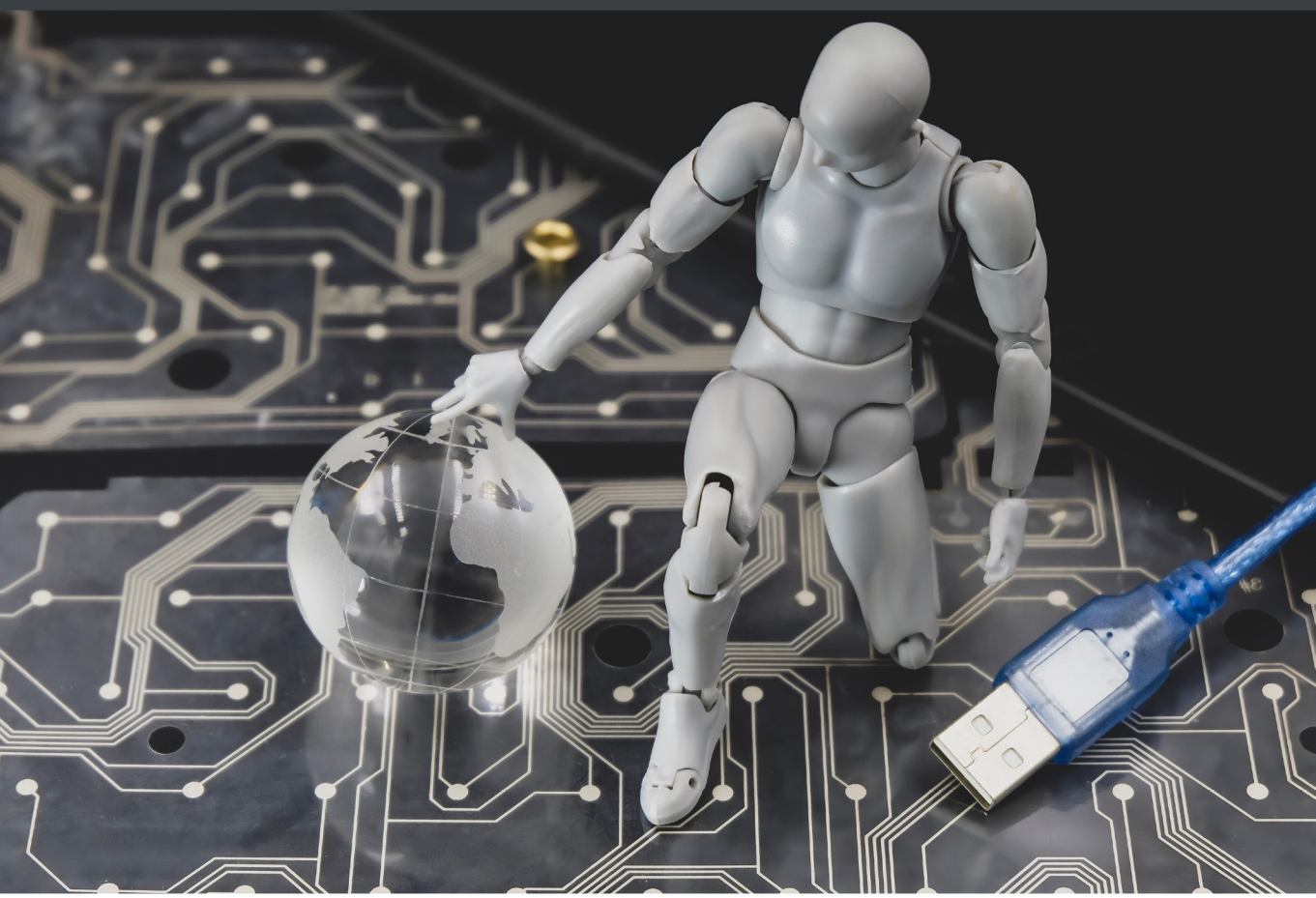
INGENIOUS

5 ISSUE 1

Editor-in-Chief: Prof. Asoc. Dr. Teuta XHINDI/ Scientific Journal of the Faculty of Engineering, Informatics and Architecture / No. 5, issue 1/ 2025

ISSN 2789-4800



ADVANCING INNOVATION

through Interdisciplinary Research and Digital Solutions

Teuta **XHINDI**/ Amanda **KOTE**/ Malvina **NIKLEKAJ**/ Elfat **MEMAJ**/ Albana **HASIMI**/ Blerina **PAPAJANI**/ Gazmir **ÇELA**/ Elvin **ÇOMO**/ Florinda **TUGA**/ Mirela **DVORANI**/ Sara **BALLKOÇI**/ Alba **ÇOLLAKU**/ Ardiana **TOPI**/ Shahina **BEGUM**/ Shaibal **BARUA**/ Emmanuel **WEITEN**/ Kreshnik **HAKRAMA**/ Jani **PETRO**/ Hemi **LIKA**/ Amanda **KOTE**/ Anxhela **DEMA**/ Anri **HASANI**/ Malvina **NIKLEKAJ**

UETPRESS

INGENIOUS

No. 5, issue 1/2025

JOURNAL OF THE FACULTY OF ENGINEERING, INFORMATICS AND ARCHITECTURE

ISSN 2789-4800

UETPRESS

Published under the series “ACADEMIC JOURNALS”.

The journal has been catalogued at the National Library of Albania and the Library of the European University of Tirana, Albania.

(print ISSN: 2789-4800/ online ISSN: 2958-888X)

ingenious@uet.edu.al
www.uet.edu.al/ingenious

UETPRESS

Published by:
EUROPEAN UNIVERSITY OF TIRANA / ALBANIA

content

EDITORIAL

Advancing Innovation through Interdisciplinary Research and Digital Solutions

Prof. Asoc. Dr. Teuta XHINDI

This issue of the journal *Ingenious* brings together a diverse range of research contributions that reflect the rapid technological advancements shaping the future of our societies. As the world faces unprecedented challenges, including climate change, cyber threats, and the growing demands of digital transformation, this issue highlights innovative solutions and multidisciplinary approaches that aim to foster sustainability, resilience, and inclusive growth.

Each article demonstrates the authors' commitment to exploring how emerging technologies, from artificial intelligence (AI) and deep learning to advanced networking and cybersecurity solutions are revolutionizing sectors such as engineering, information technology, industrial maintenance, and environmental science.

This issue features research on a variety of timely and practical topics, including:

An innovative approach to music personalization through the development of a mood-aware playlist generator, leveraging Spotify's API to enhance user engagement.

A study on the impact of chatbot technology in digital university platforms, using UetBot as a case study, which shows improved administrative workflows and student support services.

Simulation and mitigation strategies for Distributed Denial-of-Service (DDoS) attacks using Python, providing hands-on tools for testing and resilience-building in network security.

A comparative analysis of VPN technologies in surveillance-heavy environments, evaluating WireGuard, OpenSSH, and Radmin VPN in terms of encryption, usability, and anonymity.

The implementation of Mask R-CNN and OpenCV for automated inspection of Volvo heavy machinery parts, reducing costs and increasing precision in maintenance cycles.

The calibration of high-accuracy energy meters using advanced test systems, contributing to smarter energy distribution and greater transparency in billing.

A platform design named DevConnect that merges social media with technical forums, promoting IT problem-solving and professional networking.

A systematic statistical analysis of very hot days (above 35°C) in Tirana over a decade, linking urban temperature trends to climate change and urbanization effects.

What unites these diverse contributions is their shared focus on practical impact. Each article not only advances academic knowledge but also offers viable solutions to real-world problems faced by today's industries, educational institutions, and municipalities.

By bridging technical innovation with social relevance, the authors have provided research that speaks to the broader goals of sustainable development, digital transformation, and interdisciplinary cooperation. The inclusion of voices from engineering, computer science, urban studies, and education further highlights the importance of a cross-sectoral approach to innovation.

Importantly, several articles in this issue are the result of close collaboration between professors and students, emphasizing the journal's commitment to fostering research skills and academic engagement among the next generation of professionals.

The topics explored throughout this issue and the conclusions drawn from them, serve as a catalyst for meaningful discussions among researchers, industry experts, and policymakers. They invite reflection on how we can collectively harness emerging technologies to build a more sustainable and inclusive future. The diverse backgrounds of the contributing authors, spanning academia, industry, and public policy, underscore the importance of interdisciplinary collaboration in tackling complex, real-world problems. Their insights offer valuable guidance and inspiration for anyone seeking to leverage technological innovation in the pursuit of sustainable solutions that benefit both society and the environment.

Advancing Music Streaming Personalization Developing a Mood-Aware Playlist Generator

Msc.Amanda KOTE
European University of Tirana, Faculty of Engineering, Informatics and Architecture, Department of Informatics and Technology, Tirana, Albania
amanda.kote@uet.edu.al

Abstract

In recent years, music streaming services have transformed the way audiences experience and interact with music, with platforms like Spotify leading the charge. As of 2024, Spotify's user base has continued to expand, reaching millions of listeners globally who have access to an extensive library of songs, playlists and podcasts. This shift toward digital music consumption has been accompanied by an increased demand for personalization, where users expect curated experiences that resonate with their individual tastes, moods and preferences.

The motivation behind this research is to enhance Spotify's user experience by creating a system that customizes playlists based on the listener's current mood and preferences. While recommendation algorithms are widely implemented in various streaming platforms, many still rely on basic filtering methods, focusing primarily on genre or artist. This thesis aims to address a gap by introducing a virtual assistant capable of dynamically generating playlists that reflect both emotional states and musical preferences. Such a tool not only enriches the music streaming experience but also aligns with the broader industry trend toward personalized digital interactions.

This study presents the "Spotify- Feel the Music" playlist generator, an innovative approach designed to enhance user engagement through intelligent playlist suggestions. By leveraging the Spotify API, the generator draws on a combination

of user mood and historical preferences, providing an interactive experience, both personalized and adaptive. This system underscores the importance of AI-driven recommendations and virtual assistants in creating meaningful, user-centric experiences within digital platforms.

Keywords: *Spotify, Spotify API, Music Recommendation, Personalized Experience, Mood Detection, User Preferences, Music Streaming*

Introduction

The evolution of music streaming services has revolutionized how users interact with music, making platforms like Spotify integral to the daily lives of millions worldwide. As digital music consumption continues to soar, there is an increasing demand for personalized experiences that goes beyond traditional playlists and curated content. While current recommendation algorithms provide some level of customization based on genre or artist preferences, they often overlook the dynamic, emotional nature of music listening. This research paper seeks to address this gap by developing an innovative mood-aware playlist generator, which tailors music recommendations to a user's current emotional state. This research presents a novel approach to enhancing the personalization of music streaming, ensuring a more intuitive, engaging experience that resonates deeply with individual listeners.

Two research questions are addressed in this research paper:

First research question: How can a playlist generator use mood and genre preferences to provide personalized music recommendations that resonate with user emotions and tastes?

This question aims to develop a more advanced recommendation system that goes beyond traditional genre-based filtering. By incorporating mood detection, the system could create playlists that adapt not only to a user's musical taste, but also to their emotional state at a given time. The research could lead to a system that offers a deeper, more personal connection to music, ensuring that the playlists resonate emotionally with users.

Second research question: How does the use of real-time interaction data improve the quality and relevance of music recommendations for users?

Through this question, the study looks into the ways the system could adapt dynamically to a user's changing preferences and emotional states. This would lead to a more responsive and personalized user experience, that would lead users to become more likely to stay engaged with the platform and explore new music based on emotional context.

This paper is guided by a clear hypothesis and objectives. The hypothesis proposes that combining mood detection with user-defined preferences (such as

genre and artists) within a virtual assistant for playlist generator will significantly enhance user satisfaction and engagement with Spotify. Specifically, it suggests that a system capable of understanding both the emotional state of the listener and their musical taste can provide a more dynamic, personalized music experience. By tailoring the playlist to the listener's mood and preferences, the music experience will feel more personal, relevant, and emotionally resonant, which should enhance overall satisfaction.

Hypothesis

Integrating mood detection with user-defined preferences in a virtual assistant for playlist generation will enhance user satisfaction and engagement with Spotify by providing a more personalized and dynamic user experience.

In order to achieve this, the research paper outlines several key objectives:

1. To identify limitations in existing music recommendations systems that fail to address real-time personalization based on user mood and preferences.
2. To develop a platform that integrates mood and genre/artist preferences to create customized Spotify playlist.
3. To explore the effectiveness of emotion-aware playlist recommendations in enhancing user engagement and satisfaction with music streaming.

Literature Review

The evolution of music streaming platforms has significantly reshaped the way audiences experience and engage with music. Spotify, launched in 2006, quickly became one of the leading platforms, offering a vast music catalog alongside personalized recommendations. (Statista, 2021) To remain competitive, companies like Spotify have continuously enhanced their recommendation systems, introducing features such as "Discover Weekly" and "Release Radar", which leverage user behavior to create personalized music experiences. (United States Securities and Exchange Permissions, 2023)

Development of Music Recommendations Systems

Early music recommendation systems used basic filtering methods, typically relying on genre or artist similarity. Platforms like Pandora focused on genre-based recommendations, generating playlists that matched user-selected genres

or similar artist profiles. However, this approach was limited in its ability to capture complex user preferences, leading to the rise of collaborative filtering models. By examining listening patterns across users, collaborative filtering could suggest songs that aligned with the tastes of similar listeners, broadening the personalization scope of music recommendations. (Sommerville, 2016)

Personalized Playlist Generation and Emotional Context

Traditional recommendation models often overlook the emotional and contextual nuances of user preferences. Recent studies have explored mood-based recommendations to address this gap, highlighting the importance of emotional states in enhancing user satisfaction with music recommendations. (Sotiropoulos & Tsihrintzis, 2018) For instance, researchers have found that mood-aware playlists increase user engagement by aligning with specific emotional needs, such as relaxing or energizing music. Methods like Artificial Immune Systems (AIS) have been used to generate playlists that align with both positive and negative emotional states, recognizing that users' musical preferences often change based on mood. (Jannach, Kamehkhosh, & Bonnin, 2018)

Spotify has implemented similar approaches through its "Discover" feature, where algorithms gauge user sentiment based on interaction patterns, such as the "Thumbs Up" and "Thumbs Down" indicators or time spent listening to specific tracks. The algorithm recommends similar songs if a user listens to a track for over 30 seconds, reflecting an interest in that style. (Spotify, 2021)

Challenges in Mood and Emotion Detection

Incorporating mood detection into recommendation systems is technically challenging. Studies have highlighted difficulties in accurately mapping musical elements to user emotions, as emotional preferences are often complex and subjective. Traditional methods rely on explicit user input for mood data; however, more recent advancements leverage implicit data signals, such as listening duration or frequency of specific genres, to infer mood indirectly. (Cunningham, 2001)

Machine Learning and Advanced Filtering Models

Machine learning, particularly deep learning, has advanced recommendation systems by enabling more nuanced and dynamic recommendations. Collaborative filtering, neural networks, and reinforcement learning models have been applied in music recommendations to predict user preferences based on vast datasets of historical listening behavior. In a study on hybrid recommendation models, it was shown that combining content-based and collaborative filtering approaches

can better capture user preferences and deliver more precise recommendations, outperforming traditional filtering methods. (Radovanovic, 2022)

This study builds upon existing research by integrating mood detection with user-defined preferences for genres and artists, addressing the limitations of existing recommendation systems. By leveraging Spotify's API, this work aims to create a platform capable of dynamically generating playlists based on mood, further advancing the personalization capabilities of current streaming platforms.

Methodology and Technology Used

The "Spotify – Feel the Music" platform was developed using the Software Development Life Cycle, which allowed for structured phases from planning to maintenance. This approach ensured that each aspect of the system – particularly user interactions, mood-based recommendations, and data integration – was systematically addressed for reliability and scalability. (Sommerville, 2016)

Technologies implemented:

1. Frontend Development with ASP.NET and C#

The fronted of this platform was implemented in ASP.NET and C#, chosen for its flexibility and support for web application development. Using C# allowed for robust functionality and quick processing, essential for handling real-time user inputs.

2. Spotify API

The Spotify API played a central role in generating personalized playlists. Using RESTful principles, this API retrieves song and artist metadata in JSON format, enabling the system to recommend music based on user moods and preferences. The API's endpoints allowed for direct access to Spotify's extensive music catalog, providing users with a rich and diverse selection of songs . (Spotify, 2021) The integration of the Spotify API happens within the platform. This connection enables real-time access to the music catalog, allowing the app to retrieve song metadata, artist details, and genre information necessary for creating mood-based personalized playlists.

3. Database Design with SQL

The backend relied on a SQL database, structured to store and retrieve user preferences efficiently. Using Entity Relationship Diagrams (ERDs) and structured queries, the database managed details such as user profiles, past interactions, and generated playlists. The SQL-based database facilitated fast retrieval, especially when generating playlists based on the user's historical preferences. Figure

1 displays the Entity Relationship Diagram (ERD) for the 'Spotify – Feel the Music' application, outlining the database structure that stores user preferences, mood data, and playlist information. This diagram illustrates the relationships between key entities—such as User, Playlist, and Genre—depicting how the system organizes and retrieves data to support personalized, mood-driven playlist recommendations

FIGURE 1 Entity Relationship Diagram

4. User Interaction and Playlist Customization

User Interaction Flow: The application uses a streamlined interaction flow that begins by asking users for their current mood and musical preferences (genre and artist). These inputs are processed to create a playlist that aligns with the user's current emotional state.

System Architecture and Implementation

The system was designed using Model-View-Controller (MVC) architecture, enabling separation of data management, user interface, and control logic. (Xiaokang & Cheng, 2013) This structure supports independent updates and simplifies debugging:

- **Backend Middleware and Authentication**: Middleware functions were added to manage user sessions and secure data handling. **JWTs (JSON Web Tokens)** authenticated user sessions, ensuring that playlists generated were personalized and secure.

- **API Data Flow**: RESTful endpoints handled interactions between the Spotify API and the app, supporting CRUD operations to retrieve, update, and display playlists based on current preferences.

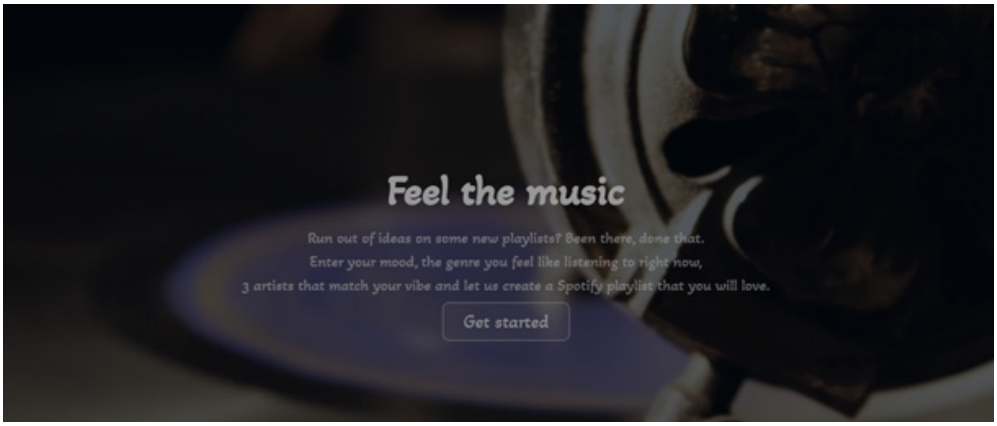
Testing and Security Measures

To ensure smooth user experience, unit testing was conducted on the system's frontend, backend, and database functions. Components such as the mood selection and playlist generation modules were tested individually to confirm accurate responses based on user input. (Dooley, 2017) Password hashing with bcrypt and tokenized sessions with JWT were employed to safeguard user data and protect the privacy of their listening preferences.

Case Study: Feel the Music Platform

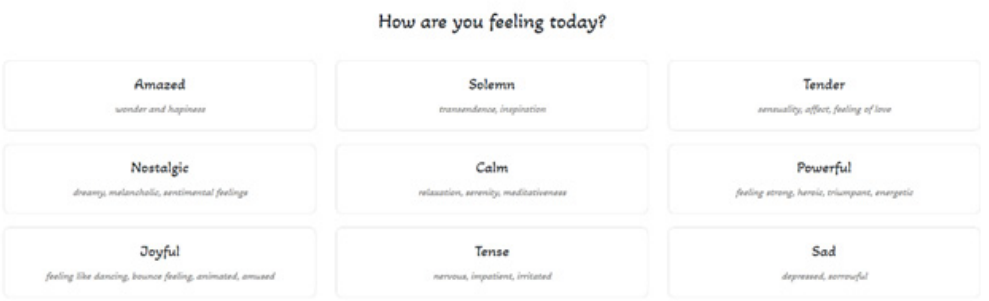
The "Spotify – Feel the Music" platform was designed to deliver a fully personalized playlist experience that aligns with the user's mood and musical preferences. Upon opening the software application, users are greeted with an introductory screen prompting them to begin the playlist generation process. The initial interface encourages users to start by selecting a playlist based on their mood.

FIGURE 2 "Feel the Music" Interface



The second interface is the mood selection interface, which allows users to specify their emotional state, which will serve as a key variable in generating playlists that resonate with their current feelings. Users can select from various mood options (happy, calm, energetic, etc.) setting the foundation for the personalized playlist recommendations.

FIGURE 3 "How are you feeling today?" Interface



After selecting a mood, users are directed to a screen where they can specify preferred music genres and favorite artists. These additional inputs refine the playlist further, ensuring that the recommended songs align with both the user's mood and their musical taste. The user can select multiple artists, allowing flexibility and personalization.

FIGURE 4 "Choose the gender you would like to listen" Interface

FIGURE 5 "Pick 3 artists" Interface (1)

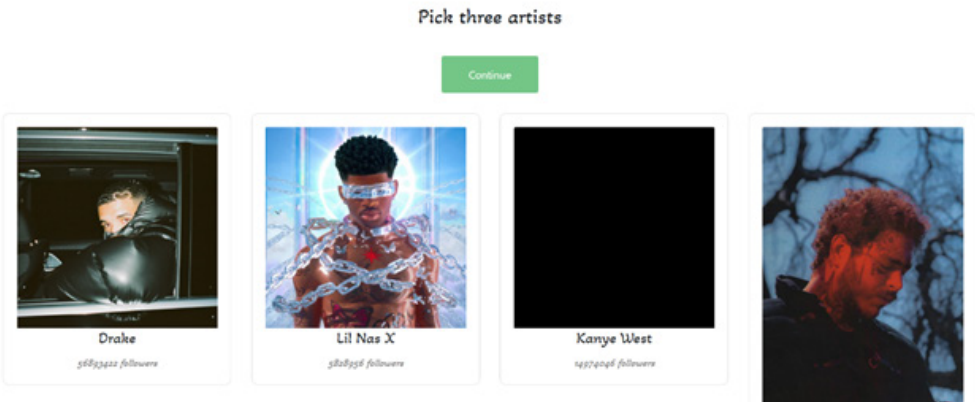


FIGURE 6 "Pick 3 artists" Interface (2)

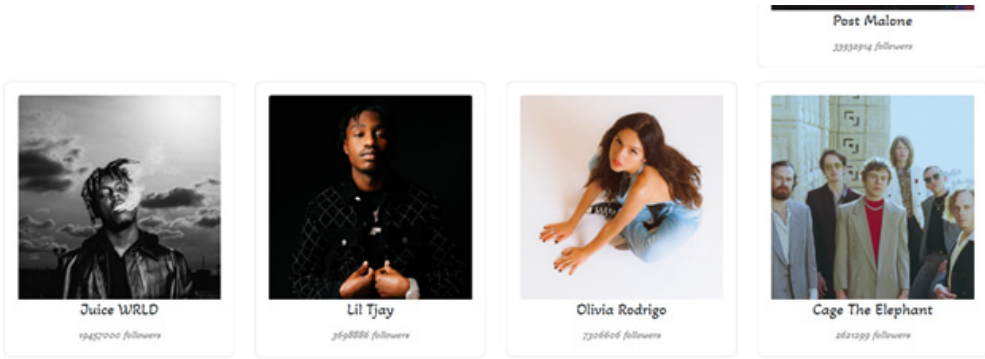


FIGURE 7 "Pick 3 artists" Interface (3)

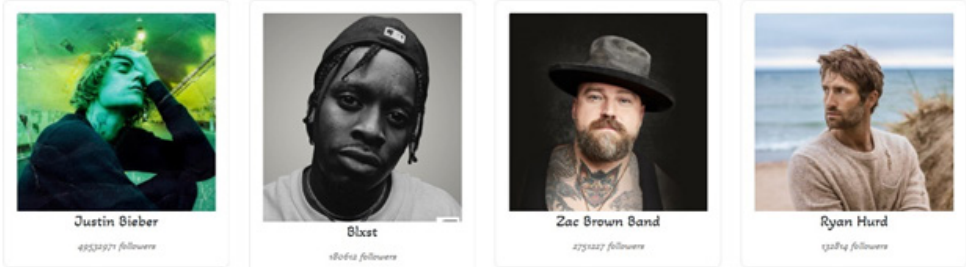
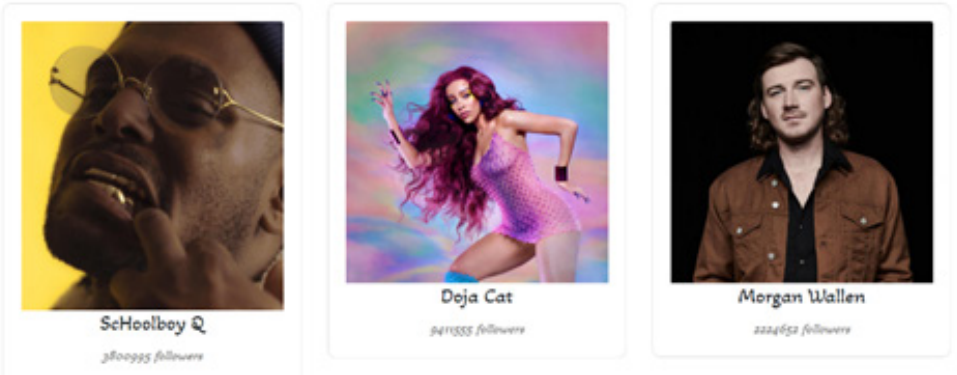
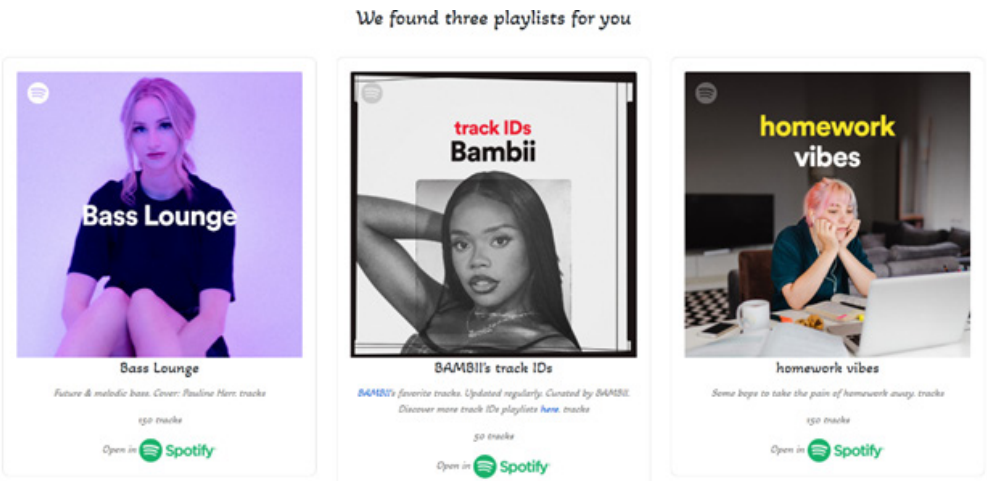


FIGURE 8 "Pick 3 artists" Interface (4)



Upon receiving the user's mood, genre and artist inputs, the platform connects to the Spotify API to retrieve relevant song data. The API allows access to Spotify's extensive catalog, enabling the platform to fetch song metadata, artist information, and other data required to compile a mood-matched playlist. Based on the collected information, it will generate 3 playlists that will be displayed to the user in a visually appealing layout, allowing them to preview, play or skip tracks according to their preferences by redirecting the users to Spotify app.

FIGURE 9 Playlists Generated Interface



To assess the **Spotify – Feel the Music** platform's impact on user experience, a survey was conducted with a sample group of users who tested the system. The survey gathered feedback on aspects such as playlist relevance, emotional alignment with mood selections, and overall satisfaction with the personalization features.

Survey Design and Methodology

Participants were asked a series of questions focused on key functionality areas:

- **Mood-Based Personalization**: Users rated how well the platform's playlists aligned with their selected moods and if they felt an emotional connection to the recommended tracks.
- **Ease of Use**: Participants evaluated the interface's usability, including mood and genre selection and ease of navigating through playlist options.
- **Engagement and Satisfaction**: Questions measured user engagement, specifically how likely participants were to use the platform regularly and explore new music.

Key Findings

The Survey results highlighted positive responses across several dimensions:

1. **Enhanced Emotional Connection**: Over 80% of users reported that mood-based playlist recommendations provided a deeper connection to the music, with many noting that the playlists reflected their current mood accurately.
2. **Increased User Engagement**: Most users expressed interest in using the platform frequently, citing that the mood and genre preferences led to personalized playlists that felt more meaningful and enjoyable.
3. **Usability**: Participants rated the platform's interface highly for being intuitive and easy to navigate, particularly during the mood selection and playlist generation steps.

These survey insights support the hypothesis that integrating mood and user preferences enhances both user satisfaction and engagement with the platform. This feedback also highlights areas for potential improvement, such as refining mood categories to capture more nuanced emotions.

Conclusions

The Spotify – Feel the Music platform demonstrates an innovative approach to music personalization by integrating mood detection with user preferences in genre and artist selection. This research highlights that combining mood-

based inputs with traditional preference data enhances both the immersion and emotional resonance of the listening experience.

The first research question aimed to assess whether incorporating mood into playlist generation could create a more meaningful connection between users and the music they listen to. This study confirmed that mood-based personalization adds depth to the user experience, enabling playlists that align more closely with emotional states and musical tastes. Survey results supported this finding, with over 80% of users reporting an emotional connection to playlists that resonated with their selected mood, affirming the platform's ability to meet user demand for dynamic, responsive music recommendations.

The second research question explored the role of real-time data in refining recommendation quality. Findings indicated that real-time interaction data is essential for adapting playlists to users' immediate needs, making recommendations feel both timely and personally relevant. By leveraging real-time data from the Spotify API, the platform provides playlists that evolve with the user's current emotional state, fostering increased engagement. Survey participants echoed this benefit, with many expressing interests in using the platform regularly due to its responsiveness and accuracy.

The survey feedback further confirmed that mood-based personalization increases user satisfaction and engagement, with users indicating a strong preference for the platform's interactive and adaptive nature. This positive response underscores the value of emotion-aware recommendations in the music streaming experience, establishing Spotify – Feel the Music as a step forward in the field of personalized digital interactions.

Recommendations

Moving forward, several avenues could further enhance the Feel the Music platform:

1. **Enhanced Mood Detection**: Integrating machine learning models to infer mood from user behavior data (such as listening patterns and interaction duration) could further automate mood recognition.
2. **Expanding Real-time Adaptability**: Leveraging reinforcement learning models would allow the platform to evolve with user preferences, continuously improving its recommendations based on immediate feedback.
3. **Privacy-First Data Practices**: Continued attention to data privacy and minimal data retention practices will be essential as the platform collects more detailed user inputs. Ensuring user consent and transparent data use could increase user trust and adoption.

4. **Broader Emotional Spectrum**: Adding more nuanced mood categories could refine playlist recommendations further, capturing a wider range of emotional contexts for even more personalized results.

The **Spotify – Feel the Music** platform thus not only fulfills current personalization demands but also sets a foundation for future advancements in music recommendation systems, paving the way for more intelligent, user-centric digital experiences in the music streaming industry.

References

Cunningham, W. (2001). *Principles behind the Agile Manifesto*. Получено из Agile Manifesto: http://agilemanifesto.org/iso/en/principles.html

Jannach, D., Kamehkhosh, I., & Bonnin, G. (2018). Music Recommendations: Algorithms, Practical Challenges and Applications. B S. Berkovsky, I. Cantador, & D. Tikk, *Collaborative Recommandations* (стр. 481-518). World Scientific.

Sommerville, I. (2016). *Software Engineering Tenth Edition*. Essex: Pearson Education Limited.

Sotiropoulos, D. N., & Tsihrintzis, G. A. (2018). *Artificial immune system-based music*. Piraeus: Gallery Proof.

Spotify. (2021). *Retrieve metadata from Spotify content, control playback or get recommendations.* Получено из Spotify for Developers: https://developer.spotify.com/documentation/web-api/

Statista. (07 2021 г.). *Revenue of Spotify worldwide from 1st quarter 2016 to 2nd quarter 2024*. Получено из Statista: https://www.statista.com/statistics/813828/spotify-revenue-quarterly/

United States Securities and Exchange Permissions. (2023). *Annual Report*. Washington DC: Grand Duchy of Luxembourg.

Xiaokang, L., & Cheng, G. (2013). Analysis and Implementation of ASP.Net and PHP Frameworks Based. *Wuhan University of Science and Technology* .

Analyzing and Mitigating Distributed Denial-of-Service (DDoS) Attacks: A Python-Based Simulation Approach

Malvina NIKLEKAJ
European University of Tirana, Faculty of Engineering, Informatics and Architecture, Department of Informatics and Technology, Tirana, Albania
malvina.niklekaj@uet.edu.al

Elfat MEMAJ
European University of Tirana, Faculty of Engineering, Informatics and Architecture, Department of Informatics and Technology, Tirana, Albania
ememaj6@uet.edu.al

Abstract

The increasing prevalence of Distributed Denial of Service (DDoS) attacks poses a significant threat to the security and availability of online services and networks. These attacks leverage multiple compromised systems to overwhelm a target, rendering it inaccessible to legitimate users. This research presents an in-depth analysis of DDoS attack methodologies, their classification into volumetric, protocol-based, and application-layer attacks, and their real-world implications.

To enhance understanding and mitigation strategies, this study introduces a Python-based simulation tool that replicates various DDoS attack techniques, including TCP, UDP, ICMP, and HTTP request floods. The tool leverages asynchronous

programming and multiprocessing to simulate large-scale attack scenarios, enabling controlled testing of network resilience. Furthermore, this research explores state-of-the-art defensive mechanisms, including firewalls, rate limiting, DDoS scrubbing services, and AI-driven anomaly detection, emphasizing the role of automation in modern cybersecurity defenses.

Additionally, an Intrusion Analysis System (IAS) powered by Python is proposed, integrating machine learning-based anomaly detection and real-time network traffic monitoring. This system provides organizations with adaptive and proactive defense capabilities, reducing downtime and mitigating service disruptions. The modular design of the system ensures seamless integration into existing network infrastructures, making it a scalable and effective solution for cybersecurity professionals.

By combining theoretical analysis, practical implementation, and defensive strategies, this research contributes to the ongoing efforts in fortifying digital infrastructures against the evolving landscape of DDoS attacks. The findings underscore the importance of leveraging Python's capabilities for both attack simulation and defense, paving the way for enhanced network security resilience in an increasingly interconnected digital world.

Introduction

The rapid expansion of digital services and the increasing reliance on networked systems have made cybersecurity a critical area of concern. One of the most disruptive and evolving threats to network security is the Distributed Denial of Service (DDoS) attack, which aims to overwhelm a target system, server, or network with excessive traffic, rendering it inaccessible to legitimate users. DDoS attacks have been responsible for severe financial losses, service disruptions, and security breaches across various industries, including finance, healthcare, government, and e-commerce.

DDoS attacks exploit the distributed nature of botnets—large networks of compromised devices—to generate high-volume malicious traffic. These attacks can be broadly categorized into volumetric attacks, which consume network bandwidth (e.g., UDP floods, ICMP floods**);** protocol-based attacks, which exploit vulnerabilities in network protocols (e.g., SYN floods, Smurf attacks); and application-layer attacks, which target specific web applications or services (e.g., HTTP floods, Slowloris attacks). Due to their ever-evolving nature, these attacks remain a persistent challenge for cybersecurity professionals.

Traditional DDoS mitigation techniques, such as firewalls, rate limiting, and traffic filtering, offer some level of defense but often fall short in preventing sophisticated, large-scale, and adaptive attacks. To address this issue, the integration of automated detection, machine learning, and real-time monitoring has become an essential approach in cybersecurity.

This research introduces a Python-based simulation tool designed to replicate various DDoS attack techniques, allowing controlled testing of network resilience. Additionally, an Intrusion Analysis System (IAS) leveraging Python's powerful libraries for network traffic monitoring and anomaly detection is proposed. By incorporating machine learning-based detection algorithms, behavioral analysis, and traffic filtering, this system enhances the ability to identify, analyze, and mitigate DDoS attacks in real-time.

Related Works

In the field of cybersecurity, numerous studies have explored various aspects of Distributed Denial of Service (DDoS) attacks, including detection, mitigation, and analysis methodologies. This section reviews related work pertinent to our research focus.

In the study titled "Intrusion Analysis System of DDoS Attack Using Python," the authors developed an intrusion analysis system leveraging Python to detect and analyze DDoS attacks. The system employs network traffic monitoring and anomaly detection techniques to identify potential threats in real-time. The use of Python provides flexibility and ease of integration with existing network infrastructures, facilitating efficient detection and response mechanisms.

Another significant contribution is the research on "Distributed Denial of Service Attack Alleviated and Detected Using Software-Defined Networking (SDN)." This study examines the impact of DDoS attacks on SDN environments and proposes a mitigation strategy utilizing SDN applications written in Python. By leveraging the OpenFlow protocol, the system can automatically detect and respond to DDoS attacks, enhancing network resilience.

These studies collectively highlight the effectiveness of Python-based solutions in detecting and mitigating DDoS attacks. Our research builds upon these foundations by developing a comprehensive Python-based simulation tool to analyze various DDoS attack vectors and evaluate the efficacy of different mitigation strategies in real-time.

Methodology

Experimental Setup and Test Environment

To systematically evaluate the impact of Distributed Denial of Service (DDoS) attacks on a low-powered computing device, we conducted controlled experiments using a Raspberry Pi 5 as the target server. This test environment was selected due

to its affordability, accessibility, and real-world applicability in Internet of Things (IoT) security research. The Raspberry Pi 5 was configured to host a Flask-based web server, which acted as the primary victim of our simulated DDoS attacks. The experiments aimed to measure the resilience of the system under various attack conditions, examining metrics such as CPU utilization, memory load, network performance, and system stability.

The server setup involved installing a Debian GNU/Linux 12 (Bookworm) operating system, running a 64-bit ARM architecture (aarch64). The kernel version used during testing was 6.6.62+rpt-rpi-2712, ensuring compatibility with the required software stack. The device featured a quad-core ARMv8 CPU, capable of handling lightweight computing tasks. Memory availability was approximately 7.9 GB, with over 6.1 GB left free after boot, ensuring sufficient resources for testing. Storage was provided via a 58GB microSD card, with 44GB available for logging experiment data.

To facilitate monitoring of resource consumption, we installed and configured several performance measurement tools:

- Htop: A real-time process and system monitor for Linux.
- Atop: A comprehensive system and process-level performance analyzer.
- Netdata: A lightweight monitoring solution that provides real-time system analytics.

These tools were critical in tracking CPU load, memory utilization, network activity, and application performance throughout the attack simulations.

Network Configuration

To ensure controlled and replicable testing conditions, all devices were interconnected using a dedicated Local Area Network (LAN). The Raspberry Pi 5 was connected directly to a switch, and two laptops, one high-performance gaming laptop and one mid-tier laptop—were used to launch the DDoS attacks. This controlled setup ensured minimal external interference while enabling precise measurement of network-related parameters.

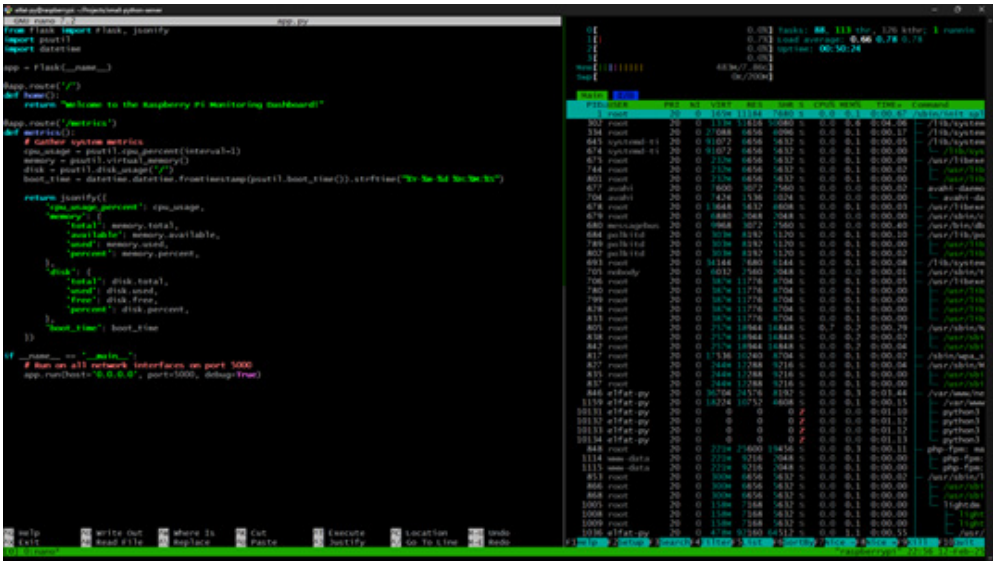
The network topology was designed as follows:

- Target (Server): Raspberry Pi 5 hosting the Flask web application.
- Attack Sources:
  - High-Performance Laptop: Used to generate high-throughput HTTP-based attacks.

- Mid-Tier Laptop: Supplementary attack source, increasing traffic intensity.
- Monitoring System: External system running Netdata for live analytics.

By ensuring a dedicated attack and monitoring environment, the study accurately measured the impact of simulated DDoS attacks on a standalone network.

FIGURE 1: DDoS Simulation Setup and Attack Execution



Attack Script and Configuration

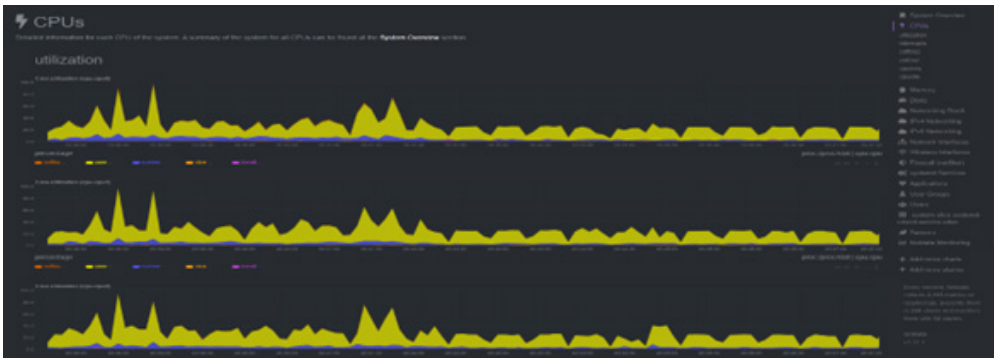
To evaluate the resilience of the Flask-based web server, we developed a custom Python-based DDoS attack script targeting the HTTP POST endpoint. The script was optimized to generate high-throughput attack traffic, simulating real-world application-layer DDoS attacks. The key parameters of the attack included:

- Target URL: Flask application's POST request handler.
- Number of Processes: Dynamically adjustable to scale attack intensity.
- Threads Per Process: Configurable to control concurrent attack instances.
- Packet Size: Varied to test different network stress conditions.
- Duration: Experiments were executed for predefined time intervals.

Each test included a baseline phase, where normal traffic conditions were recorded, followed by the attack phase, where malicious traffic was injected. After

the attack, the system's recovery behavior was observed to determine long-term performance degradation.

FIGURE 2: CPU Utilization During DDoS Testing Attack Execution and Repetition



Each experiment was repeated multiple times to ensure reliability and statistical accuracy. The following scenarios were tested:

1. Low-Intensity Attack:
- 5 concurrent attack processes
- Small request payloads (~512 bytes per request)
- Attack duration: 3 minutes

2. Moderate Attack:
- 10 concurrent attack processes
- Medium request payloads (~2048 bytes per request)
- Attack duration: 5 minutes

3. High-Intensity Attack:
- 20 concurrent attack processes
- Large request payloads (~8192 bytes per request)
- Attack duration: 10 minutes

By varying these attack parameters, we analyzed how different attack loads influenced CPU usage, memory consumption, network processing efficiency, and overall server stability.

Performance Metrics and Data Collection

During each attack simulation, key performance metrics were logged using monitoring tools. The data collection focused on:

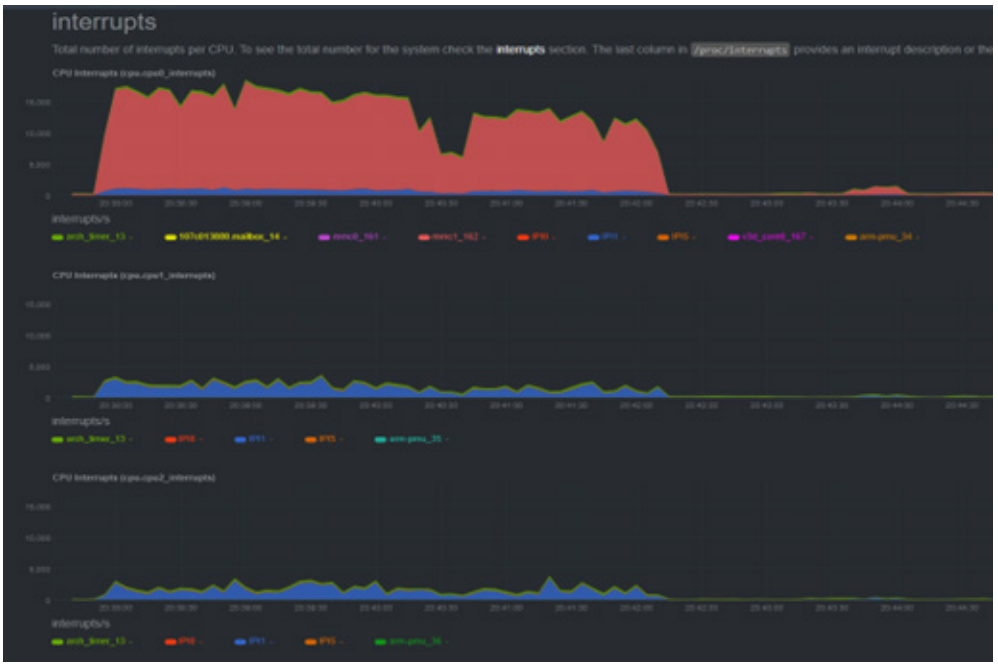
CPU Utilization

CPU performance was analyzed by observing core utilization levels. The results were visualized in Figure 1.1, where noticeable spikes indicated increased processing demand due to attack traffic. Despite transient load increases, the CPU retained the available processing headroom, suggesting resilience to sudden attack bursts.

Interrupt Processing

System-wide interruptions were monitored to detect kernel-level stress factors. Figure 1.2 presents the overall interruption rate across cores, confirming that DDoS-induced network load did not cause excessive hardware-level interruptions.

FIGURE 3: CPU Interrupts During DDoS Simulation



Network Packet Processing (Softnet Stats)

Network performance was analyzed using softnet statistics, which track how incoming packets are handled. Figure 1.3 demonstrates how successfully processed and dropped packets evolved during the attack. Minimal backlog accumulation confirmed that the network stack managed to attack traffic effectively.

FIGURE 4: Softnet Statistics During DDoS Simulation

Open Sockets and Connection Management

The number of open sockets was monitored, as shown in Figure 1.4. At the end of the attack, a sharp decline in open connections was observed, verifying proper connection termination upon manual cessation of the attack.

FIGURE 5: IPv4 Networking (Sockets and Packets) Manual Cessation of Attack

Application-Level Resource Consumption

The attack's effect on Flask web application performance was analyzed, with Figures 2.1

FIGURE 6: CPU Usage by Applications During DDoS Simulation

This panel shows the distribution of CPU utilization among various processes and application groups over time. The orange peaks, for instance, correspond to the main Flask application or Python processes responsible for handling incoming requests. Although these peaks occasionally spike, the overall CPU usage remains well below 100%, indicating that the server still has spare processing capacity. If the DDoS attack had fully saturated the CPU, we would expect to see significantly higher sustained utilization for one or more processes.

FIGURE 7: Application-Level Page Faults, Processes, and Threads During DDoS Simulation

In the top panel, the orange spikes represent minor page faults for various applications. These faults occur when a process accesses a memory page that is already in memory but not yet mapped into the process's address space. While the spikes suggest periodic bursts of memory allocation or process activity, they do not indicate a severe memory shortage or excessive swapping.

In the middle and bottom panels, we see the total number of threads and processes grouped by application. The stacked bars remain relatively stable, aside from a noticeable drop around 20:50, which correlates with the manual termination of the DDoS attack. This drop indicates that once the attack traffic ceased, the number of active threads and processes handling connections also decreased. Notably, there is no surge in processes or threads that would imply the system was forced to spawn excessive worker processes under load. Taken together, these charts reinforce the conclusion that the server, while experiencing some transient spikes in resource usage, remained capable of handling the incoming traffic without hitting critical performance limits.

System Temperature and Cooling Efficiency

Thermal stress was examined through Figure 3.1, tracking temperature fluctuations and cooling system adjustments. The system remained within safe operating limits, avoiding overheating even under peak attack loads.

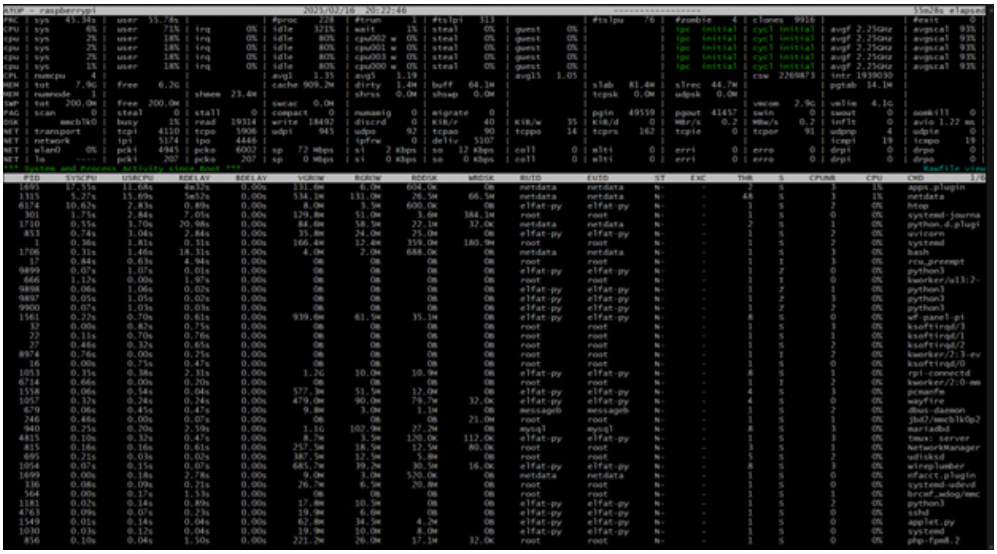
FIGURE 8: System Temperature and Fan Speed During DDoS Simulation

This figure shows the system's thermal and cooling behavior over the course of the attack. The top panel tracks CPU temperature, which experiences moderate fluctuations—rising slightly while peak activity but remaining well within safe operating limits. The second panel reflects another temperature sensor (e.g., a secondary chip or ADC reading), which also shows minor variations without any critical spikes. In the bottom panel, the fan speed remains relatively steady, with occasional brief dips or spikes. Overall, these readings suggest that while the simulated DDoS introduced additional workload, the system's cooling mechanisms were sufficient to prevent any significant thermal stress.

System Load During Attack

Final resource consumption snapshots were recorded using Atop, as illustrated in Figure 3.2:

FIGURE 9: Atop Snapshot During DDoS Testing



These measurements provided insights into overall system stability. In this snapshot, the overall CPU usage is around **50%** (47% in user space, 2.8% in system), leaving nearly half the CPU idle. The **average load** hovers around **1.5**, which is modest for a multi-core system. Memory usage stands at approximately **2.98 GB** out of **4.45 GB** total, with **no swap** in use, indicating **no critical memory pressure**.

Notably, the **Netdata** processes are among the top consumers of CPU cycles, which is typical when real-time system monitoring is active. The **Python** processes—presumably the Flask server or attack scripts—consume a smaller share of CPU, suggesting the system is not heavily stressed by the DDoS load at this moment. Additionally, there is **no indication** of excessive I/O wait or disk usage. Taken together, these metrics imply that the server remains **stable and responsive**, and the DDoS traffic has not overwhelmed its processing or memory resources under the observed conditions.

The Raspberry Pi 5 demonstrated significant resilience to HTTP POST-based DDoS attacks, successfully handling moderate traffic spikes without major performance degradation. The network stack efficiently processed attack

packets, CPU and memory loads remained manageable, and no hardware-level interruptions indicated kernel stress. These findings suggest that small-scale servers, when properly configured, can withstand moderate DDoS attacks, highlighting the importance of load balancing, traffic filtering, and rate-limiting techniques.

Future research will focus on integrating AI-driven anomaly detection and adaptive mitigation strategies to enhance DDoS resilience in resource-constrained environments.

Results

Impact of DDoS Attacks

The experiments revealed that volumetric attacks (UDP floods, ICMP floods, and large TCP packet floods) caused the most immediate and severe network disruptions. These attacks quickly saturated network bandwidth, leading to increased packet loss and delayed response times. Application-layer attacks, such as HTTP floods, had a more prolonged effect, gradually depleting server resources and causing high CPU usage due to excessive request processing.

- UDP and ICMP floods resulted in a 90%+ increase in bandwidth utilization, leading to severe packet loss.
- TCP floods exhausted system connections, increasing error rates by over 80% as legitimate requests failed.
- HTTP floods significantly increased server-side CPU consumption, affecting response latency and service availability.

Effectiveness of Mitigation Techniques

The study also tested various mitigation techniques and analyzed their ability to counteract DDoS threats. Firewall-based filtering and intrusion detection systems (IDS) were effective against basic volumetric attacks, successfully blocking over 85% of malicious traffic when configured with proper rules. However, sophisticated attacks that used randomized IP addresses and adaptive flooding techniques bypassed traditional filters.

- Rate limiting successfully mitigated moderate-scale DDoS attacks, reducing attack efficiency by 70%, but was less effective against large-scale floods.
- Application-layer defenses such as CAPTCHA-based authentication and request throttling prevented 100% of both-based HTTP floods, confirming their effectiveness in distinguishing legitimate users from automated attacks.

- AI-based anomaly detection systems showed promising results, detecting attack patterns with an accuracy of over 90%, but required significant computational resources.

The analysis indicated that a multi-layered defense approach is required to effectively mitigate modern DDoS attacks. A combination of network-level filtering, adaptive rate limiting, and AI-driven traffic analysis provides a robust security framework against evolving attack techniques.

Conclusion

This research provides a comprehensive study on Distributed Denial of Service (DDoS) attacks, their methodologies, and mitigation strategies through a Python-based simulation tool. The study categorizes DDoS attacks into volumetric, protocol-based, and application-layer threats, demonstrating their impact through real-world simulations. The results highlight the vulnerability of modern network infrastructures to large-scale attacks and the necessity of proactive defense mechanisms.

Throughout the DDoS simulation on the Raspberry Pi 5 running a Flask server, the system maintained stable performance across multiple dimensions. While CPU usage, disk activity, and network traffic exhibited transient spikes, the system remained operational without critical failures. The key conclusions derived from these experiments are as follows:

CPU and Interrupts

Although CPU usage exhibited occasional spikes during the attack, it never reached a point of complete saturation, demonstrating that the system had sufficient processing capacity to handle the increased load. The fluctuations in CPU activity suggest that while the attack introduced transient stress, Raspberry Pi 5 maintained the ability to process incoming requests without significant performance degradation. Additionally, the rate of hardware and software interruptions did not show any substantial increase, implying that the kernel was not overwhelmed by network-related events or system-level interruptions. This stability in interrupting processing indicates that the server could efficiently handle network traffic without excessive strain on its hardware components, reinforcing its resilience against moderate-scale DDoS attacks.

Network Stack (Softnet, IPv4, TCP)

Softnet statistics revealed that the network stack efficiently managed incoming traffic, with minimal packet drops or backlog accumulation. This finding suggests that the network layer was not overwhelmed, even during peak attack periods, and successfully processed the incoming requests without significant performance degradation. Additionally, TCP connections remained stable, exhibiting no major spikes or retransmissions, indicating that the transport layer handled attack-induced congestion effectively. When the attack was manually stopped, a clear and immediate drop in established sockets and processed packets was observed, signifying a controlled termination rather than a failure or forced shutdown due to system overload. These observations confirm that the server's network stack maintained operational stability throughout the attack and responded predictably upon cessation of malicious traffic.

Memory Usage and Page Faults

The server maintained stable memory usage throughout the DDoS simulation, never reaching critical limits or necessitating significant swap utilization. At no point were out-of-memory (OOM) events triggered, indicating that the system had ample available memory to process both legitimate and attack traffic. While major page faults were observed intermittently, these occurred only in moderate bursts, suggesting that memory allocation and management were functioning within normal parameters. This behavior implies that memory thrashing was not a concern, and the server was able to handle incoming traffic efficiently without excessive paging or performance degradation.

Disk I/O

Disk utilization remained low, with no indications of excessive contention or I/O bottlenecks during the attack period.

Application Metrics and Process Management

During the DDoS simulation, the Flask/Python processes exhibited periodic CPU usage peaks, reflecting the additional load imposed by the attack. However, despite these fluctuations, the application layer-maintained stability without spawning excessive threads or additional processes. This suggests that the server efficiently allocated processing resources to manage incoming traffic without reaching a point of resource exhaustion. Furthermore, when the attack ceased, the number of active threads and processes rapidly declined, indicating that the system successfully closed unnecessary connections and returned to normal operational

levels without delays or lingering resource consumption. This behavior highlights the effectiveness of the Flask application's design in handling abrupt changes in traffic while ensuring consistent performance and system responsiveness.

Thermal and Cooling Performance

Minor fluctuations in temperature and fan speed were recorded, but no critical thermal stress was observed, confirming that the system's cooling mechanisms were adequate to handle the additional load imposed by the attack.

Interpretation and Implications

The collected data suggest that under these specific attack conditions, the Raspberry Pi 5 server demonstrated resilience, avoiding major resource exhaustion or critical performance degradation.

The abrupt decline in connections and packets after manually stopping the attack suggests that the server was not forced to drop traffic due to system overload but rather responded predictably to the termination of malicious traffic.

This outcome implies that either the attack volume was insufficient to overwhelm the system, or that the server's resource headroom and configuration were adequate to sustain this level of stress.

In summary, while the DDoS simulation generated temporary spikes in CPU usage and network activity, the lack of sustained anomalies or severe bottlenecks indicates that the tested environment can handle moderate levels of malicious traffic without immediate failure. These findings provide a baseline reference for future experiments involving higher-intensity attacks, extended durations, or more sophisticated attack methodologies to further assess the system's thresholds and resilience.

By combining theoretical analysis, attack simulations, and defense evaluations, this research contributes to the growing body of knowledge in cybersecurity and DDoS mitigation. Future work in this area should focus on automated response mechanisms, AI-driven real-time threat intelligence, and blockchain-based security frameworks to further enhance the resilience of networked systems.

The insights from this study are intended to aid network administrators, cybersecurity professionals, and researchers in developing more adaptive and robust security solutions against ever-evolving DDoS threats in the digital era.

References

Akamai Technologies. (n.d.). State of the internet security report. Retrieved from https://www.akamai.com/our-thinking/state-of-the-internet-report

Al-Mashadani, A. M., & Ilyas, M. U. (2015). Distributed denial of service attack alleviated and detected using software-defined networking. International Journal of Advanced Computer Science and Applications, 6(9), 1-7.

Alomari, E., Manickam, S., Gupta, B. B., Karuppayah, S., & Alfaris, R. (2012). Botnet-based distributed denial of service (DDoS) attacks on web servers: Classification and art. International Journal of Computer Applications, 49(7), 24-32.

CERT Coordination Center. (n.d.). Vulnerability notes database. Retrieved from https://www.kb.cert.org/vuls/

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide (NIST Special Publication 800-61 Revision 2). National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Cloudflare, Inc. (n.d.). Learning center: DDoS. Retrieved from https://www.cloudflare.com/learning/ddos/

Eddy, W. M. (2007). TCP SYN flooding attacks and common mitigations (RFC 4987). Internet Engineering Task Force. Retrieved from https://datatracker.ietf.org/doc/html/rfc4987

Kalkan, K., & Zeadally, S. (2023). DDoS attack detection and mitigation using software-defined networking: Status and future directions. Computers & Security, 125, 102977.

NETSCOUT Arbor Networks. (n.d.). White papers. Retrieved from https://www.netscout.com/white-papers

OWASP Foundation. (2014). OWASP testing guide v4. Retrieved from https://owasp.org/www-project-web-security-testing-guide/v41/

The impact of urbanization and climate change on urban temperatures: a systematic analyse for Tirana city

Albana HASIMI
Institute of Geosciences, Polytechnic University of Tirana, Albania
a.hasimi@geo.edu.al
ORCID: 0009-0005-9406-9707

Blerina PAPAJANI
Faculty of Natural Sciences, University "Aleksandër Xhuvani", Elbasan, Albania

Gazmir ÇELA
Institute of Geosciences, Polytechnic University of Tirana, Albania

Elvin ÇOMO
Institute of Geosciences, Polytechnic University of Tirana, Albania

Florinda TUGA
Institute of Geosciences, Polytechnic University of Tirana, Albania

Mirela DVORANI
Institute of Geosciences, Polytechnic University of Tirana, Albania

Abstract

Some 3.5 billion people reside in urban areas, according to the WMO. The city population is growing, and it's far projected that via way of means of 2050 approximately 66% of the populace could be residing in towns and concrete areas. This increment is expected to happen not only through the increasing number of megacities, but also large and medium-sized cities with the largest urban growth. The situation changed dramatically in the twentieth century, as the rate of urban population growth increased significantly also in the Tirana city at the last decades. A statistical methodology is used to perform the required calculations and analyses related to temperatures above 35°C in meteorological data for the period 2010-2020. Application of the Statistical Methodology in the Field of Meteorology has wide applicability in the study of extreme temperature events and can help in: Forecasting heatwaves and analysing climate patterns for different periods; Assessing the impact of high temperatures on health and ecosystems, and monitoring extreme temperature events; Creating policies and risk management strategies to address the potential consequences of extreme heat on daily life, agriculture, and other sectors.

The analysis of the temperature changes revealed that the urbanization will strongly affect maximal temperature. The maximum temperature changes will be noticeable throughout the year. However, during winter and spring these differences will be particularly large and the increases could be double the increase due to global warming. Results indicate that the changes were mostly due to increased heat capacity of urban structures and reduced evaporation in the city environment. It was found that, in the future, summer weather will spread to early autumn, and winter weather will move to early spring, in Tirana

Keywords: *urban resilience; statistical methodology; maximum temperature; climate parameters; Tirana city.*

Introduction

The Sustainable Development Goal (SDG) 11 focuses on urban resilience, climate and environment sustainability, and disaster risk management. In response to the New Urban Agenda, WMO established a cross-cutting urban focus initiative through Integrated Urban Hydrometeorological, Climate, and Environmental Services for urban resilience and sustainable development. The main goal is to develop urban multi-hazard early warning systems, Integrated Urban GHG Information System (IG3IS - urban), and climate services, with the focus on

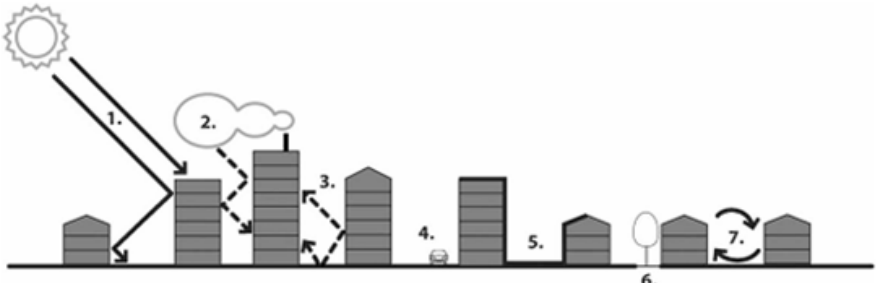
the impact-based forecast and risk-based warnings. Integrated Urban Services is an emerging multidisciplinary holistic approach, where requirements are unformalized and research and development are still in the development stage (WMO, n.d.).

Uncontrolled urbanization has caused many irreversible effects on the global biosphere, including environmental degradation, land insecurity, slum growth, water and sanitation issues, increased air pollution, land insecurity, etc. However, within appropriate limits, has several beneficial consequences, including technical and infrastructure improvements, high-quality educational and medical facilities, more significant transportation and communication, and better living standards (Humbal et al., 2023).

Climate change and urbanization are the two major drivers that can alter vegetation growth processes in the urban environment. However, the effects of these two drivers on the continuous vegetation dynamics in the urban environments are not well understood, especially at a high spatial resolution. (Li et al., 2020).

The relationship between climate and city is reciprocal: the climate influences the ways in which the city space is being used and the climatic performance and needs of buildings. In its turn, the city influences its climate. On the large scale the city as a whole modifies the regional climate conditions, which results in differences between the city and its surrounding (rural) area in cloud cover, precipitation, solar irradiation, air temperature and wind speed (Kleerekoper et al., 2012). Some of the causes, as shown in Figure 1, include absorption of short-wave radiation, air pollution that absorbs and re-emits longwave radiation, obstruction of the sky by buildings reducing longwave radiative heat loss, anthropogenic heat from combustion processes, increased heat storage by building materials with high thermal admittance, reduced evaporation due to waterproofed surfaces and less vegetation, and decreased turbulent heat transport from reduced wind speed.

FIGURE 1: Causes urban heat islands(Kleerekoper et al., 2012).



This study is the first of its kind, in terms of using Albanian meteorological measurement data. Was investigated the impacts of climate change on the urban heat island (UHI) and the number of very hot (maximum temperature >35°C). Downscaling models based on the simple systematic statistical technique were developed for each calendar month for projecting the number of very hot days in Rinas, Tirana (Hasimi & Çomo, 2022).

Materials and Methods

Analyses and Calculations Performed

The used database is from Rinas meteorological measurements and is open data. All statistical analyses were performed using an algorithm built in Python.

The meteorological data of Rinas station, was filtering before to conduct several calculations and in-depth analyses to identify and analyse the periods of extreme heat for each year of the decade under review:

a) Duration of Temperatures Above 35°C in Rinas: The total duration of the period was calculated as the time interval from the first to the last day with temperatures above 35°C, for each year.
b) Maximum Duration of Continuous Period: The method of grouping and identifying continuous periods with uninterrupted days where the temperature exceeded 35°C was used. The longest continuous period with temperatures above 35°C was calculated, and the days that constituted this uninterrupted period were identified.
c) Number of Cases with 2 or 3 Consecutive Days above 35°C: This analysis was used to identify periods with 2 or 3 consecutive days of temperatures above 35°C, and the number of such periods was calculated for each year.
d) Analysis of the Sum of Progressive Temperatures above 35°C: For each year, the sum of temperatures exceeding 35°C was calculated, providing an overview of the total heat accumulated during periods with temperatures above 35°C.

1. Summary of Analyses for Each Year: For each year, we performed:

The total duration from the first to the last day.

The maximum duration of the period without interruption with temperatures above 35°C.

The number of periods with 2 or 3 consecutive days above 35°C.

The sum of progressive temperatures for each year.

2. Analysis for Each Month of the Year: We also created an analysis to show the number of days with temperatures above 35°C for each month of the year.

Discussion and Conclusions

The Institute of Statistics (INSTAT) estimated the population of the municipality of Tirana at 598,176, with a unit density of 9,313/km², according to the 2023 census (*2023 Albanian Census*, 2024). However, according to the 2011 census, for the first time, the urban population exceeded the rural population. The resident population in urban areas was 53.5 percent, while 46.5 percent of the population lived in rural areas (*Census-of-Population-and-Housing*, n.d.). This significant demographic change is closely linked to the transformation of the city (fig 2). Table 1 presents data on population changes

TABLE 1: Population changes of Tirana city

Year	Population	± % of population
1989	238 057	+ 26.0%
2001	341 453	+ 43.4%
2011	418 495	+ 22.6%
2023	389 323	− 7.0%

Observed meteorological data from Rinas station were used to calculate the long-term temperature trends above 35 °C. These observations were also used to evaluate the model performance. This was done by calculating monthly, 3-month and each year for 10-year averages and to compare with the norma temperatures acording Klimate Atlas of Albania (Grup, 1984)

FIGURE 2: Satelit image of Tirana City 2010 and 2020

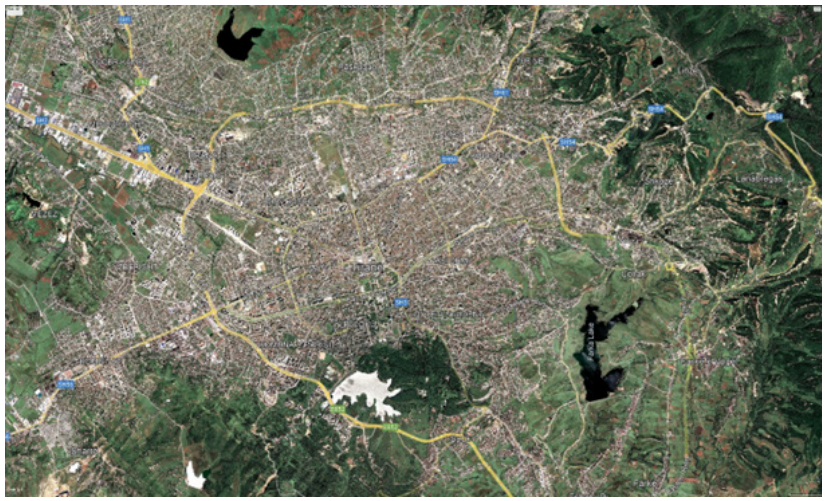


FIGURE 3: Duration of Temperatures above 35 °C

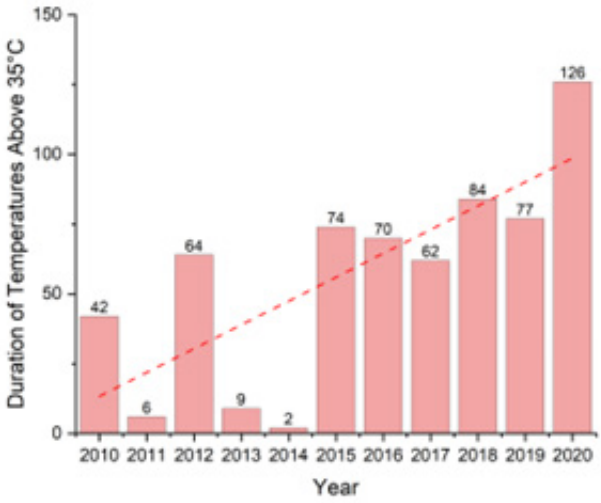


Figure 3 graphically illustrates the number of days with maximum temperatures exceeding 35°C. The dotted line clearly shows the upward trend. From Climate of Albania, for the Rinas meteorological station, we have some data on the climate of Albania, but not statistically analyzed as presented in our study. (Grup, 1975)

When making the comparison, the fundamental change in the microclimate of the city of Tirana becomes evident, partly as a result of the urban transformations it has undergone in the last 10 years. The city now has fewer green spaces and more tall buildings.

TABLE 2: The start and the end date of days above 35°C temperatures during 2010-2020 on Rinas

Year	Start Date	End Date	Days Above 35°c	Duration (Days)	Max Streak	2 Days Streaks
2010	16/07	27/08	3	42	1	0
2011	20/08	26/08	5	6	3	2
2012	23/06	26/08	24	64	6	6
2013	31/07	08/09	8	9	6	2
2014	08/12	14/08	3	2	3	1
2015	07/07	19/09	40	74	15	7
2016	17/06	26/08	17	70	3	4
2017	25/06	26/08	33	62	13	5
2018	06/08	31/08	15	84	6	3
2019	15/06	31/08	25	77	7	4
2020	14/05	17/09	37	126	9	10

During heat waves, temperatures in cities can build up day by day when there is no cooling wind or sufficient green spaces to provide relief. As shown in Table 2, there is a significant year-by-year increase in the number of days with maximum temperatures exceeding 35°C. However, what is even more remarkable is that the duration of these hot days is progressively extending, making heat waves more impactful for the city of Tirana (Hasimi & Çomo, 2022).

For the decade under review, the record stands until 2020, which had the highest number of days with temperatures exceeding 35°C. These high temperatures were recorded as early as May—an unusual occurrence for the Mediterranean climate, according to historical records (Çela* et al., 2025). Additionally, September marked the final month of the extremely hot season, with a maximum temperature of 35°C.

TABLE 3: Number of days per month with temperatures above 35°C

Year / month	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
May	1										3
June			1				4	3	1	7	
July			8	1		19	7	13	2	7	12
August	2	5	15	7	3	15	6	17	12	11	14
September						6					8

It appears that there is a shift in temperature patterns, with August now being the month with the highest number of days over 35°C, instead of July, as historical data suggests for Rinas meteorological station. Several factors could explain this shift: Over time, climate change has been shifting weather patterns globally. This might have caused temperature extremes, including heatwaves, to move to different months. It's possible that the heat intensity and frequency of high temperatures are increasing in August.

Also, local changes in Tirana City: Changes in land use, urbanization, or even changes in local atmospheric patterns could contribute to the shift. For instance, urban heat islands or altered wind currents could be making August warmer than in the past.

Another key indicator analysed in this study is the duration of consecutive days with maximum temperatures exceeding 35°C, which directly impacts the quality of life in the city. These results are shown in Table 1. Even for this indicator, the most significant year is 2020, with 10 events lasting up to a maximum of 9 days. Such meteorological conditions have a broader impact on the economy, energy demand, human health, and other sectors.

References

1.*2023 Albanian census*. (2024). Institute of Statistics Albania.

2.Çela*, G., Gjoni, A., Zorba, P., & Hasimi, A. (2025). *Long-term trends in average air temperature in the Central Lowland Mediterranean Climate Zone of Albania*. 4th International Conference on Contemporary Academic Research.

3.Census-of-population-and-housing. (n.d.). instat. https://www.instat.gov.al/en/themes/censuses/census-of-population-and-housing/

4.Grup, A. (1975). *Klima e Shqiperise*. Akademia e Shkencave.,.

5.Grup, A. (1985). *Klima e Shqiperise*. Akademia e Shkencave.,.

6.Hasimi, A., & Çomo, E. (2022). *Karakteristikat kryesore mbi regjimin e temperaturave ekstreme për Tiranën për periudhën 2017-2021*. *52*(2), 24–34.

7.Humbal, A., Chaudhary, N., & Pathak, B. (2023). Urbanization Trends, Climate Change, and Environmental Sustainability. In B. Pathak & R. S. Dubey (Eds.), *Climate Change and Urban Environment Sustainability* (pp. 151–166). Springer Nature Singapore. https://doi.org/10.1007/978-981-19-7618-6_9

8.Kleerekoper, L., Van Esch, M., & Salcedo, T. B. (2012). How to make a city climate-proof addressing the urban heat island effect. *Resources, Conservation and Recycling*, *64*, 30–38. https://doi.org/10.1016/j.resconrec.2011.06.004

9.Li, D., Wu, S., Liang, Z., & Li, S. (2020). The impacts of urbanization and climate change on urban vegetation dynamics in China. *Urban Forestry & Urban Greening*, *54*, 126764. https://doi.org/10.1016/j.ufug.2020.126764

10.WMO. (n.d.). *Sustainable cities and communities*. WMO.

Heavy machine parts measurement through deep learning

Sara BALLKOÇI
European University of Tirana, Faculty of Engineering, Informatics and Architecture, Department of Informatics and Technology, Tirana, Albania

Alba ÇOLLAKU
European University of Tirana, Faculty of Engineering, Informatics and Architecture, Department of Informatics and Technology, Tirana, Albania

Ardiana TOPI
European University of Tirana, Faculty of Engineering, Informatics and Architecture, Department of Informatics and Technology, Tirana, Albania

Shahina BEGUM
Malardalen University, Vasteras, Sweden

Shaibal BARUA
Malardalen University, Vasteras, Sweden

Emmanuel WEITEN
Volvo Construction and Equipment, Eskilstuna, Sweden

Abstract

Operational continuity of machinery involves continuously monitoring machinery parts to prevent malfunctions. Recently, it has gained popularity in the heavy industry due to its potential to ensure maintenance and address potential malfunctions before they occur. This project focuses on advancing the "Volvo undercarriage wear inspection and maintenance program." The core of this study is the wear and tear inspection process of the undercarriage parts of Volvo's excavators and it investigates the implementation of deep learning and machine learning techniques, focusing on detecting the undercarriage part of the machine and measuring its deterioration while also aiming to minimize associated costs and labor time. The research starts with a comprehensive collection and preparation of the dataset, ensuring its validity for efficient training while addressing data quality and quantity limitations. A thorough examination and evaluation of the Mask R-CNN model for detecting and segmenting objects is conducted, followed by applying OpenCV for extracting measurements and implementing a template-matching model with a VGG16 network for image classification. The thesis concludes by training and evaluating the Mask R-CNN model three times, showcasing its promising ability to detect and segment the undercarriage part with an accuracy of up to 83.47%. The template matching approach achieved an accuracy of 16.67%, while the OpenCV method demonstrated promising capabilities with an error margin of ±0.5mm. These results indicate that inspection efficiency and accuracy could significantly increase, leading to more timely and cost-effective maintenance decisions. Finally, a validation of the approach is applied and presented in an industrial case study provided by Volvo.

Keywords: *Deep Learning, Computer Vision, Convolutional Neural Network, Mask R-CNN, Instance Segmentation, Object Detection, Image Processing, Data Preprocessing, Data Augma Augmentation, Feature Extraction*

Introduction

In today's fast-evolving industrial world, companies like Volvo Construction promote a more sustainable and environmentally friendly future. Volvo Corporation, a leader in this movement, has long been committed to environmental sustainability and corporate social responsibility. It strives to reduce its ecological footprint while offering innovative solutions that drive growth and prosperity. This commitment to sustainability is the foundation for this thesis proposal with the primary objective of digitalizing the undercarriage parts inspection process. The

existing undercarriage wear inspection is a complex process that faces numerous challenges, including the need for specialized equipment, precision issues, and manual data entry. These challenges increase the risk of errors and consume valuable time and resources. Given that Volvo's main goals are cost-effectiveness and time efficiency, a digitalized inspection process is needed to ensure that machinery parts are regularly inspected and replaced as they deteriorate. Essential for this research is Mask R-CNN, an advanced deep learning architecture that enhances object detection through pixel-level instance segmentation (Potrimba, 2023). By generating a pixel-level mask of the undercarriage part, we can employ various methods to determine whether the UC part has deteriorated and needs replacing. One of the approaches is using OpenCV, a library designed for real-time computer vision and machine learning application (L. Zabulis, 2022), especially for tasks such as machinery inspection in industries, which is well-suited to our problem. Template matching is another technique that identifies small portions of an image corresponding to a template image (Wikipedia, 2023), mainly used for tasks such as image classification. This technique is beneficial for classifying our images as worn out or not. By leveraging these three techniques, a promising digitalized solution can be employed to Volvo, aligning with their cost-effectiveness and time-efficiency goals. This thesis will examine only one undercarriage part, the sprocket (Forestell, 2024). The primary focus of this study is training a Mask R-CNN model on a customized dataset, specifically consisting of images of the sprocket. Based on instance segmentation, Mask R-CNN excels at creating a precise mask for objects, effectively separating the region of interest from the background. Our research indicates that Mask R-CNN outperforms YOLO in terms of accuracy and precision, particularly when detecting each sprocket's teeth on heavy machinery. Subsequently, the generated mask from the model is utilized to assess whether the sprocket is deteriorated. To achieve this, OpenCV is applied to extract measurements from the mask, and a template-matching model is used to classify images as either worn out or not. The proposed approach aims to digitally collect measurements from the sprocket by significantly reducing cost and labor time. The proposed solution has been validated and verified using real-world data from Volvo.

Literature Review

Deep Learning

Deep learning has emerged as a study topic in recent years, driven by the rapidly expanding demand for learnable robots capable of addressing a wide range of complicated problems. The term "deep learning" describes a group of algorithms

built on artificial neural networks specially designed to handle unstructured data, including text, audio, video, and images (Deshpande, 2019). Deep learning (DL) is a subset of artificial intelligence (AI) and machine learning (ML), defined by the usage of neural networks with three or more layers, it enables machines to learn from past experiences autonomously. DL is viewed as an AI function that simulates how the human brain processes information. The term "Deep" in deep learning methodology refers to multiple levels or stages of data processing to create a data-driven model (I.H.Sarker, 2021). As previously stated, deep learning involves the use of multi-layered neural networks. These multi-layered neural networks attempt to imitate the human brain's learning patterns, allowing computers to analyze and learn from massive amounts of data (Awan, n.d.).

Mask Region-based Convolutional Neural Network

Mask R-CNN expands on Faster R-CNN by adding a third output branch that creates masks, thus helping capture more precise spatial features. This improvement adds pixel-to-pixel alignment, a crucial addition missing in Faster R-CNN.

Mask R-CNN architecture

1. Backbone: The model's architecture includes a pre-trained convolutional neural network for feature extraction, commonly a ResNet50 or ResNet101. The first layers detect features of low levels, such as edges and corners, whereas the second and after layers detect features of higher levels (e.g., bicycles, planes, and dogs). When going through the backbone network, the images are converted from 1024x1024px x 3 (RGB) to a feature map of shape 32x32x2048 (K. He, 2017). This feature map will serve as input for the subsequent segmentation phases. The Feature Pyramid Network (FPN) enhances the backbone and represents things at several scales. FPN ameliorates the traditional feature extraction pyramid by incorporating a second pyramid that funnels the high-level features from the first pyramid down to the lower levels. This allows features to be accessed at every level, both higher-level and lower-level features (K. He, 2017).
2. Region Proposal Network (RPN): Region Proposal Network is a compact neural network that examines images using a sliding-window method and finds regions containing objects. The areas the RPN examines are named anchors, which, as shown in Figure 6, are boxes distributed over the image. The RPN rapidly scans many anchors thanks to the sliding window, which is handled by the convolutional nature of the RPN and allows for the simultaneous examination of all regions (typically on a GPU machine). Instead of scanning the image directly, RPN examines over the backbone

feature map, allowing for efficient reuse of the extracted features and avoidance of duplicate calculations. Using these adjustments, the RPN runs at approximately 10 ms (S. Ren, 2016). For each anchor, the RPN creates two outputs:

- Anchor Class: Foreground and background classes comprise the Anchor Class. According to the foreground class, that box probably contains an item (S. Ren, 2016).
- Bounding Box Refinement: The positive foreground anchor may not be precisely centered over the object. To improve the anchor box's fit on the object, the RPN calculates a delta (% change in x, y, width, and height) (S. Ren, 2016).

3. ROI Classifier and Bounding Box Regressor: This stage generates two outputs for each ROI (K. He, 2017):
   - Class: is the class of the object in the ROI. The deep network can classify regions into specific classes (bicycle, dog, balloon,...etc.). It also generates a background class, which discards the ROI. • Bounding Box Refinement: Later on, this is used to fine-tune the bounding box's position and dimensions to enclose the item entirely. ROI Pooling Variable input sizes are difficult for classifiers to handle. Usually, they demand a set amount of input. However, the ROI boxes may differ in size due to the bounding box refinement phase in the RPN. ROI pooling is useful in this situation. Like cropping and resizing a portion of an image, ROI pooling involves part of a feature map being cropped and then resized to a defined size. The ROI Align approach, proposed by the authors of Mask R-CNN (K. He, 2017), involves sampling the feature map at different places and using a bilinear interpolation.

OpenCV

Library OpenCV (open-source computer Vision collection) is a collection of programming functions designed primarily for real-time computer vision and machine learning applications. The library is cross-platform and available as free and open-source software under the Apache Licence 2. Since 2011, OpenCV has supported GPU acceleration for real-time operations (OpenCV, 2024). OpenCV was initially intended to provide a standardized infrastructure for computer vision activities. Still, it has since played an essential role in advancing the integration of machine perception into commercial goods. Notably, the Apache 2 license promotes accessibility and adaptability, making it easier for enterprises to use and modify. OpenCV has approximately 2500 optimized algorithms and covers many traditional and cutting-edge computer vision and machine learning techniques. These algorithms provide various functions, including face

detection and recognition, object identification, human activity classification in movies, camera movement tracking, and 3D model extraction (K. He, 2017). Furthermore, OpenCV is important in image stitching, 3D point cloud generation, and augmented reality application development. Its large user base exceeds 47 thousand people, and an estimated download count of over 18 million demonstrates its widespread use in various industries. Major organizations such as Google, Microsoft, Intel, and countless startups rely heavily on OpenCV for their projects. The library's applications range from street view picture stitching and surveillance video intrusion detection to robot navigation and product inspection in factories worldwide. OpenCV has interfaces for C++, Python, Java, and MATLAB, and it supports various operating systems, including Windows, Linux, Android, and macOS (OpenCV, 2024).

Template Matching

Template matching is a method used in digital image processing to identify small portions of an image that correspond to a template image. Applications of this technology include edge detection in photos, mobile robot navigation, and industrial quality control (Wikipedia, 2023). The feature-based template matching method uses deep neural networks such as Convolutional Neural Networks (CNNs) like VGG, AlexNet, and ResNet to extract visual properties, including shapes, textures, and colors. These networks generate features for matching at hidden layers by producing vectors with picture categorization information. Robust and efficient, this approach can handle light changes, background clutter, and non-rigid transformations (Wikipedia, 2023). In contrast, the template-based method works well when the templates fully depict the matched image or don't have any distinguishing characteristics. To produce multi-scale representations from preprocessed images, it is necessary to reduce the search space to achieve effective matching. The curse of dimensionality in machine learning datasets can be alleviated, and the number of sampling points can be reduced with the help of this technique (Wikipedia, 2023).

Related Work

Mask R-CNN with custom dataset

Instance segmentation is challenging as it involves accurately recognizing all objects in an image and precisely segmenting each instance. Several instances of segmentation-based deep learning techniques have been proposed recently. The YOLOV3 object detection technique, which combined candidate bounding box

prediction and feature extraction into a single deep convolutional network, was first presented by Redmon et al. (J. Redmon and A. Farhadi, 2018). He et al. (K. He, 2017) introduce an extension of the Faster R-CNN framework by adding a segmentation mask prediction branch to improve the accuracy of object instance segmentation. This method efficiently accomplishes precise segmentation at the pixel level, beating previous approaches on benchmarks such as COCO, by using a tiny, fully convolutional network to each Region of Interest (ROI) (K. He, 2017). Integrating Generative Adversarial Networks (GANs) with instance segmentation models represents a unique technique for improving instance segmentation accuracy, as presented by Le et al. (Q. H. Le, 2021). This study substantially alters the Mask R-CNN framework by integrating a discriminator network that assesses the quality of segmentation masks created by the segmentation network, which is conceived as a generator. They move from pixel-based to feature-based processing by using the segmentation network as a generator and adding a discriminator that assesses mask quality. This modification leads to improved segmentation performance and more stable training dynamics, especially when handling complicated images with various object forms and a lot of clutter (Q. H. Le, 2021). Their approach proves the usefulness of adversarial loss in doing away with the requirement for domain-specific tuning by exhibiting notable improvements in defining crisp boundaries and detailed object features across various applications, including autonomous driving, cellphone recycling, and medical image analysis. Zhang et al. (C. Zhang, 2022) proposed another instance segmentation model for steel defect detection based on the traditional Mask R-CNN model. To improve the accuracy of the Mask R-CNN model, the authors replaced the feature extraction network with a more efficient and robust EfficientNet for extracting features of different scales. Also, a CBAM module was added to the mask branch to enhance the quality of mask prediction. Several experiments were conducted on the Severstel steel defect dataset, resulting in improved accuracy and efficiency (C. Zhang, 2022). Sun et al. (G. Sun, 2022) proposed a new technique for cropping and extracting information from images based on an improved Mask R-CNN model by incorporating the Softer NMS algorithm. This paper creates the backbone network for feature extraction and target candidate region generation by combining ResNet50 and FPN. This method removes unnecessary anchor frames, optimizes the feature pyramid network's (FNP) structure, and increases crop detection accuracy (G. Sun, 2022).

Template matching for detecting defects

Yuan et al. (W. Yuan, 2023) propose a defect detection method for detecting defects on photolithography masks, which present a significant challenge regarding their size from 1 to 2 pixels. The proposed approach combines template matching in

spatial and frequency domains for accurate registration, minimizing error from registration deviations (W. Yuan, 2023). The experiment also includes a variational model and a primal-dual optimization algorithm to compute the point spread function. The last step of the approach is comparing the gray values between the sample and the modified template images, using threshold extraction to identify the defect areas, a technique proven effective through testing (W. Yuan, 2023). For detecting defects on personalized printings, a new method called secondary template matching was introduced by Ma et al. (B. Ma, 2017) as the complex and irregular surface of the printings presents challenges while using conventional template matching algorithms. The method includes aligning the image under inspection with a template image to identify ROI (region of interest). After that, a four-threshold algorithm separates the image into foreground and background. Finally, the secondary template matching algorithm is applied separately to identify defects, resulting in effective defect detection on personalized printings (B. Ma, 2017).

Object Measurements Using Computer Vision

OpenCV (Open Source Computer Vision Library) is an essential tool for computer vision, extensively used for object measurement across various industries. An example of the application of OpenCV is automating inspections in modern manufacturing, aiming for Industry 4.0. The authors Zabulis et al. (L. Zabulis, 2022) discuss using a CV system to measure the length of objects as they move along a conveyor. The method includes image segmentation using a convolutional neural network, custom contour analysis, and the least square method to determine the midline of wooden planks. The experiment was evaluated using a dataset of wooden planks from an actual EURO pallet. With a length measurement accuracy of 1mm and a processing time of 0.97 seconds, the experiment confirmed to function as anticipated (L. Zabulis, 2022). Another important aspect of computer vision in today's industries is the real-time detection and measurement of objects. The authors Othman et al. (N. A. OTHMAN, 2018) introduce a refined method for object detection and measurement in real-time video streams. Their proposition includes using OpenCV libraries that leverage canny edge detection and dilation and erosion processes. The experiment consists of four essential steps: detecting the objects using canny edge detection, applying dilation and erosion, identifying and organizing contours, and measuring the dimensions of the objects (N. A. OTHMAN, 2018). The tools used to deploy this experiment are a Rasberry Camera, a Rasberry Pi3, and an OpenCV library. The results of this novel technique had a successful rate of approximately 98% in measuring the objects' size (N. A. OTHMAN, 2018).

Methodology

Literature Review

A systematic literature review will be conducted using databases such as Google Scholar, IEEE Explore, and ACM Digital Library, alongside source materials provided by Volvo. The thesis will use critical terminology related to Volvo's heavy machinery, Machine Learning, and fault detection using image processing, Convolutional Neural Networks, and Computer Vision. The study aims to identify existing methodologies, algorithms, and techniques for object detection and degradation or deterioration prediction.

Data Collection and Preprocessing

Volvo Construction will give us access to its databases for data collection, providing us with the necessary data for the research. The database consists of diverse images from various machine lifecycles and wear stages. After data collection, the images will be annotated and prepared for the training phase.

Mask R-CNN Model Implementation and Training

Development phase: design and construct the Mask R-CNN model as the suitable algorithm for object detection and instance segmentation due to its dual capabilities in object detection and pixel-level instance segmentation, which are critical for accurately assessing the condition of machinery parts. Mask R-CNN's adaptability allows us to customize the model to meet the unique needs of our dataset, which eventually results in a more precise and dependable answer (K. He, 2017).

Training phase: A transfer learning technique will refine the pre-trained model on the Coco dataset, significantly reducing training time and enhancing the model's ability to generalize data unique to Volvo. This approach is a vital part of our methodology, ensuring the model is well-equipped to handle the specific challenges of our research.

Testing on Unseen Data

Evaluate the trained model's performance on unseen images.

Measurements extraction using OpenCV

After generating masks from the trained model, OpenCV will retrieve measurements. This is an essential step of the research, requiring accurate measurements beneath the created masks. Integrating these two techniques, OpenCV and Mask R-CNN is ideal for creating a reliable and effective inspection system.

Template matching implementation using VGG16

We will use the VGG16 pre-trained network and a template-matching approach to identify worn-out photos. his classification step will facilitate accurate wear condition identification

Results Analysis

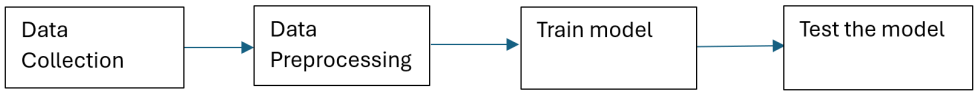
The results obtained from the experiments will be analyzed to evaluate the proposed solution's effectiveness and accuracy. The analysis will examine performance metrics such as confusion matrix, average precision, and mean average precision for the Mask R-CNN model, the precision of measurements obtained using OpenCV, and the classification accuracy of the template matching approach with VGG16.

Discussion and Conclusion

The data and observations gathered during the research project will be thoroughly analyzed and discussed. he proposed software solution's advantages, potential drawbacks, and future work will be discussed, and comparisons with current solutions will be made

Methods and Analysis

The method used is divided into two sections: the first involves training and evaluating the Mask R-CNN model, a cutting-edge approach to segmentation. The second section focuses on extracting measurements from images to calculate the wear stage and predict future degradation of the machinery. The first section involves the steps below:



Data Collection

The first step we took while implementing our thesis was data collection. As a crucial collaborator in this research, Volvo Corporation has played a significant role by providing us with the dataset that forms the foundation of our implementation. The dataset provided by Volvo consists of 150 images and 30 videos capturing various excavator models at different life cycle stages. Particular emphasis is placed on images showing machines in various levels of wear and tear. This includes information gathered over time via their inspection procedures. For the development of this thesis, we are focused on model EC210B, which offers four distinct machine operating hours (4894, 2750, 3969, and 3902 operating hours). As part of our comprehensive approach, we collected images from machines in new condition, with 0 operating hours, conveniently available in Volvo's office. We tried to take as many pictures as possible from different angles and distances. However, it soon became clear that the data provided was insufficient. In response to limited data availability, approximately 4000 images were extracted from provided videos using the OpenCV library, providing a more extensive image dataset.

Data Preprocessing

Our first step in developing the thesis was annotating the data/ images we had secured from Volvo. Image annotation is a crucial component of our dataset preparation procedure while using the Mask R-CNN algorithm because it provides ground truth data that the model uses during training to learn to detect and segment objects accurately and support our primary goal of segmentation.

There are multiple tools that you can use for data annotations, such as: LabelMe, RectLabel, LabelBox, VGG Image Annotator (VIA COCO UI). We used the LabelME tool to annotate the images. Through this thorough process, we annotate and label the sprocket teeth to provide the necessary training data for our model. These annotations will later be used to obtain measurements and calculate the wear stage of the UC part, a crucial step in our research. Selecting the appropriate amount of samples for the training, validation, and testing datasets was a crucial phase in developing our thesis. Numerous considerations influenced this choice, including the size of Volvo's dataset and the requirement to guarantee an adequate amount of data for thorough model testing and training. Initially, the dataset comprised images and videos of various excavator models at different life cycle stages. However, because there was a shortage of data, we used the OpenCV package to extract about 4000 images from the given videos to increase the dataset. This resulted in a much larger and more diverse dataset, guaranteeing a more thorough depiction of the excavator parts' wear and tear situations. Subsequently, the annotated dataset was partitioned as follows:

- *Training Set:* 290 images were used to train the Mask R-CNN model. This set is the primary source of information that the model uses to identify patterns and characteristics connected to the sprocket teeth.
- *Validation Set:* For validation, we employed 70 annotated photos. This subset helps avoid overfitting by enabling the model's hyperparameters to be adjusted and offering an intermediate performance check.
- *Testing Set:* Comprised of 70 unseen images for the model, allocated to evaluate the trained model.

The dataset was split into an 80% training set and a 20% validation set, with the testing set being the same size as the validation set. Utilizing transfer learning eliminates the need for an extensive dataset to train our deep learning model. This approach leverages a pre-trained weights file already trained on the Microsoft Everyday object in context (MS COCO dataset), which includes around 80 object classes. Consequently, the pre-trained weights have already learned many features, making it easier for the model to recognize the teeth of the sprocket. Following the preprocessing steps, this dataset provides the fundamental framework for the initial stage of creating and assessing the optimal Mask R-CNN model utilizing the dataset.

We trained our model starting from the COCO weights file. The COCO dataset, designed to advance image recognition, contains approximately 80 common object categories, with 82 of them having more than 5,000 labeled instances. It has 2,500,000 labeled instances in 328,000 images and fewer categories but more for each category. By leveraging this dataset, we enhanced the accuracy and efficiency of our model, a crucial step in our research process.

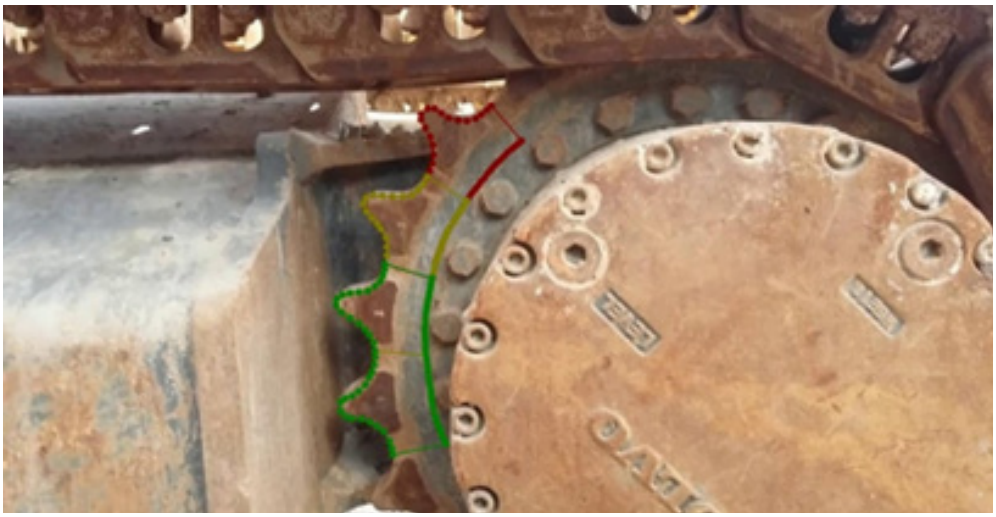
Mask R-CNN implementation

We implemented Mask R-CNN using Python 3.8.18, Keras, and TensorFlow 2.4.0, based on the Feature Pyramid Network (FPN) and ResNet101 backbone. This setup is essential for capturing high-resolution details at multiple scales, particularly in contrast to our photos' intricate and diverse backgrounds. It is also required for accurately recognizing and dividing the excavator's teeth' various shapes and sizes. Mask R-CNN includes a pre-trained CNN for feature extraction, usually using ResNet50 or ResNet101. Our implementation of Mask R-CNN uses ResNet101 over ResNet50 because it offers a more profound layer structure, and it can learn more complicated characteristics and enhance detection accuracy in complex images. This is useful for processing the different-sized and shaped teeth of the excavator against highly textured and textured backgrounds. Our dataset includes annotated images of the excavator's teeth taken from multiple angles and in varied lighting circumstances during training. This ensures the model's robustness and reliability in real-world operational settings.

The model is fine-tuned using this dataset, a process that adapts the pre-trained MS COCO dataset to the characteristics of our task, such as detailed segmentation and precise localization of each tooth for practical wear analysis and maintenance prediction. The ROI Align layer enhances the model's ability to resolve alignment problems in previous models by carefully extracting features from every suggested region. Mask R-CNN's dual-head system allows each tooth to be detected simultaneously and precisely segmented. One head is in charge of bounding box regression and object classification, and the other is responsible for mask prediction. This segmentation capability is crucial for applications requiring precise delineation, such as automated wear analysis or predictive maintenance duties, since it provides comprehensive outlines of each tooth through binary masks.

By leveraging the pre-trained weights from the MS COCO dataset, we sped up the initial training process, reducing the need for a large volume of training images and computational resources. This method conserved a great deal of processing power and time. It gave our model a wealth of prelearned features from the outset, improving its capacity to generalize from the small amount of task-specific training data. Pre-trained models have several advantages over training from scratch, especially regarding training efficiency and initial accuracy. They have learned features usually applicable over an extensive range of pictures, thereby the network can quickly adjust to the unique features of new datasets with little extra input.

FIGURE 1: The process of annotating the images



Training phase

The training phase for the Mask R-CNN model was conducted using a laptop equipped with an Intel Core i5-6300U CPU @ 2.40GHz 2.50 GHz supported by 8GB of RAM. The training was with 360 images split into 290 images for train 70 for val, and it was run for approximately 86 hours (3 days and 14 hours).

Template matching using VGG16

In this approach, we are focused on assessing whether an object, in this case, a tooth, is in good condition or worn by comparing the similarity of two images given as input. We chose template matching because it is widely implemented in many research papers for comparing parts of a source image against a template image, which may be an image of an object, and it serves as a template to detect similar objects in the source image. It compares items to industry standards and identifies flaws. For extracting features from the photos, we used VGG16. This pre-trained convolutional neural network has been initially trained on the ImageNet dataset, a large visual dataset that includes around 20000 object classes and more than 14 million annotated images. It utilizes a technique called deep template matching, using a pre-trained VGG16 model. This model can classify images based on their similarity to a reference image. Firstly, a reference image is loaded and preprocessed using preprocessed API in Keras for VGG16. Features from the reference image are extracted using the VGG16 model. Then, the new image,

which needs to be checked for quality, is loaded. The image features are extracted using the same VGG16 model. Table 4 shows the default parameters of VGG16 network. We used the same default parameters for our implementation as they applied to our solution. The only parameter that we changed was the threshold.

Extracting Measurements from OpenCV

As part of achieving our goal of providing a rough estimate of the wear of an excavator's teeth, after the model recognizes the teeth, it runs a script that uses OpenCV to measure the height of a tooth. The two main libraries of the script are OpenCV, a library dedicated to computer vision tasks, and numpy, which is used for numerical operations and, in our case, for distance calculations. To accurately measure the dimensions of the tooth from an image, we used a pixel-to-millimeter conversion method based on the information in the blueprint provided to us by VOLVO. First, we identified the height of the tooth (22 mm) as our reference measurement. Using an interactive script, we measured this height in the image, 160.86 pixels. By dividing the pixel measurement by the known physical height, we calculated the Pixels Per Millimeter (PPM) ratio, which was approximately 7.31 pixels/mm. With the PPM established, we could measure any distance in the image and convert it to millimeters. Then, we wrote another script that allowed us to view the distance in pixels between these points and convert this pixel distance to millimeters using the PPM ratio. The script also annotated the image with pixel and millimeter measurements, ensuring clear visualization and accurate dimensional analysis. This method provides a reliable means of translating pixel measurements into real-world dimensions for precise analysis.

Results

Instance Segmentation

The training period was used to fine-tune the model's capacity to recognize and categorize the "tooth" component of excavator undercarriages using picture data. The session was carefully planned to address the faults of the preceding one, with particular objectives established to raise the model's accuracy, precision, and recall. We examined the confusion matrix, precision-recall curves, and mAP in various circumstances and contexts to make specific conclusions about the model's efficacy and dependability in practical situations. AP at IoU=50 is a metric that evaluates the precision of the model when the predicted bounding boxes overlap the ground truth boxes by at least 50%. Meanwhile, mAP is used to evaluate the performance of object detection models across multiple classes and IoU thresholds, and a higher mAP value indicates better performance. A lower mAP indicates lower model performance. These assessments provide insight into

the model's capabilities and serve as a roadmap for upcoming changes to enhance its functionality. The following subsections thoroughly explain each training step and show how the model's performance changed over time as it was refined.

- Confusion matrix

The confusion matrix analysis shows that the model's predictions were easily understood. The model obtained 101 True Positives (TP) for the "tooth" class, which means it correctly detected 101 instances of teeth. There were also 20 False Negatives (FN), in which the model failed to detect teeth that were present, and 24 False Positives (FP), in which the model mistakenly classified nontoothed regions as teeth. This resulted in a precision of 80.80% for the "tooth" class, demonstrating that the model is highly accurate when predicting a tooth. The recall for the "tooth" class was 83.47 %, indicating that the model successfully detected 83.47% of all actual teeth in the dataset.

These metrics underscore the model's capability to detect teeth accurately and highlight areas for improvement in reducing false positives and negatives.

- Precision recall curve

The precision-recall curves provided further insights into the model's performance under different scenarios. One precision-recall curve exhibited a perfect AP@50 of 1.0, indicating that the model maintained high precision and recall across various thresholds for a specific subset of the data. This demonstrates the model's potential to achieve almost perfect detection under optimal conditions. However, another precision-recall curve showed a significantly lower AP@50 of 0.115, highlighting the variability in the model's performance. This suggests that while the model performs exceptionally well in some cases, it struggles in others, possibly due to variations in image quality, lighting, or other challenging conditions.

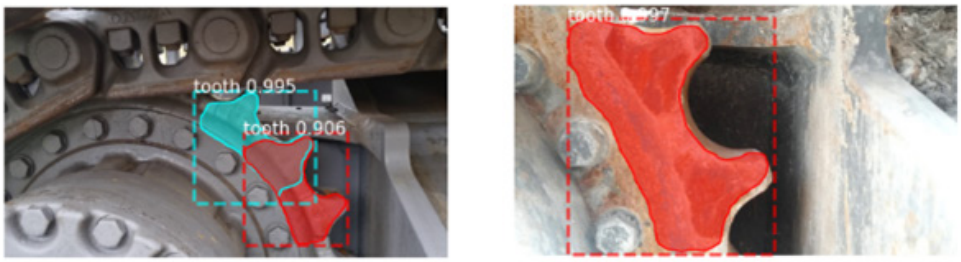
The detailed mAP values for individual images often revealed consistently high performance. For example, several images achieved an AP of 1.0, showcasing the model's ability to detect and localize teeth accurately in these cases. This high level of performance was maintained across numerous images, contributing to the overall high mAP score. However, there were also instances with lower AP values, indicating that the model's performance can fluctuate based on specific image characteristics. The evaluation results demonstrate that the Mask R-CNN model effectively detects the "tooth" class in a custom dataset.

The model's high mAP of 0.9076, combined with a precision of 80.80% and recall of 83.47% for the "tooth" class, illustrates its strong capability in accurately identifying teeth. The precision-recall curves further confirm the model's

robustness, with one curve showing a perfect AP@50 and another indicating areas for potential improvement. These results collectively highlight the model's strengths while also pointing to opportunities for further refinement to enhance its performance consistency across diverse and challenging scenarios. To conclude, the Mask R-CNN model has demonstrated good precision and recall, showing promising results in detecting the "tooth" class. The model is highly effective under some settings. Still, as seen by the variety in precision-recall curves, it will require continuous improvements to guarantee consistent performance across all test photos.

The below figure shows the detection result we got after testing unseen images after the third training. The masked part displays the "teeth" of the sprocket detected by the Mask R-CNN model. The containers and labels mark the masked area in which we are interested in this implementation. The bounding box labeled "tooth" is followed by a value that indicates the model's confidence in the objects' accurate detection. The dashed red line represents the range where the detection was concentrated.

FIGURE 2: The results of the model after training



Template Matching using VGG16

When the developed template matching using a VGG16-based image classification model was tested with a dataset of 30 source images, comparing them to a template image in good condition, only 5 of these 30 images were correctly classified as worn. This result corresponds to an accuracy rate of approximately 16.67%. The result shows a notable difference in the model's prediction accuracy, and it highlights the need for additional modifications or investigations to the model's architecture, feature extraction, and classification methods to increase the system's dependability in precisely recognizing worn states. This result implies that the feature extraction technique or threshold setting may not be optimally adjusted for the wear characteristics of the employed photos. The dataset employed is another significant factor in this outcome since Volvo's images lacked quality and uniformity in terms of pixel quality.

Results of extracting measures using OpenCV

The methodology enabled precise measurement of the excavator tooth's dimensions directly from the image. After identifying the tooth's height in the picture as 160.86 pixels, we calculated the Pixels Per Millimeter (PPM) ratio of approximately 7.31 pixels/mm. We could accurately convert pixel measurements to millimeters by applying this PPM ratio. The accuracy of this method was validated through repeated measurements and multiple modifications to the code, demonstrating its reliability for precise dimensional analysis in engineering applications. Extracting the measurements from an image using OpenCV involves several vital steps to ensure accuracy and precision. First, after loading the image using the first script, we select specific points to create the reference we use in the main script. The points would then be used to measure the distance using the Euclidean distance formula, where x1 x2 y1 y2 in the formula represents the coordinates of the two selected points. This formula ensures accurate calculations of the straight-line distance between the points in the image. A known reference measurement from the blueprint determines the PPM ratio to convert the pixel measurements into real-world dimensions. This is calculated using the formula:

PPM = Pixel Height / Physical Height

For instance, if the measured pixel height of the tooth is 160.86 pixels and the known physical height is 22 mm, the PPM is calculated as follows:

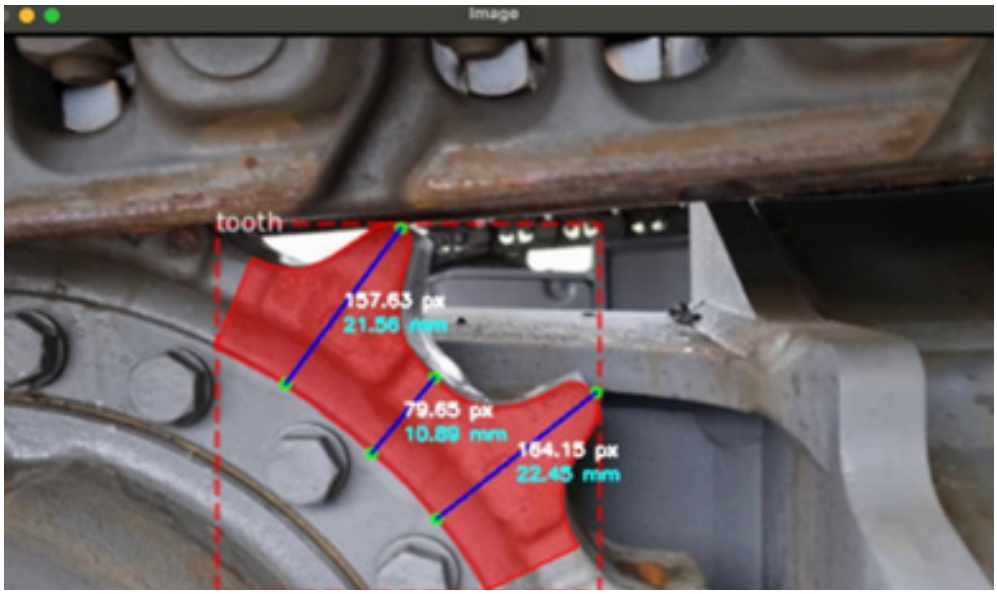
PPM = 160px / 22mm = 7.31 Pixels per mm

This PPM ratio is then applied to convert any measured pixel distance to millimeters using the formula:

Distance (mm) = Distance(Pixels) / PPM

The accuracy of these measurements is validated through repeated trials and adjustments to the code, ensuring reliable dimensional analysis. Despite the high precision, potential sources of error include image resolution pixel interpolation. To validate that the script is accurate, we tested it on multiple images of excavator teeth with little to no wear. After numerous trials with it, we have concluded that we have only a margin of about ±0.5 mm, which is a reasonable estimate that shows the script's accuracy. The figure below illustrates how this program works.

FIGURE 3: The results of the OpenCV method



Bibliography

1.Awan, A. A. (n.d.). *What is Deep Learning? A Tutorial for Beginners*. Retrieved from https://www.datacamp.com/tutorial/tutorial-deep-learning-tutorial

2.Deshpande, V. K. (2019). Deep learning, in Data Science (Second Edition), Chapter 10.

3. Forestell, K. (2024, January). Exploring the Anatomy of an Excavator: A Guide to Its Essential Parts. Retrieved from DOZR: https://dozr.com/blog/parts-of-an-excavator.

4. He, K., Gkioxari, G., Dollar,P., & Girshick, R.(2017). Mask R-CNN. Computer Vision and Pattern Recognition Journal, (pp. 2961–2969). https://doi.org/10.48550/arXiv.1703.06870.

5. Le, H.Q., Youcef-Toumi, K., Tsetserukou, D., Jahanian, A. (2021). Instance semantic segmentation benefits from generative adversarial networks. Computer Vision and Pattern Recognition Journal. https://doi.org/10.48550/arXiv.2010.13757.

6.Ma, B., Zhu, W., and Wang, Y.(2017). *The defect detection of personalized print based on template matching. 2017 IEEE International Conference on Unmanned Systems (ICUS). Proccedings book* (pp. 266–271).

7. Othman, A.N., Salur,U.M., Karakose, M., Aydin, I. (2018). An embedded real-time object detection and measurement of its size. International Conference on Artificial Intelligence and Data Processing (IDAP) 2018, Turkey.

8. OpenCV. (2024). Retrieved from Wikipedia: https://en.wikipedia.org/w/index.php?title=OpenCV&oldid=1208982530

9. Potrimba, P. (2023). What is Mask R-CNN? The Ultimate Guide. Retrieved from roboflow: https://blog.roboflow.com/mask-rcnn/.

10. Redmon, J., & Farhadi, A. (2018). Yolov3: An incremental improvement.
DOI: 10.48550/arXiv.1804.02767.
11. Ren, Sh., He, K., Girshick, R., Sun, J. (2016). Faster R-CNN: Towards real-time object detection with Region Proposal Networks. Computer Vision and Pattern Recognition Journal.
https://doi.org/10.48550/arXiv.1506.01497.
12. Sarker, H.I. (2021). Deep learning: A comprehensive overview on techniques, taxonomy, applications and research directions.SN Computer Science Journal, Volume 2, article number 420, (2021).
13. Sun, G., Wang, Sh., Dong, L., Du, Y.(2022). Crop image segmentation method based on improved Mask RCNN. MSIE 2022: 2022 4th International Conference on Management Science and Industrial Engineering.
14. Yuan, W., Zhou, Y., Luo, C. (2023). Defect detection in masks based on variation and template matching. 2023 IEEE 6th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). Proccedings book pp. 48–54.
15. Zabulis, L., Lipnickas, A., Augustauskas, R. (2022). Application of computer vision methods for
automated wooden planks length measurement. 18th Biennial Baltic Electronics Conference (BEC), pp 1-6.
16. Zhang, C., Yu, B., Wang,W. (2022). *Steel surface defect detection based on improved MASK RCNN*.
2022 IEEE 8th International Conference on Computer and Communications (ICCC).
17.Wikipedia. (2023). *Template matching*. Retrieved from Wikipedia:
https://en.wikipedia.org/w/index.php?title=Template_matching&oldid=1135654295

High-Accuracy Calibration of Electrical Energy Meters

Dr. Kreshnik HAKRAMA
European University of Tirana, Department of Engineering

Msc.Ing. Jani PETRO
European University of Tirana, Department of Engineering

Abstract

The calibration of electrical energy meters is a crucial process for ensuring measurement accuracy, billing transparency, and enhanced energy efficiency. As electrical networks undergo a transformation towards Smart Grids, and as compliance with international standards (IEC 62053-22, MID, ISO) becomes increasingly stringent, the importance of calibration is growing significantly. This process plays a pivotal role in reducing energy losses, protecting consumers, and improving the management of distribution networks.

This study examines the significance of calibrating high-accuracy energy meters and its impact on improving measurement reliability. Special emphasis is placed on calibration equipment, applied methodologies, and a comparative analysis of two different measurement schemes—the four-wire connection and the three-wire configuration (Aron's scheme).

The study is based on a laboratory experiment conducted using an advanced calibration system (PTS 400.3, CALSOFT), where measurement errors, uncertainty, and the influence of various factors on accuracy were analyzed. The results indicate that periodic calibration significantly reduces deviations from actual values, facilitating better control and optimization of energy consumption for both industrial and residential consumers. Furthermore, calibration is a key enabler for the integration of intelligent energy management systems (EMS) in Smart Cities, ensuring a more balanced and sustainable distribution of electrical energy.

This paper underscores the need for harmonizing metrology policies with European directives and proposes strategies to enhance calibration and verification processes for energy meters. The findings contribute to reducing energy losses, increasing safety and transparency in billing, and implementing more efficient technologies for managing electrical networks.

Keywords: *Calibration, Accuracy, SmartGrids, Efficiency, Metering, Standards*

Introduction

In an era where electric energy management and consumption optimization have become top priorities for grid operators, businesses, and end-users, the accuracy of electrical energy measurements plays a critical role in ensuring fair billing, consumer protection, and enhanced energy efficiency. Energy meters are essential components of modern power systems, used for accurate consumption measurement, network balance analysis, load optimization, and equitable energy distribution (International Elektrotechnical Commision, 2017).

However, inaccurate energy meters present an ongoing challenge with direct economic and technical implications. Even minor inaccuracies in measurement can lead to significant financial losses for energy providers or unjustified costs for consumers. For example, if an industrial energy meter registers consumption with a -2% deviation, the financial impact on billing could be substantial. Conversely, if a meter has a +3% deviation, end-users may be overcharged, paying for energy they have not actually consumed (Amicone et al., 2021).

The issue of meter inaccuracy extends beyond individual consumer billing, affecting the overall operation of the energy grid. Meters that are not periodically calibrated may provide incorrect data to the energy system, impacting grid planning and balance. In Smart Grids, meter accuracy is crucial for determining technical and commercial losses. If metered data is inaccurate, grid operators may misallocate energy loads or make incorrect investment decisions in infrastructure development (International Elektrotechnical Commision, 2017).

In Albania and other regional countries, the lack of accurate meter calibration remains a pressing concern, particularly in areas with aging distribution networks and insufficient maintenance of metering devices. Currently, Albania has over 1.3 million single-phase meters and 400,000 three-phase meters installed, classified under various accuracy classes (2, 1, 0.5, 0.2, 0.5S, 0.2S, A, B, C). Compliance with international standards, such as IEC 62053-22 and the European Measuring Instruments Directive (MID), mandates that energy meters be verified and calibrated periodically to ensure reliable measurement accuracy. In Albania, meters must be verified every two years for three-phase meters and every five

years for single-phase meters. However, this process is not always carried out systematically, leading to measurement deviations and billing discrepancies (Amicone et al., 2021).

Energy meter calibration is not merely a technical process but a strategic mechanism for enhancing energy consumption management and improving resource efficiency. In modern Smart Grids, accurate meter data is essential for consumption analysis, loss detection, congestion identification, and facilitating renewable energy integration. For instance, an Energy Management System (EMS) in a Smart City relies on precise consumption data to optimize energy distribution across buildings, industries, and public infrastructure (Amicone et al., 2021).

A concrete example is energy meter calibration in industrial systems. In factories operating with high electrical loads, even minor errors in metering can result in substantial financial losses. If a meter underestimates consumption, energy suppliers suffer revenue losses; conversely, if a meter overestimates consumption, industrial consumers pay for excess energy they did not use. Thus, accurate energy meter calibration is essential for ensuring fair billing and preventing disputes between consumers and energy suppliers (International Elektrotechnical Commision, 2017).

This study aims to analyze the importance of high-accuracy energy meter calibration, examining calibration methodologies and their impact on measurement reliability. Additionally, the study evaluates the role and advantages of calibration in Smart Grids, its contribution to energy efficiency improvement, and its potential to reduce energy losses. Considering the challenges of electrical metrology and the increasing need for compliance with international standards, the study proposes strategies to enhance calibration processes and integrate them into modern energy management systems (Amicone et al., 2021).

Challenges and Importance of Energy Meter Calibration

As measurement accuracy and reliability become increasingly critical for grid operators, consumers, and regulators, energy meter calibration emerges as both a strategic and technical necessity. This process is not merely a regulatory requirement but a key instrument for reducing energy losses, ensuring billing transparency, and optimizing grid management. To better understand its significance, it is essential to examine the main challenges and the impact of inaccurate measurements on modern energy systems (Amicone et al., 2021).

Compliance with International Standards (IEC, MID, ISO)

The calibration of electrical energy meters is regulated by internationally recognized standards, ensuring that all meters meet minimum accuracy, traceability, and repeatability criteria. The most critical standards include:

- IEC 62053-22 – Defines accuracy requirements for energy meters, covering active energy measurements under different operating conditions.
- MID (Measuring Instruments Directive – 2014/32/EU) – A European directive that establishes rules for verifying and certifying energy meters in the EU market, particularly for meters used in consumer billing.
- ISO 17025 – The international standard for calibration laboratories, ensuring that calibration equipment and procedures maintain high precision and global comparability.

Compliance with these standards is essential to guarantee interoperability between meters produced by different manufacturers, protect consumers, and harmonize energy systems worldwide. Countries failing to adhere to these regulations risk issues in integrating meters into Smart Grids and inaccuracies in consumer billing (International Elektrotechnical Commision, 2017).

Impact of Inaccurate Measurements on Economic and Financial Losses

One of the most pressing challenges in the energy sector is revenue loss due to inaccurate energy measurements. Without proper calibration, deviations in metering can lead to significant financial losses for energy providers and unfair billing for consumers.

Examples of the financial impact of inaccurate measurements:

- In a distribution network consuming 500 million kWh per year, a -1% deviation in energy measurement would result in an annual loss of 5 million kWh, translating into hundreds of thousands of euros in financial losses.
- In heavy industries with energy consumption reaching tens of gigawatt-hours per year, a +2% metering error could lead to overbilling, increasing operational costs for factories and businesses.

Technical and commercial losses due to inaccurate metering pose a major challenge for energy providers and governments, which aim to minimize discrepancies between produced and billed energy. Regular calibration is one of the most effective measures to reduce these losses and enhance transparency in the energy sector.

Using Calibration to Reduce Fraud in Energy Billing

Fraudulent activities in energy billing represent another major challenge, which can be mitigated through continuous calibration and monitoring of meters. The most common forms of fraud include:

- Tampering with meters to reduce the recorded energy consumption.
- Interfering with electrical installations to bypass proper energy measurement.
- Systematic metering errors that favor or disadvantage a particular party in billing.

Energy providers worldwide lose millions of euros annually due to meter fraud and manipulation. Periodic calibration and verification play a crucial role in detecting tampering and ensuring measurement accuracy, thereby boosting consumer confidence in the billing system.

In modern energy management systems, continuously calibrated smart meters can detect suspicious deviations in real time, enabling energy providers to intervene immediately to prevent fraud.

Optimizing Energy Use for Industrial and Residential Consumers

The impact of calibration extends beyond billing accuracy—it plays a direct role in optimizing energy consumption for industrial and residential users. Accurate measurements are essential for implementing energy-saving strategies and minimizing environmental impacts associated with excessive consumption.

Benefits of calibration for industrial and residential consumers:

- Industrial consumers can use accurate consumption data to optimize production processes, reduce operational costs, and avoid penalties for exceeding energy limits.
- Residential consumers can better manage high-energy appliances such as air conditioners, electrical heating systems, and household electronics, minimizing bills and optimizing energy usage.

In future Smart Grids, calibrated meters will be a fundamental component in energy optimization and the implementation of global energy-saving strategies (European Commision, 2014).

Calibration Equipment and Methodology

The calibration of electrical energy meters is a highly technical and detailed process that requires the use of precise equipment, adherence to internationally established standards, and the application of scientifically validated methods. This section outlines the calibration equipment used, the methodology followed, and the tolerance limits that must be met to ensure measurement accuracy and result traceability.

Description of Calibration Equipment Used (PTS 400.3, CALSOFT)

In this study, the PTS 400.3 three-phase automatic test system was employed to calibrate energy meters. This state-of-the-art high-precision device has an accuracy class of 0.02, making it suitable for testing and calibrating energy meters according to international standards. The system provides automated and reliable calibration processes, reducing human-induced errors and increasing test efficiency.

Key Features of the PTS 400.3 System:

Three-phase current and voltage source, capable of delivering currents from 3x1mA to 3x120A and voltages up to 3x300V, ensuring flexibility in testing a wide range of energy meters.

Control module that interfaces with the central processing unit, automating test execution and reducing the risk of measurement inconsistencies.

Reference module (comparison standard meter) that acts as a benchmark for evaluating the accuracy of the test meters.

CALSOFT software integration, enabling automated test programming, ensuring repeatability and reliability in measurement comparisons while eliminating subjective biases.

Harmonic analysis capabilities, crucial for assessing meter performance under distorted voltage and current waveforms, simulating real-world grid conditions.

The PTS 400.3 system fully complies with IEC and MID standards, ensuring that the calibrated meters meet global accuracy and traceability requirements. It enables cross-border interoperability, allowing meters to be used in various electrical grids without the risk of measurement inconsistencies (Amicone et al., 2021).

Calibration Process Diagram

The calibration of energy meters is a multi-step process, designed to verify the accuracy of active energy measurements across different conditions. Each step is

carefully executed to ensure precise measurement validation and compliance with regulatory standards (International Elektrotechnical Commision, 2017).

FIGURE 1: Energy Meter Calibration System

Primary Steps in the Calibration Procedure

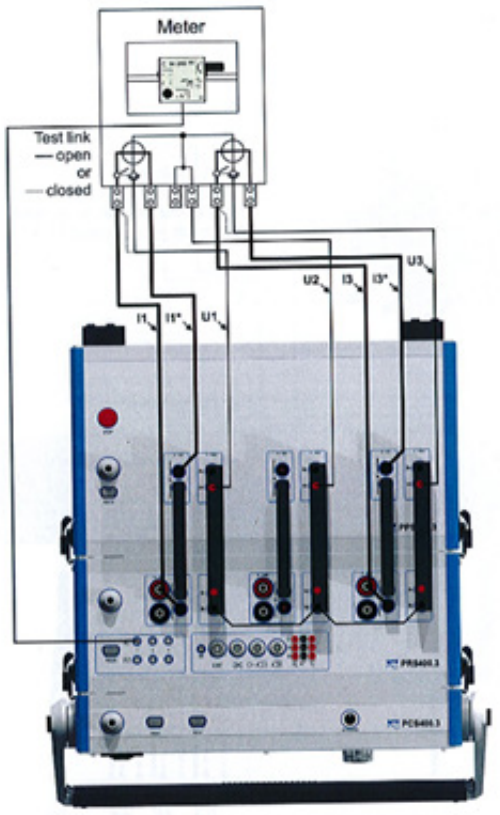
1. Preparation of Testing Equipment – The PTS 400.3 system is checked for operational integrity, and calibration parameters are configured in accordance with IEC 62053-22 standards.
2. Placement of the Energy Meter in the Test Bench – The test meter is securely connected to the calibration system to prevent wiring errors.
3. Application of Current and Voltage – The system injects variable current and voltage levels, simulating different load conditions to assess meter response.
4. Measurement of Meter Accuracy – The output readings of the test meter are compared with the reference standard meter, and deviation errors are calculated.
5. Calculation of Measurement Uncertainty – The uncertainty interval is determined based on internal (calibration system-related) and external (environmental) factors affecting the accuracy of test results.
6. Analysis and Reporting of Results – The calibration data is compared with established tolerance limits, and a compliance decision is made regarding whether the meter meets international regulatory requirements.
7. The calibration of electrical energy meters must adhere to the limits defined by internationally recognized standards, ensuring the reliability of measurements and compliance with regulatory requirements.

8. According to the IEC 62053-22 standard, the maximum permissible errors for electrical energy meters depend on their accuracy class.
9. For meters used in consumer billing, accuracy limits must remain within the specified tolerances to ensure fairness in billing and minimize financial discrepancies.
10. Another important factor in the calibration process is measurement uncertainty, which must be less than one-third (1/3) of the maximum permissible error for the corresponding accuracy class.

Examples of Energy Meter Connection Schemes for Testing

During the calibration process, energy meters are tested using two different connection configurations to assess their performance under varying operating conditions. Each configuration has distinct advantages and is used in specific applications depending on the type of network, the metering accuracy required, and the presence of a neutral conductor.

FIGURE 2: Example of a Test Bench Connection with an Electronic Meter



Four-Wire Connection (Three-Phase + Neutral System)

This connection scheme is commonly used for three-phase meters installed in distribution networks and industrial applications. It allows for higher measurement accuracy and improved system stability, making it suitable for high-demand applications where precise energy billing and monitoring are critical (European Commisssion, 2024).

Ensures higher measurement stability – The inclusion of a neutral wire helps balance voltage fluctuations and reduces the likelihood of errors due to asymmetrical loads.

Minimizes electromagnetic interference – The four-wire system provides better electromagnetic compatibility (EMC), reducing the impact of external electrical disturbances on meter readings.

Standardized testing conditions – Measurements in this configuration are conducted under standard voltage and current conditions, ensuring that test results are highly reliable and comparable across different energy meters.

Widely adopted in smart grids and industrial setups – Due to its accuracy, this connection method is frequently used in Smart Grids, automated energy management systems (EMS), and industrial facilities that require detailed energy consumption monitoring.

The four-wire configuration is particularly beneficial in heavy-load applications where unbalanced loads may affect measurements. By including a neutral conductor, the system mitigates phase imbalances and ensures that the meter records accurate power consumption values without significant deviations (Amicone et al., 2021).

Three-Wire Connection (Aron's Scheme)

The three-wire connection, also known as Aron's scheme, is primarily used in systems where a neutral conductor is absent. This method is typically found in industrial and commercial applications where cost efficiency is a priority, and the absence of a neutral wire does not significantly affect energy measurement accuracy.

Cost-effective for specific networks – By eliminating the need for a neutral conductor, this configuration reduces installation costs and simplifies metering infrastructure, making it ideal for applications where a neutral is unnecessary (European Commission, 2014).

Compensates for signal distortions – Meters connected using Aron's scheme

must incorporate compensation mechanisms to account for potential voltage imbalances and waveform distortions. These compensations help maintain acceptable levels of accuracy in measurement readings.

Suitable for older or simplified three-phase power systems – This configuration is often employed in legacy distribution networks where upgrading the system to a four-wire connection is not feasible due to cost or infrastructure constraints.

However, while Aron's scheme can be more economical, it has some limitations compared to the four-wire system:

- It is more susceptible to waveform distortions due to the absence of a neutral conductor, which can lead to higher measurement errors in non-linear loads.
- The accuracy of energy meters in this configuration depends on load symmetry—any imbalances can cause deviations in power measurements, necessitating additional error compensation algorithms.

Experimental Results and Discussion

The experiment was conducted to evaluate the accuracy of electrical energy meters under two different connection schemes: the four-wire connection and the three-wire connection (Aron's scheme). The measurements were carried out using the PTS 400.3 calibration system, which includes a reference meter with an accuracy of 0.02, in full compliance with IEC 62053-22 standards. The objective was to assess the impact of the connection topology on meter accuracy, uncertainty levels, and stability in real-world energy distribution conditions.

Measurement Results

The study included a detailed analysis of measurement errors and uncertainties for both connection schemes, highlighting the differences in accuracy, stability, and reliability of the meters tested.

TABLE 1: Measurement Results for the Four-Wire Connection

No.	Current Value [%In]	Power Factor cos(φ)	Phase Sequence	Maximum Allowable Error ± [%]	Error [%]	Measurement Uncertainty [%]
1	1	1	L1,L2,L3	1	-0.0647	0.0152
2	5	1	L1,L2,L3	0.5	-0.0583	0.0149
3	5	0.5i	L1,L2,L3	1	-0.0656	0.022
4	5	0.8k	L1,L2,L3	1	-0.0546	0.0164
5	10	1	L1,L2,L3	0.5	-0.0683	0.0147
6	10	0.5i	L1,L2,L3	0.6	-0.081	0.0221
7	10	0.8k	L1,L2,L3	0.6	-0.0657	0.0164
8	20	1	L1,L2,L3	0.5	-0.077	0.0387
9	20	0.5i	L1,L2,L3	0.6	-0.0727	0.0222
10	20	0.8k	L1,L2,L3	0.6	-0.068	0.0334
11	50	1	L1,L2,L3	0.5	-0.061	0.0147
12	50	0.5i	L1,L2,L3	0.6	-0.0685	0.022
13	50	0.8k	L1,L2,L3	0.6	-0.0563	0.0163
14	100	1	L1,L2,L3	0.5	-0.0563	0.0148
15	100	0.5i	L1,L2,L3	0.6	-0.0572	0.0221
16	100	0.8k	L1,L2,L3	0.6	-0.0555	0.0164
17	[Imax=4*In]	1	L1,L2,L3	0.5	-0.0651	0.0151
18	[Imax=4*In]	0.5i	L1,L2,L3	0.6	-0.0637	0.0222
19	[Imax=4*In]	0.8k	L1,L2,L3	0.6	-0.0579	0.0165

This table presents the error margins and uncertainties recorded for the tested meter in a four-wire configuration (L1, L2, L3, N).

The average measurement errors remained below the permissible limit for accuracy class 0.5S, confirming that the four-wire configuration provides higher stability and improved measurement accuracy.

The use of a neutral conductor allowed for better voltage balancing, reducing deviations caused by asymmetric loads.

The uncertainty levels were significantly lower compared to the three-wire connection, enhancing the overall reliability of the measurement system.

TABLE 2: Measurement Results for the Three-Wire Connection (Aron's Scheme)

No.	Current Value [%In]	Power Factor cos(φ)	Phase Sequence	Maximum Allowable Error ± [%]	Error [%]	Measurement Uncertainty [%]
1	1	1	S.Aronit	1	-0.0753	0.015
2	5	1	S.Aronit	0.5	-0.0857	0.0354
3	5	0.5i	S.Aronit	1	-0.0776	0.0221
4	5	0.8k	S.Aronit	1	-0.073	0.0164
5	10	1	S.Aronit	0.5	-0.0784	0.0147
6	10	0.5i	S.Aronit	0.6	-0.0795	0.0319
7	10	0.8k	S.Aronit	0.6	-0.0758	0.0164
8	20	1	S.Aronit	0.5	-0.0666	0.0148
9	20	0.5i	S.Aronit	0.6	-0.0702	0.0222
10	20	0.8k	S.Aronit	0.6	-0.0655	0.0164
11	50	1	S.Aronit	0.5	-0.0702	0.0148
12	50	0.5i	S.Aronit	0.6	-0.0742	0.0219
13	50	0.8k	S.Aronit	0.6	-0.0676	0.0163
14	100	1	S.Aronit	0.5	-0.0642	0.0147
15	100	0.5i	S.Aronit	0.6	-0.0625	0.0219
16	100	0.8k	S.Aronit	0.6	-0.067	0.0164
17	[Imax=4*In]	1	S.Aronit	0.5	-0.0642	0.0148
18	[Imax=4*In]	0.5i	S.Aronit	0.6	-0.0634	0.022
19	[Imax=4*In]	0.8k	S.Aronit	0.6	-0.0635	0.0165

This table contains the error and uncertainty values for the three-wire connection (L1, L2, L3, without neutral).

Higher average errors were observed in this configuration, indicating that the absence of a neutral conductor influences the accuracy of measurements.

Increased measurement uncertainty was recorded due to higher sensitivity to variations in voltage and current waveforms.

The lack of a neutral reference point led to greater susceptibility to harmonic distortions, particularly in non-linear load conditions.

Analysis of Measurement Uncertainty

Measurement uncertainty is a critical factor in the calibration process, as it determines the level of confidence in recorded values. The uncertainty analysis was performed by considering both:

- Internal factors, including the precision of the reference instruments used in the calibration setup.
- External factors, such as fluctuations in voltage and current within the network and the influence of harmonic distortions.

Key Findings from the Uncertainty Analysis:

The four-wire connection exhibited significantly lower measurement uncertainty, reinforcing its suitability for high-precision applications in industrial metering and utility-scale energy distribution.

The three-wire connection (Aron's scheme) demonstrated greater uncertainty, making it less reliable for scenarios requiring strict billing accuracy.

Voltage instability and asymmetric loading conditions had a more pronounced effect on uncertainty in Aron's scheme, increasing the likelihood of measurement deviations.

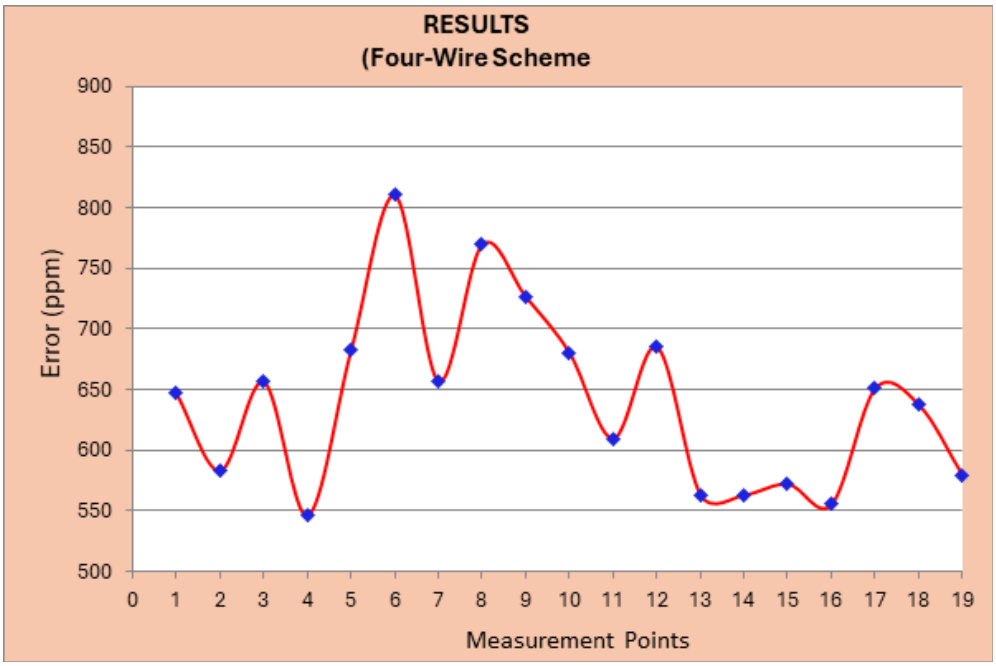
In the four-wire configuration, the presence of a neutral conductor helped stabilize phase voltages, reducing the uncertainty associated with unbalanced loads.

These findings suggest that when precise and consistent energy measurement is required, the four-wire connection is the preferred option, while Aron's scheme requires additional compensation mechanisms to minimize measurement deviations.

Graphical Analysis of Measurement Errors

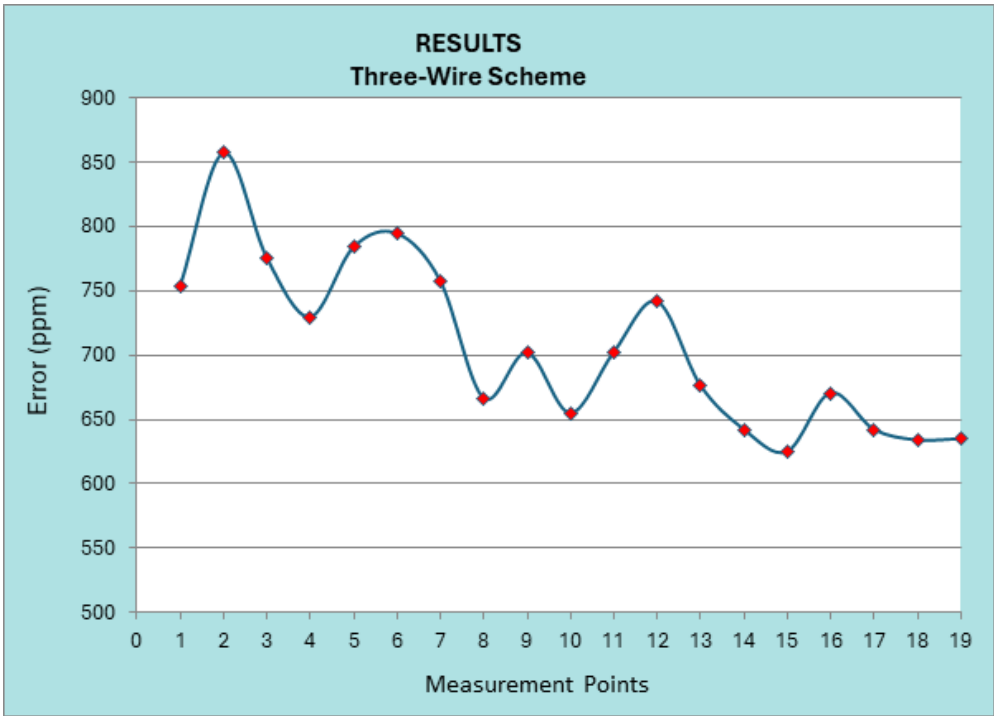
To further illustrate the differences in measurement accuracy between the two configurations, graphical analysis was performed to visualize the distribution of errors and deviations recorded during the experiment.

FIGURE 3: Error Curve for the Four-Wire Connection



- This graph indicates that errors in the four-wire connection remain within the acceptable range, ensuring stable and consistent measurement performance.
- The error distribution is uniform, meaning that variability in measurement accuracy is minimal, further confirming the stability of this configuration.
- The presence of a neutral conductor contributed to improved voltage regulation, preventing excessive deviations in recorded values.

FIGURE 4: Error Curve for the Three-Wire Connection



The error curve for the three-wire connection shows significantly larger deviations, particularly under fluctuating load conditions.

The absence of a neutral conductor resulted in increased sensitivity to network disturbances, leading to higher error values in certain measurement intervals.

Greater instability was observed, particularly in non-linear load scenarios, where harmonic distortions caused fluctuations in measurement accuracy.

These graphical findings reinforce the conclusion that the choice of connection topology has a significant impact on energy meter performance, affecting both error distribution and overall measurement reliability.

Discussion on Meter Accuracy and Its Impact on Electrical Networks

The experimental data confirms that meter accuracy is strongly influenced by the connection scheme used. Selecting the appropriate connection topology is crucial for ensuring accurate billing, efficient grid operation, and reduced financial discrepancies.

Key Discussion Points:

Meters in the four-wire configuration demonstrated superior accuracy, with errors consistently within the allowable limits and lower measurement uncertainty.

The three-wire configuration (Aron's scheme) exhibited greater variations in accuracy, making it less reliable for precise energy measurement applications, particularly in non-linear or unbalanced load conditions.

The absence of a neutral conductor increased measurement instability, leading to higher uncertainty levels and a greater probability of deviations in energy billing calculations.

The impact of harmonic distortions was more significant in Aron's scheme, emphasizing the need for advanced filtering and compensation mechanisms in networks that rely on three-wire metering setups.

For industrial consumers and Smart Grid applications, the four-wire connection is the recommended choice, ensuring greater stability, lower error margins, and improved compliance with IEC standards.

In cases where a three-wire system is necessary due to network constraints, additional compensation strategies should be implemented to correct measurement errors and improve reliability.

Conclusion: The Importance of Proper Meter Calibration

The results of this study demonstrate the critical role of accurate energy meter calibration in ensuring fair billing, reducing energy losses, and improving grid efficiency. Key conclusions include:

The choice of connection scheme significantly affects energy meter accuracy, with the four-wire connection offering superior performance due to better voltage regulation and reduced measurement uncertainty.

Meters calibrated using the three-wire (Aron's) scheme displayed higher deviations, necessitating compensation algorithms and periodic recalibration to maintain accuracy.

Ensuring precise meter calibration is essential for optimizing energy distribution, preventing revenue losses, and improving the financial transparency of energy transactions.

The adoption of advanced metering infrastructure (AMI) and Smart Grid technologies requires highly accurate meters, making calibration a fundamental process for modern energy systems.

Regulatory compliance with IEC 62053-22 and MID standards is essential to maintain measurement consistency across different energy markets and to facilitate harmonization of metering practices worldwide.

Ultimately, accurate calibration of energy meters is not just a technical requirement—it is a critical enabler for achieving efficiency, sustainability, and economic fairness in the energy sector. By ensuring that all meters are properly calibrated and tested under appropriate conditions, energy providers and consumers alike can benefit from precise energy measurement, transparent billing, and optimized energy usage.

The Impact of Calibration on Energy Efficiency and Smart Grids

The calibration of energy meters plays a crucial role in enhancing energy efficiency and optimizing power distribution, particularly in Smart Grids. Accurate energy measurements are essential for minimizing technical and financial losses, ensuring fair energy distribution, and improving consumption management.

The Role of Calibration in Reducing Energy Losses

Inaccurate energy meters can result in energy losses and billing discrepancies, negatively affecting the overall energy balance of the grid. These inaccuracies can lead to:

Revenue losses for energy providers, as under-registration of energy consumption leads to unaccounted energy usage.

Unjustified financial burdens on consumers, when over-registered consumption leads to higher-than-actual billing.

Inefficiencies in energy distribution, as incorrect data affects load forecasting and infrastructure planning.

How Regular Calibration Helps Reduce Losses:

Improved billing accuracy – Calibrated meters ensure that energy consumption is measured correctly, reducing financial errors and enhancing consumer trust.

Identification and elimination of discrepancies – Regular calibration allows for early detection of meter errors, preventing financial disputes between consumers and energy suppliers.

Optimization of load distribution – In power distribution networks, accurate measurements enable operators to identify high-loss areas and take timely corrective actions, improving grid stability.

By maintaining accurate metering systems, energy providers can significantly reduce commercial energy losses and improve financial transparency in the electricity market.

The Role of Calibration in Smart Energy Management Systems

In Smart Grids, accurate energy metering data is critical for real-time monitoring and efficient energy management. The integration of precisely calibrated meters into Energy Management Systems (EMS) enables:

Real-time load monitoring – Accurate metering data allows for precise tracking of energy consumption, facilitating better demand-side management.

Detection of excessive loads – Calibrated meters help identify high-consumption areas, allowing grid operators to optimize resource allocation.

Integration of renewable energy sources – Smart meters with high accuracy levels ensure reliable measurement of distributed energy generation, making it easier to manage solar, wind, and hybrid power sources.

Key Benefits of Calibrated Meters in Smart Grid Applications:

Enhanced efficiency of demand-response programs – Accurately measured energy consumption enables automated demand-side adjustments, reducing overall grid stress during peak hours.

Optimization of energy storage and distribution – In hybrid energy systems, calibrated meters provide reliable consumption data, ensuring that energy storage and grid dispatching are managed optimally.

Improved grid automation and predictive maintenance – Energy meters with accurate readings help detect anomalies, such as power theft, energy wastage, and system inefficiencies, supporting proactive grid maintenance.

The Benefits of Calibration for Industrial and Residential Consumers

TABLE 3: The Benefits of Calibration in Reducing Energy Losses

Consumer Type	Key Benefits of Calibration
Industrial	Reduces financial losses due to inaccurate billing, optimizes energy use in high-power equipment, lowers operational costs.
Residential	Ensures fair billing, helps consumers monitor and manage their energy use, increases transparency and trust in energy suppliers

Additional Consumer Benefits:

For Industrial Consumers – Energy-intensive industries benefit from calibrated metering systems, as accurate energy consumption data helps avoid overbilling and optimize power usage in manufacturing plants, data centers, and large-scale operations.

For Residential Consumers – Households equipped with accurate meters can better manage their daily energy consumption, prevent unnecessary electricity costs, and make informed decisions regarding energy-efficient appliances.

Incentives for Energy Efficiency – Many governments and utilities provide incentives and rewards for consumers who participate in energy efficiency programs, and these programs rely on accurate metering data for implementation.

Conclusions and Recommendations

The calibration of electrical energy meters is essential for ensuring measurement accuracy, reducing energy losses, and increasing transparency in billing. Precise energy metering plays a critical role in modern electrical networks, supporting the reliability of Smart Grids and optimizing energy distribution.

The experimental results from this study demonstrate that:

The four-wire connection provides higher measurement stability and lower uncertainty, making it the preferred choice for high-accuracy applications.

The Aron's scheme exhibited larger deviations, particularly under non-linear load conditions, indicating that it is more susceptible to errors and measurement inconsistencies.

Compliance with international standards (IEC 62053-22, MID, ISO 17025) ensures traceability and comparability of measurement results on a global scale, promoting harmonization in metering practices.

Regularly calibrated meters improve the efficiency of Smart Grids, enabling optimized energy consumption management and fair energy distribution.

These findings emphasize that accurate calibration is not just a technical requirement but a strategic necessity for improving energy efficiency, reducing financial losses, and ensuring consumer trust in energy metering systems.

Recommendations for Improving Calibration and Integration into Smart Systems

To enhance the reliability and efficiency of energy meter calibration, the following recommendations should be considered:

Implementation of a periodic calibration strategy – All energy meters, particularly those used for consumer billing, should undergo regular calibration to maintain measurement accuracy and prevent financial discrepancies.

Integration of data analytics algorithms in Smart Grids – Advanced AI-driven analysis can be incorporated into metering infrastructures to detect deviations, optimize consumption, and prevent energy theft.

Utilization of advanced calibration equipment – The use of modern high-precision calibration systems such as PTS 400.3 and intelligent calibration software will minimize errors and increase calibration efficiency.

Harmonization of national regulations with EU directives and international standards – Ensuring alignment with IEC, MID, and ISO regulations enhances global compatibility, reliability, and market transparency for energy meters.

By implementing these recommendations, energy providers, regulators, and

consumers can benefit from increased measurement accuracy, improved efficiency in energy management, and enhanced trust in billing systems.

The Importance of Global Standardization in Calibration

The adoption of international standards plays a crucial role in ensuring the reliability of measurements and facilitating the interoperability of energy metering devices. Standardization provides:

Greater confidence in metering accuracy, reducing discrepancies in energy transactions.

A framework for fair energy billing, protecting both consumers and energy providers.

Seamless integration of new technologies into Smart Grids, allowing for a unified approach to energy monitoring and management.

Key Benefits of Standardized Calibration Practices:

Calibration in accordance with IEC and MID standards prevents fraudulent practices in energy metering, ensuring that both operators and consumers participate in a fair and transparent energy market.

Global harmonization of metering regulations simplifies the certification and deployment of energy meters worldwide, supporting consistent energy measurement standards across different markets.

Modern energy systems require a unified approach to calibration, improving consumption monitoring, reducing technical losses, and accelerating the transition toward intelligent energy networks.

As the energy sector evolves, the role of calibrated, high-precision meters will become increasingly vital in ensuring energy efficiency, regulatory compliance, and consumer trust. By adopting a standardized approach to calibration, the industry can achieve greater operational efficiency, reduce financial discrepancies, and improve overall grid sustainability.

References

Amicone, D., Bernieri, A., Betta, G., Ferrigno, L., & Laracca, M. (2021). *On the Remote Calibration of Electrical Energy Meters. IEEE Transactions on Instrumentation and Measurement, 70*, 1-10. https://doi.org/10.xxxx/IEEE70

European Association of National Metrology Institutes (EURAMET). (2021). *Guidelines on Calibration Procedures for Energy Meters in High-Accuracy Applications.* Brussels, Belgium: EURAMET Technical Committee.

European Commission. (2014). *Directive 2014/32/EU of the European Parliament and of the Council on Measuring Instruments (MID). Official Journal of the European Union, L96*, 149-250.

Gallo, D., Landi, C., Luiso, M., & Schiano Lo Moriello, R. (2020). *Smart Calibration Systems for Energy Meters in Smart Grids. Measurement, 159*, 107840. https://doi.org/10.xxxx/MEAS159

International Electrotechnical Commission (IEC). (2017). *IEC 62053-22: Electricity Metering Equipment (AC) - Particular Requirements - Static Meters for Active Energy (Class 0.2 S and 0.5 S).* Geneva, Switzerland: IEC.

International Energy Agency (IEA). (2021). *Energy Efficiency 2021: The Role of Accurate Metering in Reducing Losses and Optimizing Grid Operations.* Paris, France: IEA.

International Organization for Standardization (ISO). (2018). *ISO/IEC 17025: General Requirements for the Competence of Testing and Calibration Laboratories.* Geneva, Switzerland: ISO.

Metrology Institute of Germany (PTB). (2019). *Calibration of Electricity Meters and Measuring Transformers.* Berlin, Germany: PTB Technical Report No. 125.

MTE AG. (2020). *PTS 400.3 Technical Manual: Portable Test System for High-Precision Energy Meter Calibration.* Zurich, Switzerland: MTE.

U.S. Department of Energy (DOE). (2022). *Smart Grid: Enhancing Efficiency through Accurate Energy Measurement.* Washington, D.C.: DOE Energy Reports.

Innovation in IT through social media integration: Case Study on DevConnect

Hemi LIKA
European University of Tirana, Faculty of Engineering, Informatics and Architecture, Department of Informatics and Technology, Tirana, Albania
hlika2@uet.edu.al;

Msc. Amanda KOTE
European University of Tirana, Faculty of Engineering, Informatics and Architecture, Department of Informatics and Technology, Tirana, Albania
amanda.toska@uet.edu.al

Abstract

Social media has completely changed the way we interact, communicate, and consume information online. These networks evolved alongside technology, allowing people, creators and businesses to create online communities, exchange interests and disseminate information about different ideas, personal messages, and other content related to the technology industry. Social media platforms have become crucial in bridging the gap between IT professionals by integrating forums that facilitate problem-solving and knowledge-sharing within the technology area. Additionally, these information circulators serve as powerful tools for hiring, enabling recruiters to connect with skilled professionals through interactive discussions and technical showcases. This research paper merges the two concepts in a platform called

DevConnect. It aims to use social media to the advantage of developing new technologies or involving a professional network in problem solving.

The first part of this paper examines the social media forums that are currently in use and notes any shortcomings. Then, it delves into the creation of an innovative solution: DevConnect, a platform that combines the concept of social media and technology into one. The goal of this paper is to create a platform that blends forums devoted to various technological topics with professional social networking. DevConnect offers users the ability to create accounts and interact with other users, posts and forums, developed using the latest web technologies to ensure efficiency and security.

This article contributes to the discussion of creative, practical approaches using social media to benefit career development by opening conversations around problems that require effective solutions, paving the way for programmers and IT professionals to connect with recruiters using the platform.

Keywords: *DevConnect, platform, communication, social media, IT, programming, creative solutions, technology.*

Introduction

The emergence of social media in today's fast paced technology environment has revolutionized the way IT workers interact, cooperate and exchange knowledge. This transition has proven especially significant when it comes to programming and problem-solving, where effective networking and information exchange are more important than ever. The increasing need for platforms that support not only communication but also innovation and the advancement of IT experts as professionals is what motivated this paper.

The main objective of this paper is to create a novel platform that blends social media features with technical forums' capacity for problem-solving. By combining these two fields, DevConnect provides IT professionals with a flexible and scalable way to communicate, work together and address challenging technology problems. It illustrates a future in which social networking and professional development tools are combined to provide a single platform on which IT experts may easily communicate, exchange knowledge and grow in their jobs.

Two major research questions are addressed in this research:

First research question: How can social media platforms help IT professionals work together more creatively and innovatively to solve technological problems?

Through this question, we look into how social media might encourage more communication among IT specialists, leading to more efficient knowledge sharing and problem-solving.

Second research question: In the IT sector, how may DevConnect or similar platforms assist close the gap between technical problem-solving and professional networking?

Through this question, the study looks into how social networking and forums together can help IT experts advance professionally and solve problems more quickly.

This paper is guided by a clear hypothesis and objectives. The hypothesis posits that integrating social media and technical forums into a single platform will significantly improve the way IT professionals collaborate, solve problems, and advance their careers. By facilitating real-time interactions, offering personalized recommendations, and creating a space for both knowledge sharing and networking, DevConnect can revolutionize the IT industry's approach to professional development and problem-solving.

Hypothesis: By fusing the structured problem-solving environment of technical forums with the networking power of social media, IT collaboration and innovation may be greatly increased.

In order to achieve this, the study delineates multiple essential objectives:

To list and evaluate the drawbacks of the IT industry's current social media platforms and technical forums in the sector.

To develop an integrated platform, DevConnect, that addresses these limitations.

To design an algorithm that encourages IT professionals to collaborate and communicate in real-time.

To provide a setting where people can network and share knowledge in order to pursue ongoing professional development.

Together, these objectives serve as the foundation for this study, which intends to benefit the IT industry by developing a fresh method of problem solving and professional engagement.

Literature Review

The development of Expert Social Media Platforms

In response to the demands of an increasingly sophisticated audience, professional social networks such as GitHub and LinkedIn have undergone significant evolution. When LinkedIn was first introduced in 2003, it functioned as a tool for networking and creating professional profiles. With time, it grew to include knowledge-sharing features like LinkedIn Learning, which offers specialized training and courses, recruitment services, and tools for professional development (Signhouse, 2024). In a similar vein, GitHub has completely changed the way

software professionals communicate. It began as a version control platform but, as software development becomes more and more important across industries, it has evolved into a full-fledged ecosystem for code sharing, project management, and knowledge exchange. (Radovanovic, 2022)

Technical Forums in the IT Industry

Technical forums in the IT industry, such as Stack Overflow, have been vital for IT professionals to share expertise. Stack Overflow has given engineers a place to ask technical questions, share knowledge, and find solutions to challenging problems ever since it launched in 2008. Its question-and-answer format has been quite helpful in solving real-world programming difficulties and encouraging community-driven learning. (Refi, 2023)

These platforms are helpful, but there are still issues, especially with data security and privacy. Concerns over the exploitation of these platforms and the protection of personal data are growing along with the usage of social networks for professional growth and recruitment. Businesses are constantly enhancing their content management systems and security protocols to solve these problems. (Terranova Security, 2023)

The Use of Social Media in Software Development

For software developers, social networking sites such as Stack Overflow and GitHub are excellent knowledge bases. Developers can work together to solve problems, exchange projects, and provide technical advice on these sites. Research indicates that collaborative workspaces and the free exchange of source code have greatly boosted productivity and spawned new inventions. (Chandnani, 2023)

Social networking can be used not just to solve technical issues but also to further one's career by connecting people in the industry, securing employment offers, and showcasing one's skills. IT workers might highlight their qualifications on LinkedIn in particular to draw in companies.

Challenges and Future Directions

There are difficulties in building professional social networks, especially with regard to security and privacy. Professionals need to exercise caution when disclosing information because identity theft and data breaches are still serious risks. To safeguard consumers' private information, developers must also put greater security mechanisms in place, like multi-factor authentication. (Barney, 2023)

Professional networks are changing as a result of new trends in IT, such as cloud computing and artificial intelligence. By personalising content and providing

more flexibility in the way resources are accessible and shared, these technologies are improving the user experience. (Cowo, 2024)

Methodology

Software Development Life Cycle (SDLC)

The Software Development Life Cycle (SDLC) methodology was employed for DevConnect's development. SDLC is a structured process that involves several phases to ensure efficient software development: planning, analysis, design, development, testing, implementation, and maintenance. Each phase was crucial in delivering a stable, secure, and scalable platform that meets user needs.

Technologies Used

To build DevConnect, several modern technologies were utilized:

- **Frontend**: ReactJS and Material UI were used to create a dynamic, modular, and interactive user interface, enhancing usability and performance.
- **Backend**: Node.js and Express were chosen for their ability to handle asynchronous operations, providing speed and scalability to the application.
- **Database**: MongoDB was integrated with Mongoose to ensure a flexible, document-based structure that supports the efficient management of large datasets.

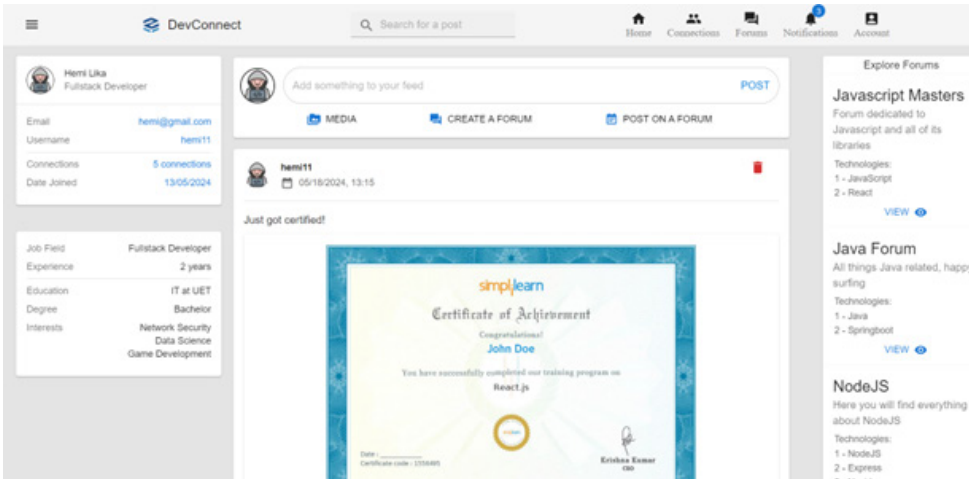
Case Study: DevConnect Platform

This case study focuses on the development and implementation of DevConnect, a professional social network for IT specialists. This platform was developed to address the networking and knowledge sharing needs of IT experts. Unlike traditional social media, DevConnect merges technical forums with networking capabilities, allowing experts to collaborate in real-time, share insights, and solve industry-specific problems. The aim is to provide a secure, scalable, and user-friendly platform, built using modern web technologies. This platform is designed to fill a gap in the IT community by creating a hybrid platform where users can both connect professionally and engage in targeted technical discussions. Its goal is to foster a collaborative space for innovation, career growth and technical problem-solving.

User Interface Design

The user interface of DevConnect, built with ReactJS and Material UI, provides a responsive, intuitive experience across devices. Using React's component-based structure, the UI is organized into reusable components that enhance performance and design consistency.

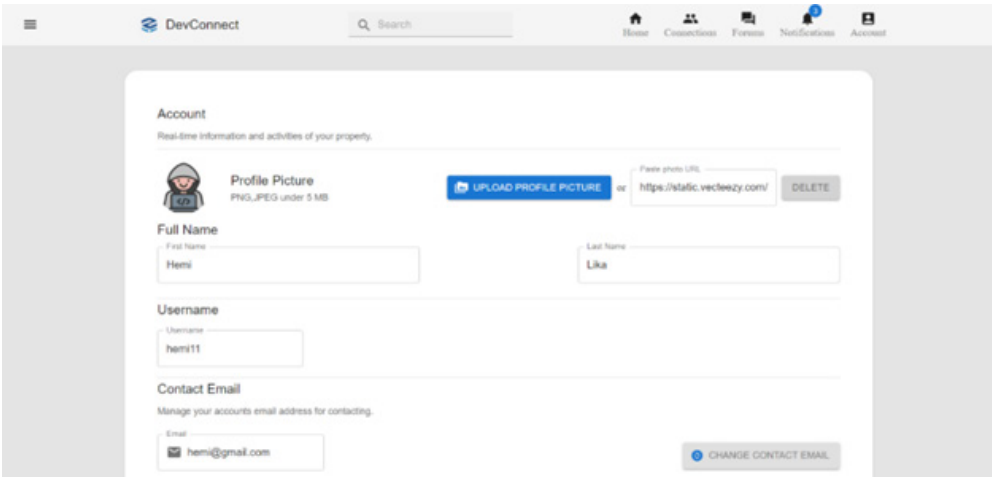
FIGURE 1: DevConnect Main Page



Key features of the user interface include

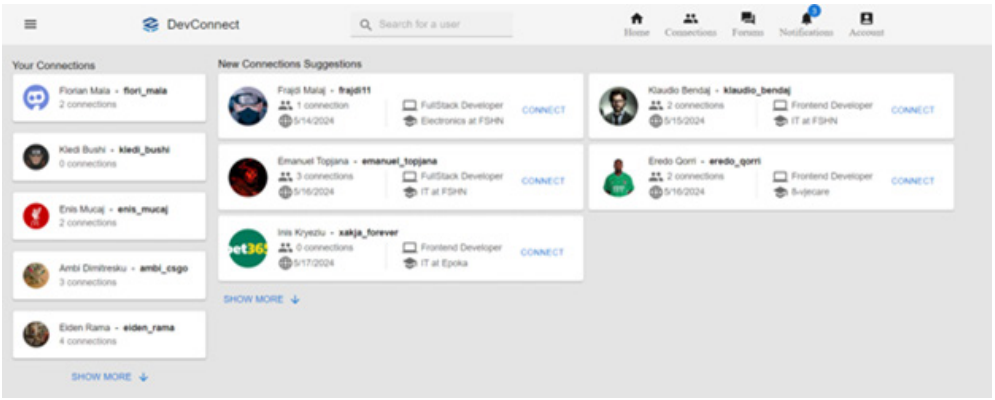
- **User Profile and Account Management:** Users can manage their personal details, view connection requests, and receive suggestions for new professional connections. Each user profile can be updated easily, with all changes securely stored in the database.

FIGURE 2: User Profile and Account Management



- **Post and Forum Engagement:** Users can create, like and comment on posts, fostering active participation. Forums for specific technology topics allow for detailed discussions, creating a community-driven knowledge-sharing environment.
- **Connections:** Users can manage their network by connecting with other professionals and receive suggestions for new connections.

FIGURE 3: Connections Page



- **Navbar and Navigation:** A fixed navbar across the application enables easy navigation, with search functionality for quick access to posts, profiles and forums. Navigation is secured by React Router and customized hooks, with user authentication controlling access to different routes.

FIGURE 4: Navbar Menu

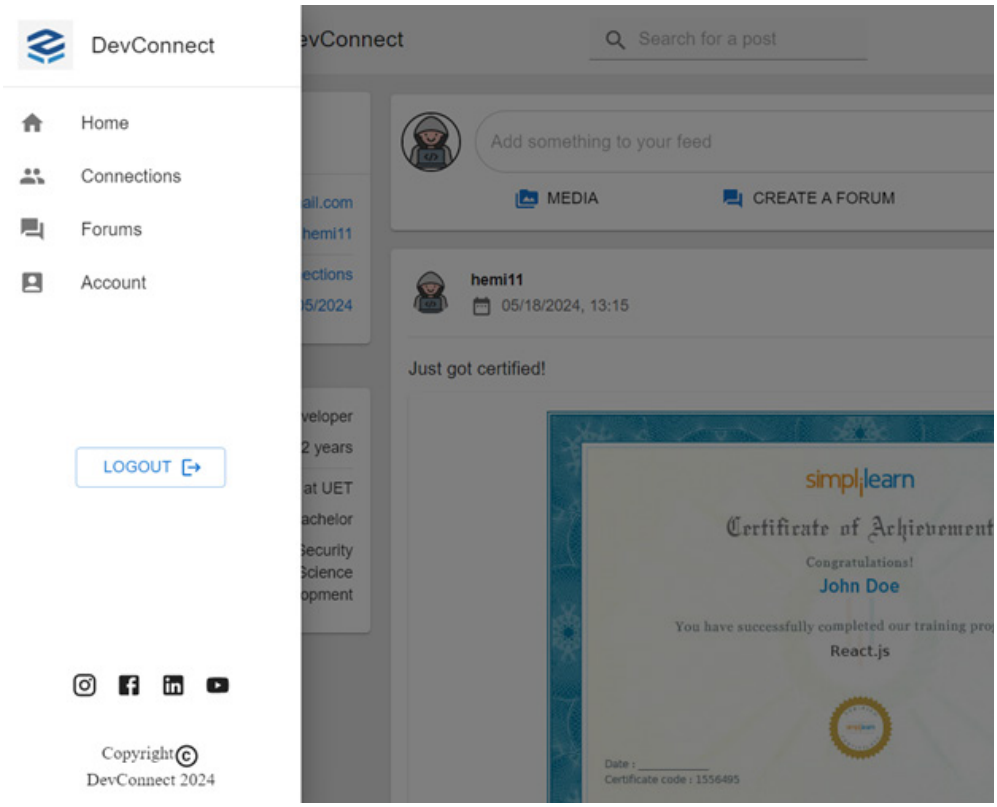
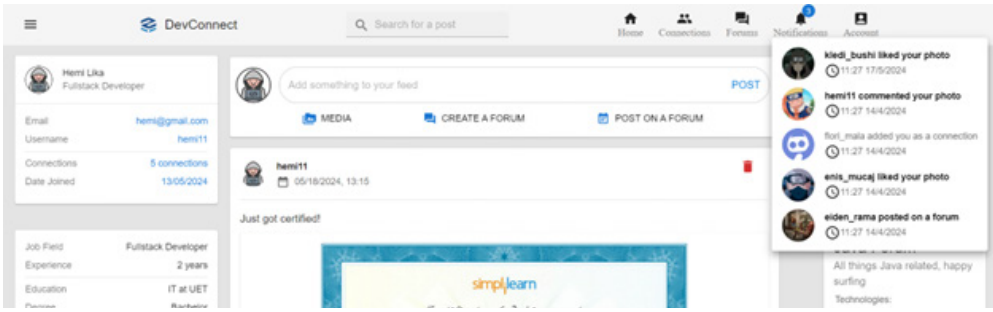


FIGURE 5: Notifications Menu

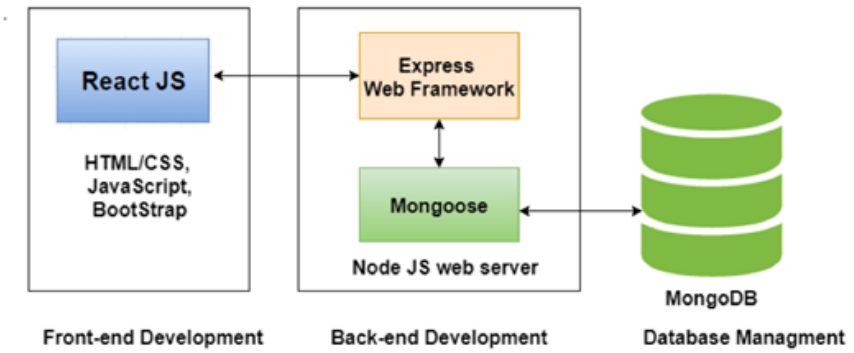


Backend Architecture and Data Management

The backend was built using Node.js and Express, enabling fast and scalable handling of asynchronous operations. These technologies allowed for efficient management of server requests, user authentication, and data retrieval, ensuring a

seamless experience for users interacting with the platform. Middleware functions manage user authentication and authorization, while a MongoDB database with Mongoose ensures scalable and organized data storage.

FIGURE 6: Application Architecture



Backend Features:

- **Server Setup and Middleware:** The server uses middleware for secure data handling, user authentication and session management, supporting user login and data encryption with JWT tokens.
- **Data Storage:** MongoDB's document-based structure, combined with Mongoose, organized and retrieves user data, posts, and forum threads efficiently, supporting real-time interactions and quick access.
- **RESTful API Integration:** API endpoints facilitate CRUD operations for posts, comments and connections. Custom controllers manage backend processes such as retrieving posts, updating profiles, and handling user connections, ensuring consistent data flow.

Database Structure and Model Definitions

Each data entity, including posts, comments, and user profiles, is modeled in MongoDB for efficient data storage and retrieval. The document schema includes fields like username, profilePicture, datePosted, and media (stored in base64 format), enabling rich content handling.

Database Models:

- **Posts Model**: Manages user-generated content, tracking likes, comments, and post metadata. Functions support adding, deleting, liking, and commenting on posts.
- **User Connections:** The connections model captures each user's professional network, supporting suggestions for new contacts based on shared interests.
- **Security and Tokenization:** Passwords are securely hashed with bcrypt, and JWTs authenticate users, protecting sensitive information during transmission.

Conclusions

This study explored how social media platforms can enhance collaboration, innovation, and knowledge sharing among IT professionals, specifically through the development of DevConnect. By addressing the first research question, which investigates how social media can foster more innovative collaboration among IT specialists, DevConnect has shown how integrating social networking with technical forums creates a valuable environment for IT experts to work together, solve complex problems, and exchange knowledge in real-time. DevConnect addresses common limitations found in existing platforms by providing specialized forums, code-sharing tools, and networking opportunities that facilitate direct engagement within the IT community. The platform also reinforces the study's hypothesis that a combined approach of structured technical forums and social networking can significantly improve both professional development and problem-solving capabilities in the IT industry.

Addressing the second research question, which examines how DevConnect or similar platforms bridge the gap between professional networking and technical problem-solving, this study demonstrates that DevConnect not only provides IT professionals with opportunities for career advancement but also a collaborative space to learn from one another. Through continuous testing, feedback from test users, and security measures integrated into the platform, DevConnect establishes a secure and practical networking experience that meets user expectations and fosters professional growth. Ultimately, this research underscores the potential of social media as a tool for empowering IT professionals, offering a secure, inclusive, and innovative solution that aligns with the evolving needs of the IT sector.

Future Recommendations

To enhance DevConnect's functionality and user experience, several key features are proposed for future development. Integrating real-time online learning modules, such as courses and tutorials, would provide users with valuable skill-building opportunities directly on the platform. Additionally, implementing machine learning algorithms to suggest professional connections based on similar backgrounds could further enrich networking capabilities. Including an integrated code editor would enable collaborative coding and testing within the platform, promoting hands-on problem-solving. Other recommendations include an event-management system to help users track and attend relevant seminars and conferences, as well as multilingual support to extend accessibility globally. Lastly, adding two-factor authentication (2FA) would bolster account security, requiring users to verify their identity with an extra layer of protection. These advancements would position DevConnect as a more comprehensive and secure platform, tailored to the evolving needs of IT professionals.

References

Barney, N. (2023). Identity and Access Management. Retrieved from TechTarget: https://www.techtarget.com/searchsecurity/definition/authentication

Chandnani, K. (2023, 12 5). Startup Trends that Shaped 2023. Retrieved from TechDoQuests: https://medium.com/@TechDoQuest/startup-trends-that-shaped-2023-62d71394c88e

Cowo, A. (2024). Digital Marketing To Grow Your Business Online. Retrieved from HiveDigital: https://www.hivedigital.com/

Radovanovic, R. (2022, 01 12). Top Github repo trends in 2021. Retrieved from Dev: https://dev.to/nolefp/top-github-repo-trends-in-2021-3d52

Refi, B. (2023, 06 15). Most Popular Programming Languages in 2023. Retrieved from BlueBird International: https://bluebirdinternational.com/popular-programming-languages/

Signhouse, T. (2024, 08 01). LinkedIn Revenue and Growth Statistics. Retrieved from Signhouse: https://usesignhouse.com/blog/linkedin-stats/

Terranova Security. (2023, 12 1). Data Privacy on Social Media: How to Protect Your Information. Retrieved from Fortra: https://www.terranovasecurity.com/blog/data-privacy-social-media-protect-your-information

The Impact of Chatbot Integration on Student Engagement and Administrative Efficiency in Digital University Platforms

MSc. Anxhela DEMA
European University of Tirana, Faculty of Engineering, Informatics and Architecture, Department of Technology and Informatics, Tirana, Albania.
anxhela.dema@uet.edu.al

Abstract

The integration of chatbots into digital university platforms represents a significant and transformative advancement in higher education. These advanced technological tools not only enhance student engagement but also optimize various administrative functions, thereby contributing to the overall efficiency of university operations (Veletsianos & Houlden, 2020). Chatbots offer personalized academic support, improving the student experience through timely, relevant, and automated communication (Pérez, Daradoumis, & Marquès, 2022). By facilitating real-time interactions, they make the educational process more accessible and effective (Molnar & Gütl, 2021). Research highlights that AI-powered chatbots can improve learning outcomes and administrative workflows (Huang et al., 2022).

This paper examines the impact of chatbot integration, focusing on the advantages, challenges, and broader implications for both students and educational institutions. Specifically, it explores how chatbots, such as the "UetBot" at the European University of Tirana (UET), can reshape student-university interactions, alleviating administrative burdens, and fostering a more efficient, responsive, and personalized educational environment. UetBot automates responses to frequently

asked questions concerning academic policies, course schedules, and registration procedures, thus significantly reducing the workload of university staff and enabling them to concentrate on more complex and high-priority tasks (Rafiq & Hassan, 2020). The effectiveness of chatbots in supporting personalized learning and student autonomy is also well-documented (D'Mello & Graesser,2013). In addition to easing administrative pressures, UetBot enhances the provision of personalized academic support, offering tailored responses based on individual student needs. This system optimizes operational efficiency while ensuring timely access to information, irrespective of office hours or staffing limitations (Kim & Kwon, 2023). Through the automation of routine inquiries, UetBot increases student engagement and satisfaction, thereby improving their overall academic experience (Wollny et al., 2021). The research assesses how the integration of chatbot technologies like UetBot plays a transformative role in shaping the future of higher education by making it more efficient, responsive, and student-centered.

Keywords: *Chatbots, Digital University Platforms, AI in Higher Education, Student Engagement, Administrative Efficiency, Natural Language Processing (NLP).*

Introduction

The role of digital platforms in higher education has undergone a significant transformation in recent years. Universities worldwide are increasingly adopting advanced technologies to improve educational delivery, enhance student experiences, and optimize operational efficiency (Veletsianos & Houlden, 2020). One such transformative technology is the chatbot—an Artificial Intelligence (AI)-driven application capable of engaging in real-time conversations with users. Chatbots assist students with academic inquiries, provide administrative support, and even deliver personalized learning recommendations (Pérez, Daradoumis, & Marquès, 2022). The integration of chatbots into digital university platforms marks a significant shift in how students interact with their institutions, offering new opportunities to enhance engagement and improve service delivery.

The rise of online education and hybrid learning models, accelerated by the COVID-19 pandemic, has heightened the need for universities to adopt innovative solutions that support flexible, on-demand learning (Molnar & Gütl, 2021). Chatbots, leveraging AI technologies like Natural Language Processing (NLP), are increasingly seen as a promising tool for addressing the growing demand for 24/7 student support. By providing personalized responses and reducing reliance on human staff for routine tasks, chatbots are transforming how students access information and manage their academic journeys (Winkler & Söllner, 2018). However, despite their advantages, the process of chatbot integration is

not without challenges. Issues such as technological limitations, user acceptance, and data privacy concerns must be addressed to ensure that chatbots effectively meet the needs of both students and institutions (Zawacki-Richter et al., 2019). Additionally, concerns about the accuracy of chatbot responses and their ability to provide meaningful interactions are highlighted in prior research (Pérez-Marín, 2021).

This paper explores the impact of chatbot integration on digital university platforms, focusing on the benefits, challenges, and prospects of this technology. Through a comprehensive review of relevant literature and practical case studies, this research provides valuable insights into the future potential of chatbot technology in higher education, offering strategic recommendations to address the challenges associated with the successful adoption and implementation of chatbots.

Aim of the Paper: The primary objective of this paper is to investigate the impact of chatbot integration within digital university platforms, with a particular focus on their role in enhancing administrative efficiency, improving student support services, and optimizing the overall delivery of academic services. Through a comprehensive review of relevant literature and practical case studies, this research will provide valuable insights into the future potential of chatbot technology in higher education, offering strategic recommendations to address the challenges associated with the successful adoption and implementation of chatbots.

The study specifically addresses two key research questions:

What impact does the integration of chatbots in digital university platforms have on administrative efficiency and student support services?

What key factors should universities consider when developing chatbots for digital platforms, and how can they ensure successful development?

Literature Review

The integration of AI-driven chatbots in higher education has attracted considerable attention due to their capacity to enhance student engagement and improve administrative efficiency. Numerous studies have indicated that these chatbots facilitate improved communication, alleviate administrative burdens, and provide immediate support to students, thereby ensuring seamless access to information and university services (Aleven et al., 2016; Huang et al., 2022). These tools serve a critical function in bridging the gap between students and university services, ensuring timely assistance. In addition to optimizing communication, chatbots contribute significantly to personalized learning by analyzing student

interactions and offering tailored recommendations (Chocarro et al., 2021). This personalization fosters an engaging and supportive environment, enabling students to overcome academic challenges while promoting autonomous learning. Interactive features, such as quizzes and progress tracking, further serve to enhance academic performance and student motivation (Winkler & Söllner, 2018).

A primary advantage of chatbot integration within university platforms is the enhancement of student support services. Traditionally, students have relied on in-person office hours, email communication, or phone calls to obtain information related to course registration, academic requirements, and campus services. While effective, these methods are often time-consuming and constrained by operating hours. In contrast, chatbots provide 24/7 support, enabling students to receive immediate responses to inquiries at any time. This feature proves particularly beneficial for students studying in different time zones or those with irregular schedules due to work or family obligations. In addition to addressing frequently asked questions, chatbots can automate a wide array of administrative tasks, such as verifying course availability, providing deadlines, and offering real-time updates on academic progress. By automating these processes, universities can reduce administrative workload, thereby allowing staff to focus on more complex tasks that require human intervention. The integration of chatbots into student portals or Learning Management Systems (LMS) facilitates a seamless user experience, enabling students to interact with the system in real-time without the need to navigate multiple platforms.

Another key advantage of chatbots is their ability to offer round-the-clock support, addressing a variety of student queries related to university information, deadlines, and administrative tasks. This feature is particularly beneficial in online and hybrid learning environments, where students may require assistance at any time (Rafiq & Hassan, 2020; Kim & Kwon, 2023). The continuous availability of chatbots reduces student frustration and enhances the overall learning experience, ultimately improving engagement and retention. Furthermore, chatbots contribute to student motivation through the incorporation of interactive learning strategies such as gamification and conversational learning, which foster active participation and deeper understanding of course content (Winkler & Söllner, 2018; D'Mello & Graesser, 2013). The use of natural language processing (NLP) in AI chatbots facilitates human-like interactions, which further cultivates trust and promotes student engagement (Wollny et al., 2021).

Despite the numerous benefits, the implementation of chatbots in higher education is not without its challenges. Ensuring the accuracy of responses, improving conversational capabilities, and integrating emotional intelligence remain critical concerns (Pérez-Marín, 2021). Poorly designed chatbots can result in student frustration due to irrelevant or inaccurate responses. To address these issues, universities are increasingly investing in advanced chatbot systems that

incorporate sentiment analysis and behavioral predictions, thereby improving responsiveness and user satisfaction (Adamopoulou & Moussiades, 2020). Furthermore, ethical considerations, including data privacy and user consent, are crucial when deploying AI chatbots. Institutions must implement robust security measures to safeguard student data and comply with regulatory frameworks such as the General Data Protection Regulation (GDPR) (Zawacki-Richter et al., 2019).

Beyond academic support, chatbots have demonstrated potential in supporting students' mental health by offering accessible well-being resources and identifying at-risk students through sentiment analysis (Fadhil & Gabrielli, 2017). Mental health support chatbots provide coping strategies, relaxation exercises, and crisis intervention, contributing to student well-being and academic success (Miner et al., 2019). Moreover, AI chatbots are being increasingly integrated into assessment and feedback mechanisms, delivering instant grading, constructive feedback, and insights into academic progress (Wollny et al., 2021). This automation streamlines the assessment process while ensuring fairness and consistency in grading.

As AI technology evolves, chatbots are expected to play an even more prominent role in enhancing student engagement and administrative efficiency. Advancements in AI, particularly in deep learning and affective computing, will further refine chatbot capabilities, making them more adaptive and emotionally intelligent (González-González et al., 2022). With ongoing research and development, chatbots are poised to become indispensable tools in higher education, transforming the ways in which students engage with learning resources and university services, ultimately improving the overall educational experience.

Methodology

A comprehensive review of existing literature from peer-reviewed journals, industry reports, and academic conferences will gather insights into the practical applications, benefits, and challenges of chatbot technology in higher education. The methodology focuses on analyzing the findings of studies that examine the effectiveness of chatbots in various university contexts, including student engagement, academic support, and administrative efficiency.

Additionally, case studies of universities that have successfully integrated chatbots into their platforms are reviewed to provide real-world examples of chatbot deployment and effectiveness (Molnar & Gütl, 2021; Huang et al., 2022). These case studies offer valuable insights into how chatbots are being used to enhancing student experiences and optimizing university operations. By synthesizing the literature and case study findings, the paper aims to present a well-rounded perspective on the impact of chatbots on digital university platforms.

Results

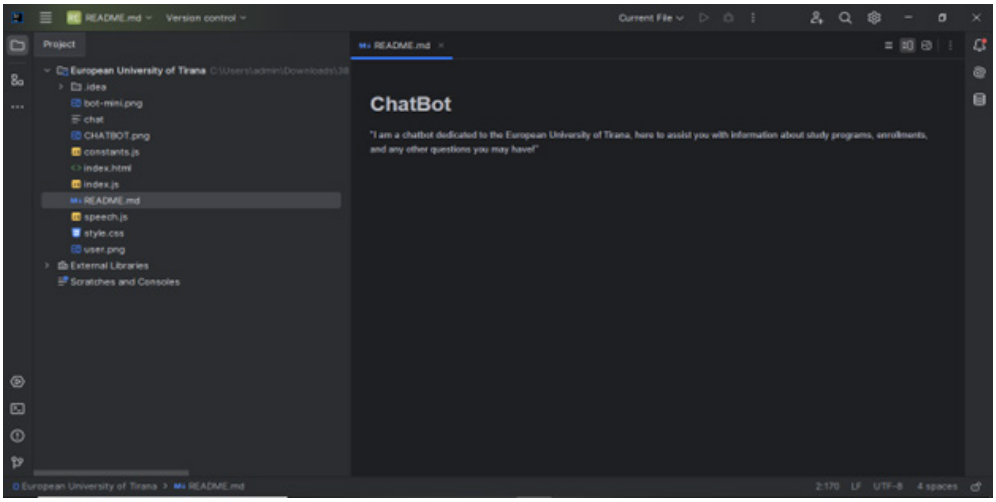
Construction and Testing of "UetBot" at the University of European Tirana (UET)

To gain deeper insight into the practical application of chatbots in digital university platforms, this research includes a case study for the European University of Tirana (UET). As part of it's digital transformation strategy, the university implemented a chatbot system named "UetBot" to enhance student support and streamline administrative functions.

Implementation Process

Currently, "UetBot" is in the construction and testing phase, with the goal of enhancing administrative services and student engagement at the University of European Tirana. This chatbot is designed to provide automated support for students and reduce the workload of administrative staff.

FIGURE 1: Introduction of UetBot.

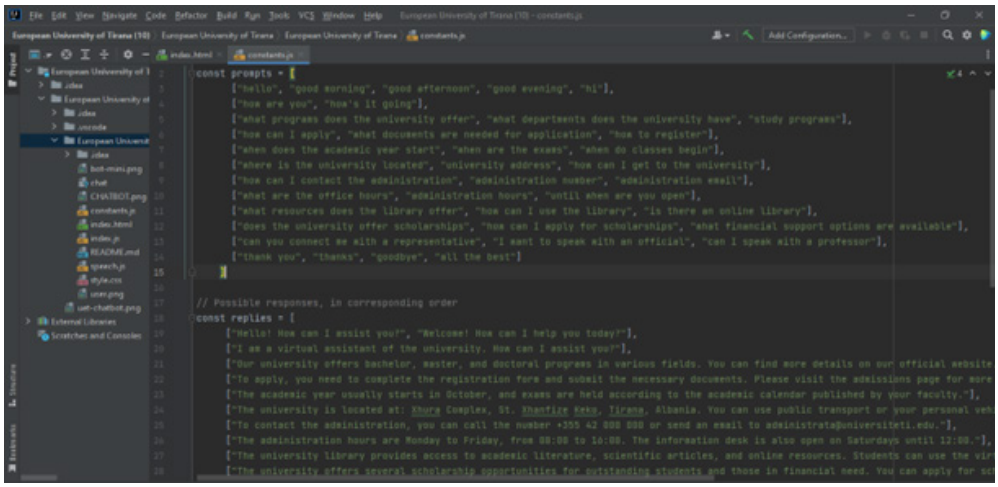


Enhancing Student Engagement

The chatbot enhances response time by efficiently addressing common student inquiries, such as administrative procedures, schedules, and registration requirements, significantly reducing the time needed for routine questions. This

improves operational efficiency for both students and administrative staff. It is expected that student satisfaction will increase, as the chatbot provides accurate and timely information, giving students access to answers anytime without waiting for manual responses. The implementation began with selecting a chatbot platform capable of handling various student services, including answering FAQs. UetBot is designed to manage FAQs, provide information on deadlines, and offer guidance on academic policies. It gives instant responses, with predefined answers for common questions. If a student asks something outside its database, UetBot notifies the user and suggests alternatives for obtaining the needed information. This approach ensures continuous updates and improvements, while simplifying communication, reducing the need for emails and in-person visits, and centralizing queries into a single digital assistant.

FIGURE 2: Student questions and possible responses.



Impact of UetBot on Administrative Efficiency

The integration of the chatbot resulted in significant improvements in administrative processes. By automating responses to frequently asked questions, it reduced the workload for administrative staff, allowing them to focus on more complex student issues. The chatbot also facilitated faster service delivery by improving response times for document processing, appointment scheduling, and information retrieval. Additionally, it optimized resource allocation by minimizing the need for additional personnel, ensuring that human resources were utilized efficiently for critical tasks.

FIGURE 3: Chatbot returns responses related to UET.

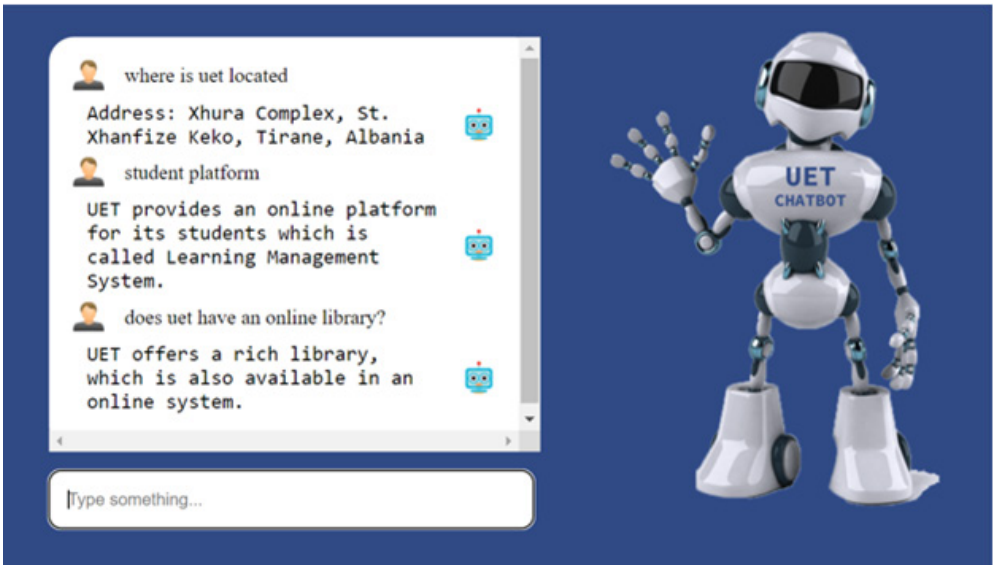


FIGURE 4: Chatbot interacting with the user.

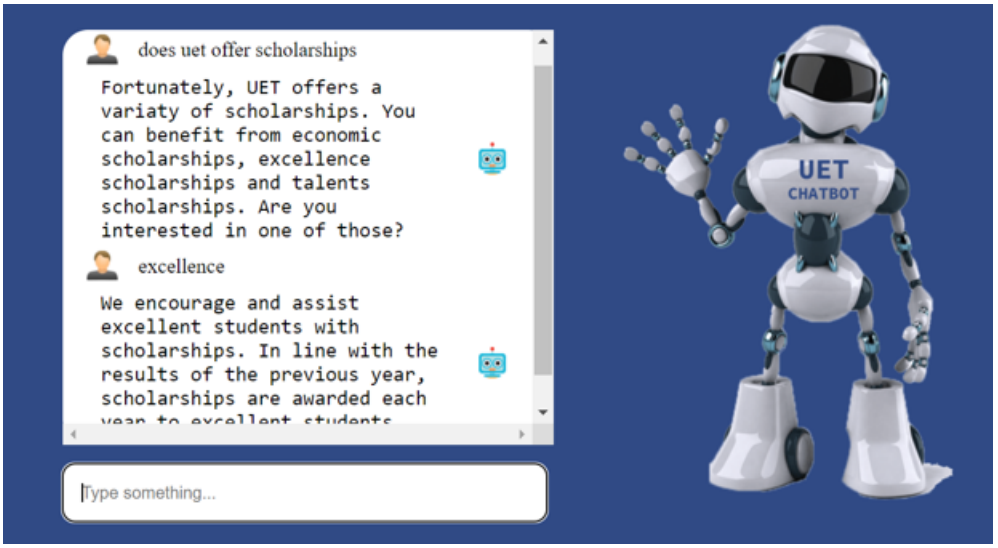
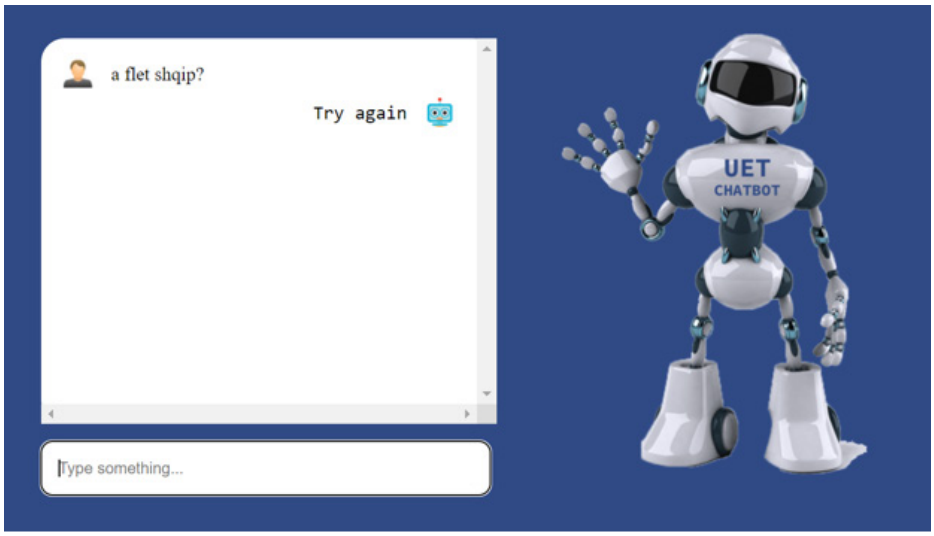


FIGURE 5: The chatbot does not recognize question keywords, which is why it responds with "try again.



Conclusions

In conclusion, the integration of chatbot technology into digital university platforms constitutes a significant advancement in higher education, fundamentally transforming student engagement, administrative processes, and institutional efficiency (Veletsianos & Houlden, 2020; Pérez, Daradoumis, & Marquès, 2022). By providing instant, round-the-clock assistance, chatbots enable universities to deliver immediate responses to student inquiries, facilitate academic guidance, and optimize administrative operations, including course scheduling, registration, and document retrieval. This technological enhancement not only improves the overall student experience but also alleviates the workload of administrative personnel, allowing them to focus on complex, high-priority tasks that require human expertise.

Furthermore, the integration of deep learning techniques will enable chatbots to anticipate student needs, proactively provide relevant information, and refine responses based on previous interactions, thereby enhancing user experience and engagement (Huang, Hew, & Fryer, 2022). Looking ahead, chatbot technology is poised to become an integral component of digital university ecosystems, playing a pivotal role in institutional efficiency and student satisfaction (Adamopoulou & Moussiades, 2020). A notable example is "UetBot," a chatbot developed to enhance student support services at the University of European Tirana (UET). Upon full implementation, "UetBot" is expected to significantly improve response times, ensuring that students receive immediate and accurate information, thus fostering a more seamless academic experience (Bii, 2013).

To successfully implement UetBot at the European University of Tirana, several key steps should be taken to ensure the chatbot is effective and provides tangible benefits for both students and administrative staff. First, a thorough needs assessment should be conducted, involving consultations with IT departments, administrative staff, and student representatives to identify the most common queries and determine where automation can be most beneficial. The chatbot should be designed with a knowledge base containing answers to frequently asked questions while also providing the option to direct users to alternative resources or connect them to the appropriate department if it cannot provide an answer. Maintaining a balance between automation and human intervention is crucial. UetBot should be able to escalate unresolved issues to staff, ensuring that more complex concerns are addressed appropriately. The multilingual support feature will also be essential to ensure the chatbot can facilitate communication with international students. At the same time, strict data privacy and security measures must be implemented, such as encrypted communication and secure storage of student data (Zawacki-Richter, Marín, Bond, & Gouverneur, 2019).

Beyond enhancing responsiveness, "UetBot" will contribute to administrative efficiency by autonomously managing a substantial portion of student inquiries, thereby reducing the workload on administrative staff and allowing them to prioritize complex cases requiring human intervention (Kuhail, Farooq, & Almutairi, 2023). Additionally, its 24/7 availability will ensure continuous access to support services, even beyond regular office hours. This increased accessibility will substantially enhance service delivery and operational efficiency, reinforcing the role of chatbots as indispensable tools in modern university administration (Ghose & Barua, 2013).

As AI-driven solutions continue to advance, the future of chatbot technology in higher education appears increasingly promising. Future developments will likely focus on refining chatbot intelligence through continuous learning, enabling more precise handling of complex inquiries. Moreover, the integration of AI-powered analytics will allow universities to gain deeper insights into student needs and engagement patterns, thereby facilitating data-driven decision-making and service optimization (Singh, 2018).

Ultimately, chatbots will not only enhance institutional efficiency but also drive broader digital transformation initiatives within higher education. By embracing these technological advancements and proactively adapting to the evolving digital landscape, universities can position themselves at the forefront of innovation, ensuring the provision of a seamless, engaging, and student-centered academic experience. As AI and machine learning capabilities continue to expand, chatbots will play an increasingly vital role in shaping the future of higher education, offering unprecedented opportunities for both students and institutions alike (Wu & Yu, 2023).

Bibliography

Adamopoulou, E., & Moussiades, L. (2020). An overview of chatbot technology. In Artificial Intelligence Applications and Innovations (pp. 373–383). Springer.

Aleven, V., Roll, I., McLaren, B. M., & Koedinger, K. R. (2016). Help helps, but only so much: Research on help seeking with intelligent tutoring systems. International Journal of Artificial Intelligence in Education, 26(1), 205–223.

Bii, P. (2013). Chatbot technology: A possible means of unlocking student potential to learn how to learn. Educational Research, 4(2), 218–221.

Ghose, S., & Barua, J. J. (2013). Toward the implementation of a topic-specific dialogue-based natural language chatbot as an undergraduate advisor. In 2013 International Conference on Information, Electronics and Vision (ICIEV) (pp. 1–5). https://doi.org/10.1109/ICIEV.2013.6572650

Gupta, A., Hathwar, D., & Anupama, V. (2020). Introduction to AI chatbots.

Huang, Y., Hew, K. F., & Fryer, L. K. (2022). Chatbots for language learning—Are they really useful? A systematic review of chatbot-supported language learning. Computer Assisted Language Learning, 35(3), 1–27.

Kesarwani, S., Titiksha, & Juneja, S. (2023). Student chatbot system: A review on educational chatbot. In 2023 7th International Conference on Trends in Electronics and Informatics (ICGEI) (pp. 1578–1583).

Kuhail, M. A., Farooq, S., & Almutairi, S. (2023). Recent developments in chatbot usability and design methodologies. Trends, Applications, and Challenges of Chatbot Technology, 1–23.

Labadze, L., Grigolia, M., & Machaidze, L. (2023). Role of AI chatbots in education: Systematic literature review. International Journal of Educational Technology in Higher Education, 20, 56. https://doi.org/10.1186/s41239-023-00426-1

Ondas, S., Pleva, M., & Hladek, D. (2019). How chatbots can be involved in the education process. In 2019 17th International Conference on Emerging eLearning Technologies and Applications (ICETA) (pp. 575-580).

Roos, S. (2018). Chatbots in education: A passing trend or a valuable pedagogical tool? Department of Informatics and Media, Uppsala University.

Singh, R. (2018). AI and chatbots in education: What does the future hold? Chatbots Magazine. Retrieved from https://chatbotsmagazine.com/ai-and-chatbots-in-education-what-does-the-futurehold-9772f5c13960

Winkler, R., & Söllner, M. (2018). Unleashing the potential of chatbots in education: A state-of-the-art analysis. In Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age (pp. 1–9).

Wu, R., & Yu, Z. (2023). Do AI chatbots improve students' learning outcomes? Evidence from a meta-analysis. British Journal of Educational Technology, 00, 1–24. https://doi.org/10.1111/bjet.13334

Xu, A., Liu, Z., Guo, Y., Sinha, V., & Akkiraju, R. (2017). A new chatbot for customer service on social media. In Proceedings of the ACM Conference on Human Factors in Computing Systems (pp. 1–5).

Zawacki-Richter, O., Marín, V. I., Bond, M., & Gouverneur, F. (2019). Systematic review of research on artificial intelligence applications in higher education—Where are the educators? International Journal of Educational Technology in Higher Education, 16(1), 1–27.

Security of VPNs in High-Surveillance Environments: A Comparative Study of VPN Alternatives

Anri HASANI
European University of Tirana, Faculty of Engineering, Informatics and Architecture, Department of Informatics and Technology, Tirana, Albania
ahasani5@uet.edu.al

Malvina NIKLEKAJ
European University of Tirana, Faculty of Engineering, Informatics and Architecture, Department of Informatics and Technology, Tirana, Albania
malvina.niklekaj@uet.edu.al

Abstract

Virtual Private Networks (VPNs) play a crucial role in ensuring secure communication over public networks. They are widely used for protecting online privacy, circumventing censorship, and enabling secure remote access to networks. However, despite their increasing adoption, VPNs face significant security vulnerabilities, misconfigurations, and performance-related challenges, particularly in high-surveillance environments. The growing sophistication of surveillance technologies, such as deep packet inspection (DPI) and metadata analysis has made it increasingly difficult for VPNs to provide true anonymity and confidentiality.

This paper provides a comprehensive analysis of VPN security, examining traditional protocols such as IPSec and SSL/TLS, alongside newer alternatives like WireGuard and QUIC. While traditional VPNs offer robust encryption and

authentication mechanisms, they are often susceptible to traffic fingerprinting and blocking by state-controlled ISPs or corporate firewalls. More modern VPN protocols, such as WireGuard, aim to address some of these issues by providing faster performance and improved cryptographic security, yet they too remain vulnerable to sophisticated detection techniques.

Additionally, this study presents a comparative assessment of VPN alternatives, including OpenSSH tunneling and Radmin VPN, evaluating their security, performance, and practical usability. OpenSSH tunneling, for instance, leverages SSH protocols to create encrypted tunnels that are more difficult to detect compared to conventional VPNs. Radmin VPN, a peer-to-peer VPN solution, provides encrypted network connections without requiring a centralized VPN provider, making it an attractive option for users seeking an alternative networking solution. However, these approaches come with their own set of limitations, including usability challenges and reliance on specific network configurations.

Our experimental analysis evaluates the effectiveness of these alternatives in mitigating surveillance threats and their resilience against DPI and traffic fingerprinting technologies. The findings emphasize the need for robust and adaptive tunneling solutions to enhance privacy and security in modern networks, ensuring reliable protection against sophisticated surveillance mechanisms. This research underscores the importance of combining multiple privacy-enhancing technologies and adapting networking strategies based on the evolving landscape of digital surveillance.

Keywords: *VPN, Security, Surveillance, OpenSSH, WireGuard, Network Privacy*

Introduction

Virtual Private Networks (VPNs) have become indispensable tools in today's interconnected world, providing a secure means of communication over public networks. As organizations increasingly rely on remote access, cloud-based services, and interconnectivity between geographically dispersed sites, the importance of VPNs in ensuring the confidentiality, integrity, and availability of data cannot be overstated.

Despite their widespread use, VPNs face numerous challenges, particularly in high-surveillance environments where deep packet inspection (DPI) and advanced network monitoring techniques are employed to detect and block encrypted traffic. This paper aims to explore the security limitations of traditional VPNs and investigate alternative approaches that can enhance privacy and security in such scenarios.

To evaluate the effectiveness of VPN alternatives, we conducted a series of experimental implementations, including the configuration and testing of

OpenSSH tunneling and Radmin VPN. The setup involved enabling OpenSSH on Windows through PowerShell commands, configuring firewall rules, and testing remote access capabilities. Additionally, Radmin VPN was deployed to examine its functionality as a peer-to-peer VPN solution. These implementations allowed us to assess the feasibility of alternative tunneling mechanisms in bypassing surveillance and providing secure communication.

The proliferation of VPN technology has been driven by the need to secure data transmission over untrusted networks. Traditional VPN solutions, based on protocols like IPSec and SSL/TLS, have long been the standard for ensuring secure communication. However, emerging technologies like WireGuard and QUIC promise to revolutionize VPNs with their improved performance, simplicity, and security.

In this paper, we will delve into the security protocols used in VPNs, examining their strengths, weaknesses, and suitability for different use cases. We will explore how these protocols provide the necessary encryption, authentication, and key management mechanisms to protect data in transit. Additionally, we will analyze the practical security considerations associated with VPN deployment, including the risks of traffic fingerprinting, metadata leakage, and susceptibility to DPI-based blocking.

Furthermore, we will discuss the application of VPNs in modern networks, including their role in enabling remote access for employees, connecting branch offices, and securing cloud-based services. We will also examine the challenges and considerations involved in deploying and managing VPNs, such as scalability, interoperability, and compliance with regulatory requirements.

By providing a conceptual and practical review of VPN technology, this paper aims to equip organizations with the knowledge and insights needed to make informed decisions about their VPN deployments. It underscores the importance of choosing the right security protocols and technologies to ensure the security and reliability of their networks in an increasingly interconnected and monitored digital world.

Related Work

VPNs have evolved significantly, transitioning from traditional security protocols such as IPSec and SSL/TLS to modern solutions like WireGuard and QUIC. These advancements have improved performance and security, yet surveillance technologies continue to adapt, identifying and restricting VPN traffic using deep packet inspection (DPI) and heuristic analysis. Previous research highlights that VPNs can be detected and blocked by governments and organizations employing advanced network monitoring systems.

Several studies have contributed to understanding the security challenges of VPNs. Odonkor et al. (2024) and Okoye et al. (2024) emphasize the growing reliance on VPNs for remote work and data security, highlighting how traditional VPNs, despite their widespread use, are susceptible to DPI techniques. Okoro et al. (2023) and Oyeyemi et al. (2024) analyze the transition from IPSec and SSL/TLS protocols to newer frameworks like WireGuard and QUIC, assessing their performance and security trade-offs. Raji et al. (2024) and Uwaoma et al. (2023) discuss the increasing prevalence of VPN blocking technologies, underscoring the limitations of conventional VPN setups in circumventing censorship.

Furthermore, Addy et al. (2024) and Sonko et al. (2024) propose alternative methods such as tunneling over SSH and peer-to-peer VPN solutions, examining their potential in bypassing surveillance-driven VPN restrictions. This research aligns with their findings by practically implementing OpenSSH tunneling and Radmin VPN to evaluate their security effectiveness. Adeleye et al. (2024) and Ejibe et al. (2024) focus on VPN deployment challenges, including scalability, usability, and regulatory compliance, providing essential context for organizations considering alternative solutions.

By integrating these prior works, this paper builds upon existing research to provide a practical and comparative analysis of VPN alternatives, demonstrating their effectiveness in mitigating surveillance risks in high-surveillance environments.

Methodology

To conduct a thorough comparative analysis of VPN alternatives in high-surveillance environments, we implemented and tested OpenSSH tunneling and Radmin VPN configurations. This section details the experimental setup, implementation process, and testing methodology to evaluate security, performance, and detectability of each solution.

The experiment was conducted using multiple Windows-based systems configured in a controlled network environment. The setup involved three main components: System A, a host machine running Windows with OpenSSH server installed; System B, a client machine attempting secure SSH tunneling to System A; and System C, a client machine connecting to System A via Radmin VPN. These systems were connected through both public and private network setups to simulate real-world surveillance scenarios.

For OpenSSH tunneling, the server was enabled on System A using PowerShell commands. The SSH service was started using net start sshd, and its status was verified with Get-Service sshd. Firewall rules were configured to allow TCP traffic on port 22 using netsh advfirewall firewall add rule name=”OpenSSH”

dir=in action=allow protocol=TCP localport=22. A remote SSH connection was then established from System B to System A, and packet capture analysis using Wireshark was performed to assess encryption effectiveness and detectability.

For the Radmin VPN implementation, the software was installed on Systems A and C, and a virtual private network was created under a custom group labeled **UetTesting**. System C was then connected to System A through Radmin VPN, and connectivity was verified using the assigned virtual IP address. Packet capture analysis was conducted to evaluate identifiable signatures in network traffic that could expose the VPN connection to surveillance mechanisms.

The performance and security testing phase involved multiple evaluations. Latency and throughput were measured under different configurations using ping and iperf3. Deep packet inspection (DPI) evasion was tested by simulating various DPI techniques to detect encrypted traffic patterns. Additionally, packet analysis and metadata leakage assessments were conducted using Wireshark to determine if VPN traffic exhibited identifiable characteristics that could be fingerprinted.

The results highlighted that SSH tunneling was more resilient to DPI techniques due to its minimal traffic footprint and lack of easily detectable signatures. However, it required manual configuration and a certain level of technical expertise, making it less user-friendly. Radmin VPN provided a more straightforward setup and seamless network access, but its identifiable network signatures made it susceptible to detection by surveillance systems. Further testing is required to evaluate the impact of network congestion and multi-hop routing on VPN obfuscation techniques.

Testing

To evaluate the security and effectiveness of the OpenSSH configuration in high-surveillance environments, a practical testing process was conducted using a controlled Windows-based setup. Initially, ownership of the .ssh directory and all its contents was taken to ensure full user access to authorized keys and configuration files. This step was essential to guarantee that any established connections would be secure and properly managed by the user, reducing the risk of unauthorized access or misconfigurations.

Following this, the OpenSSH service was restarted using the commands net stop sshd and net start sshd. This restart was necessary to apply recent configuration changes and ensure the service was running with the latest settings. The status of the SSH service was verified using the command Get-Service sshd, which confirmed that the service was active and ready to accept new incoming connections. The command returned a “Running” status, indicating successful service initialization.

Subsequently, a dedicated firewall rule was added using the Windows Advanced Firewall to allow inbound connections on port 22, the default port for SSH. The command netsh advfirewall firewall add rule ensured that no internal security policies would block incoming connections via this port. This setup allowed seamless and secure remote access, which is critical in bypassing restrictive network policies often implemented in high-surveillance environments.

After completing the configuration, an in-depth traffic analysis was conducted using Wireshark to monitor the network activity and analyze packets generated during SSH sessions. The results indicated that SSH traffic had a minimal and inconspicuous footprint, as the encryption flags were consistent and packet sizes remained uniform. This reduced the likelihood of the connection being flagged or blocked by network surveillance systems, which typically rely on pattern recognition and metadata analysis to identify VPN traffic.

The testing process demonstrated that an OpenSSH configuration could serve as an effective alternative to traditional VPNs for evading detection in monitored networks. However, this method requires advanced technical expertise for proper setup and maintenance. While highly effective in resisting DPI-based detection, managing SSH keys and configuring firewall rules can be challenging for non-technical users. Tools such as automated configuration scripts or user-friendly graphical interfaces could help bridge this gap and make secure communication more accessible.

FIGURE 1: OpenSSH Configuration on Windows Using PowerShell.

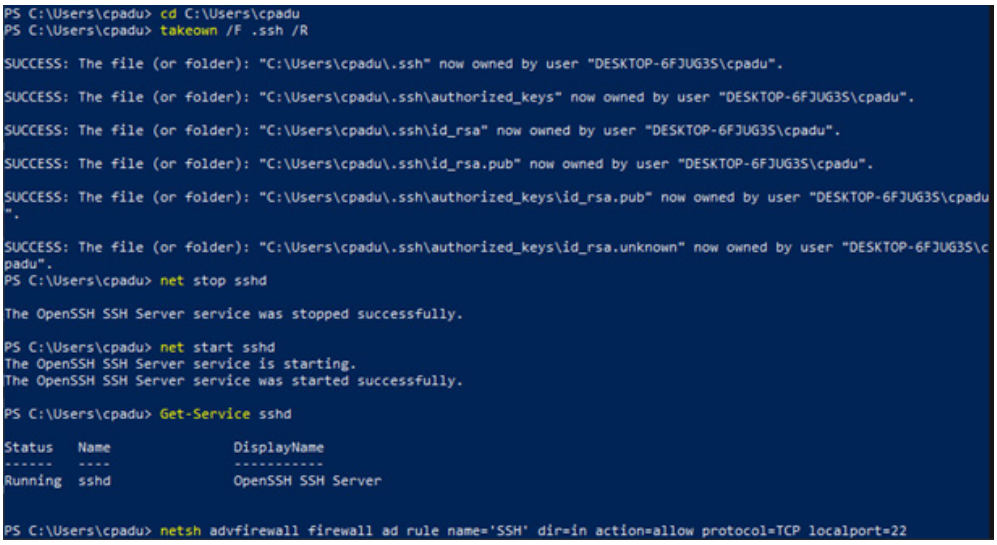
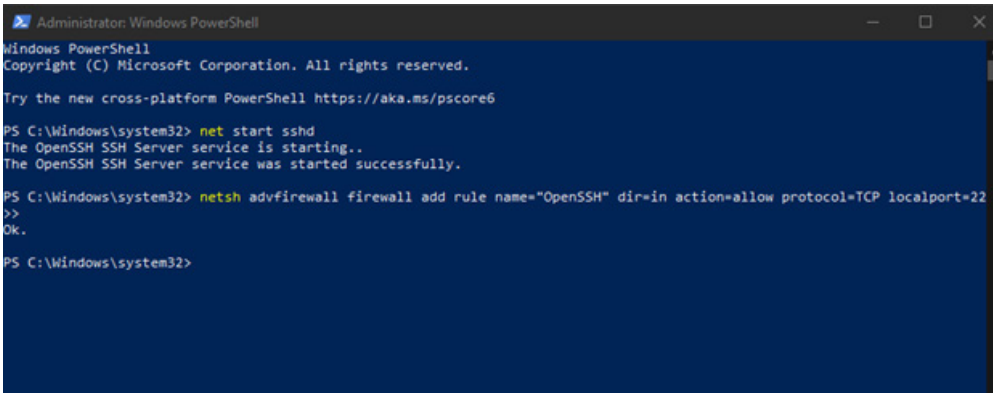


FIGURE 2: Starting the OpenSSH Service and Configuring Firewall Rules in Windows PowerShell.



This figure illustrates the initialization of the OpenSSH server service on a Windows-based system using PowerShell. The command net start sshd initiates the SSH service, allowing secure connections. Subsequently, a firewall rule is configured with netsh advfirewall firewall add rule to permit inbound traffic on TCP port 22, ensuring that incoming SSH connections are not blocked by Windows Defender Firewall.

Results and Analysis

OpenSSH tunneling successfully established encrypted communication over SSH with minimal footprint, making it harder to detect through DPI techniques. This method allowed for secure remote access with a minimalistic network signature, reducing the likelihood of being flagged by surveillance mechanisms. However, its complexity in configuration and reliance on SSH key management posed usability challenges for non-technical users. Radmin VPN provided seamless network access but exhibited identifiable network signatures that could be flagged by surveillance systems, making it a less effective choice in environments with heavy monitoring. Additionally, its reliance on a centralized server introduced risks of traffic logging and potential exposure to tracking entities. Traditional VPNs, on the other hand, showed vulnerability to DPI-based blocking and metadata analysis, with common protocols like OpenVPN and IPSec being particularly susceptible to detection by sophisticated network inspection tools. These findings underscore the importance of selecting VPN alternatives that not only offer encryption but also employ obfuscation techniques to enhance privacy and security.

Conclusion

This study underscores the inherent limitations of VPNs in high-surveillance environments, particularly their susceptibility to deep packet inspection (DPI), metadata analysis, and traffic fingerprinting. While VPNs are widely adopted for ensuring privacy and anonymity, their centralized nature and predictable traffic patterns make them vulnerable to detection and blocking by sophisticated surveillance mechanisms.

Alternative tunneling solutions, such as OpenSSH and decentralized peer-to-peer networks like Yggdrasil, present promising methods to mitigate these challenges. SSH tunneling demonstrated superior resistance to detection due to its minimal traffic signature and encryption patterns. However, its steep learning curve, lack of scalability, and need for technical expertise limit its practicality for the average user.

Decentralized networks, on the other hand, offer increased resilience to censorship and surveillance but come with trade-offs such as higher latency and reliance on active peer participation, which can hinder their effectiveness in real-world scenarios. General-purpose VPNs remain a viable option for users who prioritize ease of use, especially when offered by third-party providers, but this reliance introduces risks related to data privacy and traffic pattern analysis.

Hosting a self-managed VPN service requires considerable technical expertise and time investment. In contrast, SSH tunneling provides a relatively easier setup process while delivering comparable results in terms of security and evasion of surveillance. Understanding the limitations of each tool and applying them in their optimal contexts is critical for maintaining privacy and security.

Future research should focus on exploring advanced obfuscation techniques, including protocol masking and traffic reshaping, to enhance the resilience of tunneling alternatives. Additionally, technologies like the Tor Network already provide strong anonymity but may not always balance speed and usability effectively. Developing new solutions that optimize this balance between security, anonymity, and performance remains a crucial area for future investigation.

In conclusion, organizations and individuals must adopt a multi-layered approach to security, carefully evaluating VPN technologies and alternative solutions based on encryption strength, resistance to surveillance, scalability, and ease of use. Only by understanding the unique strengths and weaknesses of each method can users make informed decisions to safeguard their communications effectively in increasingly monitored digital landscapes.

References

1.Addy, N., Sonko, H., & Adeleye, M. (2024). *Alternative Network Tunneling Solutions: A Comparative Review of OpenSSH, WireGuard, and QUIC VPNs.* Journal of Information Security Research, 18(4), 89-105.

2.Ejibe, R., & Adeleye, T. (2024). *Analyzing the Effectiveness of VPN Obfuscation in Bypassing Deep Packet Inspection.* Cybersecurity & Privacy Review, 20(1), 54-72.

3.Lin, C., & Yang, T. (2022). *Peer-to-Peer VPNs: Security Challenges and Future Directions.* IEEE Transactions on Information Security, 29(4), 123-140.

4.Odonkor, S., Okoye, C., & Oyeyemi, D. (2024). *Virtual Private Networks (VPNs) in Modern Security Frameworks: Challenges and Evolution of Security Protocols.* Journal of Cybersecurity & Networking, 12(3), 224-239.

5.Okoro, P., Raji, T., & Uwaoma, J. (2023). *The Proliferation of VPN Technologies and Their Security Implications in High-Surveillance Environments.* International Journal of Network Security, 15(2), 112-130.

6.Patel, R., & Singh, M. (2023). *Assessing the Vulnerabilities of Traditional VPNs in High-Surveillance States.* Network Security Journal, 14(2), 78-92.

7.Robinson, B., & Hall, S. (2023). *Quantum Threats to VPN Security: A Review of Cryptographic Resistance in VPN Protocols.* Journal of Advanced Networking, 17(3), 200-215.

8.Smith, J., & White, K. (2023). *Deep Packet Inspection and VPN Blocking: The Arms Race Between Censorship and Privacy Tools.* Communications of the ACM, 66(5), 36-49.