statistically significant improvement in usability. A paired-samples t-test revealed that SUS scores have significantly increased from 24.06 to 88.19 ($p < .001$), indicating a substantial enhancement in perceived usability following the redesign. This study highlights how expert evaluation findings can be effectively translated into practical redesign decisions to create a more predictable, efficient, and user-friendly university web environment. The results confirm that consistency is a critical interface design principle for improving usability and strengthening user experience in institutional websites. The study further provides practical guidance for consistency-oriented redesign and establishes a foundation for future participant-based usability validation research.

Keywords: *Consistency Design, Usability, User Experience, University Websites, Prototype Development*

e-ISBN 978-955-627-501-8

A Secure 3D Printing Service Platform

O. P. S. Dissanayake[1] and S.L.A. Haleem[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka, Sri Lanka*

[1]opsdissanayake@gmail.com, [2]ahaleemsl@seu.ac.lk

Abstract

The high rate of 3D printing technology development has allowed individuals to plan and produce customized products via online platforms but the transfer of 3D model files between customers and service providers creates a great deal of issues concerning intellectual property (IP) protection and trust. Clients may need to send STL files to various providers to get quotations and the risk of unauthorized copying and reuse is high, whereas service providers can suffer operational risks when clients do not confirm the orders after resources are allocated. This paper suggests a secure web-based 3D printing service platform that will mitigate these issues by using encryption, controlled access, and ownership checks. This system applies the Advanced Encryption Standard (AES) to encrypt 3D model files when uploading, storing, and transmitting files, and guaranteeing the security of design data. The access control is done through a token system to limit access to files to certified service providers spending a restricted time, and a lightweight watermarking method is provided to inject ownership-related content into the 3D models, which can be traced in case of misuse. Its platform is created based on role based client and service provider functions with secure backend infrastructure to support authentication, file management and project management. The anticipated results of this study are better safeguard of intellectual property, less chance of illegal file sharing, and better customer-service provider confidence. Additionally, the suggested solution will advance the safe adoption of digital manufacturing platforms and can be expanded to other file-sharing spaces that need confidentiality and restricted access.

Keywords: *3D Printing, AES Encryption, Access Control, Digital Watermarking, Intellectual Property Protection*

e-ISBN 978-955-627-501-8

Assistive Eye-Tracking System for Partially Blind Users Using Mobile Devices

M.J.A. Dilaikshan[1] and M.S. Suhail Razeeth[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]dilaikshan1445@gmail.com, [2]razeethsuhail@seu.ac.lk

Abstract

Visually impaired individuals find it extremely difficult to use the standard touchscreen mobile devices. Current systems based on eye-tracking are mostly developed with full-sighted users in mind and usually require specialized and costly equipment, thus they become unavailable in low-resource environments. To fill this gap, this research suggests a low cost, software-only mobile eye tracking that is specifically targeted towards users with a partial sight, such as those with myopia and cataract. As far as we can tell, this is one of the first methods that have been aimed at cheap mobile gaze-tracking to partially blind users in developing countries. The suggested system applies a data collection procedure via a smartphone and a multi-input Convolutional Neural Network (CNN) model to approximate gaze direction. In order to eliminate the drawbacks of a limited dataset, data augmentation and model optimization methods were used to improve the performance and generalization. The achieved refined model had a Mean Absolute Error of 0.0082 and a substantial decrease in spatial gaze estimation error in relation to the baseline model. An experimental analysis was done by carrying out a series of user sessions in a controlled and real-world environment. In indoor settings, the system obtained an average accuracy of 70% and in practical application settings of the system, the accuracy was 62 percent. These findings indicate that an eye-tracking software-only, mobile-based solution can be used to obtain reasonable accuracy even when limited amounts of training data are available. In general, this study has shown that the creation of a low-cost, user-friendly gaze-tracking systems based on smartphones is possible, which can be a promising assistive tool to partially blind users, especially in developing countries where special devices are not available to users.

Keywords: *Eye Tracking, Partially Blind Users, Convolutional Neural Network, TensorFlow Lite, Assistive Technology, Flutter, Mobile Accessibility*

e-ISBN 978-955-627-501-8

Development of a Gamified Mobile Application for Improving Kids' Physical Activity with a Focus on Usability

K.K. Bawantha[1] and A.R.F. Shafana[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]bawantha619kalindu@gmail.com, [2]arfshafana@seu.ac.lk

Abstract

In recent years, children have become increasingly engaged in sedentary mobile gaming, which negatively affects their physical health. To address this issue, this study introduces Questigo, an interactive solution that integrates physical activity with engaging gameplay using smartphone sensor technology. This research presents the design and development of a gamified mobile application aimed at improving physical activity and cognitive skills among children aged 8 to 13 years. The application utilizes built-in device sensors, particularly the accelerometer, to detect real-world actions such as jumping and tilting. These movements are mapped to in-game controls, enabling interaction through physical activity rather than traditional touch-based inputs. Two mini-games were developed to combine exercise and cognitive engagement. Active Runner is a lane-based obstacle avoidance game that uses tilt navigation and jump detection to develop reflexes, coordination, and gross motor skills. Sky Climb combines platform jumping with basic mathematical challenges, requiring players to solve equations through movement-based decisions, thereby creating a dual-task environment promoting both physical activity and cognitive performance. The system was developed using React Native and Expo to ensure cross-platform compatibility and accessibility without requiring additional hardware. Two mini-games, Active Runner and Sky Climb, were implemented, along with gamification features such as experience points, levels, and rewards to enhance user motivation and engagement. A preliminary usability evaluation involving 15 participants yielded a mean System Usability Scale (SUS) score of 62.07 (SD = 13.04), indicating marginally acceptable usability along with an engagement score of 6.34 and a low fatigue score of 2.71. However, further improvements may enhance usability and overall user experience, particularly as children may compare this application with present commercially developed games that benefit from advanced game engines, higher production quality, and more immersive gameplay experiences.

Keywords: *Sedentary Mobile Gaming, Gamification, Physical Activity, Cognitive Skills, Accelerometer, Sensor-Based Interaction, Usability Evaluation, Dual-Task Learning*

e-ISBN 978-955-627-501-8

AR Language Park: Exploring the Alphabets in an Immersive 3D World

M.P.H.R. Aberathna[1] and F. Musfira Ameer[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]rashiprabah@gmail.com, [2]ameermusfi@seu.ac.lk

Abstract

Preschool education serves as a vital educational foundation which develops essential language abilities and cognitive skills especially for children who learn English alphabet letters as their second language. The current state of preschool education in Sri Lanka depends on traditional teaching methods which include rote memorization and flashcard use, but these methods do not succeed in keeping young students interested and they do not help with permanent memory retention. This study has created AR Language Park, an Augmented Reality application which enables kids to learn alphabet letters through its interactive 3D visual displays and its various sensory learning interfaces. During the process of creating the application, this study used Unity and Vuforia software, with which it was possible to make image targets work and use animated 3D models of animals as alphabet letters. This study made up a comparative experiment involving 20 preschoolers, who were divided into the experimental group, where AR was applied for learning, and the control group using flashcards. Assessment of learning efficiency took place in the form of post-experimental test; users' involvement and usability were evaluated through observation and Likert scale questionnaire. The experimental group achieved better letter recognition results, reaching an 80% score, which surpassed the control group who obtained a 68% score. From the questionnaire analysis, it was evident that the use of the AR app was associated with complete engagement among users 100% of the time. The study findings confirm that the use of AR applications in learning has significantly improved educational outcomes and participation levels. The research confirms that AR technology is a useful tool in creating learning environments among young children through its interactive teaching techniques, thus allowing the learners to enjoy better educational content than the conventional classroom environment.

Keywords: *Augmented Reality, Alphabet Learning, Early Childhood Education, Letter Recognition, Pre-school Learning, Interactive Learning, Educational Technology.*

A Gamified Mobile Application to Improve English Vocabulary Among Sri Lankan Native Speakers

M.T.F. Farha[1] and I.M. Kalith[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]farhamtf@gmail.com, [2]imkalith@seu.ac.lk

Abstract

The way people study languages has evolved significantly in recent years due to the usage of mobile learning technologies. However, problems like a limited vocabulary, poor pronunciation, and low student engagement hinder Sri Lankan learners' ability to acquire languages effectively. Traditional learning approaches, which are often characterized by repetition, limited contact, and insufficient incentive, lead to reduced learning outcomes. In order to help native English speakers in Sri Lanka enhance their vocabulary and pronunciation, this study proposes a gamified mobile application. Vocabulary learning, interactive exams, and speech-based pronunciation practice are all included on one platform. Gamification elements such as points, levels, badges, and awards are used to boost user incentive and engagement. Flutter and Dart are utilized for cross-platform mobile capabilities, while Supabase is used for backend database management and user authentication. Additionally, the Google Speech-to-Text API is integrated to enable real-time pronunciation feedback. Safe access, efficient data management, and seamless communication between system components are all guaranteed by the system design. System design, implementation, and testing are all carried out in accordance with a structured procedure. Functional and user testing results show that the program works well and offers a delightful educational experience. Gamified learning strategies have been shown to improve vocabulary retention, user motivation, and involvement. The results demonstrate how well mobile learning, gamification, and speech recognition technologies may be used in language instruction. The proposed methodology provides Sri Lankan students with a practical and expandable method to improve their pronunciation and vocabulary in English. Future improvements like more interactive features, improved voice recognition accuracy, and a larger vocabulary can also increase the system's effectiveness.

Keywords: *Gamification, Mobile Learning, Vocabulary Learning, Speech Recognition, Supabase*

ALERTX: Smart AR System for Allergen Identification and Personalized Dietary Feedback Mobile App

A.J. Naflan[1] and M.S. Suhail Razeeth[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]naflan265@gmail.com, [2]razeethsuhail@seu.ac.lk

Abstract

Food allergies represent a major health challenge. Accidentally consuming hidden allergens in complex meals, such as burgers or pizzas, can trigger severe allergic reactions like anaphylaxis or even death. Current dietary management software either uses manual barcode scanning or passive text interfaces; neither of these techniques works in restaurants nor causes hazardous cognitive detachments. Also, using regular generative AI for medical safety is risky because the AI can make up false information, which is called hallucinations. To solve these issues, this research introduces AlerteX, a mobile application that combines edge computing, AI, and Augmented Reality (AR) to provide safe and personalized dietary guidance. Instantaneous food classification using TensorFlow Lite and RAG for clinical accuracy. The user-cryptographically secured biometric profile of his allergies is then combined with this ground-truth data to be run through the Gemini 2.5 Flash Large Language Model to produce a deterministic risk assessment. Using ViroReact and ARCore, the system will display True 6-Degrees-of-Freedom (6DoF) world-locked holographic safety warnings on the real food item. Testing on a variety of Android devices showed that the visual classification was 94% accurate. The latency of transmission through clouds was reduced to a stable 600 to 800 milliseconds using a custom image compression interceptor. RAG pipeline effectively reduces the AI hallucination feedback needed. In Sri Lanka, user acceptance testing identified the positive performance of the high-contrast Midnight Mode and the multilingual support that was dynamic. AlerteX revolutionizes spatial healthcare with performance and privacy.

Keywords: *Large Language Models (LLM), Augmented Reality, Food Allergy Detection, Retrieval-Augmented Generation (RAG), Edge Computing, TensorFlow Lite, ViroReact, Spatial Computing*

ARChemLab – Design and Evaluation of an Augmented Reality Chemistry Lab for Secondary Education

Sulaimalebbe Fathima Asra[1] and F. Musfira Ameer[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]s.asrasulaima@gmail.com, [2]ameermusfi@seu.ac.lk

Abstract

Secondary school chemistry education is crucial in developing the scientific knowledge of the students but it is usually limited by the lack of adequate laboratory facilities, safety issues and the abstract nature of chemical concepts especially in developing nations like Sri Lanka. Conventional laboratory-based instructions are costly, time-consuming and hard to apply efficiently, leading to low student participation and conceptual learning. The proposed study is ARChemLab, an interactive, safe, and affordable mobile-based Augmented Reality (AR) chemistry laboratory, which offers an affordable alternative to traditional laboratory education. The system is based on a combination of mobile AR technology and 3D interactive simulation created on the Unity 3D platform and AR Foundation and implemented on Android. ARChemLab allows students to view virtual chemistry experiments in the real world through a mobile app camera to scan flashcard, and allows them to use curriculum-aligned modules like Atomic Structure Visualization. A quasi-experimental design, which included an experimental and control group of secondary school students, was used to evaluate the system, with data being gathered by means of a pre-test and post-test, engagement surveys, and usability testing. The findings suggest that the students who studied through ARChemLab showed a significant change in the understanding of the concept, engagement, motivation, and satisfaction with learning over the standard methods, whereas the usability results showed that the system is accessible and user-friendly. The paper identifies the possibilities of AR-based mobile applications in improving chemical education through the provision of scalable, safe, and interactive learning environments, which lead to better learning outcomes and facilitates the adoption of digital technologies in secondary school education.

Keywords: *AR, Chemistry Education, Virtual Lab, Mobile Learning, AR Simulation, Interactive Learning, Secondary Education.*

e-ISBN 978-955-627-501-8

TRACK – NETWORK AND SECURITY TECHNOLOGIES

e-ISBN 978-955-627-501-8

Low-Cost Rule-Based Wi-Fi Intrusion Detection System for Deauthentication and Rogue Access Point Attacks using ESP32 for Mobile Environments

A.K.K.H. Mahendra[1] and S.L.A. Haleem[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]19ict001@seu.ac.lk, [2]ahaleemsl@seu.ac.lk

Abstract

Wi-Fi networks have become ubiquitous in homes, educational institutions, and commercial establishments. However, increasing reliance on these networks has elevated associated security risks. Deauthentication attacks are frequently utilized by malicious actors to forcefully disconnect users from their networks. Furthermore, "Evil Twin" or rogue access points are created to deceive devices into connecting, thereby facilitating the theft of sensitive data and credentials. Although large enterprises deploy expensive and complex systems to mitigate these threats, everyday users and mobile environments often remain unprotected. This research addresses this security gap by proposing a highly portable and affordable Wi-Fi analyzer. An Intrusion Detection System (IDS) was developed entirely on an ESP32-S3 microcontroller, costing under 3000 LKR. Unlike high-end security tools, the proposed system operates independently without the need for cloud infrastructure, heavy servers, or complex machine learning algorithms. Instead, rule-based detection logic is employed. The microcontroller continuously hops across Wi-Fi channels to monitor network traffic. Specific attack signatures, such as sudden floods of deauthentication frames, duplicated network names, or anomalous signal strengths, are identified to trigger immediate alerts. To ensure user accessibility, the device hosts an interactive web dashboard. Security data and threat alerts can be monitored, and trusted networks can be managed directly via a standard smartphone browser without requiring additional applications. Extensive laboratory evaluations demonstrated robust performance. Deauthentication and rogue access point attacks were detected with an accuracy ranging from 95% to 100%, while maintaining a false positive rate below 3.5%. Furthermore, continuous monitoring and web hosting were successfully managed by the ESP32-S3 without performance degradation. Ultimately, this project demonstrates that robust, real-time Wi-Fi security can be practically and affordably implemented for edge and mobile environments.

Keywords: *Rule-Based Wi-Fi IDS, ESP32 Edge Computing, Packet Sniffing, Deauthentication, Evil Twin Detection*

e-ISBN 978-955-627-501-8

Lightweight Intrusion Detection System for Wi-Fi Signal Drop Events

Anoshan Yoganathan[1] and M.J. Ahamed Sabani[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]anoshan6@gmail.com, [2]mjasabani@seu.ac.lk

Abstract

Wi-Fi signal issues, such as the sudden change in Received Signal Strength Indicator (RSSI) levels, the presence of a Virtual Private Network (VPN) without the user being aware, and random loss of network connectivity, are an increasing but unreported security threat in the home and small office (SOHO) setting. Enterprise-grade Intrusion Detection Systems (IDS) provide broad-based protection; however, they introduce a heavy computational load and specialised hardware, and their use of deep packet inspection methods is unfeasible in resource-limited and non-technical environments. This paper reports the design, implementation and comparative empirical analysis of two lightweight Python-based IDS prototypes designed to target SOHO Wi-Fi settings. Model 1 is written entirely with the standard library modules of Python, i.e. subprocess, socket, struct, threading, and collections, which results in a zero-dependency deployment that can be run on any machine running Python 3.7 or later without installation. Model 2 uses the pywifi third-party library to communicate with Wi-Fi hardware over an object-oriented interface and allows the acquisition of more detailed scan-level signal data. The two models apply the same set of features: real-time RSSI monitoring, a live graphical dashboard, rule-based anomaly detection and configurable thresholds (−70 dBm warning, −80 dBm critical), VPN detection using a novel baseline-snapshot mechanism, automatic failover to a backup network, desktop notifications, and a user interface written in Tkinter. An empirical assessment of 6 test scenarios based on controlled situations proves that Model 2 attains better RSSI resolution (96.8 vs. 91.2), VPN detection accuracy (95 vs. 89), whereas Model 1 consumes considerably fewer resources (34 MB RAM, 8.6% CPU vs. 58 MB and 11.2%). The two prototypes were able to cover the scenario 100% with zero false positives during startup, which confirms the baseline-snapshot VPN detection design as a credible and new contribution to lightweight home network security.

Keywords: *Intrusion Detection System, Python Standard Library, RSSI Monitoring, SOHO Network Security, VPN Detection, Wi-Fi Security*

SMS Phishing Detection in Sinhala Language using Rule-Based Filtering and Natural Language Processing

W.G.P.B. Wijerathna[1] and M.J. Ahamed Sabani[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]buddhika.pradeep345@gmail.com, [2]mjasabani@seu.ac.lk

Abstract

Mobile communication technology is common in Sri Lanka, which has made most people rely on Short Message Service, SMS, as a constant means of communication. As a result, SMS based phishing, which is often referred to as smishing, has become a serious cybersecurity issue. One such notable trend is the progressive use of the Sinhalese language in phishing texts, which contributes to increased trust in a message and increases the chances of user response. Though this trend is clear, the majority of the available detection systems are optimized to identify English language content, and thus they do not work well to identify data in Sinhala SMS. The study suggests a hybrid system of detection of Sinhalese SMS phishing, specifically, by combining machine learning with rule-based analysis. A model-development dataset of Sinhalese SMS messages with phishing and legitimate samples of SMSs was annotated. Mixed Sinhala-English text was preprocessed to normalize and standardize it to enhance consistency, and all numerical values were transformed into text prior to extracting features via the TF, IDF method. It was then classified using the Multinomial Naive Bayes algorithm with the addition of a rule-based layer that could detect phishing features like suspicious links and language of urgency. This system uses the pipeline architecture, where the rule-based filtering is done, and the uncertain cases are then passed on to machine learning classification. The results of the evaluation show good classification performance, which allows identifying both obvious and nuanced phishing attacks. All of these results point to the significance of language-specific cybersecurity solutions and affirm the feasibility of the proposed solution in the realities of the Sri Lankan setting.

Keywords: *Hybrid Approach, Machine Learning, Natural Language Processing, Rule-based Filter, Sinhalese Language, SMS Phishing*

e-ISBN 978-955-627-501-8

A Secure and Transparent E-Voting System for Sri Lanka Leveraging Permissioned Blockchain, Biometrics, and AI-Based Fraud Detection

A.C.D. Dodanthenna[1], M.M. Mohamed Mufassirin[2]

[1]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*
[2]*Department of Computer Science, Faculty of Applied Sciences, South Eastern University of Sri Lanka*

[1]Chamika.acd@gmail.com, [2]mufassirin@seu.ac.lk

Abstract

In recent years, the demand for secure, transparent, and efficient electoral systems has increased significantly, particularly in developing countries where traditional voting methods often face challenges due to fraud, lack of transparency, and operational inefficiencies. In Sri Lanka, the existing voting system is primarily paper-based, which is time-consuming, resource-intensive, and vulnerable to human errors and manipulation. These limitations highlight the need for a modern, secure, and technology-driven voting solution. This study proposes the design and implementation of a secure and transparent e-voting system for Sri Lanka by leveraging permissioned blockchain technology, biometric authentication, and Artificial Intelligence (AI)-based fraud detection. The proposed system utilizes a permissioned blockchain network to ensure controlled access, data integrity, and immutability of voting records, allowing only authorized entities such as election officials to participate in the network. Each vote is recorded as a tamper-proof transaction, ensuring transparency and preventing unauthorized modifications. To enhance voter authentication and prevent identity fraud, the system integrates biometric verification methods such as fingerprint or facial recognition, ensuring that only eligible voters can cast their votes. Furthermore, an AI-based fraud detection module is incorporated to analyze voting patterns and identify anomalies such as duplicate voting attempts, unusual voting behaviors, and potential cyber threats in real-time. The system is developed using a modern technology stack, including a React-based frontend, Node.js backend, PostgreSQL database, and blockchain frameworks such as Hyperledger Fabric or Ethereum-based permissioned networks. A structured development methodology is followed, including system design, implementation, testing, and evaluation to ensure performance, scalability, and security. The findings of this study indicate that the proposed system improves election security, transparency, and efficiency while minimizing the risks associated with centralized voting systems, which is consistent with findings reported in similar blockchain-based e-voting studies. Overall, the proposed framework demonstrates its potential to support secure digital electoral processes and contribute to the advancement of digital governance in Sri Lanka.

e-ISBN 978-955-627-501-8

Keywords: *Artificial Intelligence, Biometrics, Cybersecurity, E-Voting, Fraud Detection, Permissioned Blockchain, Sri Lanka*

Adaptive Runtime Zero Trust Orchestration with Real-Time Anomaly Detection for Secure and Performance-Aware Containerized Workloads

H.R.V. Sathsara[1] and M.J. Ahamed Sabani[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]19ict023@seu.ac.lk, [2]mjasabani@seu.ac.lk

Abstract

The rapid expansion of containerized microservice architectures has revolutionised software, and Kubernetes is the industry standard in scaling distributed applications. However, this has introduced security vulnerabilities that cannot be mitigated by traditional perimeter-based models, due to default Kubernetes configurations that allow free inter-service communication, lateral traffic, and a lack of encryption. After a container has been compromised, identity checking or behavioral surveillance is not usually effective to prevent further propagation. To overcome these shortcomings, this project proposes an Adaptive Zero Trust (ZT) orchestration of a live Kubernetes cluster system. The architecture uses Istio to encrypt mutual TLS and use identity-based authorization at the infrastructure layer. Falco is a cloud native security tool based on eBPF kernel probes that monitor runtime, threat detection can be made within less than one second, and they are mapped to the MITRE ATT&CK framework. Less than one second each, six typical attack scenarios, such as credential access, privilege escalation, reconnaissance, shell spawning, sensitive data access, and container escape attempts, were identified. Moreover, the ZT access layer had 100% accuracy in enforcing the denial of unauthorized pod communication, but not legitimate service traffic, with a 403 response. The simulated denial-of-service incident was also identified by the monitoring stack and recorded a 633% CPU spike through Prometheus and Grafana. The dashboard is created with HTML and JavaScript, with a FastAPI REST API. The framework unifies security elements and operational visibility. Experiments with performance testing reveal that mutual TLS with the Istio sidecar has a CPU overhead of around 14 millicores per pod, and the cluster overhead is only slightly more than 3.5%. The results indicate that an enterprise-grade ZT security can be implemented at the infrastructure level without any code modification, which means that the ZT Framework is operational and can be used in practice.

Keywords: *Cloud-Native Security, Kubernetes, MITRE ATT&CK, mutual TLS (mTLS), Runtime Anomaly Detection, Zero Trust Security*

AI-Powered Threat Detection in Next Generation

H.D. Amarasinghe[1], S.L.A. Haleem[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]hashinidilshara21@gmail.com, [2]ahaleemsl@seu.ac.lk

Abstract

Next-generation networks such as 5G, IoT, cloud computing, and edge computing are transforming modern communication systems by enabling high-speed connectivity, scalability, and real-time data processing. However, these advancements also significantly increase the exposure to sophisticated cyber threats such as Distributed Denial of Service (DDoS), PortScan attacks, botnet activities, and zero-day vulnerabilities. Traditional intrusion detection systems often struggle to handle these dynamic threats due to high false positive rates, limited adaptability, and reliance on signature-based detection techniques. This study proposes an AI-powered intrusion detection system using machine learning techniques to enhance threat detection accuracy and adaptability. The CICIDS2017 dataset is utilized as the benchmark dataset, and a Random Forest classifier is implemented using the Scikit-learn library to identify malicious traffic patterns effectively. The methodology includes several stages such as data preprocessing, feature engineering, feature selection, model training, and performance evaluation. The model is evaluated using standard performance metrics, including accuracy, precision, recall, and F1-score to ensure a comprehensive assessment. Experimental results demonstrate that the proposed system achieves high detection accuracy with improved reliability compared to traditional approaches. Therefore, this research contributes to the development of scalable, intelligent, and efficient cybersecurity solutions suitable for protecting next-generation network environments.

Keywords: *5G Networks, Cloud Computing, Cyber Threats, DDoS, Intrusion Detection System*

Dual Layer Security Communication using Image Steganography and Blockchain

A.P.K. Eranga[1] and M.J. Ahamed Sabani[2]

[1,2]*Department of Information and Communication Technology, Faculty of Technology, South Eastern University of Sri Lanka*

[1]keranga777@gmail.com, [2]mjasabani@seu.ac.lk

Abstract

With the rise of modern technology, the transmission of confidential data has emerged as a challenge in the digital age owing to cyber-attacks, data breaches, and illegal surveillance of individuals and organizations. Encryption methods can keep the data secure and confidential, but tend to arouse the suspicion of monitoring systems since the presence of encrypted data becomes a point of concern. Steganography is another method where secret messages are embedded within digital objects such as images. Nevertheless, this method fails to prove whether the transmitted image has undergone any changes during transit. Blockchain technology guarantees tamper-proof verification but reveals the presence of data. In this regard, a combination of both steganography and blockchain is presented in this study to build a two-layered system for secure communication. The proposed approach uses image steganography to conceal secret data through the least significant bit (LSB) technique and creates a SHA256 hash of the stego-image. The hash value obtained from the process is stored in a private Ethereum blockchain with the help of a smart contract. In this regard, the Flask package is utilized to build an application. The sender will include the message in the image and also post the hash value in the blockchain, while the receiver will retrieve the message and authenticate the genuineness of the image by means of the blockchain technique. Experimental findings indicate that the proposed approach is effective in detecting tampered images under tested conditions with consistent verification results. The results are comparable with similar studies integrating steganography and blockchain for data integrity verification, demonstrating reliable tamper detection performance in secure communication environments.

Keywords: *Blockchain, Dual Layer Security, Image Steganography, Least Significant bit, Secure Communication, SHA-256*

e-ISBN 978-955-627-501-8

Real-Time Wi-Fi Jamming Detection and Automatic Backup Router Switching System

H.B.M. Lankathilaka[1] and R.K.A.R. Kariapper[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]19ict032@seu.ac.lk, [2]rk@seu.ac.lk

Abstract

Wireless networks, particularly Wi-Fi, have become essential in modern environments such as educational institutions, libraries, and public service areas. However, their open communication medium makes them highly vulnerable to Denial-of-Service (DoS) attacks, especially Wi-Fi jamming attacks that disrupt network availability. These attacks interfere with wireless communication by introducing noise or malicious packets, preventing legitimate users from accessing network services. Existing solutions for detecting such attacks are often expensive, complex, and primarily focused on alert generation without providing automatic recovery mechanisms. This research presents the design and implementation of a real-time Wi-Fi jamming detection and automatic backup router switching system using a low-cost embedded platform. The system utilizes RSSI-based analysis to monitor signal behavior and detect abnormal fluctuations that indicate potential jamming activity. Upon detection, the system triggers immediate alerts using an OLED display and buzzer, while simultaneously activating a relay module to switch from the primary router to a backup router. The proposed system is implemented using an ESP32 microcontroller, which enables real-time monitoring and control. Experimental results demonstrate that the system can effectively detect jamming conditions with high accuracy and respond within a short time frame. The automatic switching mechanism ensures minimal network downtime by allowing client devices to reconnect seamlessly using the same network configuration. This research contributes a cost-effective and practical solution for enhancing wireless network resilience in resource-constrained environments. By integrating both detection and mitigation into a single system, the proposed approach addresses the gap between identifying attacks and maintaining network availability, making it suitable for real-world deployment in public Wi-Fi environments.

Keywords: *Wireless Networks, Denial-of-Service (DoS),Wi-Fi Jamming Detection, Network Resilience, Public Wi-Fi Security*

e-ISBN 978-955-627-501-8

A Permissioned Blockchain Framework with Smart Contract–Based SLA Enforcement for Secure Healthcare Data Interoperability

A.M.P.K. Piris[1] and I.M. Kalith[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]prabashanapiris1234@gmail.com, [2]imkalith@seu.ac.lk

Abstract

In recent years, the digitization of the healthcare sector has significantly transformed medical data management. However, challenges such as data security vulnerabilities, patient privacy risks, and a lack of cross-institutional interoperability continue to limit optimal healthcare delivery. These limitations often result in unauthorized access, data fragmentation, and difficulties in maintaining reliable, tamper-proof electronic medical records. This study proposes the development of a secure healthcare framework that integrates a permissioned blockchain network (Hyperledger Fabric) with off-chain decentralized storage (IPFS) and smart contracts to enhance data security, processing, and accessibility. The proposed system utilizes a hybrid storage model where heavy medical files are stored on IPFS, and their cryptographic hashes (CIDs) are synchronized with the blockchain to ensure an immutable chain of custody. A dedicated web application is designed to support multiple users through strict Role-Based Access Control (RBAC) functionalities, enabling seamless, authorized interaction among doctors, patients, and pharmacies. The backend infrastructure ensures secure data storage, efficient system performance, and real-time updates across the network. The system is developed using a structured methodology, including system design, implementation, and rigorous testing. Various components such as the frontend interface, backend middleware, smart contracts, and decentralized storage nodes are carefully coordinated to achieve optimal performance. The results demonstrate improved data integrity, prevention of unauthorized access, and enhanced transparency in operations. Additionally, the system provides high transaction throughput and low latency that support secure data sharing. This study highlights the potential of integrating permissioned blockchain and IPFS technologies to improve system efficiency, privacy, and scalability. The proposed framework can be adapted to various healthcare domains, contributing to secure digital transformation and improved interoperability in modern medical environments.

Keywords: *Electronic Health Records, Healthcare Interoperability, Hyperledger Fabric, Inter Planetary File System (IPFS), Role-Based Access Control*

Blockchain-Based Digital Examination Paper Leak Prevention System

J.M.I.S. Jayasundara[1] and M.J. Ahamed Sabani[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]isanksasandaruwan4@gmail.com, [2]mjasabani@seu.ac.lk

Abstract

Leaks of examination papers digitally pose a severe risk to the integrity and validity of educational systems, since traditional exam paper storage and distribution systems are based on centralized servers and passwords that are susceptible unauthorized access, insider threats, and the current systems can offer no system of reliably tracing the point of origin of the leakage. This study suggests a blockchain-based digital exam paper management system which would provide tamper-resistant storage and full traceability of exam papers through the use of Ethereum smart contracts, which would be easily detected in the case of unauthorized access. There is a two-person control system in which examiners post papers, and moderators have to approve papers so that no one person may single-handedly manage the examination system. The interfaces provided for Student, Examiner, Moderator, and Admin to upload, download, moderate, monitor and audit the system for leak detection. The system uses PDF metadata embedding, permanently connecting examiners and moderators with documents, and dynamic watermarking embedding unique identifiers into each downloaded document, with all staff access to papers monitored to ensure a full audit trail of both external and internal security controls. The leak detection tool gives administrators an opportunity to post suspected leaked PDFs and remove embedded watermarks to identify those responsible. The system was written in Node.js/Express on the back end, and modern HTML/CSS/JavaScript on the front-end dashboards, and functional testing was conducted to ensure all basic functionality worked as intended, such as secure upload, multi-signature approval, watermarked download, staff access logging, and forensic leak detection. The proposed system demonstrates that integrating blockchain technology with practical PDF security mechanisms can effectively support a secure and traceable digital exam paper management system.

Keywords: *Blockchain, Ethereum, Exam Paper Security, Leak Detection, PDF Watermarking, Smart Contract*

e-ISBN 978-955-627-501-8

An Enhanced Offline Security Framework for ATM Authentication Systems

S.S. Jayathilaka[1] and M.J. Ahamed Sabani[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]sathsarani2000@gmail.com, [2]mjasabani@seu.ac.lk

Abstract

Automated Teller Machines (ATM) have gained significant importance in modern banking since they enable people to access financial services in a rapid and convenient way, but the security of the traditional authentication systems remains a matter of serious concern, with most systems being susceptible to card skimming, PIN theft, replay attacks, and manin-the-middle attacks and are also heavily reliant upon constant network connectivity, which is not always reliable or accessible, particularly To overcome those challenges, a proposal has been made in this study to utilize an offline ATM authentication system where the mobile-based mechanism is employed by integrating QR code verification and secure token generation, combining with Near Field Communication (NFC) which is an optional feature proposed to aid the process. To enhance security, cryptographic algorithms like hash and time-based token validation have been used in such a manner that data integrity may be maintained, and replay attacks are reduced. One of the most important aspects of the system is that it can be operated even without the presence of a network, with some limited transactions being done under regulated circumstances, where transaction limits and pre-verification are implemented to minimize any risks that may arise. An Android mobile application has been used as the system with an ATM simulator written in ASP. MongoDB has been utilized in data storage and management, and functional and security testing has been done, the results of which indicate that the system offers better protection against the typical ATM-related threats, as well as remains usable. All in all, the development of mobile-based authentication, QR code verification, and secure token development has helped in improving the security of ATMs, especially in a setting where internet connectivity is not reliable.

Keywords: *ATM Security, Mobile-Based Authentication, Offline Authentication, QR Code Authentication, Token-Based Security*

e-ISBN 978-955-627-501-8

On-Device Data Loss Prevention Agent for Sri Lankan Educational Institutions

Thirunesarasah Umatharinie[1] and M.J. Ahamed Sabani[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]umaalinithiru@gmail.com, [2]mjasabani@seu.ac.lk

Abstract

In our current digital era, educational institutions increasingly rely on digitalized documents to store and manage sensitive and confidential information such as student details, personal identifiers, and academic data. With the enforcement of the Personal Data Protection Act (PDPA) in Sri Lanka, the security and proper handling of such data have become a critical requirement. However, the existing Data Loss Prevention (DLP) solutions are mostly reliant on internet connectivity and cloud storage, use GDPR/HIPAA/PCI frameworks, and are high in cost, making them unsuitable for small-scale or low-end systems that are commonly found in Sri Lankan educational institutions. This research proposes the design and development of a lightweight, on-device Data Loss Prevention (DLP) agent that works fully offline. The proposed system can scan local files and detects PDPAcovered data sets and other important keywords using a regex-based detection approach with customization feature, and the system supports multilingual keyword detection, including English, Tamil, and Sinhala, to effectively detect sensitive data within various text documents with following extensions (.txt, .doc, .docx,.xls, .xlsx,.ppt, .pptx, .pdf, .csv, .rtf). The developed system integrates multiple functionalities. such as file scanning, pattern matching with keyword customization, AES-256-based encryption and decryption, secure vault storage, and user authentication with role-based access control. The system also provides administrative features such as rule management and user management to enhance usability and flexibility. The developed DLP agent provides a cost-effective, scalable, and efficient solution for protecting sensitive and confidential data sets in text documents within local storage. It helps to improve data security practices and supports compliance with PDPA regulations in Sri Lankan educational institutions.

Keywords: *AES-256, Data Loss Prevention, Data Security, PDPA, Regex Detection, Sri Lankan Educational Institution*

e-ISBN 978-955-627-501-8

Fraud-Resistant Financial Data Transmission in IoT using Mutual TLS

V.S. Thathsarani[1] and M.J. Ahamed Sabani[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]sashividanapathirana@gmail.com, [2]mjasabani@seu.ac.lk

Abstract

The adoption of Internet of Things (IoT) technologies in financial systems over the past few years has seen a tremendous enhancement in automation, efficiency, and real-time data processing. However, problems like poor authentication systems, nonsecure communication channels, and the risk of unauthorised access still hinder the effectiveness and reliability of IoT-related financial applications, resulting in the manipulation of data, loss of money, and distrust in using such systems. This paper presents a secure IoT-based financial transaction system with Mutual TLS (mTLS) authentication to improve communication security and device verification. The suggested system is designed as a smart donation system based on an ESP32 microcontroller, an IR sensor, and user feedback devices, including an OLED display, LEDs, and a buzzer. The events of transactions are detected in real time and sent to a backend server via HTTPS with mTLS, where both the client and the server are mutually authenticated. The backend uses Flask to accept incoming data and store it in an SQLite database, enabling a robust audit trail of all transactions. A systematic approach is adopted to develop the system, consisting of system design, hardware and software implementation, and rigorous testing. The security analysis is performed by simulating an attacker and analysing network traffic to ensure that unauthorised devices cannot bypass the system and that data is encrypted during transmission. Performance analysis shows that the system has acceptable response time, high accuracy, and efficient resource utilisation. The results indicate that the proposed system can be used to enhance the security, reliability, and transparency of financial transactions made through IoT. The framework can be generalised to other applications, including smart payment systems and automated transaction platforms, to further develop secure IoT-based financial solutions.

Keywords: *Data Security, Fraud Resistant, Internet of Things (IoT), Mutual TLS (mTLS), Secure Communication, Smart Donation System*

AI-Driven Software Define Network Framework for Real-Time Traffic Optimization and Cyber Threat Mitigation in Smart Football Stadiums

R.A.J. Madhusankha[1] and M.M. Mohamed Mufassirin[2]

[1]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*
[2]*Department of Computer Science, Faculty of Applied Sciences, South Eastern University of Sri Lanka*

[1]19ict045@seu.ac.lk, [2]mufassirin@seu.ac.lk

Abstract

Modern smart football stadiums host over 50,000 spectators simultaneously, all connected through Wi-Fi networks, mobile applications, and digital services. While this enhances the fans' experience, it also introduces challenges such as network congestion and increased vulnerability to cyber-attacks. Recent incidents at major stadiums, including disruptions to ticketing systems, mobile payments, and IoT services, highlight the urgent need for effective network security solutions. This study proposes an intelligent framework that integrates Software-Defined Networking (SDN) with Artificial Intelligence (AI) for real-time DDoS attack detection and mitigation. SDN enables centralized control of the network, while AI provides the capability to identify malicious traffic patterns efficiently. The CIC-DDoS2019 dataset, containing 106,902 samples with 79 features, was used to train and evaluate machine learning models. Three algorithms, namely Random Forest, XGBoost, and Decision Tree were employed for model implementation, and the results of each algorithm were compared. The Random Forest model achieved the best performance with 99.8% accuracy, 99.7% precision, 99.9% recall, and a 99.8% F1-score. The model was integrated with the RYU SDN controller to enable automated attack mitigation, where detected attackers are blocked within 5 seconds. The proposed system was validated using a Mininet-based smart stadium network simulation. Results demonstrate that combining SDN and machine learning provides an effective and scalable solution for securing smart football stadium environments.

Keywords: *Software-Defined Networking, DDoS Detection, Machine Learning, Random Forest, Smart Football Stadium, Network Security*

e-ISBN 978-955-627-501-8

Design and Evaluation of a Lightweight Ensemble Machine Learning-Based Intrusion Detection System for University BYOD Networks

M.F.F. Nasma[1] and M.S. Faathima Fayaza[2]

[1]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*
[2]*Department of Information Technology, South Eastern University of Sri Lanka*

[1]fhmbnth20@gmail.com, [2]fayaza@seu.ac.lk

Abstract

Over the last few years, the high rate of networked systems growth combined with high usage of bring your own device (BYOD) type of environments has greatly exposed modern networks to various cyber threats. Especially within universities where various heterogeneous types of devices are interconnected with institutional systems. The environments present key security issues because it lacks a centralized control mechanism, the devices are vulnerable, and the network behavior is extremely dynamic. Conventional intrusion detection systems (IDS), whose detection methods largely depend on signature-based approaches, are usually not effective in detecting unknown attacks, evolving attacks and zero-day attack patterns. To overcome these challenges, this paper suggests a lightweight hybrid intrusion detection system that incorporates rule-based detection with machine learning-based anomaly detection. The system uses CICIDS data set as secondary data to train and test the system. Isolation Forest and Autoencoder are two unsupervised machine learning methods that are used to detect network traffic anomalies. Further, rule-based mechanisms are used to effectively identify typical attacks like TCP flood, UDP flood, ICMP flood and port scanning in real time. An ensemble decision mechanism is a method of combining the results of both models in order to enhance the accuracy in detection and minimize false positives. The system achieved an accuracy of 85%, a precision of 57%, a recall of 99% and an F1-score of 73% for attack detection. This indicates moderate effectiveness in identifying malicious traffic while maintaining strong performance in normal traffic classification. The system's ability to detect live network threats is confirmed by real-time validation against simulated Kali Linux attacks.

Keywords: *Autoencoder, Intrusion Detection System, Isolation Forest, Machine Learning, Network Security*

Lightweight Anomaly Detection of Replay Attacks in WPA2/WPA3 4-Way Handshakes using Header-Only Packet Analysis

W.H.B.M.G.U. Basnayaka[1] and M.J. Ahamed Sabani[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]upekshagimhani91@gmail.com, [2]mjasabani@seu.ac.lk

Abstract

WPA2 and WPA3-protected Wi-Fi networks are based on the 4-way Extensible Authentication Protocol over LAN (EAPOL) handshake to exchange session keys between an access point and a client device. This mechanism of handshakes has been known to be susceptible to replay attacks, most prominent of them being the Key Reinstallation Attack (KRACK), which can induce nonce reuse and enable an adversary to decrypt traffic without knowing the network password. In this project, a lightweight, real-time detection system of replay attacks in WPA2 and WPA3 Wi-Fi handshakes is provided. RouterSec can only inspect EAPOL header fields, namely replay counters, cryptographic nonces, message types, and timing properties, without any encrypted payload data and is therefore privacy-preserving and computationally efficient. The system uses a dual-layer detection engine that considers a combination of eight deterministic rule-based checks and a trained Random Forest machine learning classifier that uses twelve derived features. The rule engine identifies known patterns of attacks with zero false positives, and the ML model is able to identify subtle statistical anomalies that cannot be detected using rules. Running on one Linux laptop with two Wi-Fi interfaces, RouterSec can process around 47,000 frames per second with a latency of inference of about 0.02 milliseconds per frame and a model size of about 0.2 MB. Experimental analysis of WPA2-PSK, WPA3-SAE and WPA2/WPA3 transition mode proves that RouterSec can effectively detect all types of attack KRACK Message 3 replay, simple replay, nonce reuse, replay counter regression, and timing anomalies in real time. It is written in Python 3.11 and is open-source under the MIT licence, and has a complete automated test pipeline through a single shell script.

Keywords: *Anomaly Detection, EAPOL, KRACK, Machine Learning, Packet Analysis, Replay Attack*

e-ISBN 978-955-627-501-8

Design and Implementation of a High-Security Smart Wi-Fi Router with Biometric Authentication and IoT Firewall

K. Punu Vinura[1] and M.S.S. Razeeth[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]punuvinura2000@gmail.com, [2]razeethsuhail@seu.ac.lk

Abstract

The rapid growth of wireless networks and Internet of Things (IoT) devices in home and small office environments has exposed limitations in conventional router security, particularly reliance on static passwords that enable unauthorized access and weak user accountability. This study proposes a smart Wi-Fi router framework that introduces a layered access-control mechanism combining biometric verification, session-based credential distribution, device-level tracking, and network-level policy enforcement. The system is implemented on a Raspberry Pi configured as a wireless access point and routing controller using hostapd and dnsmasq, with Python-based control logic, SQLite for local data storage, and iptables for traffic filtering and isolation. In the proposed workflow, user authorization is initiated through a fingerprint sensor connected to the Raspberry Pi, after which a time-limited QR code is generated containing a temporary onboarding token rather than static Wi-Fi credentials. Upon scanning, the connecting device is registered and its MAC address is recorded as a secondary reference for session tracking, although not relied upon as a primary security mechanism due to spoofing limitations. IoT device isolation is achieved through firewall rules and controlled network segmentation policies that restrict communication between device categories and limit lateral movement within the local network. Logging and administrative monitoring are provided through a lightweight Flask-based interface, enabling visibility into access events and device activity. While the system does not claim complete protection against all attack vectors and does not include advanced encryption protocols or quantitative performance evaluation, it demonstrates the feasibility of integrating biometric authentication, token-based onboarding, and policy-driven network control into a unified, low-cost router platform, contributing a practical approach to improving access management and internal network security in resource-constrained environments.

Keywords: *Smart Wi-Fi Router, Biometric Authentication, QR Token, MAC Address Tracking, IoT Firewall, Raspberry Pi, Network Isolation*

e-ISBN 978-955-627-501-8

Prevention of BLE-Based Payment System Man-in-the-Middle Attacks Using Zero Trust Architecture Principles

V. Keerthana[1] and R.K.A.R. Kariapper[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]keerthanavikneswaran640@gmail.com, [2]rk@seu.ac.lk

Abstract

Because of its low power consumption and widespread use in smartphones, Bluetooth Low Energy (BLE) technology is becoming more and more popular for contactless payment systems. However, these systems are extremely susceptible to active Man-in-the-Middle (MITM) attacks, such as transaction tampering, replay attacks, and endpoint impersonation, because to the underlying security assumptions of BLE, such as implicit trust following pairing and inadequate application-layer integrity. These dynamic, resource constrained wireless environments are outside the scope of traditional perimeter-style security concepts. In order to stop MITM attacks in BLE-based payment workflows, this study suggests a novel security architecture that uses Zero Trust Architecture (ZTA) principles. Authenticated pairing, transaction-bound cryptographic integrity, anti-replay protection, and characteristic-level micro-segmentation down to the Generic Attribute Profile (GATT) level are all enforced by the suggested design. A continuous verification mechanism, incorporating real-time trust scoring and telemetry analysis, replaces the static trust model. A dual-prototype system (baseline vs. ZTA-enhanced) was developed and evaluated through controlled experiments simulating adversarial scenarios. The results demonstrate that the ZTA-enhanced design effectively mitigates MITM attack vectors, such as amount tampering and replay attempts, while maintaining acceptable latency overhead for real-time transactions. The architecture provides granular, auditable policy enforcement and continuous session validation. This study concludes that embedding ZTA principles directly into BLE payment interactions significantly strengthens security posture, offering a practical and evidence-based framework for building resilient proximity payment systems against sophisticated wireless attacks.

Keywords: *Zero Trust Architecture, Bluetooth Low Energy, Man-in-the-Middle Attack, Mobile Payment Security, Micro-segmentation*

e-ISBN 978-955-627-501-8

DermaTrust: A Blockchain-Based Smart System for Real-Time Skincare Product Authentication

B.J.F. Jatheela[1] and F. Musfira Ameer[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]bjf.jatheela@gmail.com, [2]ameermusfi@seu.ac.lk

Abstract

Counterfeit skincare products have become a major international problem which raises consumer safety issues, diminishes brand value and damages supply chain integrity. Static barcode and QR code-based authentication solutions are ineffective because the codes can be easily replicated, replaced or counterfeited. Existing approaches with digital traceability or physical verification with QR codes or RFID tags do not address the multidimensional issues of complex counterfeiting practices. Here we present DermaTrust, a blockchain based product authentication framework that provides real-time verification of skincare products through AI and cross references with the blockchain. The system takes advantage of the blockchain to create an immutable record of product registration, movement through the supply chain, and authenticity verification, tracking a product throughout the supply chain, from its producer to its consumer. Along with the blockchain, the AI anomaly detection model uses Vision Transformer (ViT) architecture to analyze the barcode images and recognize any slight distortion or duplication artifacts that may signal tampering. The combination of these technologies provides an added level of assurance and protection, both physically and digitally. The methodology of the development included data generation and augmentation, model training and validation, and, finally, blockchain deployment on the Ethereum Testnet. Finally, the solution was put together in the form of a React Native mobile application, that allows real time consumer verification of products by scanning product barcodes and receiving feedback such as "Authentic", "Tampered Barcode" or "Unverified". Accuracy, precision, recall, F1-score and response time results indicate that the DermaTrust system offers an effective and scalable solution against counterfeiting and outperforms the existing methods for verifying the legitimacy of products. Our AI-driven authentication and blockchain-based trust can also be applied in other fields greatly affected by counterfeiting. Scaling this effort, domain adaptation, and using advanced anomaly detection methods offer paths for future exploration.

Keywords: *Block-chain Technology, Barcode Anomaly Detection, Counterfeit Detection, Skincare Product Authentication*

A Privacy-Preserving Blockchain-Based Secure Data Sharing System for Paddy Cultivation Using Smart Contracts, IPFS, and Zero-Knowledge Proofs

K.M.C.K. Senarathna[1] and I.M. Kalith[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]chandimakavishka12@gmail.com, [2]imkalith@seu.ac.lk

Abstract

In the context of Aid and Development, both models are tightly bound up with effective data management practices and trust in institutional processes, as an explanation for their importance to economies based at least partially on agriculture, particularly in developing countries with rural populations. Despite advancements in agricultural data sharing, most existing systems lack transparency and are vulnerable to data manipulation while providing insufficient protection of sensitive farmer information used such as financial records and personal information. Blockchain technology has been pursued to resolve the original state of trust and data integrity, but its intrinsic transparency brings up a new concern about privacy when sensitive information is made available to several stakeholders. In light of the above, this research introduces a blockchain-based data sharing system for paddy cultivation that is privacy-preserving by relying on smart contracts, IPFS, and ZKP. The farmers are able to send the cultivation and crop damage data through a secure channel, while officers can verify and save validated data on the blockchain. Sensitive information, such as bank account details and crop damage details are secured using cryptographic mechanisms and Zero-Knowledge Proofs (ZKP) that permit verification without disclosing or exposing actual information. Data is made available to researchers, but sensitive information is protected and access is controlled so that data utility does not come at the expense of privacy. This proposed solution introduces a new paradigm where data integrity, transparency and security are maintained through sensitive and selective blind data disclosure. The paper is a pioneering work of integrating blockchain with ZKP and decentralized storage in agricultural data sharing, indicating that this solution can effectively enhance trust and privacy in safe agricultural data sharing systems and shows the feasibility for modern smart agriculture applications.

Keywords: *Agricultural Data Security, Blockchain, IPFS, Smart Contracts, Zero-Knowledge Proofs*

Privacy-Preserving Blockchain-Based Student Certificate Verification System using Zero-Knowledge Proofs (ZKPs)

D.H. Gamage[1] and M.J. Ahamed Sabani[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]19ict070@seu.ac.lk, [2]mjasabani@seu.ac.lk

Abstract

This paper presents a blockchain-based and Zero-Knowledge Proofs (ZKPs) academic certificate verification framework that is secure and does not compromise privacy. The traditional certificate verification system is based on centralized databases, which are susceptible to data breaches, hacking, and ineffective manual verification systems. Furthermore, the current digital verification procedures tend to involve exposing sensitive personal data, posing a serious privacy issue. In a bid to overcome these shortcomings, a decentralized verification system was created based on the Ethereum blockchain. The main objective of this study is to develop a secure, decentralized, and privacy-preserving certificate verification system using blockchain and Zero-Knowledge Proofs.The hashes of certificate cryptographs in the proposed system are calculated with the help of the hash function of the SHA-256 algorithm and deposited on the blockchain with the help of smart contracts that guarantee the integrity of the data and its irreversibility. To improve privacy, the real certificate information is stored off-chain. Zero-Knowledge Proofs are combined with the ZoKrates framework to allow checking the authenticity of certificates without disclosing underlying sensitive data. The interface was implemented as a web-based application with the help of React.js, where secure user authentication and communication with the blockchain were provided with the help of MetaMask. The functional testing and performance analysis were conducted on the system. The results show that the proposed system effectively prevents certificate forgery, ensures tamper-proof storage, and enables reliable verification without the need for centralized authorities. It also demonstrates that Zero-Knowledge Proof integration successfully preserves user privacy during the verification process. However, the system introduces additional computational overhead and blockchain transaction costs.

Keywords: *Blockchain, Certificate Verification, Privacy Preservation, Smart Contracts, Zero-Knowledge Proofs*

e-ISBN 978-955-627-501-8

A Secure Mobile Application for Remote Monitoring and Management of Layer 3 Switch Setup

K.L.D.R. Perera[1] and M.J. Ahamed Sabani[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]drasanjanaperera@gmail.com, [2]mjasabani@seu.ac.lk

Abstract

Enterprise network administrators have a nagging issue to deal with: they still need to be physically present at the Layer 3 switch to be able to manage it. The current tools that are in use, like CLI terminals and desktop programs, do not have any feasible mobile option, and administrators are unable to respond to network incidents even when not at work or during off-hours. This study suggests and deploys NetShell, a safe Android mobile app for monitoring and controlling Layer 3 network switches. The system consists of a four-layer design that includes a Java-based Android frontend, a Firebase Cloud Firestore backend, a dual-protocol communication layer (with both SSH and Telnet), and an AI-based visual switch port detector written in YOLOv8. NetShell offers an interactive CLI terminal, role-based access control (RBAC) with per-user permission management, multi-tenant workspace and device management, and an artificial intelligence-driven Image Process feature that interprets camera images of physical switches to generate a formatted Switch Port Analysis report. An annotated YOLOv8 Nano model trained on 1,199 annotated DLink switch port images in Google Colab using a Tesla T4 was found to have a mAP50 of 99.2%, a precision of 92.3%, and a recall of 95.6%. The model was translated into TensorFlow Lite and implemented on the Android device, inference taking about 600 milliseconds per frame. Functional testing with a GNS3 simulation environment with Cisco IOU Layer 3 switches was used to verify the successful connection with Telnet, VLAN configuration, interface management, and hostname changes are all possible, totally via a mobile device. The gap that is addressed in this research is quite well defined: no previous studies included mobile CLI terminal management, role-based access control, real-time network monitoring, and YOLO-based port detection into the scope of a single Android app to manage a Layer 3 switch.

Keywords: *Layer 3 Switch, Mobile Network Management, Remote Monitoring, Role-Based Access Control, Switch Port Detection*

e-ISBN 978-955-627-501-8

Standard-Compliant NFC Provisioning for Next-Generation IoT Frameworks (Matter, Zigbee, Wi-Fi Alliance)

K.D.S. Pabodha[1] and M.J. Ahamed Sabani[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]sithumpabodha@gmail.com, [2]mjasabani@seu.ac.lk

Abstract

As Internet of Things (IoT) networks continue to grow rapidly, setting up these devices securely and easily has become a major challenge. Current setup methods usually rely on SoftAP or Bluetooth Low Energy (BLE). However, these approaches often leave network credentials unprotected at the application layer. They are also usually locked to just one specific communication protocol. This project proposes a standard-compliant NFC-based provisioning system that enables secure multi-protocol configuration through a single encrypted tap. The architecture supports Wi-Fi, Zigbee and Matter networks, and has a bipartite architecture, comprising a Flutter-based Android app and an ESP32-C6 provisioning device. The mobile application wraps the credentials as JSON, encrypts with AES-256-CBC, and writes the ciphertext to a MIFARE Classic 1K NFC tag, in NDEF format. The ESP32-C6 and a PN532 NFC reader are used on the receiver side to reclaim the encrypted payload and to decode it by hardware-accelerated mbedTLS, and direct the credentials to be used based on the embedded protocol identifier. The operation was successfully validated experimentally, and Wi-Fi provisioning was enabled with only one NFC tap, and the device acquired a valid IP address. The routing logic also worked properly for the other frameworks. The firmware accurately decrypted Zigbee and Matter payloads and forwarded them to their specific handlers. Beyond just routing data, the testing used the ESP-Zigbee-SDK to prove that the ESP32-C6 could initialize as a native Zigbee coordinator and successfully form its own network. The full provisioning cycle was completed in approximately three seconds. These findings directly support the main objective of the study, which is to enable secure, fast, and multi-protocol IoT device provisioning using NFC without relying on expensive secure hardware elements. The results demonstrate that standard consumer hardware can reliably support secure onboarding for next-generation IoT environments.

Keywords: *IoT Provisioning, Matter, mbedTLS, NFC, Protocol-Agnostic Architecture, Zigbee*

e-ISBN 978-955-627-501-8

Network Intrusion Detection Systems for Cyberattack Prevention in Sri Lankan Organizations

M.G.G Arunashantha[1] and S.L.A. Haleem[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]gayanarunashantha264@gmail.com, [2]ahaleemsl@seu.ac.lk

Abstract

As digital technologies continue to evolve, cyber threats are increasing, making traditional security mechanisms such as firewalls less effective. Network Intrusion Detection Systems (NIDS) play a critical role in monitoring network traffic and identifying malicious activities. Signature-based detection is effective for known attacks, while anomaly-based detection can identify unknown threats but may produce higher false positives. In the Sri Lankan context, the effective implementation of NIDS is challenged by limited resources, a lack of expertise, and variations in local network environments. This study evaluates the effectiveness of NIDS in Sri Lankan organizations using a mixed-method approach, combining literature review with practical data analysis. The UNSW-NB15 dataset was used as the primary data source, supported by packet-level analysis using Wireshark. Data preparation and analysis were conducted using Microsoft Excel. The results indicate a balanced distribution of normal and attack traffic, with major attack categories including Generic, Exploits, Fuzzers, DoS, and Reconnaissance. TCP and UDP were identified as dominant protocols, while DNS and HTTP were the most frequently used services. Evaluation based on detection rate and false positive rate highlights the importance of accuracy in intrusion detection. Overall, the study demonstrates that NIDS-based traffic analysis is effective in detecting suspicious network behavior and can significantly enhance cybersecurity in Sri Lankan organizational environments.

Keywords: *Network Intrusion Detection Systems (NIDS), Cyber Threats, Signature-Based Detection, Anomaly-Based Detection, UNSW-NB15 Dataset*

TRACK – SOFTWARE TECHNOLOGIES

e-ISBN 978-955-627-501-8

Performance Comparison of G-LEACH and a Round-Adaptive Energy-Efficient CH Selection Method for Small-Scale WSNs

S. Madhusha[1] and M.J. Ahamed Sabani[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]madhushamadhu719@gmail.com, [2]mjasabani@seu.ac.lk

Abstract

There is an increasing number of wireless sensor networks used in various areas, such as medicine, environmental studies, and industries, due to their many uses. There are certain limitations, such as limited energy sources, ineffective Cluster Head (CH) selection, and inflexibility, which affect network performance. These limitations often lead to inefficient use of energy resources, which in turn affects the network lifetime of WSNs and makes the system ineffective. Therefore, this proposal involves the deployment of a round-adaptive energy-efficient clustering technique integrating the Q-Learning algorithm for efficient Cluster Head (CH) selection. The new algorithm utilises the Q-Learning and K-means algorithms to effectively choose cluster heads based on multiple factors, including residual energy, distance to the sink, and load balancing. Energy-conscious WSN models are used to simulate networks in Python to compare G-LEACH with the proposed approach. The back-end simulator compares the most important performance indicators, such as energy use, clustering, and network life. The combination of a systematic approach based on clustering algorithms, energy models, and performance evaluation methods is considered to achieve the best result. Results show that energy consumption is less and that the model is more energy efficient and thus has a longer network lifetime than the G-LEACH model. Besides, the system also has dynamic decision-making, which results in improved network performance. The study reveals the possibility of machine learning (Q-Learning) solutions to enhance energy efficiency and network lifetime of Wireless Sensor Networks.

Keywords: *Cluster Head Selection, Energy Efficiency, G-LEACH, K-Means Clustering, Q-Learning, WSN Lifetime*

e-ISBN 978-955-627-501-8

A Comparative Empirical Study of Azure Kubernetes Service and Virtual Machine Scale Sets for Diverse Workloads Considering Performance, Scalability, Cost, and Fault Tolerance

M.K.N Sandeepa[1] and A. Mohamed Aslam Sujah[2]

[1,2]*Department of Information and Communication Technology, Faculty of Technology, South Eastern University of Sri Lanka*

[1]sandeepakick436@gmail.com, [2]ameersujah@seu.ac.lk

Abstract

Cloud computing is a key enabler of software systems, offering scalable, on-demand resources for diverse workloads. However, selecting the most suitable platform remains challenging due to differences in workload characteristics and the need to evaluate multiple operational criteria simultaneously. In practice, platform selection is often driven by intuition or limited to isolated performance metrics, which may not accurately reflect real-world requirements. This research presents a comparative empirical evaluation of two Microsoft Azure deployment platforms: Azure Kubernetes Service (AKS), and Virtual Machine Scale Sets (VMSS). The evaluation was conducted across three representative workload categories: Microservices, Web Applications, and Big Data processing using four key criteria: performance, scalability, cost efficiency, and fault tolerance. All experiments were performed under controlled conditions within Azure environment. The results demonstrate that platform suitability is strongly dependent on workload characteristics. VMSS achieves superior performance and cost efficiency in Microservices and Big Data workloads, primarily due to reduced orchestration overhead and more direct resource utilization. In contrast, AKS provides stronger scalability and fault tolerance, making it more suitable for Web Application workloads that require dynamic scaling and high availability. The final comparative analysis indicates that VMSS is the preferred platform for Microservices and Big Data workloads, while AKS is more suitable for web applications. To support structured and objective decision-making, a multi-criteria decision support model integrating the Analytic Hierarchy Process (AHP) and Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) was developed and implemented as an Excel-based tool. The model enables users to input workload-specific metrics, adjust the relative importance of evaluation criteria, and obtain ranked platform recommendations.

Keywords: *Azure Kubernetes Service, Cloud Computing, Microsoft Azure, Multi Criteria Decision Making, Virtual Machine Scale Sets*

e-ISBN 978-955-627-501-8

SEUSL-SMARTBOT: Intelligent FAQ Chatbot for South Eastern University of Sri Lanka using LLM and RAG

M.Y. Fathima Nuha[1] and A. Mohamed Aslam Sujah[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]ahunfathi000@gmail.com, [2]ameersujah@seu.ac.lk

Abstract

The increasing demand for efficient and accessible student support systems in higher education institutions has highlighted the limitations of traditional information delivery methods such as static websites and manual inquiry handling. This research presents SEUSL SmartBot, an intelligent FAQ chatbot designed for South Eastern University of Sri Lanka (SEUSL), leveraging Large Language Models (LLMs) and Retrieval Augmented Generation (RAG) to provide accurate, context-aware, and real-time responses to student queries. The proposed system integrates a hybrid retrieval mechanism combining dense retrieval using vector embeddings and sparse retrieval using keyword-based ranking (BM25). These results are fused using Reciprocal Rank Fusion (RRF) to enhance the relevance of retrieved information. The chatbot utilizes a curated knowledge base constructed from university-related documents, including handbooks, course catalogues, and official web content. Local inference is performed using an LLM deployed via Ollama, ensuring privacy and reducing dependency on external APIs. To evaluate system performance, a dataset of 140 domain-specific questions was developed, and multiple evaluation metrics were applied, including accuracy-based measures and NLP metrics such as BLEU and ROUGE. Additionally, user experience was assessed using the System Usability Scale (SUS), achieving a score of 78.4, indicating good usability. The results demonstrate that SEUSL SmartBot effectively improves information accessibility, reduces response time, and enhances user satisfaction. This research contributes a practical and scalable framework for implementing intelligent chatbot systems in academic environments, particularly for multilingual contexts such as English and Tamil.

Keywords: *Hybrid Retrieval, LangChain, Large Language Models, Natural Language Processing, Ollama, Reciprocal Rank Fusion, Retrieval Augmented Generation*

e-ISBN 978-955-627-501-8

A Blockchain-Based Framework for Transparent Fund Allocation in State Universities

D.M.K. Sandeepani[1] and M.J. Ahamed Sabani[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]19ict062@seu.ac.lk, [2]mjasabani@seu.ac.lk

Abstract

State universities in Sri Lanka are highly dependent on government funding, but current centralised systems of fund allocation are still marred with lack of transparency, efficiency of tracking and accountability. These gaps are likely to create delays, bad management, and distrust between the stakeholders. In order to reduce these problems, this paper proposes a blockchain-based model of transparent funds distribution that will be a pilot system in a state university in Sri Lanka. The study aims at creating an easy-to-use web-based application on React.js and Typescript, combined with Ethereum blockchain technology, to provide financial transactions that are secure, traceable, and cannot be altered. The processes of submitting and approving fund requests are automated with the help of smart contracts written in Solidity, enabling real-time monitoring but not allowing any unauthorised changes. The methodology has a systematic process that is composed of requirement analysis, system design, implementation, and evaluation. The research method is a mixed method approach that involves literature review, requirement gathering, prototype development and system evaluation. Ganache is used to create the local Ethereum blockchain environment and authenticate and validate transactions with the help of MetaMask. The prototype illustrates the use of decentralised ledger technology to provide greater transparency, reduce errors, and increase trust in financial processes. The results have shown that the blockchain-based system suggested is more efficient, accountable, and transparent than traditional fund allocation systems. The paper concludes that additional research and practical implementation of these frameworks can immensely enhance financial management within state universities and drive towards transparency in governance.

Keywords: *Blockchain, Ethereum, Financial Accountability, Smart Contracts, State Universities*

e-ISBN 978-955-627-501-8

Design and Development of a Persuasive Mobile Application to Improve Study Focus and Reduce Academic Procrastination among University Students

A.F. Lufna[1] and I.M. Kalith[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]af.lufna@gmail.com, [2]imkalith@seu.ac.lk

Abstract

Academic procrastination is one of the major problems among university students, which has a negative impact on their productivity, academic success, and psychological health. The main purpose of the research is to create and test a convincing mobile application, FocusFlow, that would help students to be more concentrated in their studies and reduce procrastination. The survey was a survey of 60 university students in a Google Form survey to conduct an initial needs assessment to determine patterns, causes, and effects of procrastination. The results showed that the prevalence of procrastination is very high, and the main factors that contribute to it are social media distractions, lack of motivation, and poor time management. Relying on these insights, a mobile app with persuasive design features like the Pomodoro timer, AI-based task breakdown, gamification, mood tracking, and visualization of progress was created. An evaluative prototype of high fidelity was tested by 10 participants to determine usability and perceived usefulness. The findings showed that people responded positively to the design, ease of use, and relevance of the features of the application. After that, a fully worked application was tested on 20 students, and quantitative (Google Form), as well as behavioral data (Firebase database) were obtained. Through the SPSS and descriptive analysis, it was revealed that the application was relatively user-friendly and moderate in reducing procrastination and enhancing study focus. Pomodoro timer was pointed out as the most useful feature, whereas AI task breakdown and gamification needed to be improved. The results prove that persuasive mobile applications are capable of significant contributions to self-regulated learning and alleviation of academic procrastination of students.

Keywords: *Academic Procrastination, Gamification, Mobile App, Persuasive Technology, Pomodoro Technique, Student Productivity*

TRACK – UBIQUITOUS COMPUTING TECHNOLOGIES

e-ISBN 978-955-627-501-8

Smart Socket System for Intelligent Fault Detection and Controlled Isolation of Pinhole Leaks, Cracks and Corrosion in Oil, Water, and Gas Pipeline Networks

C.W.C.B. Weerawardhana[1] and R.K.A.R. Kariapper[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka, Sri Lanka*

[1]19ict010@seu.ac.lk, [2]rk@seu.ac.lk

Abstract

The limits of conventional inspection techniques, which are frequently manual, time consuming, and unable to provide real-time problem identification, have been brought to light by the growing need for effective and dependable monitoring of oil, water, and gas pipeline networks. Undetected flaws including corrosion, cracks, and pinhole leaks can cause serious financial losses as well as environmental risks. Using Internet of Things (IoT) technologies, this study suggests a Smart Socket System for intelligent defect detection and controlled isolation in pipeline networks. Several Smart Socket Units are placed throughout the pipeline as part of the system's distributed architecture. To continuously monitor pipeline conditions, each unit incorporates a flow sensor, temperature sensor, and air pressure sensor that are coupled via an air trap mechanism. In order to identify anomalous conditions, an ESP32 microcontroller uses threshold-based logic to interpret the sensor data in real time. Long range, low-power data transfer between devices and a central monitoring system is made possible by LoRa communication technology. A Node-RED dashboard offers real-time viewing of sensor data, alarms, and system status, and the system uses the MQTT protocol for effective data transmission. Based on sensor behavior, a multi-parameter detection method is employed to differentiate between leakage and blockage circumstances. A servo motor mechanism is also used to automatically isolate problematic pipeline segments. Experimental results show that the system performs reliably in communication and has good detection accuracy, with reaction times between two and fourteen seconds. The proposed system offers a scalable and cost-effective solution for modern pipeline monitoring applications.

Keywords: *Smart Socket System, IoT, Pipeline Monitoring, Leak Detection, Fault Detection, Smart Infrastructure*

e-ISBN 978-955-627-501-8

IoT and AI-Based Motorcycle Anti-Theft and Real-Time Tracking System

S.G.L.C. Samarasinghe[1] and M.S. Faathima Fayaza[2]

[1]*Department of Information and Communication Technology, South Eastern University of Sri Lanka, Sri Lanka*
[2]*Department of Information Technology, South Eastern University of Sri Lanka*

[1]19ict022@seu.ac.lk, [2]fayaza@seu.ac.lk

Abstract

Two-wheelers are the primary mode of daily transport for most Sri Lankans. However, two-wheeler thefts continue to be a persistent problem across Southeast Asian countries. The security measures that are presently accessible in the consumer market, ranging from mechanical steering locks to aftermarket GPS trackers, tend to operate in a reactive manner and typically notify the vehicle owner only after the theft has already taken place. This makes recovery difficult. This study addresses this issue by combining several complementary technologies into a single embedded device. This study builds a hardware prototype around the LilyGO T-Call ESP32 development board with an integrated SIM800L GSM modem. Further, the prototype used a PN532 NFC module used for contactless card-based arming and disarming, an MPU-6050 inertial measurement unit to capture six-axis motion data for theft detection, a NEO-7M GPS receiver used provides real-time location coordinates, and a relay module used enables remote engine immobilization. Feedforward Multilayer Perceptron neural network was trained on 2,000 labelled accelerometers and gyroscope samples, quantified to a lightweight embedded AI model and deployed directly onto the ESP32. Further, this study developed MotoTracker Android mobile applications to facilitate the owners. The application supports real-time GPS visualization on an interactive map, live speed and coordinate readouts, one-tap engine disables and theft confirmation controls, and biometric fingerprint authentication fallback for situations where the NFC card is unavailable. SMS alerts containing GPS coordinates are dispatched automatically when the AI model flags suspicious motion or when an unauthorized NFC card is detected. Evaluation of the AI classifier on a held-out test set of 400 samples showed 99.75 per cent accuracy, with precision and recall values at or above 0.99 for both the parked and theft classes, an area under the ROC curve of 1.000, and on-device inference times between 0.10 and 0.21 milliseconds per sample.

Keywords: *Edge AI, ESP32, GPS Tracking, NFC Authentication*

e-ISBN 978-955-627-501-8

Smart Plastic Collecting Bin with Arduino-Based Monitoring System

M.C. Madhusan[1] and R.K.A.R. Kariapper[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka, Sri Lanka*

[1]cshan356@gmail.com, [2]rk@seu.ac.lk

Abstract

The rapid increase in the population, increased use of plastics, and poor waste management systems has been the cause of excessive plastic waste accumulation becoming a serious environmental challenge in urban areas. Conventional approaches to waste management that rely on fixed schedules and manual monitoring usually lead to overflowing garbage bins, environmental contamination, health hazards, and unnecessary use of fuel by collection trucks due to lack of live information on the status of the garbage bins. This project aims at solving these challenges through the development of a Smart Plastic Collecting Bin using an Arduino-Based Monitoring System. The system comprises an ultrasonic sensor (HC-SR04) that determines the fill level of plastic waste, an ESP32 processor responsible for the processing of data, a GPS sensor (NEO-6M) for tracking the real-time location of the bin, and a LoRa communication device (SX1276/SX1278) for transmitting data wirelessly over extended ranges. Upon the attainment of a predetermined fill capacity, for example, 90%, the system raises automatic alerts through the established communication link. Data on fill levels, location, and the bin status is stored in the cloud-based Firebase database, where it can be accessed using a Flutter-designed mobile application. Objectives include automating bin fill level determination, providing individuals with means of real-time tracking of the bins, implementing route planning based on GPS data and sending notifications to garbage collectors. Additionally, the proposed solution should be cost-effective, utilize minimal power resources (the system will be powered by solar energy), and scalable, allowing for deployment in developing countries or remote locations where the use of costly smart waste solutions is impractical. Research will result in a prototype creation, central management system, mobile application, and evaluation report. The purpose of this project is to address sustainable plastic waste management and enhance urban environmental quality through minimization of manual interaction, prevention of bins overflow, and operational decisions based on empirical data.

Keywords: *IoT, Smart Bin, ESP32, Ultrasonic Sensor, Real-time Monitoring*

e-ISBN 978-955-627-501-8

IoT-Based Smart Home Energy Management System with Real-Time Monitoring and Energy Theft Detection

G.M.P. Sankalpa[1] and M.M. Mohamed Mufassirin[2]

[1]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*
[2]*Department of Computer Science, Faculty of Applied Sciences, South Eastern University of Sri Lanka*

[1]malithapiumal02@gmail.com, [2]mufassirin@seu.ac.lk

Abstract

Increased demands for electricity, higher costs associated with energy supply, and widespread energy theft highlight the need for a robust yet simple energy consumption monitoring system with real-time capability, control features, and reliable detection of potential energy theft. Conventional energy meters lack the ability to provide timely updates and control opportunities while offering poor anti-theft performance. This paper highlights the design and implementation of an IoT-enabled Smart Home Energy Monitoring System with anti-theft capabilities. The proposed solution includes several inexpensive components, including ESP32, ACS712 current sensors, and ZMPT101B voltage sensors to track electrical parameters in real-time. All collected data are transmitted to cloud service providers, allowing access through web-based or mobile app-based dashboards. Theft prevention is performed by comparing mains and residential electrical loads, identifying deviations from regular trends that can indicate potential theft. In this context, the threshold approach defines any deviations larger than 5-10% in currents observed within a limited timeframe as abnormalities. Some basic preprocessing techniques are used to filter noisy readings and correct any drift caused by temperature or other factors. To improve the reliability of detecting abnormalities, artificial intelligence methods were used. More precisely, an artificial intelligence-based algorithm was implemented to learn and detect any irregularities in energy consumption based on typical consumer behavior. The proposed approach included a feed-forward neural network trained on the basis of historical data by supervised machine learning algorithms. In particular, voltage and currents were the input parameters for the neural network. The system allows the user to receive notifications when abnormalities detected. High accuracy in monitoring and theft detection has been achieved, with measurement error being less than 2% and detection accuracy being above 95%.

Keywords: *IoT, Smart Energy Meter, Energy Theft Detection, Arduino, Real-Time Monitoring*

e-ISBN 978-955-627-501-8

Development of a Smart IoT and AI-Integrated System for Real-Time Monitoring and Quality Prediction of Rubber Latex in Sri Lanka

V.Sangeerthan[1] and M.S.S. Razeeth[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka, Sri Lanka*

[1] sangeerthanetech@gmail.com, [2]razeethsuhail@seu.ac.lk

Abstract

Natural rubber latex is a valuable raw material in both agricultural and industrial industries of Sri Lanka and the quality of it directly determines the commercial value, efficiency of the processes and its appropriate use as raw material used in the manufacturing industry. Nevertheless, today the quality of latex was traditionally measured with the usage of traditional laboratory-based tests, including Dry Rubber Content (DRC), Total Solid Content (TSC), pH measurement, and Volatile Fatty Acid (VFA) analysis. These techniques are technically sound, but are time consuming, labor intensive and cannot be used in real time ongoing monitoring. This weakness defines the need to design a low-cost smart system that can be used to facilitate much faster and smarter quality analysis. This paper suggests that a smart Internet of Things (IoT) and Artificial Intelligence (AI)-based real-time monitoring and quality prediction of rubber latex be developed in Sri Lanka. The presented system employs four quality-related parameters, e.g. density, pH, temperature, and turbidity, which are determined by sensors with an ESP32 microcontroller. Summary Sensor readings are sent through Wi-Fi to Firebase real-time database and stored and synchronized in the cloud. To track and interpret sensor values and prediction output, a React-based web dashboard was created to monitor live sensor values and prediction outputs. As a part of the prediction, Random Forest, Decision Tree, and K-Nearest Neighbors (KNN) models were created and compared, the former had the highest accuracy of 0.98, which led to its being chosen as the final model. The findings indicate that the created prototype manages to combine sensor-implemented monitoring, the cloud, and dashboard visualization and AI-based prediction into a single useful system. The paper concludes that the suggested solution is a viable and effective one to enable monitoring of rubber latex quality and subsequent digital transformation in Sri Lanka.

Keywords: *Rubber Latex Quality, Internet of Things, ESP32, Firebase Realtime Database, Random Forest, Real-Time Monitoring, Smart Agriculture*

e-ISBN 978-955-627-501-8

IoT-Enabled Smart Shoe for Early Detection of Diabetic Foot Ulcer Risk

M.H.M. Ajas[1] and M.S.S. Razeeth[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka, Sri Lanka*

[1]mohamedajas90715@gmail.com, [2]razeethsuhail@seu.ac.lk

Abstract

DFU is among the gravest complications of diabetes mellitus that can result in infection, prolonged hospitalization, decreased mobility, amputation of lower limbs, and poor quality of life.DFU risk has been hard to detect due to the nature of conventional assessment, as periodic and clinic-based assessments are common in healthcare facilities. This research presents an IoT-based smart shoe prototype that helps identify DFU risk by combining multimodal sensors and artificial intelligence-powered classification. The suggested system consists of sensors for plantar pressure, humidity, temperature, moisture, pulse, SpO_2, pH, and thermal hotspot intensity, monitoring foot health conditions related to ulcer formation. Hotspot temperature is obtained using an infrared thermal sensor as a structured feature, but not through image classification. The sensor measurements are recorded via a wearable IoT framework and sent to a cloud-based service, with a Flutter-based app for patients and a web-based dashboard for clinicians for visualizing risks, alerts, and preventive advice. The research was prepared with a dataset of 5000 samples split into three classes: Low Risk, Moderate Risk, and High Risk. Normalization and cleaning of data were carried out with Min-Max scales; the labels were reduced to integers, and the model input was prepared. 80 percent of the data was used for training and 20 percent for testing using stratified sampling. Four models have been tested, i.e., Dense Neural Network, CNN-LSTM, Decision Tree, and Random Forest. The findings indicated high predictive performance with Dense Neural Network and Random Forest achieving the highest test accuracy on the prepared dataset, whereas Decision Tree and CNN-LSTM achieved 99.80 and 99.60, respectively. The most practical model was the Dense model due to its ease of export to TensorFlow Lite. Altogether, the results indicate that multimodal IoT sensing, aided by AI, offers a promising basis for deployment-based DFU risk surveillance in wearable healthcare systems.

Keywords: *Diabetic Foot Ulcer, IoT, Smart Shoe, Multimodal Sensing, Artificial Intelligence, Wearable Healthcare*

e-ISBN 978-955-627-501-8

Smart AI-Powered Glass Waste Collecting Robot for Home Floor Safety

J. P. S. P. K. B. Wimalasena[1] and M.S.S. Razeeth[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka, Sri Lanka*

[1]surangaprabhash@gmail.com, [2]razeethsuhail@seu.ac.lk

Abstract

The presence of broken glass fragments on indoor floors poses a serious safety risk, particularly for children, pets, and individuals who walk barefoot. Even after cleaning, small fragments may remain due to incomplete inspection, increasing the risk of unnoticed injuries. Existing robotic cleaning systems do not specifically detect or handle such hazardous materials. This research presents the design and development of an AI-powered glass fragment collecting robot aimed at improving indoor safety by targeting visible fragments commonly missed during routine cleaning. The system uses a YOLOv8-based object detection model running on a Raspberry Pi 4 Model B to identify glass fragments in real time using a USB camera. The Raspberry Pi acts as the main processing unit and communicates with an Arduino Nano to control movement, sensors, and the collection mechanism. The robot features a four-wheel drive system, obstacle detection, and a brush-based mechanism for collecting small fragments. Detected objects are classified into four categories. Small fragments are collected automatically, while large or multiple fragments trigger an alert and stop the robot for user intervention. Glass-like objects prompt a user decision through a mobile application. The system also monitors battery level and dustbin capacity to ensure safe operation. A Flutter based mobile application integrated with Firebase enables real time monitoring and notifications. Experimental results demonstrate effective detection and collection across various indoor surfaces, highlighting the system's potential to enhance household safety.

Keywords: *YOLOv8, Object Detection, Autonomous Robot, Glass Fragment Detection, Embedded Systems, Firebase, Real-Time Monitoring*

e-ISBN 978-955-627-501-8

Secure IoT-Based Remote Solar Power Management for Grid Stability in Sri Lanka

K.T.D.T. Kalhara[1] and M.M. Mohamed Mufassirin[2]

[1]*Department of Information and Communication Technology, South Eastern University of Sri Lanka, Sri Lanka*
[2]*Department of Computer Science, Faculty of Applied Sciences, South Eastern University of Sri Lanka*

[1]20.kalhara@gmail.com, [2]mufassirin@seu.ac.lk

Abstract

Residential solar power generation in Sri Lanka is growing rapidly. This rapid growth is fed into the national grid without control. It has the potential to destabilize the national grid. When solar power generated in homes is fed into the main grid without the supervision and control of the relevant authorities, the main grid becomes unstable due to voltage surges and a complete power outage occurs. For this purpose, an IoT system was created that can monitor and manage residential solar power in real time and remotely. An ESP32 Wi-Fi microcontroller is used as the central processing unit, and a ZMPT101B AC voltage sensor is used to measure the voltage added to the main grid and an SCT-013 AC current sensor is used to measure the current. A relay is connected to stop and reconnect the electrical current added to the main grid by solar power. HTTPS/TLS encryption was used over Wi-Fi to securely transmit the data collected by the sensors to the Firebase Realtime database. Firebase Authentication Access Management was used to provide observers and live data access. A web dashboard was built using ReactJS for live data monitoring and relay control. If the residential solar power generation exceeds certain safety limits, it can be monitored through the web dashboard and the relevant operators can stop adding solar power to the main stream through remote relays. This can eliminate the instability of the network. There is a role-based management system. It allows administrators to delete and edit solar units and manage users. Officers have solar unit editing permissions. A single household prototype was designed and tested, focusing on the accuracy of sensor measurements, data transmission latency, user-friendly web interface, and safety of AC. The results show that this can provide operators with real-time and direct intervention capabilities. It was found that this prototype could be used practically for the future expansion of remote solar management solutions throughout Sri Lanka.

Keywords: *Internet of Things, Solar Power Monitoring, Grid Stability, Firebase, Cybersecurity, Smart Grid*

e-ISBN 978-955-627-501-8

IoT-Based Smart Medicine Box for Personalized Medication Management with Remote Guardian Alerts

P.K.S.N. Senevirathna [1] and M.S.S Razeeth[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka, Sri Lanka*

[1]nishara12288@gmail.com, [2]razeethsuhail@seu.ac.lk

Abstract

Medication non-adherence remains a serious healthcare problem, especially among elderly patients and individuals with chronic illnesses who require regular and timely medication. Although many reminder-based solutions have been proposed, most existing systems do not verify the identity of the person accessing the medicine and do not confirm whether the medication was retrieved. This research presents the design and development of an IoT-based Smart Medicine Box for personalized medication management with remote guardian alerts. The proposed system consists of three integrated components: a Flutter-based mobile application, a cloud-based model training pipeline, and an IoT medicine dispensing device built on a Raspberry Pi Zero 2 W. The mobile application is used for patient registration, multi-pose face image capture, medication schedule configuration, dispense history monitoring, and remote fingerprint enrollment. The training pipeline uses PyTorch to train a personalized lightweight facial recognition model from the captured images and exports the model to ONNX format for edge deployment. The IoT device combines fingerprint authentication, face recognition, a servo-controlled dispensing mechanism, an IR sensor for pill retrieval detection, and caregiver alerting through Firebase-based notifications. At each scheduled medication time, the system initiates a dispensing cycle in which the patient is first verified through fingerprint authentication and then through personalized face recognition. Medication is released only when both verifications are successful. After dispensing, the IR sensor monitors the tray to confirm pill retrieval, and the event is recorded in the Firebase Realtime Database. Guardians are notified in both successful and missed-dose situations, enabling more effective remote monitoring. The study shows that integrating dual biometric verification, edge-based ONNX inference, retrieval confirmation, and real-time guardian alerts can improve both medication security and adherence monitoring in a practical and cost-effective manner.

Keywords: *IoT, Smart Medicine Box, Face Recognition, Fingerprint Authentication, Medication Adherence*

e-ISBN 978-955-627-501-8

IoT Based Smart Soil Moisture Monitoring and Automated Irrigation System for Sugarcane Cultivation in Pelwatte Area

A.K. Ediriweera[1] and R.K.A.R. Kariapper[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka, Sri Lanka*

[1]19ict077@seu.ac.lk, [2]rk@seu.ac.lk

Abstract

Agriculture is a cornerstone of Sri Lanka's economy, with sugarcane cultivation playing a vital role in industrial sugar production. Traditional irrigation practices in the Pelwatte region rely on manual monitoring and fixed schedules, often resulting in water wastage, inconsistent crop growth, and increased labor costs. This study proposes the design and implementation of an IoT-based smart soil moisture monitoring and automated irrigation system tailored for sugarcane cultivation. The system integrates soil moisture sensors, DHT22 temperature and humidity sensors, and pH monitoring with ESP32 microcontrollers and wireless communication modules. Real-time data is transmitted to a control unit, displayed on an LCD dashboard, and used to automate irrigation decisions. A relay-controlled water pump is activated when soil moisture falls below a threshold, while an emergency stop mechanism ensures operational safety. Experimental results demonstrate that the system reduces water wastage, improves irrigation efficiency by approximately 30%, and supports healthier crop growth. By combining automation, environmental monitoring, and cloud integration, the proposed framework provides a cost-effective and scalable solution for smart agriculture in Sri Lanka. This research highlights the potential of IoT technologies to transform traditional irrigation practices, contributing to sustainable resource management and improved productivity in largescale sugarcane plantations.

Keywords: *IoT, Smart Irrigation, Soil Moisture Monitoring, ESP32, Sugarcane Cultivation, Cloud Integration, Agricultural Efficiency*

e-ISBN 978-955-627-501-8

Budget IoT-Based Motorcycle Health Monitoring System

M.D.P.L. Kavinda[1] and R.K.A.R. Kariapper[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka, Sri Lanka*

[1]19ict095@seu.ac.lk, [2]rk@seu.ac.lk

Abstract

In recent years, Internet of Things (IoT) technologies have been widely applied to smart monitoring systems across various fields, including transportation. However, most motorcycle monitoring solutions remain costly and inaccessible to average users, particularly in developing countries. Traditional motorcycles also lack real-time health monitoring features, making it difficult to detect issues such as engine overheating, battery faults, accidents, and theft at an early stage. This highlights the need for a cost-effective and reliable monitoring system. This research focuses on developing a budget-friendly IoT-based motorcycle health monitoring system by integrating low-cost hardware with a mobile application and cloud platform. The system employs an ESP32 microcontroller with sensors including a temperature sensor for engine heat, a voltage sensor for battery condition, and an MPU6050 sensor for tilt and crash detection. A GPS module is added to track real-time location. Sensor data is transmitted to a Firebase real-time database, enabling smooth communication with a Flutter-based mobile application. The app provides a simple interface displaying speed, temperature, battery voltage, and tilt angle in real time, enhanced with a speedometer-style gauge for visualization. An alert mechanism informs users of critical conditions such as overheating, crashes, low battery, or theft, ensuring quick response. The system also supports basic remote-control functions, including ignition and engine start/stop, enhancing convenience and security. Development followed a structured process of design, implementation, and testing. Results confirm accurate real-time data, reliable alerts, and efficient communication, all at low cost. This research demonstrates that an effective and affordable motorcycle monitoring system can be built using IoT technology. Future improvements may include predictive maintenance and fuel monitoring, contributing to smarter and more efficient transportation solutions.

Keywords: *Motorcycle Health System, Low-cost Hardware, Real-time Alerts, Cloud Integration, IoT Based Monitoring*

e-ISBN 978-955-627-501-8

Design and Development of an AI-Driven IoT Framework with Watchdog-Based Reliability for Adaptive Food Dehydration Under Variable Environmental Conditions

Y.M.V.S. Weerakoon[1] and M.S.S. Razeeth [2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]ymvihanga@gmail.com, [2]razeethsuhail@seu.ac.lk

Abstract

In recent years, food dehydration has become a common preservation technique that lowers the amount of moisture and inhibits the growth of microorganisms, therefore improving the shelf life of food items. However, traditional dehydration systems are usually based on constant temperature options and manual control that restrict their adaptability to various environmental factors. Such restrictions usually lead to ineffective drying, uneven quality of products, and waste of energy. In order to overcome these challenges, this research paper suggests an AI-driven IoT-based food dehydration system, which is reliably monitored by watchdog-based reliability. The system employs a temperature and humidity sensor-driven ESP32-based IoT platform to provide real-time feedback on the environmental conditions in the dehydration chamber. The sensor data is sent to a cloud-based server to access and store the sensor data remotely. Real-time and historical data are analyzed with ML methods, such as regression-based models (Random Forest) to predict the best drying conditions and specify the endpoint of drying. The system has both heating and cooling systems with the cooling system specially designed to remove moisture in the air in the chamber to provide effective humidity control. To enhance the reliability of long-duration processes, a watchdog-based fault detection and recovery mechanism is in place that automatically causes system failures and recovers the system to normal functioning. A user interface that is mobile-based allows real-time access and communication with the system. The system is created by combining hardware and IoT communication and prediction based on ML. The projected results show increased drying efficiency, less manual intervention, better consistency of the product, and reliability of the system as opposed to the traditional methods of dehydration. The effectiveness of this research is that the combination of IoT and AI methods with fault-tolerant mechanisms can be used to create an adaptive and intelligent system of food dehydration.

Keywords: *Smart Dehydration System, Internet of Things (IoT), Artificial Intelligence (AI), Machine Learning (ML), Watchdog Timer, Food Preservation, Remote Monitoring and Controlling*

e-ISBN 978-955-627-501-8

Smart Transit: A Real-Time Public Bus Tracking and Route Information System

W.M.S.V Wijerathna[1] and M.M Mohamed Mufassirin[2]

[1]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*
[2]*Department of Computer Science, Faculty of Applied Sciences, South Eastern University of Sri Lanka*

[1]productionvidu@gmail.com, [2]mufassirin@seu.ac.lk

Abstract

Public transportation serves as a key aspect of day-to-day mobility in developing countries, such as Sri Lanka. However, at present, the bus systems do not support real-time tracking, which leads to uncertainties, longer wait times, and lack of visibility for passengers. In light of the above issues, the following study proposes the development of the system named "Smart Transit." This system aims to provide real-time bus tracking, along with route information, to increase comfort and ease for passengers. In order to achieve the stated objectives, the proposed system is developed in the form of a mobile application for the Android platform. Specifically, the developed application integrates Firebase Realtime Database and Google Maps APIs. To track the bus location, the coordinates provided by the GPS sensors installed in the driver's phone are uploaded in real time. As a result, users can view the actual location of the buses on a map displayed by the application. Apart from tracking bus locations, the system contains an Artificial Intelligence–based sentiment analysis module used for processing user feedback. Specifically, the pre-trained model(Hugging Face API) that uses natural language processing to determine whether a comment left by a passenger is positive, negative, or neutral is applied. To use this technology, the application connects to Hugging Face's API in order to analyze textual feedback. Furthermore, an estimated time of arrival (ETA) calculation module based on the geographical coordinates of drivers and users is implemented in the application. Specifically, the distance and ETA are calculated based on the geographical coordinates (Latitude/Longitude) and the results provided by Google Maps. The developed Smart Transit system was tested in terms of its performance, reliability, accuracy, usability, and scalability. Experimental observations show that the proposed solution allows delivering almost real-time tracking with sufficient GPS accuracy. Furthermore, The use of cloud-based services ensures reliable data synchronization and supports system scalability.

Keywords: *Android Application, Firebase Realtime Database, Google Maps API, GPS Tracking, Hugging Face, Intelligent Transportation Systems, Real-Time Bus Tracking, Sentiment Analysis, Smart Transportation System*

Smart Car Park System Using Machine Learning and IoT with Integrated Payment Functionality

H.C. Dilipun[1] and A.R.F. Shafana[2]

[1,2]*Department of Information and Communication Technology, South Eastern University of Sri Lanka*

[1]hchiraji@gmail.com, [2]arfshafana@seu.ac.lk

Abstract

Rapid urbanization and increasing vehicle ownership have created major challenges in urban parking management worldwide. Studies estimate that nearly 30% of urban traffic congestion is caused by drivers searching for available parking spaces. Conventional parking systems rely on manual ticketing and cash payments, lack real-time monitoring, and are often inefficient, slow, and insecure. This research proposes an intelligent parking system integrating IoT, machine learning–based Automatic Number Plate Recognition (ANPR), and contactless NFC payments to improve efficiency and user convenience. The system uses infrared sensors for real-time detection of parking slot occupancy and an ESP32 microcontroller for centralized control, data acquisition, and communication. A cross-platform web dashboard enables administrators to monitor parking operations in real time, including slot availability, revenue tracking, and vehicle history management. The backend infrastructure uses a SQLite database for secure data storage and Flask-based RESTful APIs for efficient performance and communication. Key modules include ANPR processing using OpenCV and EasyOCR, servo motor gate control, NFC payment integration, and LCD-based user feedback. Experimental results demonstrate strong system performance. The ANPR module achieved an accuracy of 89.2% under varying lighting conditions, while parking sensors recorded 99.5% reliability. NFC payment transactions were completed within 1–2 seconds. Average vehicle entry processing time was 3–5 seconds, while exit processing required 5–8 seconds, representing a 60–70% reduction in transaction time compared with conventional manual systems. In addition to faster processing, the system provides real-time operational insights that support informed decision-making and efficient resource management. The findings highlight the potential of integrating IoT, machine learning, and contactless payment technologies to deliver scalable, reliable, and intelligent parking solutions. The proposed framework is adaptable to shopping malls, hospitals, airports, and corporate facilities, supporting digital transformation and improved operational efficiency worldwide today.

Keywords: *Smart Parking, Internet of Things, Automatic Number Plate Recognition, NFC Payment, ESP32*

e-ISBN 978-955-627-501-8

URCDICT 2026

Department of ICT
Faculty of Technology
South Eastern University of Sri Lanka
University Park
Oluvil
Sri Lanka

www.seu.ac.lk

#urcdict
#urcdict2026
#dictft

Media Support:

Technical Support:

e-ISBN 978-955-627-501-8