

Keyshield: Preventing Fake Accounts Through Locker-Based Authentication

Sathishkumar. P¹, Chandrakala. S², Baraninishanth.P³, Gokulraj.M⁴, Gurukishore.T⁵

¹Assistant Professor, Dept. of Cybersecurity, Paavai Engineering College

²Assistant Professor, Dept. of Cybersecurity, Paavai Engineering College

³Student, Dept. of Cybersecurity, Paavai Engineering College

⁴Student, Dept. of Cybersecurity, Paavai Engineering College

⁵Student, Dept. of Cybersecurity, Paavai Engineering College

Abstract - The rapid growth of social media platforms has led to a significant increase in fake and duplicate accounts, which are widely used for spam, misinformation, scams, and cyber threats. Existing systems primarily focus on detecting fake accounts after their creation, allowing malicious users to exploit platforms temporarily before being identified. This paper proposes a secure locker-based authentication system, "KeyShield," designed to prevent fake account creation at the initial stage. The system introduces a centralized digital locker that generates a unique authentication key for each verified user based on their email and phone number. This key is mandatory for accessing social media platforms, ensuring that each individual can maintain only a single authentic identity. By shifting from detection to prevention, the proposed system enhances security, reduces duplicate account creation, and improves trust in online platforms. The framework is scalable, efficient, and suitable for integration with modern digital ecosystems.

Key Words: Fake Account Prevention, Authentication System, Digital Locker, Unique Key Generation, Cybersecurity, Social Media Security

1. INTRODUCTION

In today's digital world, social media platforms play a crucial role in communication, networking, and information sharing. However, the rapid growth of these platforms has also led to an increase in fake and duplicate accounts. These accounts are often used for malicious activities such as spreading misinformation, performing scams, and launching cyber attacks. Traditional authentication systems rely on usernames, passwords, or third-party login services, which are vulnerable to misuse. Moreover, most existing solutions focus on detecting fake accounts only after they have been created, which allows attackers to operate temporarily and cause damage. To address this issue, this project introduces "KeyShield," a locker-based authentication system that prevents fake account creation at the initial stage. The system generates a unique authentication key for each user through a secure digital locker. This key acts as a mandatory credential for accessing social media platforms, ensuring that each user

maintains only one verified identity. By focusing on prevention rather than detection, the proposed system aims to enhance security, reduce duplication, and create a safer digital environment.

2. PRIMARY OBJECTIVES OF THE STUDY

- The primary objective of the proposed KeyShield system is to establish a secure, scalable, and prevention-oriented authentication framework capable of eliminating fake and duplicate account creation in social media platforms. Unlike traditional systems that rely on reactive detection mechanisms, this approach focuses on enforcing identity uniqueness at the initial stage of user registration.

- A key objective is to design a centralized digital locker architecture that functions as an independent identity provider. This locker securely stores user credentials and ensures that each individual is verified using unique identifiers such as email address and phone number. By integrating validation mechanisms, the system guarantees that only legitimate users can proceed with the registration process.

- Another critical objective is the generation of a unique authentication key for every registered user. This key acts as a secure digital identity token, which is required for accessing third-party platforms. The system enforces a strict one-user-one-key policy, thereby preventing users from creating multiple accounts using different credentials.

- Ensuring seamless integration with social media platforms is also an important goal. The proposed system is designed to function similarly to existing authentication providers, enabling easy adoption without disrupting current workflows. This enhances usability while maintaining high security standards.

- Furthermore, the system aims to improve trust and reliability in digital ecosystems by reducing malicious activities such as spam, impersonation, and automated bot attacks. By combining centralized authentication with strong identity validation, the KeyShield framework aspires to create a safer and more accountable online environment.

3. LITERATURE SURVEY

A comprehensive review of existing research reveals that the problem of fake and duplicate account creation in social media platforms has been widely studied using various detection-based methodologies. These approaches primarily focus on identifying malicious accounts after their creation through behavioral analysis, machine learning techniques, and identity verification mechanisms. While each method offers certain advantages, they also exhibit significant limitations in terms of prevention, scalability, and accuracy.

3.1 Machine Learning-Based Fake Account Detection

A considerable body of research has explored the application of machine learning algorithms for detecting fake accounts. Techniques such as Support Vector Machines (SVM), Random Forest, and Neural Networks are commonly used to classify user accounts based on features like posting behavior, friend networks, and activity frequency. These models are trained on large datasets to identify patterns associated with malicious behavior. The primary advantage of this approach lies in its ability to detect complex and evolving attack patterns. However, its effectiveness is highly dependent on the quality and size of the training dataset. Inadequate or biased data can lead to inaccurate predictions, resulting in both false positives and false negatives. Moreover, these systems operate only after account creation, allowing malicious users to remain active for a certain period.

3.2 Behavioral and Pattern Analysis

Another widely adopted approach involves analyzing user behavior and activity patterns to identify suspicious accounts. This includes monitoring login frequency, interaction patterns, content sharing habits, and network connections. Systems based on this methodology attempt to establish a baseline of normal user behavior and detect deviations from this norm. While behavioral analysis is effective in identifying abnormal activities, it suffers from high computational complexity and delayed response. New accounts may not exhibit sufficient activity initially, making early detection difficult. Additionally, legitimate users with unusual behavior may be incorrectly flagged, leading to usability issues.

3.3 Multi-Factor Authentication Systems

Multi-factor authentication (MFA) has been introduced as a method to enhance account security by requiring multiple forms of verification, such as passwords, OTPs, and biometric data. This approach strengthens login security and reduces the risk of unauthorized access. However, MFA does not effectively address the issue of duplicate account creation. Users can still create multiple accounts using different credentials, as the system lacks a centralized identity verification

mechanism. Furthermore, MFA increases user friction and may affect usability in large-scale applications.

3.4 Identity Verification and Centralized Authentication

Recent studies have explored the concept of centralized identity management systems, where a single identity provider verifies users across multiple platforms. This approach aims to reduce redundancy and improve trust by ensuring consistent identity validation. Although centralized systems provide better control, many implementations rely on third-party providers such as Google or Facebook login services. These systems are not specifically designed to prevent fake account creation and may still allow multiple identities for a single user. Additionally, privacy concerns arise when user data is managed by external entities.

3.5 Blockchain-Based Identity Systems

Emerging research has proposed blockchain-based identity verification frameworks to ensure secure and tamper-proof identity management. These systems use decentralized ledgers to store user credentials, making it difficult for attackers to manipulate identity data. Despite their strong security features, blockchain-based solutions face challenges such as high implementation cost, scalability issues, and complexity. The requirement for widespread adoption further limits their practical applicability in current social media ecosystems.

4. GAP ANALYSIS

The analysis of existing literature highlights a critical gap in current approaches. Most systems focus on detecting fake accounts after their creation rather than preventing them at the source. This reactive nature allows malicious users to exploit platforms before being identified. Additionally, the absence of a strict one-user-one-identity mechanism remains a major limitation across all existing solutions.

To address these challenges, the proposed KeyShield system introduces a prevention-based approach using a locker-based authentication framework. By generating a unique authentication key for each verified user and enforcing centralized identity control, the system aims to eliminate fake account creation at its origin, thereby overcoming the limitations of existing methods.

4.1 DRAWBACKS OF EXISTING SYSTEM

Despite the implementation of various authentication and detection mechanisms, existing systems exhibit several critical limitations that affect their overall effectiveness. One of the major drawbacks is the ability of users to create multiple accounts using different email addresses or phone numbers, which leads to duplication and misuse. Additionally, most detection techniques operate only after

account creation, allowing malicious users to exploit the system temporarily. Traditional password-based authentication methods remain vulnerable to cyber threats such as phishing and brute-force attacks. Furthermore, multi-factor authentication enhances login security but fails to enforce identity uniqueness. The heavy reliance on machine learning models increases computational complexity and may result in false positives, thereby affecting legitimate users and reducing system reliability.

4.2 LIMITATIONS OF CURRENT AUTHENTICATION APPROACHES

- In addition to the general drawbacks, current authentication systems suffer from structural and architectural limitations that hinder their effectiveness in large-scale environments. One of the primary issues is the absence of a unified identity management system, which allows users to maintain multiple independent identities across platforms. This lack of synchronization leads to inconsistencies and increases the risk of identity misuse.
- Another critical limitation is the reliance on decentralized verification methods, where each platform independently manages its authentication process. This results in fragmented security policies and inconsistent validation standards, making it easier for attackers to exploit weaker systems. Furthermore, existing authentication models prioritize accessibility and user convenience over strict identity enforcement, which compromises security.
- The inability to enforce a one-to-one mapping between users and accounts remains a major challenge. Without a centralized authority to validate and control identity uniqueness, duplicate account creation becomes inevitable. These limitations highlight the need for a centralized, secure, and prevention-oriented authentication framework such as the proposed KeyShield system.
- Image-Based Obfuscation: Attackers embed malicious links or “call-to-action” text within images. This method effectively bypasses text-based scanners, as optical character recognition (OCR) is rarely, if ever, applied in real time at the scale required for email filtering due to its high computational cost.

4.3 RESEARCH GAP IDENTIFICATION

The comprehensive analysis of existing authentication and detection systems reveals a significant research gap in the domain of fake account prevention. Most current approaches are inherently reactive, focusing on identifying malicious accounts only after they have been created and have already interacted within the system. This delayed detection mechanism allows attackers to exploit platforms during the initial phase, causing potential damage before mitigation measures are applied.

Furthermore, existing systems lack a robust mechanism to enforce identity uniqueness. The absence of a centralized identity verification framework enables users to create multiple accounts using different credentials, leading to duplication and misuse. Even advanced security measures such as multi-factor authentication and machine learning-based detection fail to address this fundamental issue, as they primarily secure access rather than prevent account creation.

Another critical gap lies in the lack of a prevention-oriented architecture that integrates authentication with identity control. Current systems do not provide a unified solution that ensures a one-user-one-identity model. This gap highlights the necessity for a system like KeyShield, which introduces a centralized locker-based authentication framework to eliminate fake accounts at their origin.

5. PROPOSED SYSTEM ARCHITECTURE: THE PHISH-STOP PIPELINE

To overcome the limitations of existing authentication mechanisms, the proposed system “KeyShield” introduces a prevention-oriented framework designed to eliminate fake and duplicate account creation at the initial stage. Unlike traditional systems that rely on post-creation detection techniques, this approach enforces strict identity verification before granting access to social media platforms. The system is built around a centralized digital locker that functions as an independent authentication authority, where users are required to register using verified credentials such as name, email address, and phone number. Upon successful validation, the system generates a unique authentication key that acts as a secure digital identity token. This key is permanently associated with the user and becomes mandatory for accessing connected platforms. During login, the authentication key is verified by the locker system to ensure its validity before granting access. By enforcing a strict one-user-one-key policy, the system effectively prevents multiple account creation. This proactive approach enhances security, reduces misuse, improves user trust, and provides a scalable solution for secure identity management in modern digital ecosystems.

5.1 SYSTEM ARCHITECTURE

The architecture of the KeyShield system is designed as a centralized and modular framework that integrates user registration, identity verification, key generation, and authentication processes. The system consists of two primary components: the digital locker (central authority) and the client platforms (social media applications).

- The digital locker acts as the core of the system, responsible for managing user identities and authentication keys. It securely stores user credentials and ensures that each user is verified before being granted access. The locker maintains a database containing user

information and their corresponding unique authentication keys.

- The system architecture follows a structured workflow. Initially, the user registers in the locker by providing personal details such as email and phone number. The system validates these details to ensure uniqueness. Upon successful verification, a unique authentication key is generated and stored securely.
- When a user attempts to log in to a social media platform, the platform communicates with the locker system to verify the provided authentication key. The locker checks the validity of the key and confirms the user's identity. Based on this verification, access is either granted or denied.
- This centralized architecture ensures consistent authentication across multiple platforms and eliminates the possibility of duplicate accounts. It also simplifies integration, as external platforms only need to interact with the locker system for authentication, reducing complexity and improving security.

5.2 SYSTEM WORKING AND FLOW

The working of the KeyShield system follows a sequential and well-defined process that ensures secure user authentication and prevents duplicate account creation. The system operates in multiple stages, beginning from user registration to final access validation.

- i. The first stage involves user registration within the digital locker. The user provides essential details such as name, email address, and phone number. The system performs validation checks to ensure that the provided information is unique and not already registered.
- ii. In the second stage, once the user is successfully verified, the system generates a unique authentication key. This key acts as a digital identity token and is securely stored in the locker database. The key is then provided to the user for future authentication purposes.
- iii. The third stage involves login verification. When the user attempts to access a social media platform, the system requires the authentication key instead of traditional login credentials. The platform sends a verification request to the locker system along with the provided key.
- iv. In the final stage, the locker system validates the authentication key by comparing it with stored records. If the key is valid and matches the user's identity, access is granted. If the key is invalid or does not exist, the system denies access, preventing unauthorized or duplicate account usage.
- v. This step-by-step workflow ensures that only verified users can access the platform, thereby eliminating fake account creation. The system provides a secure, efficient, and scalable authentication mechanism suitable for modern digital environments.

6. IMPLEMENTATION MODULES

The KeyShield system is divided into several functional modules that collectively ensure secure authentication and prevention of fake account creation. Each module performs a specific task within the system, contributing to the overall efficiency and reliability of the framework. The major modules include User Registration, Locker Authentication, Unique Key Generation, Social Media Login Verification, and Security Monitoring. These modules are interconnected and operate in a sequential manner to ensure proper identity verification and access control. The modular design enhances system scalability, simplifies implementation, and allows easy integration with existing platforms while maintaining high security standards.

6.1 Module 1: USER REGISTRATION MODULE

The User Registration Module serves as the entry point of the KeyShield system, where users establish their digital identity within the centralized locker environment. This module is designed to ensure that every user undergoes a secure and verified onboarding process before accessing any connected platforms.

During registration, users are required to provide essential personal details such as name, email address, and phone number. These details act as primary identifiers and are used to distinguish each user within the system. The input process is designed to be user-friendly while maintaining strict validation standards.

The system performs multiple validation checks to ensure data authenticity and uniqueness. Email verification and phone number validation mechanisms are implemented to confirm that the provided credentials belong to a legitimate user. Additionally, the system checks for duplicate entries to prevent multiple registrations using the same information.

Once the validation process is completed successfully, the user's information is securely stored in the locker database. Advanced security measures are applied to protect sensitive data from unauthorized access and potential breaches, ensuring data integrity and confidentiality.

This module plays a critical role in establishing a trusted identity foundation for the entire system. By ensuring that only verified and unique users are registered, it supports the core objective of preventing fake and duplicate account creation in the KeyShield framework.

6.2 Module 2: LOCKER AUTHENTICATION MODULE

The Locker Authentication Module acts as the central authority of the KeyShield system, responsible for verifying user identities and managing authentication processes. It ensures that only legitimate and verified users are allowed to access the system and connected platforms.

This module operates by validating user credentials during both registration and login stages. When a user submits their details or authentication key, the locker system cross-checks the information with the stored database to confirm its authenticity. This process guarantees that unauthorized users cannot gain access.

A key feature of this module is its centralized nature. Unlike traditional systems where authentication is handled independently by each platform, the locker system provides a unified verification mechanism. This eliminates inconsistencies and ensures uniform security policies across all integrated platforms.

The module also maintains a secure database that stores user credentials and their corresponding authentication keys. Advanced security techniques are applied to protect this data from unauthorized access, ensuring confidentiality and integrity. This centralized storage simplifies identity management and enhances system reliability.

Overall, the Locker Authentication Module plays a crucial role in enforcing secure access control within the KeyShield framework. By acting as a trusted intermediary between users and platforms, it strengthens authentication, prevents unauthorized access, and supports the system's goal of eliminating fake accounts.

6.3 Module 3: UNIQUE KEY GENERATION MODULE

The Unique Key Generation Module is a core component of the KeyShield system, responsible for creating a distinct authentication key for every registered user. This module ensures that each user is assigned a unique digital identity within the system.

Once the user successfully completes the registration and verification process, this module generates a secure authentication key. The key is designed using appropriate algorithms to ensure randomness and uniqueness, making it difficult to predict or duplicate.

Each generated key is permanently associated with the user's verified credentials, such as email address and phone number. This linkage ensures that the identity of

the user remains consistent and cannot be replicated across multiple accounts.

The generated authentication key is securely stored in the locker database and is also provided to the user for future login purposes. Proper security mechanisms are implemented to protect the key from unauthorized access, misuse, or leakage.

This module plays a vital role in enforcing the one-user-one-key policy, which is the foundation of the KeyShield system. By ensuring that each user possesses only a single unique key, the system effectively prevents duplicate account creation and strengthens overall authentication security.

6.4 Module 4: SOCIAL MEDIA LOGIN VERIFICATION MODULE

The Social Media Login Verification Module is responsible for managing the authentication process when users attempt to access external platforms integrated with the KeyShield system. It replaces traditional login mechanisms with a more secure and centralized approach.

In this module, users are required to provide their locker-generated authentication key instead of conventional credentials such as usernames and passwords. This ensures that only users who have completed the registration and verification process can proceed with login.

When a login request is initiated, the social media platform sends the provided authentication key to the locker system for validation. The locker system then checks the key against its stored database to verify its authenticity and association with a registered user.

If the authentication key is valid and correctly matches the stored user credentials, the system grants access to the platform. In contrast, if the key is invalid, expired, or does not exist, the system immediately rejects the login attempt, thereby preventing unauthorized access.

This module plays a crucial role in maintaining system security and enforcing identity uniqueness. By ensuring that only verified keys are accepted for login, it eliminates the possibility of fake account usage and strengthens the overall authentication process within the Key Shield framework.

7. ADVANTAGES

The proposed KeyShield system offers a significant advancement over traditional authentication mechanisms by introducing a prevention-oriented approach to security. One of its primary advantages is the ability to

prevent fake and duplicate account creation at the initial stage itself. Unlike existing systems that rely on detecting malicious accounts after their creation, KeyShield ensures that only verified users can enter the system, thereby eliminating misuse before it begins.

Another major advantage of the system is the enforcement of a strict one-user-one-key policy. Each user is assigned a unique authentication key that is permanently linked to their verified credentials such as email address and phone number. This ensures identity uniqueness and makes it extremely difficult for individuals to create multiple accounts, thereby reducing duplication and misuse across platforms.

The system also provides enhanced security compared to traditional password-based authentication methods. Passwords are often vulnerable to various cyber threats such as phishing, brute-force attacks, and credential reuse. In contrast, the KeyShield framework replaces passwords with secure authentication keys, thereby minimizing common vulnerabilities and improving overall system protection.

A key strength of the proposed system is its centralized authentication mechanism. All verification processes are handled through a digital locker, which acts as a trusted identity provider. This centralized approach ensures consistent authentication across multiple platforms and eliminates discrepancies that may arise from decentralized verification systems. It also simplifies identity management and enhances system reliability.

The KeyShield system significantly reduces the risk of malicious activities such as spam, impersonation, and cyber fraud. By restricting access to only verified users, the system creates a safer digital environment where users can interact with greater confidence. This contributes to improved trust and credibility in online platforms.

Another advantage is the reduced dependency on complex machine learning models and large datasets. Traditional detection-based systems require continuous training and high computational resources, which increases system complexity. In contrast, KeyShield focuses on prevention, thereby reducing computational overhead and enabling faster response times.

The system is also designed to be highly scalable and adaptable. Its modular architecture allows easy integration with existing social media platforms and other digital services. This flexibility makes it suitable for a wide range of applications, including e-commerce, banking, and government services.

Furthermore, the system improves user experience by simplifying the authentication process. Users are no longer

required to remember multiple passwords or manage complex login credentials. Instead, a single authentication key can be used across multiple platforms, providing convenience without compromising security.

The centralized monitoring capability of the system further enhances its effectiveness. Suspicious activities, such as repeated invalid login attempts, can be detected and controlled at the locker level. This proactive monitoring ensures that potential threats are addressed in real time.

Overall, the KeyShield system represents a robust, efficient, and scalable solution for modern authentication challenges. By combining strong identity verification, centralized control, and prevention-based security, it establishes a new standard for secure and reliable digital identity management.

8. IDENTIFIED LIMITATIONS AND ISADVANTAGES

Despite the effectiveness of the proposed KeyShield system in preventing fake and duplicate account creation, certain limitations must be acknowledged to provide a realistic evaluation of the framework. These limitations are primarily associated with system performance, usability, and implementation challenges.

One of the major limitations of the system is its dependency on a centralized authentication mechanism. Since the digital locker acts as the core authority for identity verification, any failure or downtime in the locker system can affect the accessibility of all connected platforms. This creates a single point of failure, which may impact system reliability if not properly managed with backup and redundancy mechanisms.

Another challenge is the potential increase in system complexity during implementation. Integrating the KeyShield framework with existing platforms may require architectural modifications and additional infrastructure, which can increase development effort and cost. Organizations may face difficulties in adopting the system without proper standardization and compatibility support.

The system may also introduce usability concerns for users who are accustomed to traditional authentication methods. Managing and securely storing an authentication key could be challenging for some users, especially if proper recovery mechanisms are not in place. Loss or compromise of the key may temporarily restrict access until verification procedures are completed.

Furthermore, while the system effectively prevents duplicate account creation, it does not completely eliminate all forms of cyber threats. Attackers may attempt to exploit other vulnerabilities such as social

engineering or device-level attacks. Therefore, additional security measures are required to complement the authentication framework.

Another limitation is the requirement for strict validation of user credentials, which may increase the time required for registration. While this enhances security, it may slightly impact user convenience during the onboarding process.

Despite these limitations, the proposed system provides a strong foundation for secure authentication. With proper enhancements such as distributed architecture, backup mechanisms, and improved user interfaces, these challenges can be effectively addressed in future implementations.

9. FUTURE ENHANCEMENT

Although the proposed KeyShield system provides a robust and effective solution for preventing fake and duplicate account creation, several enhancements can be incorporated to further strengthen its capabilities and expand its applicability in real-world environments. One of the most significant future improvements is the integration of biometric authentication methods such as fingerprint recognition, facial recognition, or iris scanning. By combining biometric verification with the existing locker-based authentication mechanism, the system can achieve a higher level of identity assurance and reduce the chances of unauthorized access.

Another important enhancement involves the incorporation of machine learning and artificial intelligence techniques to monitor user behavior and detect anomalies in real time. While the current system focuses on prevention, integrating intelligent monitoring can provide an additional layer of security by identifying suspicious patterns such as unusual login attempts, location-based anomalies, or abnormal usage behavior. This hybrid approach can significantly improve the system's ability to handle advanced cyber threats.

Furthermore, the system can be expanded beyond social media platforms to support a wide range of digital services, including banking, e-commerce, healthcare, and government applications. This would transform KeyShield into a universal authentication provider capable of managing digital identities across multiple domains.

Additionally, the implementation of advanced encryption techniques and secure communication protocols can further strengthen data protection and prevent potential cyber-attacks. Regular system updates and security audits can ensure that the framework remains resilient against evolving threats.

Overall, these future enhancements aim to transform the KeyShield system into a comprehensive, intelligent, and scalable authentication solution capable of addressing the dynamic challenges of modern digital ecosystems.

10. CONCLUSIONS

The rapid growth of digital platforms, particularly social media, has significantly increased the challenges associated with fake and duplicate account creation. These malicious accounts contribute to various cyber threats, including misinformation, identity theft, financial fraud, and large-scale manipulation. Existing authentication systems, which primarily rely on reactive detection mechanisms, are insufficient to address this issue effectively, as they allow attackers to exploit platforms before being identified.

The proposed KeyShield system introduces a novel prevention-oriented authentication framework that addresses these limitations by focusing on identity verification at the initial stage. By implementing a centralized digital locker and generating a unique authentication key for each verified user, the system ensures a strict one-user-one-identity model. This approach effectively eliminates the possibility of multiple account creation and significantly enhances overall platform security.

One of the key strengths of the KeyShield framework lies in its simplicity and efficiency. By replacing traditional password-based authentication with a secure key-based mechanism, the system reduces vulnerabilities associated with common cyber-attacks. Additionally, the centralized architecture ensures consistent and reliable authentication across multiple platforms, improving both security and usability.

The system also demonstrates strong scalability and adaptability, making it suitable for integration with various digital services beyond social media. Its modular design allows easy implementation and future enhancements, ensuring long-term applicability in evolving technological environments.

In conclusion, the KeyShield system represents a significant advancement in authentication technology by shifting the focus from detection to prevention. It provides a secure, efficient, and scalable solution for managing digital identities, thereby contributing to the development of safer and more trustworthy online ecosystems.

11. ACKNOWLEDGMENTS

The authors would like to express their sincere gratitude to their project guide, Mr. P. Sathishkumar, Assistant Professor, Department of Cyber Security, Paavai

Engineering College, for his continuous guidance, valuable suggestions, and support throughout the development of this project. His expertise and encouragement played a crucial role in the successful completion of this work.

The authors also extend their heartfelt thanks to the Department of Cyber Security Engineering for providing the necessary resources and facilities to carry out this research. Special appreciation is given to all faculty members and classmates for their constructive feedback, motivation, and assistance during the design and implementation phases of the project.

Finally, the authors acknowledge the support of their institution for enabling them to undertake and complete this research successfully.

REFERENCES

- [1] [1] A. Jain, P. Sharma, and K. Mehta, "Machine Learning Approaches for Fake Account Detection in Social Networks," *IEEE Access*, vol. 10, pp. 12894–12907, 2022.
- [2] M. Lee and S. Kim, "Behavioral Analysis for Detecting Malicious Social Media Accounts," *Computers & Security*, vol. 125, pp. 102947–102959, 2023.
- [3] N. Gupta and R. Verma, "Hybrid Models for Fake Account Detection Using Machine Learning and NLP," *Expert Systems with Applications*, vol. 229, 2023.
- [4] R. Patel and D. Singh, "Threat Intelligence Integration for Cybersecurity Applications," *Journal of Cybersecurity and Privacy*, vol. 5, no. 2, pp. 65–79, 2021.
- [5] L. Zhou and T. Wang, "Blockchain-Based Identity Verification Framework," *IEEE Transactions on Information Forensics and Security*, vol. 19, no. 4, pp. 451–463, 2024.
- [6] S. O. Fatayol et al., "A Review on Phishing and Identity-Based Attacks: Methods and Future Directions," *IEEE Access*, vol. 11, pp. 91705–91728, 2023.
- [7] A. Singh, "Machine Learning Techniques for Social Media Security," *IEEE Conference Proceedings*, 2022.
- [8] S. Lee and J. Kim, "Early Detection of Malicious Accounts in Online Platforms," *IEEE Conference*, 2021.
- [9] M. Mazza et al., "Detecting Social Bots and Fake Accounts in Online Platforms," *IEEE Transactions*, 2022.
- [10] Google, "Google Safe Browsing: Protecting Users from Malicious Content," [Online]. Available: <https://safebrowsing.google.com/>
- [11] PhishTank, "Phishing Data and Threat Intelligence Repository," [Online]. Available: <http://www.phishtank.com/>
- [12] OpenPhish, "Real-Time Phishing Intelligence Feed," [Online]. Available: <https://openphish.com/>
- [13] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems," NIST Special Publication, 2021.
- [14] D. Florêncio and C. Herley, "A Large-Scale Study of Web Password Habits," *ACM Conference on World Wide Web*, 2020.
- [15] Microsoft, "Digital Identity and Authentication in Modern Systems," *Technical Documentation*, 2023.