

Information Systems Engineering and Management 4

S. Manoharan
Alexandru Tugui
Zubair Baig *Editors*

Proceedings of 4th International Conference on Artificial Intelligence and Smart Energy

ICAIS 2024, Volume 2

 Springer

Series Editor

Álvaro Rocha, *ISEG, University of Lisbon, Lisbon, Portugal*

Editorial Board Members

Abdelkader Hameurlain, *Université Toulouse III - Paul Sabatier, Toulouse, France*


Ali Idri, *ENSIAS, Mohammed V University, Rabat, Morocco*

Ashok Vaseashta, *International Clean Water Institute, Manassas, VA, USA*


Ashwani Kumar Dubey, *Amity University, Noida, India*

Carlos Montenegro, *Francisco José de Caldas District University, Bogota, Colombia*

Claude Laporte, *University of Quebec, Québec, QC, Canada*

Fernando Moreira , *Portucalense University, Berlin, Germany*

Francisco Peñalvo, *University of Salamanca, Salamanca, Spain*

Gintautas Dzemyda , *Vilnius University, Vilnius, Lithuania*


Jezreel Mejia-Miranda, *CIMAT - Center for Mathematical Research, Zacatecas, Mexico*

Jon Hall, *The Open University, Milton Keynes, UK*

Mário Piattini , *University of Castilla-La Mancha, Albacete, Spain*

Maristela Holanda, *University of Brasilia, Brasilia, Brazil*

Mincong Tang, *Beijing Jiaotong University, Beijing, China*

Mirjana Ivanović , *Dept. of Mathematics and Informatics, University of Novi Sad, Novi Sad, Serbia*

Mirna Muñoz, *CIMAT - Center for Mathematical Research, Progreso, Mexico*

Rajeev Kanth, *University of Turku, Turku, Finland*

Sajid Anwar, *Institute of Management Sciences, Peshawar, Pakistan*

Tutut Herawan, *Faculty of Comp Sci & Info Tech, University of Malaya, Kuala Lumpur, Malaysia*

Valentina Colla, *TeCIP Institute, Scuola Superiore Sant'Anna, Pisa, Italy*

Vladan Devedzic, *University of Belgrade, Belgrade, Serbia*

The book series “Information Systems Engineering and Management” (ISEM) publishes innovative and original works in the various areas of planning, development, implementation, and management of information systems and technologies by enterprises, citizens, and society for the improvement of the socio-economic environment.

The series is multidisciplinary, focusing on technological, organizational, and social domains of information systems engineering and management. Manuscripts published in this book series focus on relevant problems and research in the planning, analysis, design, implementation, exploration, and management of all types of information systems and technologies. The series contains monographs, lecture notes, edited volumes, pedagogical and technical books as well as proceedings volumes.

Some topics/keywords to be considered in the ISEM book series are, but not limited to: Information Systems Planning; Information Systems Development; Exploration of Information Systems; Management of Information Systems; Blockchain Technology; Cloud Computing; Artificial Intelligence (AI) and Machine Learning; Big Data Analytics; Multimedia Systems; Computer Networks, Mobility and Pervasive Systems; IT Security, Ethics and Privacy; Cybersecurity; Digital Platforms and Services; Requirements Engineering; Software Engineering; Process and Knowledge Engineering; Security and Privacy Engineering, Autonomous Robotics; Human-Computer Interaction; Marketing and Information; Tourism and Information; Finance and Value; Decisions and Risk; Innovation and Projects; Strategy and People.

Indexed by Google Scholar. All books published in the series are submitted for consideration in the Web of Science.

For book or proceedings proposals please contact Alvaro Rocha (amrocha@gmail.com).

SERIES EDITOR:

Álvaro Rocha, ISEG, University of Lisbon, Portugal

ADVISORY BOARD:

Abdelkader Hameurlain, Université Toulouse III - Paul Sabatier, France

Ashwani Kumar Dubey, Amity University, India

Carlos Montenegro, Francisco José de Caldas District University, Colombia

Fernando Moreira, Portucalense University, Portugal

Francisco Peñalvo, University of Salamanca, Spain

Gintautas Dzemyda, Vilnius University, Lithuania

Jezreel Mejia-Miranda, CIMAT - Center for Mathematical Research, Mexico

Mário Piattini, University of Castilla-La Mancha, Spain

Mirjana Ivanović, University of Novi Sad, Serbia

Mirna Muñoz, CIMAT - Center for Mathematical Research, Mexico

Sajid Anwar, Institute of Management Sciences Peshawar, Pakistan

Tutut Herawan, University of Malaya, Malaysia

Valentina Colla, Scuola Superiore Sant’Anna - TeCIP Institute, Italy

Vladan Devedzic, University of Belgrade, Serbia

S. Manoharan · Alexandru Tugui · Zubair Baig
Editors

Proceedings of 4th International Conference on Artificial Intelligence and Smart Energy

ICAIS 2024, Volume 2

 Springer

Editors

S. Manoharan
JCT College of Engineering and Technology
Coimbatore, Tamil Nadu, India

Alexandru Tugui
Department of Business Informatics
Alexandru Ioan Cuza University
Iasi Romania, Romania

Zubair Baig
School of Information Technology
Deakin University
Geelong, Australia

ISSN 3004-958X ISSN 3004-9598 (electronic)
Information Systems Engineering and Management
ISBN 978-3-031-61474-3 ISBN 978-3-031-61475-0 (eBook)
<https://doi.org/10.1007/978-3-031-61475-0>

© The Editor(s) (if applicable) and The Author(s), under exclusive license
to Springer Nature Switzerland AG 2024

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

If disposing of this product, please recycle the paper.

We would like to dedicate this proceeding to all members of the advisory committee and program committee for providing their excellent guidance. We also dedicate this proceeding to the members of the review committee for their excellent cooperation throughout the conference. Additionally, we extend our sincere thanks to all the authors and participants.

Preface

Welcome to the second volume of the book, *Artificial Intelligence and Smart Energy*, where innovative research and cutting-edge technologies converge to address the challenges of our time. This volume presents a comprehensive collection of research chapters from diverse domains, each contributing significantly to the advancement of energy and sustainability.

This book reflects the collective efforts of researchers, scholars, and practitioners from around the globe, showcasing their dedication to exploring novel solutions to complex problems. From securing cyber-physical systems to revolutionizing healthcare with artificial intelligence and robotics, the topics covered here highlight the ways to leverage sustainable research.

Moreover, this volume is particularly focused on smart and sustainable energy solutions, which plays a major role in building a greener future for generations to come. From advancements in solar panel efficiency and fault analysis to the development of fuzzy-controlled converters for grid-tied photovoltaic systems, the chapters presented in this volume offer insights into the latest innovations in renewable energy technologies. On the other hand, by including the research studies on water solutions, agricultural innovations, and renewable energy technologies, this volume depicts the transformative potential of artificial intelligence, machine learning, and the Internet of Things across various domains, including smart cities, transportation, and healthcare.

We believe that the insights shared in this volume will inspire further research, enable fruitful discussions, and create real-world impact to drive toward a future defined by resilience, inclusivity, and sustainable development.

S. Manoharan
Alexandru Tugui
Zubair Baig

Contents

| | |
|---|-----|
| Efficient Detection of Cyberbullying in Social Media Platform | 1 |
| <i>V. Aishwarya, M. Amirtha, R. S. Amshavalli, D. Aishwarya, and A. Mohana Priya</i> | |
| Securing Cyber-Physical Systems: A Strategic Review | 13 |
| <i>B. Muthu Nisha and J. Selvakumar</i> | |
| Advancing Solar Still Efficiency – Pioneering Sustainable Water Solutions | 24 |
| <i>Hari Vamsi Valluru, Deva Harshini, Gopi, Muralidhar, and Mounika</i> | |
| An In-Depth Investigation into Automatic Dubbing Leveraging ASR, Machine Translation and Deep Voice 3 | 34 |
| <i>K. Hema Priya, N. Akhilan, R. Aravindh, and K. Janardhana</i> | |
| LEWRY Your Smart Home Security Robot | 49 |
| <i>E. Annadevi, S. Keertana, D. Moshmi, and Sonal Verma</i> | |
| Ensemble Based Attrition Prediction in Corporate Settings | 64 |
| <i>Malliga Subramanian, A. Chandramukhi, S. Arunaa, R. Gokulkrishna, and Kogilavani Shanmugavadivel</i> | |
| Mitigating Agricultural Challenges: A Comprehensive Study on the Impact of Crop Diseases on Rice Production in India | 81 |
| <i>Sunitha Maddhi, Ratnam Dodda, Azmera Chandu Naik, and K. Sinduja</i> | |
| Human Object Interaction: A Survey on Models and Their Key Challenges and Potential Applications in Future Fields | 93 |
| <i>Rathod Dharmendrasinh, Amit Thakkar, Devraj Parmar, and Kishan Patel</i> | |
| Streamlining the Bone Fracture Detection Using X-Ray Imaging and Seamless PACS Data Exchange | 107 |
| <i>Swarada Gade, Varshita Nukala, Shravani Walunj, Tanaya Sutar, and Avinash Golande</i> | |
| A Review on Suitability of Vertical Federated Learning in Smart City Platforms | 122 |
| <i>Komala Soares and Arundhati A. Shinde</i> | |

| | |
|--|-----|
| Land Cover Classification Using Modified U-net: A Robust Approach for Satellite Image Analysis | 135 |
| <i>Shashikant Rangnathrao Kale, Chandrakant Madhukar Kadam, Raghunath Sambhaji Holambe, and Rajan Hari Chile</i> | |
| Synergistic Evolution: Pioneering Frontiers of Artificial Intelligence and Robotics in Healthcare | 147 |
| <i>Jaspreet Kaur</i> | |
| Solar Panel Fault Analysis Using Regression Models | 158 |
| <i>P. Sampurna Lakshmi, S. Sivagamasundari, and Manjula Sri Rayudu</i> | |
| Development of Fuzzy Controlled Five Level Modular Multilevel Converter for Grid Tied PV System | 173 |
| <i>B. Kavya Santhoshi, D. Ravi Kishore, B. Hari Prasad, G. Nikhil, and M. Hari Krishna</i> | |
| Multifaceted Chatbot: A Retrieval Augmented Generation Approach for Intelligent Website Query Handling | 185 |
| <i>K. R. Radhakrishnan, R. Saran Kumar, and S. Sivarama Krishnan</i> | |
| Intelligent Monitoring and Learning System for Electric Vehicle Charging Stations | 198 |
| <i>R. Santhoshkumar, I. Jabez, S. B. Kannan, and Kaviarasan Kumar</i> | |
| A Global Three Wheeler Road Freight EV Cargo Cart for Value Added Services | 208 |
| <i>C. M. Usha Rani, M. S. Shalini, M. N. Rekha, V. Santhosha, and L. Agnitej</i> | |
| Android App-Oriented Smart Supervision of Water Distribution Using Internet of Things | 223 |
| <i>Raghu Ramamoorthy, S. M. Manasa, and J. A. Smitha</i> | |
| Identification of Speech Stream and the Source Localization for Hearing Prosthesis-Driven Healthcare | 238 |
| <i>Anudeep Peddi and Venkata Ramana Teppala</i> | |
| Catalyzing Urban Logistics and Road Safety: Truck Recommendation System and Real-Time Accident Severity Prediction | 248 |
| <i>M. Shajan, K. Suresh Kumar, and R. Elavarasan</i> | |
| Powering the Future: A Comprehensive Review on DC-DC Converters and Their Vital Role in Electric Vehicle Technology | 261 |
| <i>K. P. Revathy and K. Vijayakumar</i> | |

A Smart Fuzzy Metaheuristic Energy Optimisation Framework for Heterogeneous Wireless Sensor Networks 276
Neha Bhende, G. Deepika, Lakshmi Priya Ramesh, Rupa Kesavan, and L. Vijayaraja

Time Series Modeling for the Development of a Systematic, Cost Effective, and ML-Supported Cargo Tracking System: Optimizing Supply Chain Efficiency 289
Archana Ingle, Sayanna Mukharjee, Amit Vishwakarma, and Jatin Tiwari

Federated Learning in Automated Vehicles 301
Sonal Shamkuwar, Arijit Mondal, Rohan More, Smita Bodare, and Aditya Pendalwar

Analysis and Priority Based Smart Power Distribution System Using Automatic Voltage Regulator (AVR) 315
Bindu Vadlamudi, Vijayasri Nishitha Bommisetty, Vandana Vutla, and Tejavath Nagamani

Study of Automated E-Waste Classification Techniques 325
Vritika Deodhar, Riddhi Bhogaonkar, Shreya Patankar, and Harshal Dhabale

Optimizing Solid Waste Management: The Ecosort Solution 343
Yojana Fegade, Sakshi Gadhav, Pratik Godse, Swaraj Jadhav, and Amruta Hingmire

Using BERT with Modified Metaheuristic Optimized XGBoost for Phishing Email Identification 358
Milos Antonijevic, Luka Jovanovic, Nebojsa Bacanin, Miodrag Zivkovic, Jelena Kaljevic, and Tamara Zivkovic

Advancements in Providing Quality-of-Service in Cyber-Physical Systems: A Comprehensive Review 371
C. Ramakristanaiah, K. Indraveni, and Chas Murty

Framework for Securing Biometric Authentication System Using InterPlanetary File System and Blockchain Technology 384
Dharmesh Kumar Sonkar and Sarvpal Singh

Optimizing Electric Vehicle Battery Performance: A Comparative Analysis of ANFIS and AUKFM for SOC and SOH Estimation 395
M. S. Shalini, C. M. Usha Rani, and H. H. Likhitha

| | |
|---|------------|
| Customer Churn Prediction and Personalised Recommendations in Banking . . . | 409 |
| <i>Prachi Pathak, Vaishnavi Chandgadkar, Aditya Solanki, Aryansh Shrivastava, Namita Pulgam, and Tabassum Maktum</i> | |
| Designing a Secure Oil and Gas Supply Chain System with Elliptic Curve Cryptography (ECC) Enabled Blockchain | 422 |
| <i>Janmejay Kumar Vishwakarma and Rajendra Kumar Dwivedi</i> | |
| Innovative AI-Powered Image Generator: Converting Text into Images with OpenAI | 436 |
| <i>G. Soma Shiva Sai Babu and K. S. Rekha</i> | |
| IoT Node Authentication Using Du-KAuth with Strong Access Control Model in Smart City Application | 447 |
| <i>Gundala Venkata Rama Lakshmi, R. Deeptha, and K. Venkatesh Sharma</i> | |
| Analysis of Placement in FPGA Using Genetic and Hybrid Genetic and Simulated Annealing Algorithms | 458 |
| <i>P. Sudhanya, S. P. Joy Vasantha Rani, and Saksham Goswami</i> | |
| Detection of Heart Failure Using a Convolutional Neural Network (CNN) via ECG Signals | 471 |
| <i>Medikonda Ramya, T. Kishore Babu, P. Hussain Basha, and Vikruthi Sriharsha</i> | |
| Supercapacitor Based EV Power Management System | 483 |
| <i>M. Mynavathi, K. Arun Kumar, M. Mugunthan, J. Shanmugapriya, A. L. Soundharya, and R. Ragavan</i> | |
| Formation of LMS Class Diagram | 493 |
| <i>Elov Botir Boltayevich, Toirova Guli Ibragimovna, Zuparov Talat Marufovich, and Axmedova Xolisxon Ilxomovna</i> | |
| Author Index | 511 |



Efficient Detection of Cyberbullying in Social Media Platform

V. Aishwarya, M. Amirtha, R. S. Amshavalli^(✉), D. Aishwarya, and A. Mohana Priya

Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, India

amshavalli.cse@sathyabama.ac.in

Abstract. The prevalence of cyberbullying on messaging apps like WhatsApp is a major concern nowadays. The first step in resolving this problem is developing machine learning models to automatically identify the cases of cyberbullying. In order to detect cyberbullying on the messaging app like WhatsApp, this study introduces a machine learning approach that makes use of logistic regression and support vector machines (SVMs). Collecting a dataset of WhatsApp chats, including both cyberbullying and non-bullying ones, is the first step in the proposed method. In order to clean up the data and remove any noise, text preparation methods are used. Feature extraction is a powerful tool used for capturing important environmental and vocal cues related to cyberbullying. Classification models are trained by utilizing the selected features with the help of logistic regression and support vector machines. The outcomes demonstrate the efficacy of the suggested method. While Support Vector Machines (SVMs) get up to 85% accuracy, logistic regression models have 83% accuracy when it comes to cyberbullying case classification. The results show that the machine learning algorithms were successful in detecting cyberbullying in WhatsApp conversations.

Keywords: Bidirectional LSTM · Cyberattack · Phishing · Email Detection · SVM

1 Introduction

Machine Learning is one of the viable solutions for the ever-increasing problem of cyberbullying on social media platforms. Using Logistic Regression (LR) and Support Vector Machine (SVM) approaches, this study primarily focuses on detecting cyberbullying events inside the popular messaging app WhatsApp. One of the best ways to meet new people is to use social media. However, individuals are engaging in illegal and immoral activities via these networks as their popularity has increased. Especially among young adults and teens, it is clear that individuals are developing novel approaches to cyberbullying. Bullying that takes place via the use of electronic means is known as cyberbullying. The impacts on young people have just now come to light, despite the fact that this issue has persisted for a long time. Teens and young adults who use social media are easy targets for cyberbullies, and these sites also put them at risk of cyberattacks. Using machine learning, we can establish criteria for the automated detection of cyberbullying material

and the identification of common linguistic patterns used by both bullies and their victims. Concerning cyberbullying's ability to wreak substantial damage to an individual's psychological state and general wellbeing, it poses a major danger to people. It is critical to develop effective techniques to identify and combat cyberbullying due to the growing use of social media platforms like WhatsApp. It is feasible that this pervasive problem may be mechanized and effectively addressed by using machine learning algorithms to the problem of social media bullying. These algorithms have shown promise in several domains.

Logistic regression is a popular machine learning classification method for solving binary classification issues. The system trains a logistic regression model using labelled data in order to find patterns and characteristics associated with cyberbullying incidents. Features such as angry tone, inflammatory language, and targeted personal attacks may be extracted from WhatsApp chat text data and used to train the logistic regression model. The model may be trained to detect whether a new message constitutes cyberbullying, enabling swift responses in such cases. Cyberbullying may also be detected using Support Vector Machine, another powerful method. Support vector machines (SVMs) choose the best hyperplane to divide the data into two sets, in this case, texts with cyberbullying and those without. By using appropriate feature extraction methods and text preparation processes, SVMs are able to understand the fundamental patterns and differentiate between the two groups. SVMs are an excellent fit for delicate cases of cyberbullying because of their capacity to manage non-linear correlations and high-dimensional data.

By integrating the strengths of logistic regression and support vector machine methods, the proposed machine learning approach improves WhatsApp's cyberbullying detection capabilities. The methodology overcomes the limitations of each approach while capitalizing on their unique strengths by using both strategies simultaneously. This concept may be enhanced even more by using additional methods including ensemble approaches, feature engineering, and natural language processing. Finally, using machine learning methods, particularly logistic regression and support vector machines, might be a way to detect cyberbullying using WhatsApp. Cyberbullying is a serious problem, but there may be an automated solution thanks to these algorithms' ability to learn from labelled data. By fostering constructive connections and mitigating the detrimental impacts of cyberbullying, this approach, if developed and implemented, may assist WhatsApp users in enjoying a more secure and enjoyable online experience.

2 Related Works

Gautam A.K and Bansal.A [1], presented a model for cyberstalking detection using supervised machine learning methods such as Logistic Regression, Support Vector Machines (SVM), Decision Trees, Random Forest, K-Nearest Neighbor, and Naive Bayes. Two machine learning techniques were used to two datasets with different sizes and distributions: Bag of Words and Term Frequency (TF). The acronym "IDF" stands for Inverse Document Frequency. Based on the results of their experiments, the two most Logistic regression and logistic regression with feature extraction were the methods used on the two datasets. Regression and Support Vector Machine. Ige.T and Adewale [2] has

built an AI system that employs multinomial naive Bayes and optimized linear support vector machines may be implemented to identify and prevent cyberbullying. The authors detail the steps for implementing the strategy and provide the results of their experiments to demonstrate its efficacy. Mahmud et al. [3] highlighted the usefulness of several models in identifying instances of cyberbullying was examined using the Twitter dataset. These models included LightGBM, XGBoost, Random Forest, Logistic Regression, AdaBoost, and classical models. The most successful strategy for recognizing instances of cyberbullying on social media was determined by assessing each machine learning model's properties of accuracy, precision, recall, and F-1 score. After analyzing the results of each statistic, they found that while LightGBM performed better than the others, the models were essentially interchangeable. With 84.0% accuracy, 85.0% recall, and 84.49% F-1 score, LightGBM not only outperformed the competition in accuracy, but also in precision and recall. Azeez N.A and Fadhil.E [4], used four separate datasets to evaluate both models in their study. We used seven different machine learning algorithms for the evaluation: NB, DT, KNN, LR, NN, QDA, and SVM. Also used were logistic regression, neural networks, and neural networks for NN. Ada Boosting, Gradient Boosting, Random Forest, and Max Voting were also used as ensemble learning models. This research aims to compare ensemble learning with classical classifiers for the categorization of online social media networks' instances of virtual harassment. We compared the results using twelve assessment criteria, which included: recall, specificity, accuracy, precision, and F1-measure. And The following measures were used to prove that our algorithms were correct: The user brought up a number of performance indicators often used to evaluate classification models, including Negative Predictive Value (NPV): Several statistical measures are used to assess reliability, including false positive rate (FPR), false negative rate (FNR), area under the curve (AUC), mathematical correlation coefficient (MCC), and Cohen's Kappa coefficient (KAPPA).

Ahmed M.T et al. [5] created a model using deep learning and machine learning to identify cases of cyberbullying in Bangla and Romanized Bangla writings. Recall, F1-Score, accuracy, precision, and ROC area were all included in the algorithms' comparison study. Three sets of social media data were produced: one for Bangla, one for Romanized Bangla, and one for a combination of the two. There were a combined total of 12,000 texts in Bangla and Romanized Bengal across the three datasets, including 5,000 texts in Bangla and 7,000 texts in Romanized Bangla. In order to carry out the comparison study, the preprocessed datasets were trained using deep learning and machine learning approaches, and their performance was assessed. With an astounding 84% accuracy, CNN outperformed all previous results for the Bangla Dataset. Bokolo B.G and Liu.Q [6], have used a dataset consisting of tweets on cyberbullying, the researchers tested and rated three different machine learning algorithms: SVM, Naive Bayes, and Bidirectional Long Short-Term Memory (Bi-LSTM). The importance of protecting social media platforms against cyberbullying cannot be overstated, considering the widespread use of these sites by people of all ages. With an accuracy of 98%, the Bi-LSTM model outperforms the other models according to the experimental data. The SVM model comes in second with a 97% accuracy rate, just ahead of the Naive Bayes model (85%). Results demonstrated that Bi-LSTM outperformed the two more conventional machine learning classifiers, proving that ML techniques are useful for cyberbullying detection. Obaidat.I et al. [7]

in their work, collected data from popular platforms to handle complaints of bullying, intimidation, abuse, and other forms of harassment and damage directed at students and youth in both Arabic and English. Prior to using machine learning approaches, they prepped their data for the discovery phase by removing unnecessary characters. In their mixed-methods study, the researchers used a variety of machine learning and natural language processing techniques, such as logistic regression, random forests, support vector machines, extreme gradient boosting algorithms, and Naive Bayes. The goal of the training process was to find the most accurate model.

In the research work carried out by Shakeel.N et al. [8], the issue of cyberbullying has been addressed in a variety of ways. Among the many social media platforms used by them was Twitter. They were familiar with logistic regression (LR), naïve Bayes (NB), support vector machine (SVM), and term frequency—inverse document frequency (TF-IDF), among other methods and processes. Examining how well three algorithms—Support Vector Machines (SVM), Logistic Regression (LR), and Naive Bayes (NB)—detect cyberbullying is the primary goal of this essay. In addition, the Support Vector Machine (SVM) was shown to be the most effective approach. In the proposed methodology of [9], a number of well-known algorithms have had their performance evaluated using measures such as recall, accuracy, precision, F1-score, and Extreme Gradient Boosting (XGBoost), Decision Tree, and Random Forest. By analyzing a Twitter dataset of hate speech, we find that the Random Forest algorithm is the most efficient, with a 97% accuracy rate. To evaluate the model's performance, several feature extraction techniques have been used, including bag-of-words and TF-IDF (term frequency-inverse document frequency). Combining Random Forest (RF) with TF-IDF seems to be the best method for identifying inappropriate language on social media, according to the data that was gathered.

S.Gnanavel et al. [10] proposed probabilistic model for text retrieval. It helps in eliminating the background noise so that the key content of the text can be focused for further cyberbullying detection. The proposed work of Johari.N.F.B and Jaafar.J [11] deals with the dataset, collected from Twitter by scraping tweets, uncovered six unique forms of cyberbullying. The following classifications were established according to frequently used Malay words linked to cyberbullying: non-abusive, racial, intellectual, and political. The 45,580 tweets that make up the cyberbullying dataset are not evenly distributed. Word2Vec, Bag of Words (BoW), and Term Frequency-Inverse Document Frequency (TF-IDF) are the three feature extraction methods used to construct the model. The methods of Logistic Regression (LR), Naïve Bayes (NB), Support Vector Machine (SVM), and Random Forest (RF) are mixed with these methodologies. The best model, according to the findings, is the logistic regression model with the TF-IDF feature extraction method coupled. To address the dataset's imbalance, the model was fine-tuned by adjusting its hyper parameters and using the Synthetic Minority Oversampling Technique (SMOTE). The work of V.Jain et al. [12] has predicted that, WhatsApp's machine learning system for cyberbullying detection has a number of serious flaws. To begin, logistic regression and support vector machine methods have problems in accurately identifying and classifying instances of cyberbullying. Since these algorithms rely on predetermined patterns and qualities, they may not capture the complex and ever-changing nature of cyberbullying actions. Because of the high incidence of inaccurate detection of cyberbullying

scenarios caused by false negatives, this might cause the system to produce a significant number of false positives, making it difficult to effectively identify such occurrences. In addition, sophisticated forms of cyberbullying are difficult for algorithms such as logistic regression and support vector machines to detect [13]. Because these algorithms mainly deal with numerical and categorical data, they may miss some of the verbal and contextual nuances that are often present in cyberbullying incidents. Victims' mental health may take a major hit if the system fails to detect more nuanced forms of cyberbullying, such as micro aggressions or passive-hostility.

In the research work of P.Deedeehya et al. [14], detection of cyberbullying is achieved by convolutional neural network (CNN). In CNN, multiple layers interprets the evolving strategies and behaviors of cyberbullying. Their proposed work states that the existing system struggles to keep up since it relies on supervised learning approaches. The system may face challenges in adapting and detecting changing cases of cyberbullying. Training supervised learning algorithms requires large labeled datasets, which may be time-consuming and costly to gather. This becomes even more problematic when considering the ubiquity and dynamic nature of cyberbullying. When it comes to cyberbullying, the existing system may not be able to pick up on incidents in languages other than English. Language and cultural quirks may have limited the applicability of logistic regression and support vector machine algorithms, which were built and trained on English textual data [15]. On a worldwide social media network like WhatsApp, which serves users from a variety of linguistic backgrounds, imposing this restriction might drastically reduce the system's ability to identify cases of cyberbullying. Using logistic regression and support vector machine approaches, the present machine learning strategy to detect WhatsApp cyberbullying has many drawbacks. Some of these issues include not being able to properly record and categorize incidents of cyberbullying, not being able to identify cyberbullying in languages other than English, and not being able to detect cyberbullying that is subtle or complex.

3 Proposed System

Making a machine learning system that can identify cases of cyberbullying on the popular messaging app WhatsApp is the goal of the proposed project. The main goal is to use logistic regression and Support Vector Machine (SVM) techniques to identify instances of cyberbullying and quickly step in to stop it before it does damage. In order to do this, we will gather a large dataset of WhatsApp chats and use preprocessing to extract important attributes. Tokenization, stemming, and stop word removal are some of the text preprocessing techniques that will be used to normalize the text data and reduce noise. Find out whether a certain text message shows symptoms of cyberbullying with the use of a binary classifier that is based on logistic regression. Cyberbullying and non-cyberbullying messages will be distinguished by training the system. To do this, the logistic regression model will be trained using a labeled dataset. System Architecture is shown in Fig. 1.

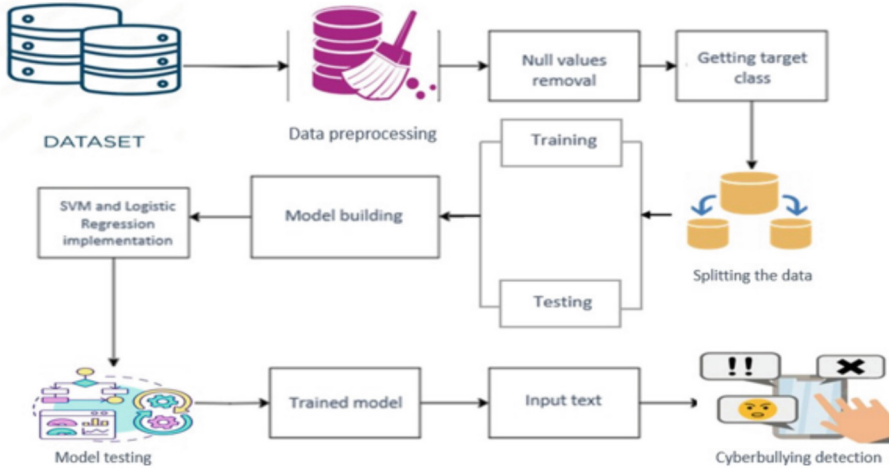


Fig. 1. System Architecture

In a similar vein, the Support Vector Machine (SVM) method will be employed in classifying the cyberbullying-related text messages into many kinds. Using the textual characteristics retrieved from the dataset, the SVM model will detect trends and define decision limits to differentiate between cyberbullying and non-cyberbullying occurrences. Some of the measures that will be used to assess the logistic regression and SVM models' performance include F1-score, recall, accuracy, and precision. We will compare the produced models to find out how well the algorithm categorizes instances of cyberbullying. Applying machine learning techniques developed for the WhatsApp social media network, the proposed initiative seeks to advance the area of cyberbullying detection. Platform management and social media moderators may benefit greatly from accurate data on cyberbullying incidents if they could respond quickly enough to stop the damage from happening. Another benefit of the suggested technique is its potential generalizability to other social media sites; this might lead to better tactics for combating cyberbullying in a variety of contexts. Data preparation is carried out after the dataset has been collected. At this point, the input dataset is prepared for model training by doing preprocessing. Methods like data purification, feature extraction, and standardization may be required for this. Among the many tasks involved in data preparation is handling missing data from the dataset. The dataset's target variables are divided into many categories. The model is trained using the Train Data, and its performance is assessed using the Test Data. These two sets of preprocessed data are created independently. Construction the machine learning model and feeding it instructions from the training data is called "model building." Support Vector Machines (SVMs) and Linear Regression are two separate classes of machine learning algorithms used in this context. It is usual practice to utilize Support Vector Machine (SVM) for classification tasks and Linear Regression for regression problems. It may be inferred from this that the two methods are being considered equally or compared when building the model. A trained model, prepared for validation and testing, is the end result of the model development stage. It

is the goal to enhance the accuracy after the initial training by using more sophisticated models, picking out key characteristics, or tweaking hyper parameters. Then, cyberbullying detection, the model's intended function, is carried out using the improved version. The user may utilize the technology to identify instances of cyberbullying that occur on various digital communication channels, such as social media. Starting with data preparation and ending with model deployment, the system architecture shows a common machine learning technique for recognizing cyberbullying behavior.

3.1 Data Preprocessing and Feature Extraction

This module gathers and preprocesses raw data from the social media network like WhatsApp in order to eliminate any redundant or unnecessary information. Preprocessing involves normalizing the text by stemming or lemmatizing it, eliminating stop words, and special characters. Following preprocessing, pertinent characteristics like sentiment scores, n-grams, and word frequency are taken out of the textual data. These qualities serve as the foundation for training machine learning models and capture significant aspects of cyberbullying texts.

3.2 Applying a Logistic Regression Approach for Model Development and Evaluation

Here, the feature set and preprocessed data are used to train the logistic regression model. Cyberbullying in WhatsApp chats may be detected using logistic regression, a well-known binary classification approach. To facilitate the training of logistic regression models, the dataset is split into two subsets: the testing set and the training set. After applying the logistic regression model to the training set, we evaluate the model's performance on the testing set using pertinent assessment measures such as F1-score, recall, accuracy, and precision. You may find the best combination of hyper parameters to maximize the model's performance using hyper parameter tuning methodologies like grid search and random search.

3.3 Training and Evaluating a Model Based on Support Vector Machine (SVM)

In order to identify instances of cyberbullying in WhatsApp discussions, this module utilizes the Support Vector Machine (SVM) algorithm. A robust machine learning technique, Support Vector Machines (SVM) can manage datasets with many dimensions and complicated interactions. As with the logistic regression module before it, the data is split into a training set and a testing set. Then, using radial, polynomial, or linear basis functions as kernels, the SVM model is trained on the training set. The trained SVM model is evaluated using a variety of metrics, and its performance may be fine-tuned using hyper parameter tuning techniques. The SVM method locates the best hyperplane to classify a dataset. In two dimensions, a line represents a hyperplane. In three-dimensional or higher-dimensional space, it is known as a hyperplane. With Support Vector Machines (SVMs), the goal in binary classification is to locate the hyperplane that maximizes the margin. A data point's margin is the greatest possible distance between its class-specific

neighbors. Support vectors are data points that are close to the hyperplane and significantly affect its direction and placement. Support vector machines (SVMs) provide margin to classifiers by using these vectors. A margin is the absolute difference in length between two lines drawn from the closest points in the same class. A straight line distance from the line to the nearest points or support vectors is used to determine this. Classifiers with a bigger margin provide less inaccurate generalizations. Data encountered in the actual world sometimes lacks linear separability. To make the input space more complicated, Support Vector Machines (SVMs) use a kernel method in such cases. This change makes it possible to use a hyperplane to correctly separate the data. Radial basis function (RBF), sigmoid, and polynomial kernels are some of the most common. The three main components of the suggested approach for identifying cyberbullying on WhatsApp are data preprocessing and feature extraction, training and assessment of logistic regression models, and training and evaluation of support vector machines. The methods used in these modules include Support Vector Machine and logistic regression. All three modules together provide a thorough way to identify and handle cyberbullying in real-time WhatsApp interactions. Precision is a performance metric that evaluates the accuracy of a model's future predictions. The term "accuracy" is used to indicate the proportion of correctly identified positive instances, or actual positive predictions, relative to the overall number of all occurrences, both positive and negative (including those that were incorrectly called positive). Recall, also known as sensitivity or the true positive rate, is a crucial metric to examine when evaluating computer vision models. The accuracy rate is the proportion of true cases found relative to the total number of relevant cases. The F1 score is a reasonable way to evaluate a computer vision model's accuracy as it takes Precision and Recall and multiplies them by one. When evaluating computer vision models, accuracy is a key performance indicator. The proportion of occurrences in a dataset that were appropriately identified as true positives or true negatives is one indicator of accuracy.

$$precision = \frac{TP}{TP + FP}$$

$$recall = \frac{TP}{TP + FN}$$

where TP stands for True Positive, FP represents False Positive, TN indicates True Negative and FN stands for False Negative. With the help of calculated values of precision and recall, F1 score can be computed as follows

$$F1score = \frac{2 * precision * recall}{precision + recall}$$

$$Accuracy = \frac{(TP + TN)}{TP + FN + TN + FP}$$

$$Specificity = \frac{TN}{TN + FP}$$

The above metrics are used for the performance evaluation.

4 Results and Discussion

WhatsApp employs a machine learning approach to identify instances of cyberbullying, utilizing logistic regression and Support Vector Machine (SVM) algorithms. Logistic regression is commonly employed when addressing binary classification problems, such as identifying occurrences of cyberbullying. Logistic regression quantifies the probability of classifying a communication as either cyberbullying or non-cyberbullying based on several features, achieved by fitting a logistic function to the data. Evaluation Metrics Score is shown in Table 1.

Table 1. Evaluation Metrics Score

| Algorithm | Accuracy | Precision | Recall |
|-------------------------|----------|-----------|--------|
| Support Vector Machines | 89.77 | 0.73 | 0.69 |
| Logistic Regression | 90.72 | 0.89 | 0.90 |

The above table presents performance metrics for two machine learning algorithms: Support Vector Machines (SVM) and Logistic Regression.

- Accuracy measures overall correctness in percentage.
- Precision (for Logistic Regression) reflects the proportion of true positive predictions among all positive predictions.
- Recall (for Logistic Regression) represents the proportion of true positive predictions among all actual positives.

In summary, both algorithms show high accuracy, with Logistic Regression having better precision and recall compared to SVM. In contrast, Support Vector Machines (SVMs) are an effective method for binary and multiple-category data classification. In order to maximize the margin between the two classes, the goal is to find the hyper-plane. Support vector machines (SVMs) enhance cyberbullying detection accuracy by

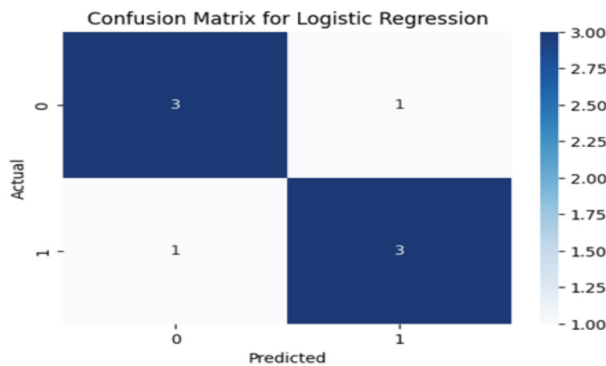


Fig. 2. Confusion matrix for Logistic Regression

handling high-dimensional feature spaces and non-linear relationships among features. This machine learning technique uses a variety of relevant data points, including content, sender, time, and emotion, extracted from WhatsApp conversations. Support vector machines and logistic regression models are trained using these attributes. Next, labelled datasets are used to train the models, which classify instances as either cyberbullying or non-cyberbullying. Before algorithms can effectively differentiate between the two sets, they need to learn to identify substantial patterns and correlations among the attributes.

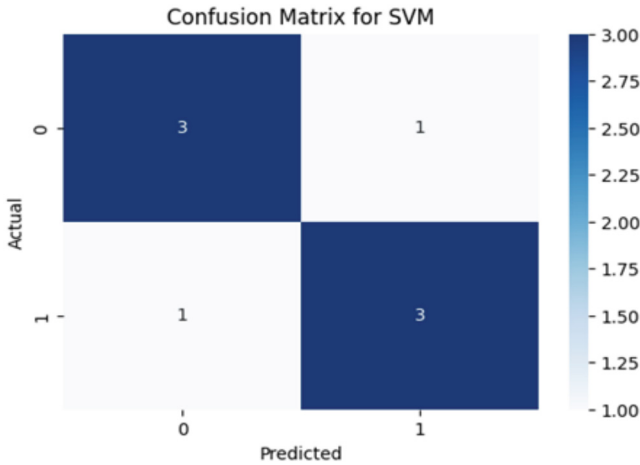


Fig. 3. Confusion matrix for SVM

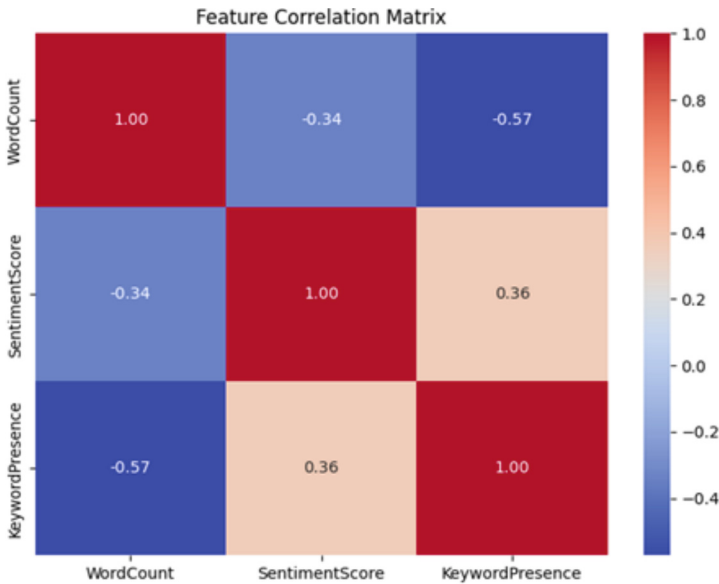


Fig. 4. Correlation matrix for features in dataset

Confusion matrix for Logistic Regression is shown in Fig. 2. Confusion matrix for SVM is shown in Fig. 3. Correlation matrix for features in dataset is shown in Fig. 4.

5 Conclusion

To summarize, an effective approach to identify cyberbullying on the social media platform WhatsApp is the utilization of machine learning techniques, specifically Logistic Regression (LR) and Support Vector Machine (SVM) algorithms. Both algorithms have exhibited efficient classification and detection abilities for identifying different cyberbullying instances. Support Vector Machine (SVM) enables robustness and the ability to handle non-linear correlations, whereas Logistic Regression (LR) leverages simplicity and interpretability. By integrating these models, the total efficacy of cyberbullying detection systems can be enhanced, enabling efficient real-time surveillance and response. By implementing further enhancements and modifications, this technique has the potential to effectively mitigate the adverse consequences of cyberbullying on the WhatsApp social media platform. When it comes to identifying instances of cyberbullying on WhatsApp, two machine learning methods that show promise are Support Vector Machine (SVM) and logistic regression. By doing remarkable analysis on text-based data, these systems may identify material that might be hazardous or dangerous.

Modern natural language processing (NLP) methods might be the subject of future studies that aim to improve these models' performance. Using generative pre-trained transformer (GPT) or transformer-based models (BERT) or recurrent neural networks (RNNs) as an example of a deep learning architecture is one option. Computers' ability to comprehend context, sarcasm, and subtle language is improved with the use of intricate NLP models, leading to more precise cyberbullying detection. Additionally, the model's performance may be greatly improved by feature engineering. Additional factors derived from language patterns, user behavior, or message metadata might possibly improve the detecting capabilities. Additionally, future study into identifying cyberbullying on WhatsApp across various media forms should explore the use of multimodal data, which includes text, images, and videos, for a more thorough analysis. Researching real-time or dynamic models that can adjust to changing user behaviors and language patterns can also be useful. It is crucial to use continuing learning techniques to continuously update the model with fresh data, making sure it remains relevant and effective, in order to fight new types of cyberbullying. In the end, the best way to understand cyberbullying on WhatsApp and find solutions that work is for psychologists, social scientists, and machine learning specialists to work together. People who use the internet, especially on social media, have been subjected to more racist and otherwise unpleasant information, as well as cyberbullying, in the last several years. Harassment in the form of insulting, unpleasant, or abusive language is one manifestation of this sort of material. Suicides and other bad social policy outcomes might result from the extreme physiological and psychological stress this would cause among adolescents and younger children. Consequently, it is critical to quickly, accurately, and intelligently detect and filter out disturbing material that is posted online. This study has built a hierarchical framework of machine learning algorithms according to the increasing computational complexity to effectively detect the abusive and aggressive content.

References

1. Gautam, A.K., Bansal, A.: Performance analysis of supervised machine learning techniques for cyberstalking detection in social media. *J. Theor. Appl. Inf. Technol.* **100**(2), 449–461 (2022)
2. Ige, T., Adewale, S.: AI powered anti-cyber bullying system using machine learning algorithm of multinomial naïve Bayes and optimized linear support vector machine. *arXiv preprint arXiv:2207.11897* (2022)
3. Mahmud, M.I., Mamun, M., Abdelgawad, A.: A deep analysis of textual features based cyberbullying detection using machine learning. In: 2022 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT), pp. 166–170. IEEE, December 2022
4. Azeez, N.A., Fadhal, E.: Classification of virtual harassment on social networks using ensemble learning techniques. *Appl. Sci.* **13**(7), 4570 (2023)
5. Ahmed, M.T., Antar, A.H., Rahman, M., Islam, A.Z.M.T., Das, D., Rashed, M.G.: Social media cyberbullying detection on political violence from Bangla texts using machine learning algorithm. *J. Intell. Learn. Syst. Appl. Intell. Learn. Syst. Appl.* **15**(4), 108–122 (2023)
6. Bokolo, B.G., Liu, Q.: Cyberbullying detection on social media using machine learning. In: IEEE INFOCOM 2023-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 1–6. IEEE, May 2023
7. Obaidat, I., Al-zou'bi, A., Mughaid, A., Abualigah, L.: Investigating the cyberbullying risk in digital media: protecting victims in school teenagers. *Soc. Netw. Anal. Min.* **13**(1), 139 (2023)
8. Shakeel, N., Dwivedi, R.K.: Performance analysis of supervised machine learning algorithms for detection of cyberbullying in Twitter. In: Raj, J.S., Shi, Y., Pelusi, D., Balas, V.E. (eds.) *Intelligent Sustainable Systems. Lecture Notes in Networks and Systems*, vol. 458. Springer, Singapore (2022). https://doi.org/10.1007/978-981-19-2894-9_29
9. Preetham, J., Anitha, J.: Offensive language detection in social media using ensemble techniques. In: 2023 International Conference on Circuit Power and Computing Technologies (ICCPCT), pp. 805–808. IEEE, August 2023
10. Gnanavel, S.: Rapid text retrieval and analysis supporting latent dirichlet allocation based on probabilistic models. *Mob. Inform. Syst.* **22**, August 2022
11. Johari, N.F.B., Jaafar, J.: A malay language cyberbullying detection model on twitter using supervised machine learning. In: 2022 International Visualization, Informatics and Technology Conference (IVIT), pp. 325–332. IEEE, November 2022
12. Jain, V., Saxena, A.K., Senthil, A., Jain, A., Jain, A.: Cyber-bullying detection in social media platform using machine learning. In: 2021 10th International Conference on System Modeling and Advancement in Research Trends (SMART), MORADABAD, India, pp. 401–405 (2021). <https://doi.org/10.1109/SMART52563.2021.9676194>
13. Khang Hsien, Y., Arabee Abdul Salam, Z., Kasinathan, V.: Cyber bullying detection using natural language processing (NLP) and text analytics. In: 2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), Ballari, India, pp. 1–4 (2022). <https://doi.org/10.1109/ICDCECE53908.2022.9792931>
14. Dedeepya, P., Karishma, D., Manuri, S.G., Raghuvaran, T., Shariff, V., Sindhura, S.: Enhancing cyber bullying detection using convolutional neural network. In: 2023 4th International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, pp. 1260–1267 (2023). <https://doi.org/10.1109/ICOSEC58147.2023.10276007>
15. Singla, S., Lal, R., Sharma, K., Solanki, A., Kumar, J.: Machine learning techniques to detect cyber-bullying. In: 2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, pp. 639–643 (2023). <https://doi.org/10.1109/ICIRCA57980.2023.10220908>



Securing Cyber-Physical Systems: A Strategic Review

B. Muthu Nisha and J. Selvakumar^(✉)

Department of Electronics and Communication Engineering, SRMIST, Kattankulathur 6032031, India

{mb1850,selvakuj}@srmist.edu.in

Abstract. The current industry focus is on the development of integrated security systems for the upcoming generation of Cyber-Physical Systems (CPS). To effectively tackle this challenge, researchers should shift their attention towards understanding attack strategies. This study delves into recent literature, identifying research gaps for future exploration. Within the context of the Internet of Things (IoT), our investigation reveals the persistent threat of side-channel attacks on CPS. Linking these attacks to contemporary technology, our research further examines potential risks to CPS. We specifically explore the substantial impact of Artificial Intelligence algorithms on side-channel analysis. Additionally, we discuss hardware security measures aimed at safeguarding CPS from potential side-channel attacks.

Keywords: Internet of Things · Artificial Intelligence · Cyber-physical systems · Side-channel attack · Side-channel Analysis · Hardware security

1 Introduction

The architecture of the Internet of Things (IoT) incorporates pivotal Cyber-Physical Systems (CPS). This CPS primarily tasked with facilitating message transmission [1]. IoT plays a multifaceted role in CPS, encompassing data collection, connectivity, processing, feedback, and scalability. By leveraging IoT technologies, CPS can achieve enhanced functionality, efficiency, and adaptability, ultimately leading to improved performance and outcomes in diverse applications. These IoT Cyber-Physical Systems employ channels for data transport to servers, exposing a potential high-risk scenario susceptible to side-channel attacks. Cryptanalysis becomes a feasible threat within this data transmission channel. Cyber-Physical Systems are susceptible to a spectrum of attacks, categorized as physical, logical, and network threats [2]. Implementing robust hardware security measures proves instrumental in mitigating these diverse assaults.

Figure 1 illustrates the comprehensive investigative methodology employed in this survey.

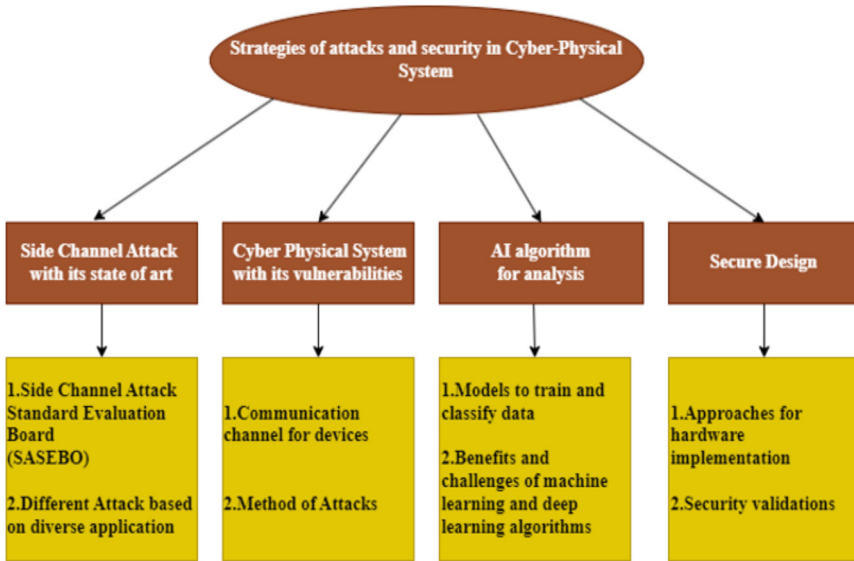


Fig. 1. An In-Depth Study Approach

1.1 Contribution of This Paper

- This study highlights key ideas behind attacks on IoT Cyber-Physical Systems, emphasizing the importance of hardware security design.
- It explores the pros and cons of deep learning and machine learning models for rank estimation.
- The paper proposes a Secure Design Approach on hardware to prevent Side Channel Attacks.

This research survey is carried out in the following order. Section 2 reviews the mode of side-channel attack and side-channel analysis through various AI (Artificial Intelligence) algorithms, Sect. 3 labels secure design, and Sect. 4 recommends future directions, Sect. 5 concludes this paper.

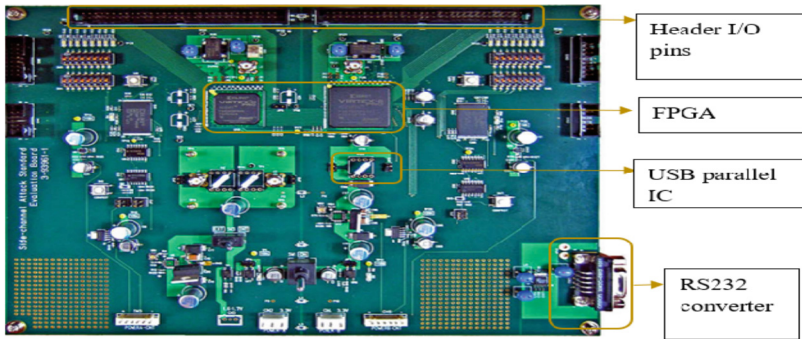
2 Exploring Side Channel Attack Modes

2.1 Side Channel Attack Standard Evaluation Board

The SASEBO(Side Channel Attack Standard Evaluation Board) board which illustrated in Fig. 2 provides researchers with a versatile and standardized framework to conduct side-channel analysis and other pertinent investigations [3]. From a practical standpoint, forthcoming inquiries in this field would benefit from its scalability, documentation, accessibility, and community support. The SASEBO board ensures scalability and future-proofing for research endeavors through its capability to accommodate a wide range of FPGA models and versions [4]. The SASEBO board's distinctive characteristics listed in Table 1.

Table 1. SASEBO Board Feature Matrix

| SASEBO Versions | Feature of FPGA Devices/Models |
|-----------------|--|
| SASEBO | Xilinx Virtex-II Pro devices/ xc2vp7 and xc2vp30 models |
| SASEBO-G | Xilinx Virtex-II Pro FPGA devices |
| SASEBO-GII | Xilinx Virtex-5 (XC5VLX30 or XC5VLX50) and Spartan-3A (XC3S400A) models |
| SASEBO-GIII | 28nm FPGA |
| SASEBO-B | ALTERA FPGA version, equipped with Stratix II EP2S15 and EP2S30 devices |
| SASEBO-R | cryptographic LSI (Large Scale Integration) chip built using TSMC 28-nm CMOS library |
| SASEBO-W | Xilinx FPGA device Spartan-6 (XC6S LX150) and an IC card socket |

**Fig. 2.** Basic Overview of the SASEBO Board

A side-channel attack refers to a non-invasive method of attack, allowing it to be executed without disrupting or unpackaging the IoT cyber-physical system. Table 2 presents various attack modes documented in current literature. This approach will be applied across multiple generations of SASEBO boards.

2.2 Algorithmic Exploration and Evaluation of Side-Channel Analysis

AI learning models can enhance the efficiency, accuracy, and success rate of side-channel analysis techniques. Additionally, they can assist in extracting valuable data from side-channel leakages. In order to ensure the reliability and effectiveness of these models in the context of side-channel analysis, it is imperative to meticulously construct, train, and evaluate them.

Table 3 provides a comprehensive overview of the advantages and difficulties associated with utilizing AI learning models for side channel investigation. The learning model can identify and evaluate trends, variations, or similarities in the behavior of the algorithm across several inputs or executions by including the Hamming weight and

Table 2. Assorted Attack Modalities

| Mode of Attack | Report of attack |
|---|--|
| Frequency-based attack [5] | This can be performed with Personal Digital Assistance like mobile devices, routers, etc |
| Error message Attack [6] | This attack was established by the addition of padding bits after encryption of the original message, which may be considered as an acknowledgment by a permitted user. |
| Pressure attack[7] | A small sensor attached to a device generates a vibration signal when a permitted user applies his password on a device, this sensor informs a hacker about the password. |
| A mixture of side-channel attacks[8] | The attack with power analysis, time analysis, and photonic with electromagnetic analysis. |
| Timing Attack [9] | This is done by gathering samples of the input and output of the device and interrelated with side-channel leakage information. |
| Power analysis attack [10] | This attack is performed by analyzing power traces. <ul style="list-style-type: none"> ✓ Simple power analysis attack: Direct analyses to obtain functionality of algorithm from the crypto device. ✓ Differential power analysis attack: Device functions can be achieved by taking more power trace analyses through vertical and horizontal data classification algorithms. |
| Electromagnetic Attack [11] | Placing a coil closer to the chip under attack induces electromagnetic fields on the coil will be the attacker's side-channel information source. |

(continued)

Table 2. (continued)

| | |
|----------------------------------|--|
| Scan based Attack [12] | The attacker makes use of the scan chain infrastructure to alter or view the IC's internal states. |
| Cache based Attack [13] | There is a cache hit and cache miss in Central Processing Unit (CPU) while cache miss there is some delay of data lading from main memory to cache memory that can be observed by the attacker to perform an attack. |
| Acoustic Attack[14] | Evasion sound produced by the machine can be observed for the attack. |
| Visible light Attack [15] | This attack can be performed in the light-built device, luminosity reflects ion observed and tried to get bathe original signal. |
| Photonic Attack[16] | If transistors are in a saturation region, they will start discharging large photons, these attacks are performed on the backside of the Integrated Circuit (IC), shorter than the bandgap energy the silicon substrate has a high amount of captivation for wavelengths. |
| Fault Attacks [17] | <ul style="list-style-type: none"> ✓ Permanent fault attack: This attack is performed by detaching data wires. ✓ Transient fault attack: while device performance at definite places like power supply, signal generator attack can be made location accessing fault. This fault can be familiarized in a fixed location like memory and registers faults in the timing process. Faults can be implanted during the specific timing of digital circuits. |

Hamming distance as features. This might aid in recognizing and categorizing algorithmic behaviors, finding anomalies, or differentiating between various processes or data values. Figure 3 Suggests that the model provides insights into the workings of cryptographic algorithms.

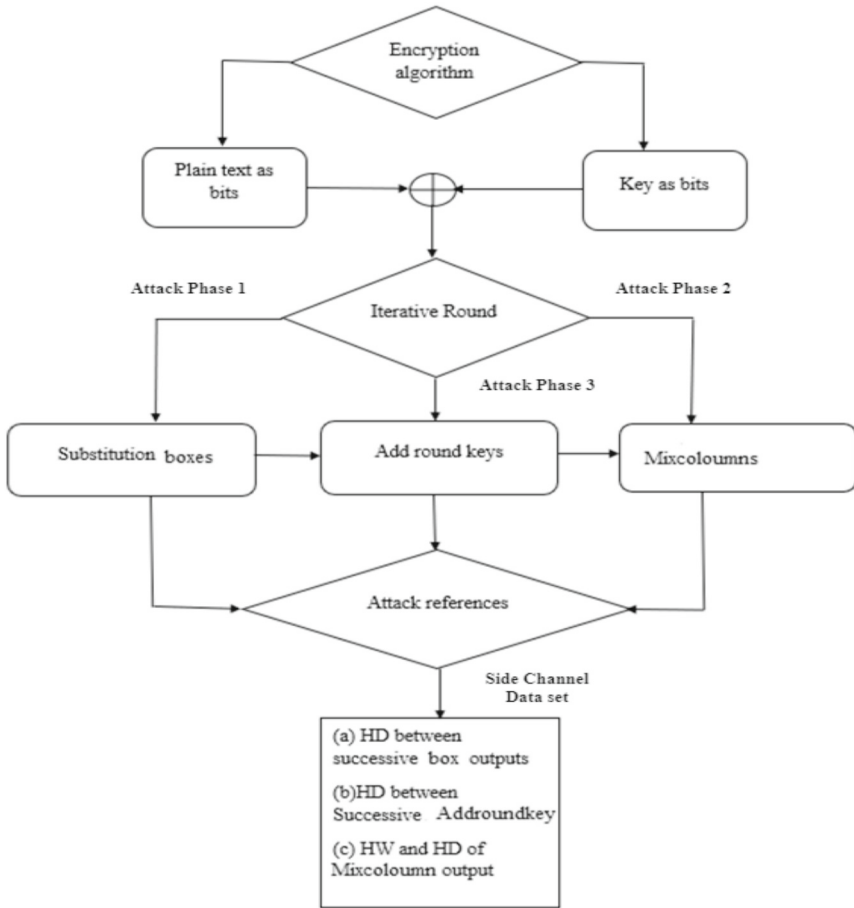


Fig. 3. Side-channel attack reference point on crypto algorithm flow

3 Safety Architecture Methods

Early research proposed that the resolution for cryptographic functions lay in algorithmic and mathematical architectures. However, contemporary security analytics methods for safeguarding cyber-physical systems are built upon adaptive clustering techniques, data mining, and physically unclonable functions.

In Fig. 4, hardware security is approached through four unique strategies and Table 4 shows each tailored to specific objectives and implementations by,

- Choose a low-complexity encryption algorithm for enhanced security.
- Incorporate physically unclonable functions to instill confidence in hardware.
- Bolster defenses against machine learning attacks through strategic obfuscation.
- Establish the hardware root of trust by rigorously validating design logic.

Table 3. Advantages and difficulties of artificial intelligence learning models.

| AI Algorithms | Learning model | Benefits | Challenges |
|---|-------------------------------|---|---|
| Machine Learning [18,19,20,22,27,28,29] | Support Vector Machines | <ul style="list-style-type: none"> ✓ Robustness to Noise ✓ Support for Non-linear classification ✓ Ability to handle high-dimensional data | <ul style="list-style-type: none"> ✓ Lack interpretability ✓ Scalability in dealing with large traces |
| | Random Forest | <ul style="list-style-type: none"> ✓ Robustness to overfitting | <ul style="list-style-type: none"> ✓ Crucial parameter tuning ✓ Curse of dimensionality |
| | K-Nearest Neighbors | <ul style="list-style-type: none"> ✓ Adaptability to new data ✓ Non-Parametric approach | <ul style="list-style-type: none"> ✓ Choice of the number of nearest neighbors (k) is critical |
| | Naïve Bayes | <ul style="list-style-type: none"> ✓ Provide interpretable results ✓ Simplicity and speed | <ul style="list-style-type: none"> ✓ Sensitivity to feature correlations |
| | Convolutional Neural Networks | <ul style="list-style-type: none"> ✓ Automatic feature extraction ✓ Spatial and temporal relationship | <ul style="list-style-type: none"> ✓ Prone to overfitting |
| | Recurrent Neural Networks | <ul style="list-style-type: none"> ✓ Sequential modeling ✓ Memory retention | <ul style="list-style-type: none"> ✓ Computational complexity |
| | Autoencoders | <ul style="list-style-type: none"> ✓ Anomaly detection | <ul style="list-style-type: none"> ✓ Determining reconstruction threshold |

(continued)