

Lecture Notes in Networks and Systems 23

G. Ranganathan
George A. Papakostas
Yong Shi *Editors*

Inventive Communication and Computational Technologies


Proceedings of ICICCT 2024

 Springer

Lecture Notes in Networks and Systems

Volume 23

Series Editor

Janusz Kacprzyk , Systems Research Institute, Polish Academy of Sciences, Warsaw, Poland

Advisory Editors

Fernando Gomide, Department of Computer Engineering and Automation—DCA, School of Electrical and Computer Engineering—FEEC, University of Campinas—UNICAMP, São Paulo, Brazil

Okyay Kaynak, Department of Electrical and Electronic Engineering, Bogazici University, Istanbul, Türkiye

Derong Liu, Department of Electrical and Computer Engineering, University of Illinois at Chicago, Chicago, USA

Institute of Automation, Chinese Academy of Sciences, Beijing, China

Witold Pedrycz, Department of Electrical and Computer Engineering, University of Alberta, Alberta, Canada

Systems Research Institute, Polish Academy of Sciences, Warsaw, Poland

Marios M. Polycarpou, Department of Electrical and Computer Engineering, KIOS Research Center for Intelligent Systems and Networks, University of Cyprus, Nicosia, Cyprus

Imre J. Rudas, Óbuda University, Budapest, Hungary

Jun Wang, Department of Computer Science, City University of Hong Kong, Kowloon, Hong Kong

The series “Lecture Notes in Networks and Systems” publishes the latest developments in Networks and Systems—quickly, informally and with high quality. Original research reported in proceedings and post-proceedings represents the core of LNNS.

Volumes published in LNNS embrace all aspects and subfields of, as well as new challenges in, Networks and Systems.

The series contains proceedings and edited volumes in systems and networks, spanning the areas of Cyber-Physical Systems, Autonomous Systems, Sensor Networks, Control Systems, Energy Systems, Automotive Systems, Biological Systems, Vehicular Networking and Connected Vehicles, Aerospace Systems, Automation, Manufacturing, Smart Grids, Nonlinear Systems, Power Systems, Robotics, Social Systems, Economic Systems and other. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution and exposure which enable both a wide and rapid dissemination of research output.

The series covers the theory, applications, and perspectives on the state of the art and future developments relevant to systems and networks, decision making, control, complex processes and related areas, as embedded in the fields of interdisciplinary and applied sciences, engineering, computer science, physics, economics, social, and life sciences, as well as the paradigms and methodologies behind them.

Indexed by SCOPUS, EI Compendex, INSPEC, WTI Frankfurt eG, zbMATH, SCImago.

All books published in the series are submitted for consideration in Web of Science.

For proposals from Asia please contact Aninda Bose (aninda.bose@springer.com).

G. Ranganathan · George A. Papakostas · Yong Shi
Editors

Inventive Communication and Computational Technologies

Proceedings of ICICCT 2024

 Springer

Editors

G. Ranganathan
Sree Sakthi Engineering College
Coimbatore, Tamil Nadu, India

Yong Shi
Department of Computer Science
Kennesaw State University
Kennesaw, GA, USA

George A. Papakostas
Department of Computer Science
(HUMAIN-Lab)
International Hellenic University
St. Loukas, Greece

ISSN 2367-3370

ISSN 2367-3389 (electronic)

Lecture Notes in Networks and Systems

ISBN 978-981-97-7709-9

ISBN 978-981-97-7710-5 (eBook)

<https://doi.org/10.1007/978-981-97-7710-5>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 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 Singapore Pte Ltd. The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

If disposing of this product, please recycle the paper.

With a great deal of dedication, 8th ICICCT 2024 is dedicated to all the authors, great scientists, academicians, young researchers, conference delegates, and students, who have research expertise on ICT technologies from all over the world. Nevertheless, this proceedings is dedicated to cover a wide spectrum of themes related to intelligent computing and communication innovations and developments.

Preface

The 2024 International Conference on Inventive Communication and Computational Technologies (ICICCT 2024) took place in Coimbatore, India, from June 14–15, 2024. ICICCT 2024 aimed to explore recent advancements and emerging trends in communication and computational technologies, fostering knowledge sharing and networking among researchers and industry experts.

The conference encompassed a wide array of topics including computing networks, security, blockchain, image processing, computer vision, recommendation systems, fault diagnosis, deep learning, and neural networks. From a total of 342 submissions received from universities and industries worldwide, 75 papers were selected for presentation based on their quality and relevance following rigorous peer review by 2–4 expert referees.

We extend our sincere appreciation to all authors for their valuable contributions to this volume. Our gratitude also goes to the referees for their insightful comments that helped enhance the quality of the selected papers. Special thanks are due to the organizing committee for their diligent efforts in ensuring the success of ICICCT 2024. Lastly, we acknowledge Springer publications for their role in producing this compilation.

Coimbatore, India

Dr. G. Ranganathan
Conference Chair
ICICCT 2024

Contents

| | |
|---|----|
| Enhancing Attack Detection on IoT Devices Using Hybrid Deep Learning Model | 1 |
| Uday Kiran Rachamsetty, Reddymalla Gyanendhar Reddy, and S. Saravanan | |
| Analysis of Routing Protocols in VANETs with Different Pause Times | 17 |
| Satveer Kour, Manjit Singh, Himali Sarangal, Varinder Kaur Attri, and Butta Singh | |
| Performance Insights of Attention-Free Language Models in Sentiment Analysis: A Case Study for E-Commerce Platforms in Vietnam | 29 |
| Nguyen Quoc Viet, Nguyen Nhat Quang, Nguyen King, and Dang Ngoc Hoang Thanh | |
| An AutoML Approach Integrated with Live Weather Data in Rain Forecasting System (RFS) | 43 |
| Syed Mazahir Mehdi Zaidi, Sheenu Rizvi, Deepak Arora, and Shivam Tiwari | |
| Decentralized Identity Management Using Self-Sovereign Identity Approach Through Blockchain | 53 |
| Khan Mohammad Anas, Sheenu Rizvi, Deepak Arora, and Shivam Tiwari | |
| Stock Price Prediction Model Using Enhanced LSTM and ARIMA | 65 |
| S. Jegadeesan, S. Kamalesh, P. Shalini, R. K. Hayvita, and A. G. Nishath | |
| Prefetching Mechanism for Distributed Cache Architecture: Trends and Challenges | 81 |
| Jayashree Mallidu and Saroja V. Siddamal | |

A Concise Review of Crop Disease Identification: Integrating Conventional and Deep Learning Feature Extraction for Effective Diagnosis and Mitigation Strategies 93
 Saritha Suvarna and Demian Antony D’Mello

Fortifying Health-Care Data Security in Cloud Environments 107
 Kakumanu Yasaswini, Madhava Reddy Kuncha,
 Mukesh Prakash Pappala, Matta Jithendra Sai Ramesh,
 and K. V. V. S. Satyanarayana

Review on the Enhancement of 5G Communications Using LEO Satellites 119
 Neil Singh, Kajal Kothari, Shiu Kumar, and Mansour Assaf

Design and Implementation of a Python-Based GUI Tool for Eye-Hand Coordination Analysis 131
 Milind Shah, Jainam Panchal, Kinjal Gandhi, and Riddhi Desai

Detection of Strabismus Using Convolutional Neural Network-Based Classification Models 147
 S. Subbulakshmi, Aditya Mani, and Divyam Gupta

Video Anomaly Detection Using Liquid Neural Networks 159
 A. V. Kanishkar, B. Nithesh, R. Nithish Kumar, S Rishi Karthigayan,
 V. Sowmya, and K. Deepak

A Blockchain Solution to Counterfeiting in the Semiconductor Supply Chain 173
 Anagha Rao, Netra Jagadish, Shristi Nadakatti, R. Thanushree,
 and Shruti Jadon

Performance Analysis of Various Encryption Algorithms for Securing Modules of Educational Chatbot 185
 Milind Shah, Avani Vasant, Priyanka Patel, Mittal Joshi,
 Mayur Chauhan, and Roopal Rajput

Implementation of a Temperature Monitoring System Utilizing Cortex-M3 with I2C-Based Sensor Integration 209
 Jayashree Mallidu, Jyoti Hulageri, Rakshita Jadhav,
 Mohammed Najeeb Mulla, and Shashank Bewoor

Unifying Perspectives: CNN-LSTM Integration for Anxiety and Depression Prediction Through Textual Analysis 219
 Sharon Susan Jacob

An Architectural Methodology for Developing Domain Ontology for Efficient Knowledge Management for AI Systems 233
 Zameer Gulzar, Fatima Amer Jid Almahri, A. Ramesh Babu,
 and P. Padmavathy

A Novel Hybrid Integration of BERT and Conventional Machine Learning Techniques for Robust Airline Twitter Sentiment Analysis 247
 M. R. Raja Ramesh, D. Venkata Ravi Kumar, Devakivada Ganesh, and A. Lakshmanarao

An Automated System with Deep Learning Technique for Posting Water-Related Issues 257
 Ede. Prashanth, Sodagudi Suhasini, Batchu Soma Siva Sai Krishna, and Thunuguntla Bhanu Sri Sai Someshu

Reliable Smart Wrist Pulse Oximeter for Hypoxemia and COVID-19 Patients 273
 Raghu Ramamoorthy, J. A. Smitha, and Anitha Velu

Optimizing Lettuce Crop Growth Modeling with XGBoost-SVM and Gaussian Process Regression Fusion 291
 C. Rukumani Khandhan, E. Gothai, P. Kanagaraju, S. Rajkumar, D. Seenivasan, and R. Anusurya

Recommendation of Personalized Learning Path in Smart E-learning Platform Using Reinforcement Learning Algorithms 309
 S. Deepa, M. S. Arunkumar, T. Kanimozhi, Balamurugan Eswaran, Vivek Duraivelu, and M. Sweatha

Detection of Printed Circuit Board (PCB) Defects Using Deep Learning Approach 319
 M. Arumugam, G. Arun, R. Mekala, and K. Anusuya

Gearbox Fault Diagnosis: A Comparative Study of Machine Learning and Deep Learning Approaches 335
 Shubhangi Suryawanshi, Sonali Gavali, Vaibhav Darwai, Sahil Patil, Atharv Wankhede, and Akash Borse

AI-Powered Trauma Chat Assistance: Identifying Trauma Symptoms from Voice and Text Communications 351
 S. Jacks Siva Sabesh, A. Jenefa, V. Edward Naveen, P. Santhiya, R. Sangeetha, and A. Lincy

Mental Chatbot Application Using Retrieval Augmented Generation 363
 Xuan Ngoc-Thanh Nguyen, Sang Ngoc Vo, and Hoang-Anh Pham

Automatic Radiology Report Generation: Approaches and Insights 377
 Nilam Sureshrao Khairnar and Shirish S. Sane

Enhancing Click-Through Rate Prediction: A Composite Approach Integrating DNN with DCN and FM-NN 391
 T. E. Ramya, P. Balasubramanie, P. Shanmughapriya, P. Ananthi, and G. Sakthiganesan

A Patch Antenna Design of S-Band for WLAN Applications 405
Md. Sohel Rana, Arpon Sarkar, Md. Mahmudur Rahman, Pranto Saha, Sohanur Rahman, Paris Chakroborty, and Sheikh Md. Rabiul Islam

Machine Learning of Social Media Data on a Spatio-Temporal Basis ... 419
Büşra Yeşilbaş, İ. Burak Parlak, and Tankut Acarman

Formation of Network Attack Detection System Architecture 431
Barno Norbekova, Aziza Komilova, Gayrat Arakulov, and Madina Adilova

Investigating Feature Extraction and Classification Algorithms for Effective Lung Disease Detection Using Chest X-Ray Images 441
E. Elakiya, Tejus Paturu, Keluth Chaithanya Naik, and V. Sai Tarun

Decentralized Crowdfunding Application Using Blockchain Technologies 457
Nagu Vadlana, N. Thirupathi Rao, and Debnath Bhattacharyya

Comparative Analysis of Multiple Deterministic Path Traversal Schemes for Localization in 3D-UWSN 469
Shreekrishna Mandloi, Nishi Yadav, and Pabitra Mohan Khilar

Facilitating Swift Reunions: A Comprehensive Web Application for Missing Children Tracking Using Face Recognition 483
Monali Chaudhari, Manpreat Kaur, Prasad Kokate, Tejas Lagwankar, and Rakshak Tapaswi

Artificial Intelligence Revolution in the Health Sector of the Moroccan Administration: Perspectives and Impacts for Systemic Transformation, Innovative Care, and Improved Public Management 493
Abdelhamid Ammar, Marouane Mkik, Hanan Amahmoud, Aziz Hantem, Ferroud Abderahim, and Ali Hebaz

Neural Prognostication of Thyroid Carcinoma Recurrence an Interdisciplinary Inquiry into Predictive Modelling and Computational Oncology 503
Ravva Amara Lakshmi Sireesha, Kandula Geetha Nandini, Srimathkandala Ch V. S. Vyshnavi, Pasam Bhanu, and Mohammed Gouse Shaik

Enhancing Cloud Data Sharing Security and Efficiency with Attribute-Based Encryption and Blockchain Integration 517
A. K. Velmurgan, S. S. Aravinth, S. Vivek, P. V. S. T. Vineela, G. Aditya, and B. Praveen

Domain Name Server Filtering Service Using Threat Intelligence and Machine Learning Techniques 529
Issac Gladin, Vinodh Edwards, and Sebastian Terence

Analyzing AprioriTID, Apriori Hybrid, and FP Growth for Association Rules in Movie Recommender Systems 541
 Garapati Gaman Sai Chowdary, Eluri Charan Raju, Pala Joshitha, Sunkara Anusree, and Mohammed Gouse Shaik

Comparative Analysis of ML Models for Electricity Price Forecasting 551
 Malti Bansal, Aditya Raj, and Aman Raj

Enhancing UNet Architectures for Remote Sensing Image Segmentation with Sinkhorn Regularization in Self-attention Mechanism 579
 Abdelaadim Khriiss, Aissa Kerkour Elmiad, and Mohammed Badaoui

Vehicle Movement Tracking and Control Using Image Processing 591
 R. Krishna Chaitanya, G. N. V. G. Sirisha, P. Ravi Kiran Varma, and Janakiram Naidu Alla

Recognition and Transformation of Style Features in Modern Architectural Images 603
 Linna Gao

YOLOv8 Image Processing for Evaluation of Stability Algorithms Based on Neural Networks: A Sports Use Case 613
 Md. Habibur Rahman, A. S. M. Mohiul Islam, Abdullah Ibnah Hasan, Mahtab Uddin, Ashek Ahmed, Asif Ahammad Miazee, and Yamin Hossain

The Effect of Changing Image Contrast on Object Recognition by a Convolutional Neural Network 623
 Dmitrii Tumakov, Dina Tuliabaeva, and Leonid Elshin

Development of Reddit API-Based Data Parsing Web System 635
 Oleksandr Holoveichuk, Oleg Pursky, Tetyana Filimonova, Tetyana Tomashevskya, Tatiana Dubovyk, and Iryna Buchatska

Deploying AI for Health Monitoring of Diadema Sea Urchins: Toward Sustainable Marine Ecosystems 651
 Mohammad Wahsha and Heider Wahsheh

An Evaluation of Testcase Recommendation Systems Through Feedback Model 661
 Minh Nguyen-Doan-Nhat, Khoa Vu-Dang, Tien Vu-Van, Huy Tran, Thanh-Van Le, Hoang-Anh Pham, and Nguyen Huynh-Tuong

NecessiPick: Data Extraction and AI Data Refinement in Food Retail Comparison 673
 Jennefer Brazil Lee, Maria Christine Cerrado Handog, Nicole Lanuza Baltazar, and Bryan Dadiz

Improved YOLOv4 for Enhanced Public Safety Management amid Civil Unrest 693
Xiaopeng Liu

Applicability Study on the ITU-R P.1546 for the Five V/UHF Radio Frequencies 703
Jian Wang, Zhongle Wu, Yulong Hao, Cheng Yang, Han Han, and Qingzhi Hao

Production Analysis for Corrugated Box Manufacturing: Simulation Study in Delhi-NCR 713
Umang Soni, Sumit Sakhuja, and Ashu Soni

Comparative Analysis of Sentiment Analysis Models on Twitter Data Using Machine Learning 729
Sai Kishore Chatla, Sarath Chandra Reddy Geeda, Koushik Pavani, Rajiv Ratna Kokkiligadda, and Mohammed Gouse Shaik

Automated Inventory Movement in Retail Using Augmented Reality and RFID 739
Sandeep Shekhawat

The Intersection of Big Data Analytics and Digital Humanities: A Systematic Review of Definitions, Applications, and Challenges 749
Alfonso Renato Vargas-Murillo, Abel Fernando Sotelo-Calderon, Juan Luis Gómez Zegarra, and Luis Roberto Zegarra-Ponce

The Role of Artificial Intelligence and Pattern Recognition in the Authentication and Analysis of Historical Documents: A Literature Review 759
Alfonso Renato Vargas-Murillo, Abel Fernando Sotelo-Calderon, Juan Luis Gómez-Zegarra, and Luis Roberto Zegarra-Ponce

Modern Farming Through Vermicompost Harvester: Redefining Farming Efficiency 769
Reymond A. Paculanang, Ernie L. Aguirre, and Paul Gene L. Empiales

MRI Image Segmentation-Based Sensitive Psychological Monitoring Signal Analysis 779
Shikang Zhang and Yanyan Zhu

Vehicle Path Planning Based on Genetic Algorithm in Intelligent Transportation System 791
Jiaofeng Wu

Fuzzy Logic Algorithm for Index Optimization in Database Query 803
Jinsong Wang

Emotion Modeling and User Experience Enhancement of Digital Media System in VR Environment 815
Yang Yuan and Juan Xu

Efficient Music Pitch Extraction Algorithm Based on Optimized Wavelet Transform 827
Mengyi Xiang

Enhancing Statistical-Based Remote Sensing Image Classification Algorithms: An Optimization Study 839
Tianyi Yu and Luyang Liu

Exploration of Machine Learning-Enabled Prediction and Control Algorithms for Railway Traffic Management 851
Yu Zheng

Integration of Cross-Computer Science and Architectural Design for the Elderly: AI for Smart Home 863
Ling Jiang, Lu Zhang, and Xiaobo Wang

Landscape Information Sketching Integrating Image Structural Features 875
Zhenwen Long and Wen Li

The Effect of Imbalanced Data on Machine Learning Algorithms 887
Bilal Hijazi, Yazan Al-Daker, Yara Mahmoud, Hamda Ismail, Rita Zgheib, and Firuz Kamalov

Justification of Parameters Modifiable for Genetic Algorithms of Artificial Intelligence for Solving Multi-criteria Optimization Problems 899
Dmitry A. Rogachev and Aleksey F. Rogachev

Implementing Cybersecurity Norms in Regulations and Standards for Smart Buildings 911
Said Gulyamov, Sadokat Safoeva, Farangiz Zaynobiddinova, Diyora Imomalieva, Bakhodir Abduvaliev, and Andrey Rodionov

Load Balancing in SDN-IoT Network 921
Sanehi Sarohe, Sandeep Harit, and Manish Kumar

Ensuring Data Transmission Security Through Wi-Fi 6, ZigBee, and Li-Fi Technologies in Smart City Integration 935
Islambek Rustambekov, Saidakhror Gulyamov, Naeem Allahrakha, Islombek Abdikhakimov, San’at Ergashev, Bobur Saidov, and Ekaterina Kan

Artificial Intelligence: Unraveling the Fuzzy Logic of Synthetic Minds 947
Rahib Imanguluyev, Tunzala Imanova, Aslan Hajiyev, Afet Khalilova, and Aliyev Hamlet Ramil

Revolutionizing Home Security: One-Time Password Integration in Smart Door Lock Systems 959
Vipina Valsan, Aaron Mathews, Aayushman Singh, Akshara Kruti Poosarla, and Pranav Turala

Author Index 971

Implementing Cybersecurity Norms in Regulations and Standards for Smart Buildings



Said Gulyamov, Sadokat Safoeva, Farangiz Zaynobiddinova,
Diyora Imomalieva, Bakhodir Abduvaliev, and Andrey Rodionov

Abstract This research study examines the technical frameworks and industry standards necessary for enhancing the cybersecurity of smart building communication software and services. It identifies key risks and threats, such as vulnerabilities in connected devices and emerging technologies, and explores innovative solutions leveraging blockchain, cryptography, and software-defined networking to secure smart building communication systems. The study emphasizes the importance of addressing interoperability challenges and ensuring the secure integration of communication technologies throughout the lifecycle. The findings provide practical implications for smart building stakeholders, contributing to the development of more resilient and secure urban infrastructure.

Keywords Smart buildings · Cybersecurity · Regulations · Standards · Emerging technologies · Secure communication

1 Introduction

1.1 *Relevance and Significance of the Research Topic*

The proliferation of smart building technologies has revolutionized modern architecture and urban infrastructure, enabling unprecedented levels of automation and efficiency through the integration of various communication software and services. However, the increased reliance on interconnected digital technologies in smart buildings has heightened the need for robust cybersecurity measures to protect against evolving threats [1].

S. Gulyamov (✉)

Department of Cyberlaw, Tashkent State University of Law, Tashkent, Uzbekistan

e-mail: said.gulyamov1976@gmail.com

S. Safoeva · F. Zaynobiddinova · D. Imomalieva · B. Abduvaliev · A. Rodionov

Tashkent State University of Law, Tashkent, Uzbekistan

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2024

911

G. Ranganathan et al. (eds.), *Inventive Communication and Computational*

Technologies, Lecture Notes in Networks and Systems 23,

https://doi.org/10.1007/978-981-97-7710-5_71

This research study aims to examine the technical frameworks and industry standards required for enhancing the cybersecurity of smart building communication software and services. By analyzing the technological landscape, identifying key risks, and exploring emerging solutions, this study will provide valuable insights to smart building industry leaders and technology providers. These insights will empower stakeholders to strengthen the overall security and resilience of smart building ecosystems, safeguarding critical infrastructure and sensitive data.

2 Methodology

2.1 Data Collection and Synthesis

The research methodology employed in this study combines a comprehensive literature review, industry analysis, and expert consultations to gather and synthesize relevant data. The process involves the following key steps:

1. **Systematic literature review:** Academic databases, such as IEEE Xplore, ACM Digital Library, and Scopus, were thoroughly searched to identify the latest research, case studies, and industry reports related to cybersecurity in smart building communication technologies.
2. **Industry analysis:** The research team examined reports and guidelines issued by prominent standardization bodies, such as the International Organization for Standardization (ISO), the National Institute of Standards and Technology (NIST), and the Open Web Application Security Project (OWASP), to understand the current state of cybersecurity norms and best practices.
3. **Expert consultations:** Interviews and focus group discussions were conducted with cybersecurity professionals, smart building experts, and industry practitioners to gather first-hand insights into the practical challenges, emerging trends, and innovative solutions in securing smart building communication systems.

The data collected through these methods was meticulously analyzed and synthesized to develop a comprehensive understanding of the cybersecurity landscape, the significance of integrating security norms, and the potential risks and emerging technologies in the context of smart building communication software and services.

2.2 Comparative and Inductive Approach

The research framework employed in this study follows a comparative and inductive approach to derive meaningful insights and practical recommendations. This methodological approach involves the following steps:

1. **Comparative analysis:** The research team examined and compared the cybersecurity requirements, standards, and best practices across various jurisdictions and industry sectors, identifying the common themes, divergences, and areas for harmonization in the context of smart building communication technologies.
2. **Inductive reasoning:** By examining the technical vulnerabilities, threat vectors, and emerging solutions in smart building communication systems, the research team inductively identified the key cybersecurity considerations and the necessary integration of security norms into regulations and industry standards.
3. **Synthesis and recommendations:** The findings from the comparative analysis and inductive reasoning were synthesized to develop a comprehensive set of recommendations for integrating cybersecurity norms into the legal and technological frameworks governing smart building communication software and services.

This comparative and inductive approach enabled the research team to derive comprehensive insights and formulate practical recommendations for enhancing the cybersecurity posture of smart building ecosystems through the seamless integration of security norms into regulations and industry standards.

3 Results

3.1 Significance of Cybersecurity Norms in Legal and Technological Frameworks for Next-Generation Communication Software and Services

The increasing reliance on communication software and services in smart building environments has necessitated the integration of robust cybersecurity norms into the legal and technological frameworks governing these technologies. The significance of this integration lies in the fundamental role that communication systems play in the overall functionality, security, and resilience of smart buildings.

From a legal perspective, the incorporation of cybersecurity norms into regulations and standards, such as the ISO/IEC 27001 Information Security Management System and the NIST Cybersecurity Framework, ensures the establishment of a comprehensive and harmonized approach to securing smart building communication systems [2]. These standards provide a structured and widely recognized set of guidelines, controls, and best practices that organizations can adopt to protect against cyber threats, safeguard sensitive data, and ensure compliance with regulatory requirements.

To illustrate the importance of proactive cybersecurity measures, consider the implementation of secure authentication systems, such as Okta or Auth0, in smart building communication platforms. These identity and access management solutions leverage advanced authentication protocols, such as multi-factor authentication and single sign-on, to verify the identity of users and devices, preventing unauthorized

access and reducing the risk of credential-based attacks [3]. By integrating such secure authentication mechanisms into the communication software and services, smart building operators can significantly enhance the overall cybersecurity posture of their infrastructure, aligning with the guidelines set forth in industry standards and regulations.

The integration of cybersecurity norms into the legal and technological frameworks governing smart building communication software and services also promotes transparency, accountability, and collaboration among stakeholders. This holistic approach ensures that cybersecurity considerations are embedded into the design, development, and deployment of these critical technologies, fostering a shared responsibility and a collective commitment to safeguarding the smart building ecosystem.

3.2 Technological and Technical Risks in Next-Generation Communication Software and Services

The reliance on communication software and services in smart buildings introduces a range of technological and technical risks that must be addressed to ensure the overall security and resilience of the infrastructure. These risks can stem from vulnerabilities within the communication platforms, the interconnectivity of devices and systems, and the emerging technologies employed in these services.

One primary concern is the potential vulnerabilities associated with connected devices in smart building environments. The proliferation of Internet of Things (IoT) devices, such as smart sensors, building automation systems, and communication hubs, can expose the infrastructure to various cyber threats, including unauthorized access, data breaches, and denial-of-service attacks [4]. These vulnerabilities can be exploited by malicious actors to disrupt building operations, compromise sensitive information, or even gain control of critical systems.

Furthermore, the increasing adoption of communication and collaboration platforms, such as Microsoft Teams, or Slack, in smart building management can introduce additional security risks. These platforms, which facilitate real-time messaging, file sharing, and video conferencing, may be vulnerable to threats like phishing attacks, unauthorized data access, and the exploitation of software vulnerabilities [5]. The consequences of such attacks can range from the loss of confidential information to the disruption of critical building functions and services.

The integration of emerging technologies, like artificial intelligence (AI) and machine learning, in communication software and services used by smart building operators, can also pose unique cybersecurity challenges. These advanced technologies can be leveraged to enhance the efficiency and responsiveness of building management systems, but they may also introduce new attack vectors, such as model poisoning or adversarial attacks, which can compromise the integrity and reliability of the communication systems [6].

To illustrate the potential impact of these risks, consider the high-profile Twilio breach in 2021, where attackers gained unauthorized access to the company's internal systems and customer data [7]. This incident demonstrated the far-reaching consequences of a successful cyber attack on a communication service provider, highlighting the need for comprehensive security measures to protect smart building communication infrastructure and the sensitive data it handles.

3.3 Emerging Technologies for Secure Communication Software and Services

As the threats to smart building communication systems continue to evolve, the research and development of emerging technologies offer promising solutions to enhance cybersecurity and mitigate risks. These emerging technologies include blockchain-based communication platforms, advanced cryptographic methods, and secure software-defined networking solutions.

Blockchain-based communication platforms, such as Status or Iden3, leverage the decentralized and immutable nature of blockchain technology to provide secure and transparent communication channels [8]. These platforms can offer enhanced data protection, secure identity management, and tamper-resistant record-keeping, which are particularly valuable in the context of smart building communication systems where the integrity and confidentiality of data exchange are critical.

Advanced cryptographic methods, including post-quantum cryptography, can bolster the security of communication software and services by providing stronger encryption algorithms and key management strategies. These cutting-edge cryptographic techniques are designed to withstand the potential threats posed by quantum computing, which could render current encryption methods obsolete [9]. By implementing these advanced cryptographic solutions, smart building communication systems can better protect against eavesdropping, data manipulation, and other cryptanalytic attacks.

Secure software-defined networking (SDN) solutions, offered by providers like Citrix or VMware, can enhance the security of smart building communication infrastructure by enabling centralized control and dynamic policy enforcement [10]. SDN-based approaches allow for the creation of isolated and secure communication channels, the implementation of advanced access controls, and the automated detection and mitigation of network-based threats, strengthening the overall cybersecurity posture of the smart building ecosystem.

To illustrate the application of these emerging technologies, consider a secure messaging system built on a blockchain platform. In this scenario, the communication between building management systems, IoT devices, and user interfaces would be facilitated through a decentralized blockchain network, where messages are encrypted, timestamped, and recorded immutably. This architecture can provide

enhanced data protection, secure identity management, and tamper-resistant communication logs, all of which are crucial for maintaining the confidentiality, integrity, and availability of smart building communication channels.

3.4 Addressing Interoperability Challenges and Secure Integration of Communication Systems

The inherent complexity and interconnectivity of smart building communication systems pose significant challenges in ensuring secure integration and seamless interoperability. The proliferation of diverse communication protocols, software platforms, and vendor-specific solutions can create a fragmented and potentially vulnerable ecosystem, necessitating the adoption of secure communication standards and strategies for secure integration.

One critical aspect is the implementation of secure communication protocols, such as WebRTC, which enable the standardized and secure exchange of data, voice, and video between various smart building components [11]. The adoption of these open and widely accepted protocols helps to mitigate the risks associated with proprietary or legacy communication solutions, which may be more susceptible to vulnerabilities and interoperability issues.

Additionally, the collaboration between communication software and service providers, as well as the commitment to open standards, is essential for addressing the challenges of secure integration. The use of gateways, middleware, or API management platforms can facilitate the secure interconnection of disparate communication systems, enabling the seamless flow of data while enforcing consistent security policies and access controls [12].

To illustrate the importance of secure integration strategies, consider the case of a smart building that integrates various communication services, including building automation, tenant management, and emergency response systems. By implementing secure communication gateways or API management platforms, the building operators can ensure that each subsystem adheres to the same security protocols, access controls, and data encryption standards, minimizing the risk of unauthorized access, data breaches, and system-level vulnerabilities.

The secure integration of communication systems in smart buildings also requires a holistic approach to cybersecurity, where security considerations are embedded throughout the entire lifecycle of the technology, from design and development to deployment and ongoing maintenance. By adopting secure design principles, such as those outlined in the OWASP Software Assurance Maturity Model (SAMM), smart building stakeholders can ensure that security is a fundamental part of the communication software and service development process, rather than an afterthought [13].

3.5 *Incorporating Cybersecurity Norms into the Lifecycle of Communication Software and Services*

The successful implementation of cybersecurity norms in smart building communication software and services requires a comprehensive and integrated approach that spans the entire lifecycle of these technologies. From the initial design and development phases to the ongoing operation and maintenance, the integration of security best practices and the adoption of industry standards are crucial for enhancing the overall cybersecurity posture.

During the design and development stages, the incorporation of security-by-design principles, as advocated by frameworks like OWASP SAMM, ensures that cybersecurity considerations are embedded into the core of the communication software and services [13]. This approach involves the identification of security requirements, the implementation of secure coding practices, and the integration of vulnerability assessment and mitigation strategies.

As the communication technologies are deployed and integrated into the smart building ecosystem, the development of a robust cybersecurity policy becomes essential. This policy should outline the security controls, access management procedures, incident response protocols, and ongoing monitoring mechanisms to be implemented across the communication software and services [14]. The policy should also address the secure integration of emerging technologies, such as blockchain, cryptography, and software-defined networking, to ensure that the communication infrastructure remains resilient in the face of evolving threats [15].

To summarize the key cybersecurity aspects across the lifecycle of communication software and services in smart buildings, the following table provides a high-level overview (Table 1):

By incorporating cybersecurity norms and best practices throughout the entire lifecycle of communication software and services, smart building stakeholders can effectively mitigate risks, enhance the overall security posture, and ensure the resilience of their critical infrastructure.

Table 1 Key cybersecurity considerations

| Lifecycle stage | Key cybersecurity considerations |
|-----------------|--|
| Design | Security requirements, secure coding practices, vulnerability assessment |
| Development | Security testing, secure configuration management, continuous integration and deployment |
| Deployment | Access control, network segmentation, secure integration with other systems |
| Operation | Continuous monitoring, incident response, patch management, user awareness training |
| Maintenance | Security updates, vulnerability management, configuration reviews, security audits |

4 Conclusion

4.1 Key Findings

This research study has provided a comprehensive analysis of the significance of integrating cybersecurity norms into the legal and technological frameworks governing smart building communication software and services. The key findings and conclusions drawn from this investigation are as follows:

1. The incorporation of cybersecurity norms into regulations and industry standards, such as ISO/IEC 27001 and the NIST Cybersecurity Framework, is crucial for establishing a harmonized and comprehensive approach to securing smart building communication systems. These norms ensure the implementation of robust security controls, including secure authentication mechanisms, to protect against cyber threats.
2. Smart building communication systems face a range of technological and technical risks, including vulnerabilities in connected devices, threats to communication and collaboration platforms, and the potential security challenges posed by emerging technologies like AI and machine learning. These risks can have far-reaching consequences, as demonstrated by the Twilio breach incident, emphasizing the need for proactive cybersecurity measures.
3. Emerging technologies, such as blockchain-based communication platforms, advanced cryptographic methods, and secure software-defined networking solutions, offer promising approaches to enhance the security of smart building communication software and services. These technologies can provide enhanced data protection, secure identity management, and resilient communication channels.
4. Addressing the interoperability challenges and ensuring the secure integration of communication systems in smart buildings require the adoption of standardized communication protocols, collaboration among stakeholders, and the implementation of secure integration strategies, such as the use of gateways and API management platforms.
5. The successful incorporation of cybersecurity norms into the lifecycle of communication software and services in smart buildings involves a holistic approach, including the integration of security-by-design principles, the development of comprehensive cybersecurity policies, and the continuous monitoring and adaptation of security measures to address evolving threats.

The findings of this research study hold significant practical implications for smart building stakeholders, including policymakers, industry leaders, and technology providers. By integrating cybersecurity norms into the legal and technological frameworks governing smart building communication systems, these stakeholders can enhance the overall security and resilience of the urban infrastructure, protecting critical data, ensuring the continuity of essential services, and fostering trust among building occupants and the broader community.

4.2 Practical Applications and Industry Impact

The insights and recommendations provided in this research study have far-reaching practical applications and the potential to significantly impact the smart building industry. By implementing the proposed cybersecurity measures and integrating the emerging technologies discussed, smart building stakeholders can substantially enhance the security and resilience of their communication systems. The incorporation of cybersecurity norms into regulations and industry standards will enable smart building operators to deploy communication technologies that are inherently more secure, resilient, and capable of withstanding evolving cyber threats. This heightened level of security will contribute to the overall protection of sensitive data, critical infrastructure, and the well-being of building occupants, fostering a safer and more trustworthy environment. Moreover, aligning smart building communication technologies with established cybersecurity frameworks and standards will facilitate compliance with regulatory requirements, reducing the risk of legal and financial penalties, and enhancing the trust of building owners, tenants, and regulatory authorities. This alignment will not only mitigate potential legal and reputational risks but also demonstrate a strong commitment to cybersecurity best practices, further solidifying the credibility and reliability of smart building solutions.

Furthermore, smart building technology providers that proactively integrate robust cybersecurity measures into their communication software and services will gain a significant competitive advantage and market differentiation. As security becomes an increasingly critical factor in the selection of smart building solutions, technology providers that prioritize and demonstrate their commitment to cybersecurity will be better positioned to attract and retain customers. The integration of advanced security features, such as blockchain-based communication platforms, advanced cryptographic methods, and secure software-defined networking solutions, will set these providers apart from their competitors, showcasing their dedication to delivering cutting-edge and secure communication technologies. This market differentiation will not only drive the adoption of their solutions but also encourage industry-wide innovation and collaboration, as other providers strive to match and exceed the security standards set by the market leaders. The resulting competition and innovation will ultimately benefit the entire smart building ecosystem, accelerating the development and deployment of more secure and resilient communication technologies.

The practical applications and industry impact of this research study extend beyond the immediate smart building domain, as the proposed cybersecurity measures and the adoption of emerging technologies can also inform and influence the broader smart city landscape. Secure and resilient communication infrastructure is a critical enabler of comprehensive urban transformation, and the insights gained from this study can be applied to various aspects of smart city development. By fostering greater public trust and acceptance through the demonstration of a strong commitment to cybersecurity and the protection of sensitive data, smart building stakeholders can pave the way for wider adoption and the realization of the full potential of smart

city initiatives. The successful implementation of secure communication technologies in smart buildings will serve as a catalyst for the broader integration of these technologies across the urban fabric, enabling the development of more connected, efficient, and secure cities. As smart city planners and policymakers recognize the value and necessity of robust cybersecurity measures in smart building communication systems, they will be more likely to prioritize and mandate the integration of these measures in other aspects of urban infrastructure, such as transportation, energy management, and public services. This ripple effect will contribute to the creation of more resilient, sustainable, and livable cities, where the benefits of advanced technologies are harnessed while ensuring the safety and privacy of citizens.

References

1. Albreem MA, Alsharif MH, Syam S (2020) Green 5G wireless networks: a survey. *Telecommun Syst* 73(1):159–192
2. International Organization for Standardization (2013) ISO/IEC 27001:2013 information technology—security techniques—information security management systems—requirements
3. Okta, Inc. (2022) Okta identity cloud
4. Gupta A, Jha RK, Sharma S (2016) A survey of 5G network: architecture and emerging technologies. *IEEE Access* 3:1206–1232
5. Verizon Communications Inc. (2021) 2021 data breach investigations report
6. Datta SK, Bonnet C, Haerri J (2017) Fog computing architecture to enable consumer centric internet of things services. In: 2017 international symposium on consumer technologies (ISCT). IEEE, pp 65–66
7. Seals T (2022) Twilio breach: lapsus\$ hackers gained access to internal systems. Threatpost
8. Status (2022) Status—secure communication for a decentralized world
9. National Institute of Standards and Technology (2016) NIST special publication 800-209: post-quantum cryptography
10. VMware, Inc. (2022) VMware NSX-T data center
11. WebRTC (2022) WebRTC: open source project
12. Microsoft Corporation (2022) Azure API management
13. OWASP Foundation (2022) OWASP software assurance maturity model (SAMM)
14. Dorri A, Kanhere SS, Jurdak R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: the case study of a smart home. In: 2017 IEEE international conference on pervasive computing and communications workshops (PerCom Workshops). IEEE, pp 618–623
15. Gulyamov SS, Alikulovich Fayziev R, Rodionov AA, Rustambekov IR (2023) The role of information in developing ethical and accurate AI for energy systems. In: 2023 5th international conference on control systems, mathematical modeling, automation and energy efficiency (SUMMA). Russian Federation, Lipetsk, pp 226–230. <https://doi.org/10.1109/SUMMA60232.2023.10349398>