IMPROVE AUTHENTICATION IN SOCIAL MEDIA APPLICATIONS USING AI AND BLOCKCHAIN

CSE 543: INFORMATION ASSURANCE AND SECURITY

SPRING 2024

GROUP 21

Kesudh Giri (Leader)	1225259867
Abhi Dineshkumar Patel (Deputy Leader)	1230038877
Shashank Venkataramana	1229385185
Saibhaskara Durga Mani Kanuri	1231965776
Vinit Maheshbhai Patel	1229950646
Niteeq Sheik	1230031584
Aswath Senthilkumar	1230661824
Akhash Senthil Kumar	1229855499

CONTENTS

Chapter 1

INTRODUCTION

1.1 MOTIVATION AND BACKGROUND

The advent of social media platforms has revolutionized modern communication, enabling unprecedented levels of connectivity and information sharing across global networks. However, this digital revolution has also introduced significant challenges regarding the security and trustworthiness of user identities. Traditional authentication methods, reliant on passwords and personal information, are increasingly vulnerable to hacking, identity theft, and data breaches. Moreover, the centralized nature of social media platforms exposes user data to exploitation by third parties, raising concerns about privacy infringement and ethical implications.

In response to these challenges, the integration of Artificial Intelligence (AI) and Blockchain technologies has emerged as a promising solution. AI algorithms offer advanced capabilities for analyzing behavioral patterns, biometric data, and user interactions, thereby enhancing the accuracy and security of the authentication process. Concurrently, Blockchain technology provides a decentralized framework for storing and managing user credentials, ensuring immutability, transparency, and resistance to tampering.

The motivation behind this research lies in the imperative to establish a more robust and trustworthy system for social media authentication. By harnessing the synergistic potential of AI and Blockchain, this study aims to empower users with greater control over their digital identities while mitigating security risks and safeguarding privacy. Through an innovative integration of these technologies, we seek to foster a more secure and trustworthy digital ecosystem, thereby addressing the pressing challenges facing modern social media platforms and advancing the broader goals of digital security and privacy protection.

1.2 GOALS AND SCOPE

Our project is driven by our collective commitment to fostering a safer and more trustworthy online environment for users worldwide. At the heart of our endeavor lies the recognition of authentication as a cornerstone for ensuring user security and confidence within digital platforms.

With this vision in mind, we are embarking on a journey to reimagine authentication methodologies by harnessing the powerful capabilities of AI and blockchain technologies. Our aim is not only to bolster the security of user authentication processes but also to instill a sense of empowerment and peace of mind among users as they engage with social media platforms.

One of the key pillars of our project involves integrating AI-driven anomaly detection and behavioral biometrics. Through meticulous analysis of security patterns and vulnerabilities, we aspire to develop cutting-edge AI algorithms capable of proactively identifying and mitigating authentication risks. Simultaneously, we are exploring blockchain solutions, such as smart contracts and decentralized authentication mechanisms, to ensure the integrity and tamper-resistance of user credentials.

Furthermore, our endeavor extends to behavioral analysis techniques aimed at combating identity theft within mobile social networks. By leveraging probabilistic generative models, we seek to equip social media platforms with advanced algorithms capable of detecting and thwarting identity theft attempts, thereby safeguarding user privacy and security.

We remain steadfast in our commitment to overcoming obstacles through rigorous research and collaboration. Our project is not just about technological innovation; it's about making a tangible difference in the lives of users, empowering them to navigate the digital landscape with confidence.

As we progress, our ultimate goal is to contribute to a future where online interactions are characterized by security, integrity, and inclusivity. Through academic papers and dissemination of our findings, we aim to spark meaningful conversations and inspire further advancements in the realm of social media authentication and information assurance.

In essence, our project embodies the fusion of technological expertise, human empathy, and a shared vision for a safer digital world. Together, we strive to create a lasting impact and usher in a new era of online authenticity and trustworthiness.

Chapter 2

PROJECT SUMMARY

2.1 SUMMARY OF AUTHENTICATION MECHANISMS USING AI

In the realm of social media, robust authentication is essential for user security. Leveraging AI offers adaptive solutions to detect anomalies in user behavior, enhancing defenses against cyber threats. Below are some key points highlighting the potential of AI-driven authentication mechanisms:

- AI enables continuous authentication, assessing behavior and touch patterns for mobile devices.
- Utilizing AI like Neural Networks enhances facial recognition for biometric authentication, improving accuracy.
- Hybrid AI models combine Blind Feature Learning and Lightweight Physical Layer Authentication for network security, assisting in risk-based two-factor authentication.
- Clustering and classification detect synthetic identity theft, while AI distinguishes between legitimate and malicious login attempts.
- AI-based authentication ensures real-time processing, driving anomaly detection.
- NLP analyzes messages for phishing, and AI monitors user engagement for bot behavior.
- Machine learning continuously updates authentication protocols.

In conclusion, integrating AI into authentication mechanisms for social media applications empowers platforms with adaptive, intelligent defenses against evolving cyber threats, bolstering user trust and security in the digital sphere.

2.2 SUMMARY OF BLOCKCHAIN-BASED SECURITY MEASURES

Blockchain technology has revolutionized digital security, acting as a robust mechanism to safeguard data and ensure transparency without compromising privacy. Here are streamlined highlights of blockchain's impact on enhancing digital safety and authenticity:

- Decentralization eliminates single failure points, securing data across networks.
- Smart contracts on Ethereum generate secure OTPs for 2FA, improving authentication.
- Encrypted biometric data stored on the blockchain prevents unauthorized access.
- Use of nonce values in public keys within blockchain systems defends against replay attacks.
- Blockchain enhances EHRs, maintaining patient data privacy and integrity.
- Combining blockchain with AI in social media boosts privacy and ensures content is genuine.
- Blockchain-based Minimal Disclosure Signatures protect user privacy during authentication.
- The immutable ledger of blockchain aids in detecting unauthorized data changes, preserving data integrity.
- Smart contracts autonomously implement security policies, minimizing human error.
- Blockchain aids in compliance with regulations through transparent, verifiable records.

This condensed summary underscores blockchain's critical role in fortifying digital security and authentication, showcasing its effectiveness against traditional vulnerabilities for a secure and transparent digital ecosystem.

Chapter 3

INDIVIDUAL ACCOMPLISHMENTS

3.1 KESUDH GIRI

- As Team Leader, Organized the overall functioning of the team and assigned work to each individual to contribute to the overall outcome of the Course Project
- Performed all tasks related to making a Survey Report by researching through relevant Reference Papers, summarizing the ideas presented in them, and then aligning the knowledge extracted from the research into arriving at a solution for the given Use-Case Statement.
- Assessed and Monitored the creation of the Weekly Report Documents over the course of the Project.
- Contributed to the Survey Report Document by writing sections of the Discussion Section(4.1), Proposed Solution(4.4), and Conclusions(5)

3.2 ABHI DINESHKUMAR PATEL

- Reviewed project title alignment with goals and objectives, initiating modifications where necessary.
- Conducted comprehensive searches for relevant research papers, assessing their alignment with the project scope.Organized and summarized identified references for inclusion in the project proposal. Collaborated on finalizing project references and updating project proposal reports.
- Completed in-depth reviews of selected three papers, enhancing project understanding and insights.

- Conducted high-level studies on various topics relevant to the project, including Blockchain applications, AI in social media, and authentication methods.

- Initiated discussions on various sections of the final report, ensuring alignment and coherence across different sections.

- Played a pivotal role in synthesizing findings and insights into the Discussion [4], Goal and Scope [1.2], Using Blockchain methodology for security [5.3], and Conclusion and Recommendation [6] sections of the final report.

- As the Deputy Team Leader, I spearheaded task delegation, facilitated weekly meetings, and meticulously reviewed the team's progress and completed tasks.

3.3 SHASHANK VENKATARAMANA

- Conducting thorough reference searches across subgroups like ”Loss of User Data” and ”Authentication Based on Touch Patterns.”

- Leading studies on emerging technologies such as blockchain-based authentication for social media security.

- Analyzing and synthesizing findings for in-depth reviews on topics like deep face recognition and minimal disclosure signature authentication.

- Investigating blockchain-based solutions for user data access control and digital identity management in secured cloud storage.

- Contributing to project reports with background information and discussing implications of blockchain for social media and AI security.

- Providing insights and recommendations for leveraging blockchain for authentication and identity management in social networking and online signatures.

- Exploring AI techniques like recurrent neural networks for biometric authentication and anomaly detection.

- Addressing challenges in social media security and data protection through innovative AI and blockchain approaches.

- Collaborating with team members to draw conclusions on blockchain's feasibility for social media authentication.

- Contributing to recommendations for future research and implementation strategies.

3.4 SAIBHASKARA DURGA MANI KANURI

- Conducted thorough web searches to identify relevant research papers aligned with our project title.

- Selected and curated a set of research papers as references, ensuring they best align with our project objectives.

- Produced three in-depth reports analyzing key aspects of selected research papers, providing high-level insights and understanding.

- Authored the "Summary of authentication mechanism using AI" section in the project report, drawing from knowledge obtained through the study of selected research papers.

- Performed detailed examinations of three research papers, contributing insights and analysis to the project report.

- Demonstrated a proactive approach to understanding and synthesizing complex research findings, enhancing the depth and quality of our project's content.

- Ensured coherence and relevance in project content by integrating findings from research papers.

3.5 VINIT MAHESHBHAI PATEL

- Spearheaded a comprehensive literature review, identifying and examining pertinent research papers across key subdomains such as Blockchain, Artificial Intelligence, Loss of User Data, and Identity Theft, which laid the foundation for the project's research direction.

- Managed the organization and detailed summarization of the project's findings, effectively overseeing the development of the ”Project Outcomes” section in the project proposal report, ensuring the outcomes were articulated clearly and persuasively.

- Led high-level studies on cutting-edge topics relevant to the project's scope, including the exploration of Blockchain and AI applications in social media, as well as innovative authentication methods, contributing to the project's forward-thinking approach.

- Conducted detailed analyses and synthesis of scholarly articles, generating in-depth reviews on specialized subjects like User Authentication via Face Thermograms and Multi-biometric Template Protection using Bloom Filters, thereby enriching the project's academic rigor.

- Played a pivotal role in shaping the Goals and Scope section of the final project report, articulating the project's aims and boundaries with clarity and precision, which guided the project's strategic direction.

- Made significant contributions to the Survey Report Document, specifically focusing on the application of blockchain for secure authentication, meticulously drafting and integrating these insights into section 4.3 of the final project report, enhancing the document's depth and breadth.

3.6 NITEEQ SHEIK

- Spearheaded comprehensive web-based research to curate a collection of research papers directly aligned with our project's objectives, ensuring a robust foundation for further investigation and application.

- Conducted weekly in-depth analyses of selected research papers, deriving key insights and understandings crucial for informing our project direction and enhancing our conceptual framework.

- Undertook high-level studies on a broad spectrum of research papers, expanding our knowledge base and propelling the project forward with innovative approaches and methodologies.

- Authored a concise yet comprehensive summary of blockchain technologies, pinpointing their potential to revolutionize authentication processes within our project scope, setting a precedent for technological integration.

- Delivered a detailed examination of three pivotal research papers, showcasing the transformative impact of AI on authentication methods, and solidifying our project's foundation with cutting-edge scientific validation.

3.7 ASWATH SENTHILKUMAR

- Conducted thorough literature reviews and reference searches on blockchain technology, AI security, and social media security, demonstrating expertise in researching relevant topics.

- Updated and maintained project timelines and Gantt charts to ensure efficient project management and progress tracking, indicating strong organizational and time management skills.

- Contributed to high-level studies and in-depth reviews on key topics such as AI-based security authentication, blockchain technology for social media authentication, and the use of AI voice authentication in security devices, showcasing expertise in emerging technologies and their applications in security contexts.

- Played a key role in compiling the final report, synthesizing discussions on preventing cryptographic attacks with AI-hard password authentication, enhancing user authentication with facial recognition, and using blockchain for authentication in digital education. Also, developed a detailed table of contents outlining key sections like AI methodology for authentication, conclusions, and recommendations, showcasing strong analytical and communication skills in structuring project deliverables.

- Contributed to Project report by writing sections of Project Motivation and Background, Summary of Blockchain based Security Measures and Conclusion.

3.8 AKHASH SENTHIL KUMAR

- Performed extensive literature review on various methods for improving the security of blockchain transactions, including machine learning techniques, consensus protocols, and smart contracts. Analyzed the problem statement, proposed solution, methods, results, and limitations for each paper in a concise manner.

- Summarized five research papers spanning different approaches for securing cryptocurrency transactions against attacks like double spending, 51% attack, and quantum computing threats. Exhibited critical thinking abilities by comparing strengths and weaknesses of different techniques analyzed in the papers.

- Performed in-depth research on 2 Papers about advanced emerging concepts like artificial immune systems and displayed adaptability by quickly learning new concepts like distributed ledgers, consensus protocols, etc., for the research project.

- Utilized scientific search tools like Google Scholar efficiently to find relevant papers on the research topic and managed time effectively to complete assigned summaries along with other coursework and responsibilities.

- Contributed to Project report by writing sections of Project summary, Discussion and Conclusion.

Chapter 4

DETAILED RESULTS

4.1 DISCUSSION

4.1.1 Social networking and identity theft in the digital society

This paper[1] examines the vulnerability of social network users to identity theft facilitated by the information they share on social networking sites. The author emphasizes that while social networking platforms offer opportunities for social interaction and sharing interests, they also bring about vulnerabilities due to exposing personal information online.

The research delves into various aspects related to the emergence of social networking in information sharing, including user motivations for sharing personal information and the reciprocal nature of information exchange on these platforms. The paper[1] highlights the potential risks associated with information sharing, particularly concerning identity crime, and discusses the challenges in dealing with this type of cybercrime.

The seriousness of identity crime is underscored by statistics from different countries, demonstrating its global impact and financial costs. The paper[1] also explores practical difficulties in convicting identity criminals, especially in an international context, and discusses the limitations of regulatory responses.

From a privacy perspective, the paper[1] delves into international responses to privacy regulation and the challenges of addressing privacy concerns related to identity crime on social networking sites. Additionally, it outlines the challenges law enforcement agencies face in gathering evidence and prosecuting identity criminals, particularly in cases that span multiple jurisdictions.

The discussion section provides insights into potential solutions, including educational programs, technological improvements, and greater accountability from social networking sites. The paper[1] concludes by emphasizing the importance of raising awareness about the risks of sharing personal information online and calls for continued research to address the challenges posed by identity crime in the digital era.

Overall, the paper[1] offers a comprehensive analysis of the relationship between social networking and identity theft, highlighting the need for multi-faceted approaches to combat this crime and suggesting avenues for future research.

4.1.2 Role of artificial intelligence and machine learning in social media

The paper[2] explores how AI and ML technologies have revolutionized user interactions, content creation, advertising tactics, and customer service on social media platforms.

A critical aspect highlighted in the paper[2] is the significant influence of AI and ML algorithms in deciphering user behavior, refining targeted advertising strategies, automating customer support processes, and optimizing content management techniques. Moreover, the vast potential of AI-powered tools such as chatbots, sentiment analysis, image recognition, and face detection in enhancing the functionalities and user experiences across various social media platforms is noted.

The core components of the paper[2] delineate the foundational frameworks of AI algorithms, machine learning models, and neural networks, driving innovation in social media platforms. These components enable sophisticated data analysis, pattern recognition, and predictive modeling, fostering personalized user experiences, streamlined content delivery, and enhanced marketing endeavors.

Additionally, the paper explores AI-powered tools and applications in leading social media platforms like Facebook, Twitter, LinkedIn, and Pinterest, illustrating their diverse functionalities and contributions to user engagement and brand management.

While the primary focus is on augmenting user engagement and marketing effectiveness, the paper briefly touches upon the security advantages of AI and ML technologies in social media contexts. It highlights AI-driven security measures such as image recognition for detecting harmful content, sentiment analysis for identifying potential threats, and automated moderation for enforcing community

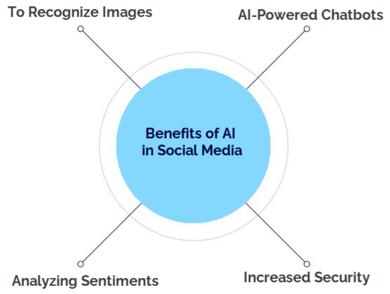


Figure 4.1: Benefits of AI usage in Social Media. Source: [2]

guidelines.

Moreover, the paper acknowledges the dynamic nature of user identities and interactions across social media channels, proposing the integration of AI and blockchain technologies for persistent identity management and real-time profile updates.

By comparing AI-driven systems with traditional approaches, the paper underscores the paradigm shift due to AI and ML technologies, emphasizing their scalability, efficiency, and adaptability in meeting evolving user demands and business objectives. Figure 4.1 lists multiple benefits brought into Social Media by AI.

Challenges and mitigation strategies are also addressed, including concerns over data privacy, algorithmic bias, cybersecurity risks, and regulatory compliance. Additionally, user experience considerations such as personalization, interactivity, accessibility, transparency, and trustworthiness are thoroughly examined to ensure inclusive and trustworthy social media environments.

4.1.3 Artificial intelligence-based security authentication: Applications in wireless multimedia networks

The research conducted by [3] explores the integration of artificial intelligence (AI) into wireless multimedia networks to enhance security measures. The focus lies on devising lightweight security protocols that efficiently authenticate devices while ensuring seamless multimedia operations.

Two primary strategies are proposed: one involves employing a support vector machine (SVM) in conjunction with multiple features, while the other utilizes deep learning for automatic feature extraction. These approaches aim to bolster security by scrutinizing various communication aspects, making it challenging for malicious actors to impersonate legitimate devices.

Results from the experiments indicate that AI-driven systems outperform traditional methods in accuracy and speed of detection. Notably, these systems achieve robust security without relying on complex encryption methods, which is significant in wireless networks where managing secret keys can be cumbersome.

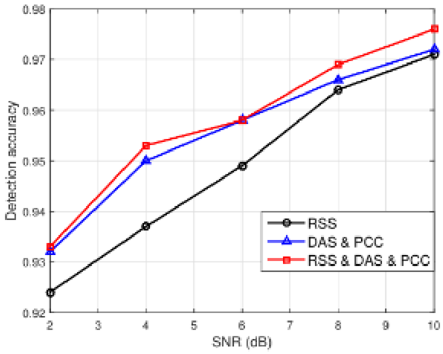


Figure 4.2: Detection performance of the LPLA scheme relying on the RSS, the DAS & PCC, and the RSS & DAS & PCC cases. Source: [3]

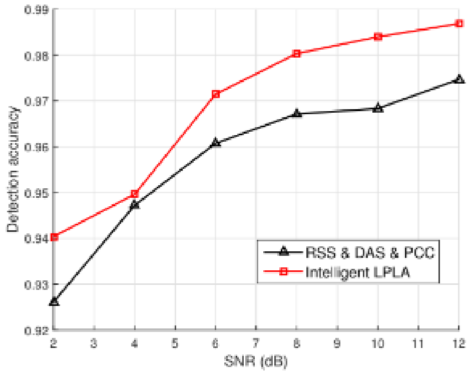


Figure 4.3: Detection performance of different LPLA schemes. (a) the multiple features-based LPLA scheme; (b) the neural network-based LPLA scheme. Source: [3]

This study underscores the potential of AI in fortifying wireless networks' security without introducing unnecessary complexity. It advocates for a shift towards AI-driven security solutions to address emerging threats effectively.

Furthermore, the inclusion of Figure 4.2 provides insights into the effectiveness of different feature combinations in identifying fraudulent devices. This visualization aids in understanding which features play a crucial role in enhancing security.

Moreover, Figure 4.3 illustrates how varying signal strengths impact the security system's accuracy, offering valuable insights into its performance under different conditions. This analysis contributes to a comprehensive understanding of the proposed security mechanisms.

4.1.4 The application of blockchain in social media: A systematic literature review

The paper [4] offers an insightful exploration into integrating blockchain and artificial intelligence (AI) within social media platforms. Its primary aim is to address pressing concerns surrounding data privacy, security breaches, and the proliferation of fake content. Through meticulous analysis, the authors propose a novel framework to enhance authentication systems within social media platforms, leveraging the unique features of blockchain technology.

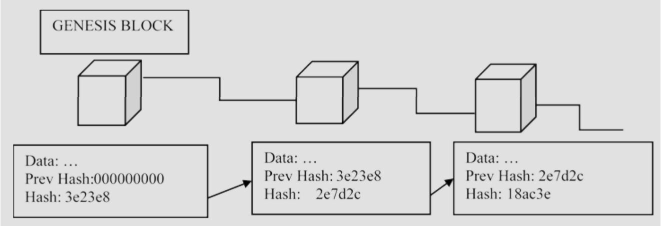


Figure 4.4: Illustration of block linkage in a chain. Source: [4]

Central to the paper's [4] discussion are the core components of the proposed model, which include decentralization, transparency, and immutability—attributes inherent to blockchain technology. 4.4 illustrates the structure of a blockchain. Additionally, integrating AI, particularly machine learning algorithms, is explored to bolster security protocols and combat the dissemination of fraudulent content within social media ecosystems.

An essential highlight of the paper[4] lies in the security advantages of integrating blockchain into social media platforms. These advantages encompass the immutability of data records and the decentralization of control, which enhance data integrity, and mitigate the risk of centralized security breaches.

The paper[4] introduces the concept of persistent identifiers (PIDs) for user authentication, akin to the structure of Open Researcher and Contributor ID (ORCID). PIDs serve as unique and permanent identities for users, facilitating streamlined identification processes and accommodating the dynamic nature of user profiles within social media platforms.

Comparative analysis with traditional authentication systems reveals significant advantages of the proposed blockchain-based authentication model. These include enhanced user control over personal information and improved security against phishing attacks. The decentralized nature of the blockchain, coupled with its immutability, significantly fortifies the security posture of the proposed authentication system.

Challenges surrounding scalability and security vulnerabilities are acknowledged within the paper[4], with mitigation strategies proposed to address these issues. Techniques such as sharding, continuous monitoring, and updates to smart contracts are suggested to overcome scalability challenges and bolster security measures.

Economic implications are also considered, with a token-based reward mechanism for incentivizing user participation and enhancing overall system security. Furthermore, user experience considerations are integral to the proposed framework, focusing on intuitive interfaces, clear instructions, and educational resources to facilitate user-friendly adoption and interaction with the blockchain-based authentication system.

4.1.5 Cyber risk and cybersecurity: a systematic review of data availability

The research conducted by Cremer et al. (Year) aims to provide a systematic review of studies related to cyber risk and cybersecurity datasets. The study categorizes datasets and analyzes their applications in various cybersecurity domains, including intrusion detection, machine learning, IoT security, network forensics, and more. The paper[5] also discusses challenges and limitations associated with existing datasets and proposes directions for future research to address these gaps.

The study identifies three main categories of datasets: general intrusion detection, intrusion detection systems with a focus on IoT, and literature reviews. Within each category, several datasets are discussed along with their applications in research and practical contexts. Examples of datasets mentioned include UNSW-NB15, CSIC 2010, KDD Cup 99, NSL-KDD, CIDDS-001, Bot-IoT, and more.

Furthermore, the paper [5] highlights the importance of datasets in cyber insurance and risk management, emphasizing the need for comprehensive and up-to-date data to accurately assess cyber risks and price insurance policies effectively. It also discusses the potential of AI-driven security solutions in bolstering cybersecurity measures, particularly in wireless networks, and advocates for the integration of AI into security protocols to address emerging threats.

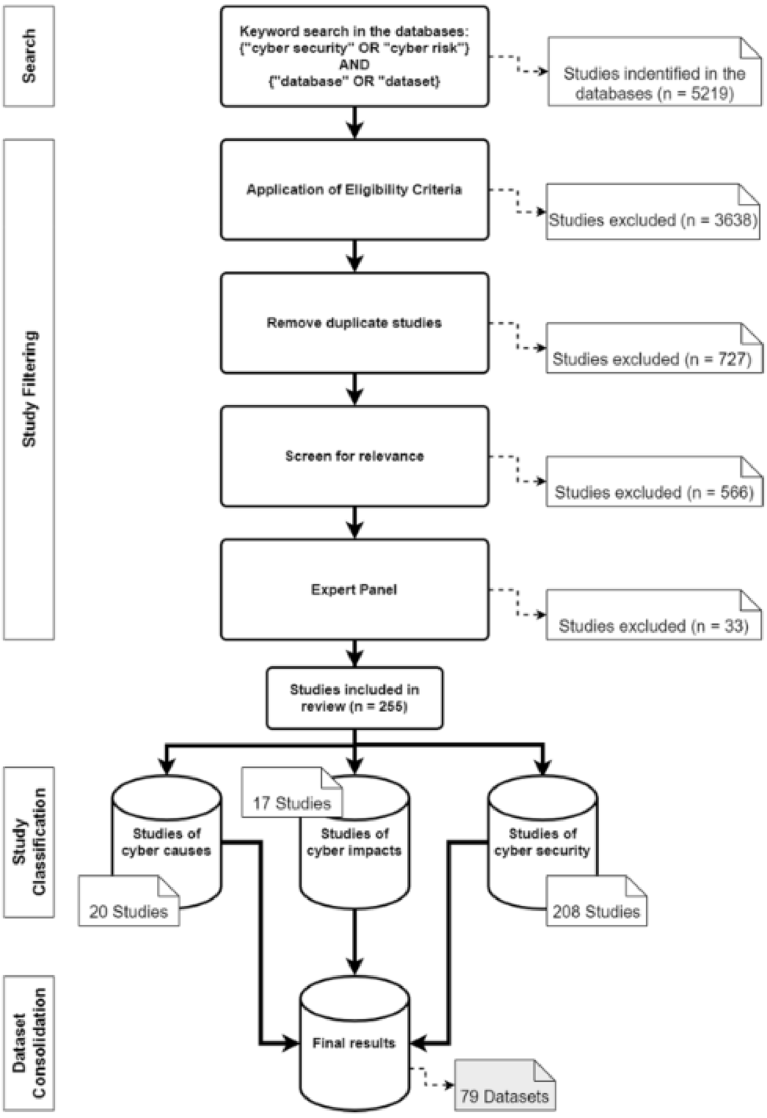

Search
Study Filtering
Study Classification
Dataset Consolidation
Keyword search in the databases: {"cyber security" OR "cyber risk"} AND {"database" OR "dataset}
Studies indentified in the databases (n = 5219)
Application of Eligibility Criteria
Studies excluded (n = 3638)
Remove duplicate studies
Studies excluded (n = 727)
Screen for relevance
Studies excluded (n = 566)
Expert Panel
Studies excluded (n = 33)
Studies included in review (n = 255)
Studies of cyber causes
20 Studies
17 Studies
Studies of cyber impacts
Studies of cyber security
208 Studies
Final results
79 Datasets

Figure 4.5: Literature search process and categorization of the studies. source: [5]

The research methodology employed in this paper [5] involved a systematic literature review to identify relevant studies on cyber risk and cybersecurity datasets. Figure 4.5 provides a visual representation of the literature search process and the categorization of the studies conducted in this paper. Through a rigorous selection process, 255 studies were reviewed and categorized into three distinct categories. This systematic approach ensured that the selected datasets were comprehensive and relevant to the scope of the research. Figure 4.5 serves as a valuable tool for readers to understand the methodology used in compiling the datasets and conducting the systematic review.

The study concludes by underscoring the significance of publicly available datasets for advancing cybersecurity research and promoting data-driven decision-making in risk management practices. It suggests avenues for future research, including the development of more diverse and adaptable datasets, the establishment of clearer benchmarks, and the promotion of open science principles to facilitate data sharing and collaboration in the cybersecurity community.

4.1.6 Social Media Security: Identity Theft Prevention

The research paper[6] conducts a comprehensive examination of enhancing authentication in social media applications through the fusion of artificial intelligence (AI) and blockchain technologies, particularly in combating identity theft. It begins by highlighting the increasing prevalence of identity theft threats within social media platforms, emphasizing the urgent necessity for advanced security measures.

Additionally, the paper discusses the integration of facial recognition and voice biometrics as supplementary layers of defense against identity theft. These biometric authentication methods significantly strengthen user identity verification processes, reducing the likelihood of unauthorized access.

Furthermore, the research underscores the pivotal role of blockchain technology in addressing concerns related to identity theft. The decentralized architecture and tamper-resistant nature of blockchain establish a secure repository for user credentials, effectively thwarting unauthorized access attempts and identity manipulation. Smart contracts are also highlighted for their role in automating and improving authentication processes, thereby minimizing vulnerabilities associated with centralized databases.

In summary, the symbiotic integration of AI and blockchain enhances authentication protocols within social media applications and also serves as a robust defense mechanism against identity theft, ultimately contributing to creating a safer and more secure online environment.

4.1.7 Enterprise data breach: causes, challenges, prevention, and future directions

The paper[7] ”Enterprise data breach: causes, challenges, prevention, and future directions” provides a comprehensive examination of the factors contributing to enterprise data breaches, the challenges faced in preventing such breaches, current prevention techniques, and future directions for research and development in this critical area of cybersecurity.

In this section, the paper[7] explores the various factors that contribute to data breaches within enterprise environments. It delves into both internal and external factors, such as employee negligence, insider threats, sophisticated cyber-attacks, vulnerabilities in third-party systems, and the increasing complexity of IT infrastructure.

The paper[7] outlines the significant challenges faced by organizations in preventing data breaches. These challenges include the ever-evolving threat landscape, the difficulty in detecting sophisticated attacks, compliance with regulations and standards, the proliferation of endpoints and data storage locations, and the shortage of skilled cybersecurity professionals.

Current Approaches to Data Leak Prevention and Detection (DLPD): The paper[7] discusses the limitations of current DLPD approaches, including signature-based detection, regular expressions, collection intersection, machine learning, behavior analysis, watermarking, and honeypots. It highlights the strengths and weaknesses of each technique and emphasizes the need for more effective methods to address evolving threats.

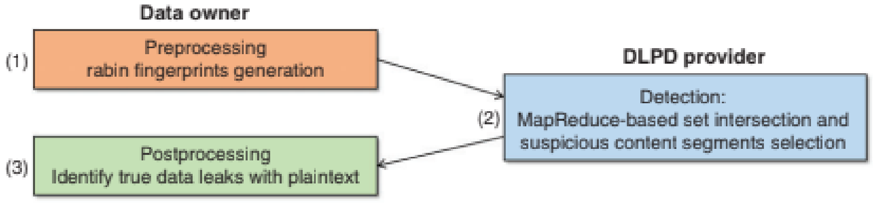

Data owner
(1)
Preprocessing
rabin fingerprints generation
(3)
Postprocessing
Identify true data leaks with plaintext
DLPD provider
(2)
Detection:
MapReduce-based set intersection and
suspicious content segments selection

Figure 4.6: Workload distribution between the data owner and DLPD provider. source: [7]

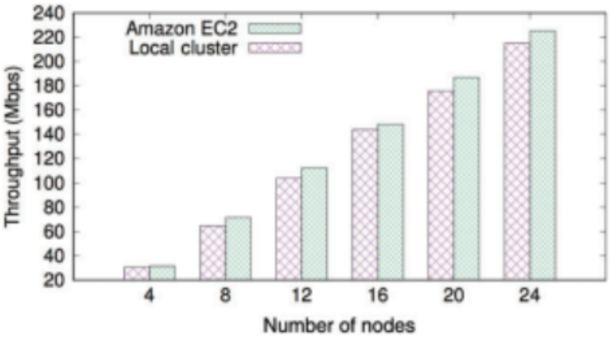


Figure 4.7: MR-DLD throughput on a local cluster and Amazon EC2. source: [7]

A Case Study: MapReduce-based Data Leak Detection (MR-DLD): The paper[7] introduces MR-DLD as a privacy-preserving data leak detection system that leverages the MapReduce distributed computing framework. It explains how MR-DLD addresses the challenges of scalability, privacy preservation, accuracy, and timeliness in detecting data leaks in the era of big data. Figure 4.6 illustrates the workload distribution between the data owner and data leak prevention and detection (DLPD) provider in the proposed MapReduce-based Data Leak Detection (MR-DLD) system. Similarly, Figure 4.7 showcases the throughput of MR-DLD on both local clusters and Amazon EC2, demonstrating its scalability and performance in processing large-scale datasets.

Further Research Opportunities: In this section, the paper[7] identifies promising research directions for improving data leak prevention and detection. These include the application of deep learning for insider threat detection, DLPD as a Cloud service, monitoring encrypted channels, and the development of benchmarks for DLPD.

In conclusion, the paper[7] summarizes the key findings regarding the causes of enterprise data breaches, the challenges in preventing such breaches, current prevention techniques, and future research directions. It underscores the importance of continuous innovation and collaboration in the ongoing effort to safeguard sensitive enterprise data.

4.1.8 Existing Solutions without AI or Blockchain

4.1.8.(i) Fuzzy Logic System for Identity Theft Detection in Social Networks

In this study, a novel method is introduced to address the pressing issue of identity theft within social networks. This paper[8] proposes a comprehensive system designed to analyze user behavior, linguistic patterns, and geolocation data to counter the threat posed by cyber-criminals exploiting user credentials for malicious purposes, such as phishing and spreading malware.

To counter this threat, this paper[8] presents a comprehensive system designed to analyze user behavior, linguistic patterns, and geolocation data. By examining factors like message frequency, unusual vocabulary usage, and login locations, the system aims to pinpoint suspicious activities indicative of identity theft.

What sets this approach apart is its adaptability and global applicability. Unlike conventional methods that focus on specific platforms or environments, this paper[8] offers a versatile solution that can be implemented across various social networks. Leveraging fuzzy logic allows for quick decision-making based on incomplete or imprecise data, enhancing both flexibility and accuracy.

The system consists of three key components: text mining, geolocation analysis, and fuzzy logic inference. This paper[8] employs text mining techniques to pre-process user data and extract linguistic patterns, while geolocation analysis detects anomalies in login locations. These inputs are then fed into the fuzzy logic inference engine, which evaluates the likelihood of identity theft based on predefined rules and linguistic variables.

An important aspect highlighted in this paper[8] is the system's ability to evolve alongside emerging threats. By incorporating new rules or variables, the system can continuously enhance its detection capabilities without requiring a complete overhaul. Additionally, fuzzy logic's inherent tolerance to inaccuracies enables the system to effectively handle noisy or incomplete data.

Figure 4.8 illustrates the architecture of the proposed system, showcasing the integration of text mining, geolocation analysis, and fuzzy logic inference to detect identity theft within social networks. This visual aid helps conceptualize the system's workflow and highlights the synergy between its components in combating cyber threats.

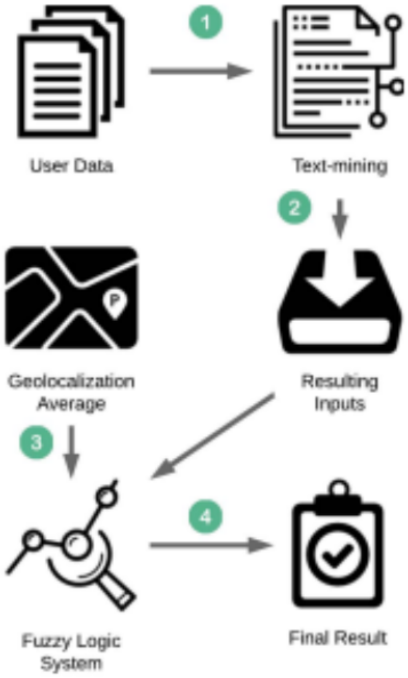


Figure 4.8: Schema of the Proposed System. Source: [8]

In conclusion, this paper's [8] innovative approach offers a promising solution to combat identity theft within social networks. By combining fuzzy logic and text mining, the system provides a robust defense against malicious activities, contributing to a safer online environment for users worldwide.

4.1.8.(ii) Multi-biometric template protection based on bloom filters

The paper[9] presents a comprehensive study on multi-biometric template protection utilizing Bloom filters, aiming to enhance security and privacy in biometric authentication systems. Introducing a novel methodology, it focuses on safeguarding various biometric templates, including face, iris, fingerprint, and finger vein data, ensuring both irreversibility and unlinkability. By employing Bloom filters, the framework establishes a robust defense mechanism against unauthorized access and identity theft, contributing to heightened data privacy and security.

A systematic approach is outlined for estimating key parameters crucial for optimizing Bloom filters in biometric data protection. Additionally, the paper proposes a general method for protected weighted feature-level fusion, enhancing verification accuracy while preserving privacy. Through extensive experimentation with diverse biometric characteristics and databases, the accuracy of the proposed methods is validated, demonstrating high verification accuracy alongside improved template security.

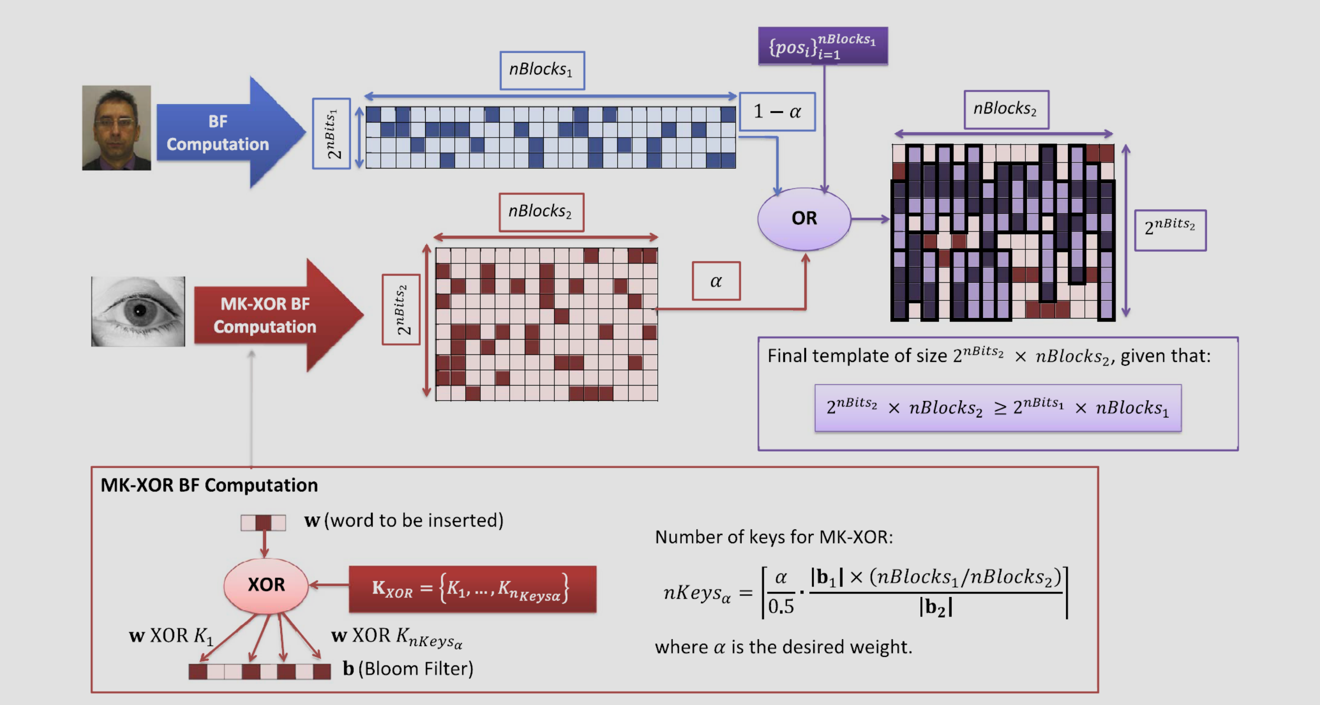

BF Computation
2^{nBits_1}
$nBlocks_1$
$\{pos_i\}_{i=1}^{nBlocks_1}$
$1-\alpha$
$nBlocks_2$
OR
2^{nBits_2}
MK-XOR BF Computation
2^{nBits_2}
$nBlocks_2$
α
Final template of size $2^{nBits_2} \times nBlocks_2$, given that:
$2^{nBits_2} \times nBlocks_2 \geq 2^{nBits_1} \times nBlocks_1$
MK-XOR BF Computation
$\mathbf{w}$ (word to be inserted)
XOR
$\mathbf{K}_{XOR} = \{K_1, \ldots, K_{nKeys\alpha}\}$
$\mathbf{w}$ XOR K_1
$\mathbf{w}$ XOR K_{nKeys_α}
$\mathbf{b}$ (Bloom Filter)
Number of keys for MK-XOR:
$nKeys_\alpha = \left\lceil \frac{\alpha}{0.5} \cdot \frac{|\mathbf{b}_1| \times (nBlocks_1/nBlocks_2)}{|\mathbf{b}_2|} \right\rceil$
where α is the desired weight.

Figure 4.9: Template Protection using multi-biometric characteristics. The smaller template is reallocated over the bigger one, followed by an OR operation to receive the final template. Multi-Key XOR is used in characteristic computation to achieve weighted fusion. Source: [9]

Security advantages are highlighted, emphasizing the irreversibility and unlinkability of protected biometric templates, which mitigate the risk of identity theft and prevent template linkage across databases or applications. The introduction of weighted feature-level fusion further bolsters privacy protection, reducing the vulnerability to parallelized attacks and enhancing system security.

Comparative analysis with traditional systems underscores the distinctive features of the proposed methodology, including its utilization of multiple biometrics, incorporation of Bloom filters for template protection, and application of Binarized Statistical Image Features (BSIF) for feature extraction. Score-level fusion adds to the system's robustness, increasing recognition accuracy compared to single biometric approaches.

Challenges such as generalization across different biometric characteristics and parameter estimation are acknowledged. Mitigation strategies include the introduction of automatic estimation methodologies and weighted feature-level fusion techniques to address these challenges effectively.

The empirical validation of the methodology through extensive experiments across various biometric traits and databases confirms its effectiveness and reliability. Overall, multi-biometric template protection using Bloom filters advances biometric authentication systems by setting a new standard for secure and private authentication mechanisms.

4.1.8.(iii) Identity Theft Detection in Mobile Social Networks Using Behavioral Semantics

The paper[10] proposes a novel solution to address the rising concern of identity theft within mobile social networks (MSNs) by introducing a behavior-based detection method, departing from traditional security measures such as passwords. Central to this approach is a probabilistic generative model based on Bayesian networks, aiming to capture the joint distribution of a user's spatial, temporal, and semantic behaviors, particularly concerning check-in events across various dimensions.

Representing check-in events as a joint distribution over the venue, time, tweet text, community, and topics, the proposed model employs Gibbs sampling to learn distribution parameters. By computing the probability that a new check-in event belongs to a specific user, potential identity theft instances can be detected by comparing this probability to a predefined threshold.

The paper[10] underscores the significance of semantic features extracted from tweets in outperforming spatial features for identity theft detection, as demonstrated through experiments conducted on Foursquare and Yelp datasets. Moreover, the study outlines future research directions, including comparisons with methods utilizing text, spatial, and LDA features independently, and evaluating the model's capability to differentiate a user's behavior from that of their friends.

Security benefits of the proposed approach include its behavior-based identity theft detection mechanism, which proves more effective than traditional methods like passwords or biometrics. Detecting identity theft post-compromise through the identification of anomalous behaviors, the model complements existing prevention techniques. Additionally, the joint modeling of spatial, temporal, and semantic user behaviors using a Bayesian approach enhances the accuracy of identity theft indicators detection, while community-specific distributions help handle data sparsity issues.

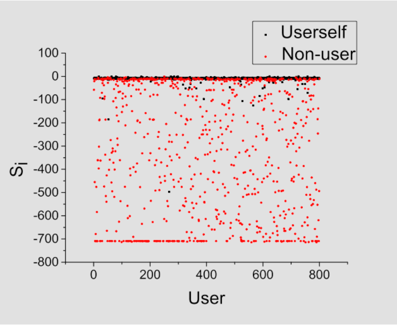


Figure 4.10: Identity Theft Detection Events based on the Spatial Distribution. Source: [10]

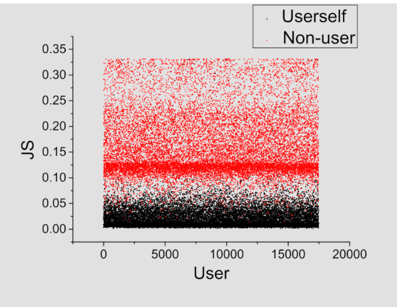


Figure 4.11: Identity Theft Events based on the Semantic Features. Source: [10]

Figure 4.10 and Figure 4.11 highlight the difference between Event Tagging when using Spatial Distribution and Semantic Features, with the semantic-based method better at tagging valid and anomalous incidents.

Despite its advantages, the approach still faces limitations, including its experimental nature and the necessity for large-scale testing to ascertain its effectiveness. Moreover, the accuracy metrics have yet to be directly compared to existing methods. However, the paper's [10] outcomes suggest that user behavioral data, particularly semantic features extracted from tweets, hold promise for effectively detecting identity theft in MSNs, potentially improving security in social media applications.

4.2 USING AI TO HELP PERFORM SECURE AUTHENTICATION

4.2.1 Authentication Based on Touch Patterns Using an Artificial Immune System

The conventional approach to mobile user authentication verifies credentials only at login, lacking ongoing checks for user control. This research proposes Continuous Authentication using an Artificial

Immune System (AIS), which continuously authenticates users based on touch behavior patterns, overcoming traditional authentication limitations.

The proposed solution in [11] leverages AIS with two mechanisms: Negative Selection (NS) and Clonal Selection (CS), inspired by the human immune system. NS mimics self-non-self-discrimination, generating detectors for self-interactions. CS selects and clones detectors to detect abnormal patterns, improving accuracy over time.

In touch-based authentication, NS creates detectors for self-interactions on a device's touch screen. AIS recognizes owner patterns, removing self-matching detectors. If unauthorized access is detected, the device locks.

AIS offers advantages over existing systems, integrating NS and CS for effective abnormal pattern detection. Compared to SVM or DT, AIS demonstrates superior accuracy, ensuring ongoing authentication on mobile devices. AIS, integrating with touch behavior, maintains user control during social media sessions. NS and CS flexibility makes AIS innovative for preventing unauthorized access.

Experimental evaluations, including CS and NS tests on three datasets, show AIS correctly authenticating 99.89% of users. This suggests AIS potential for continuous mobile device authentication, addressing traditional method gaps.

4.2.2 User Authentication by Face Thermograms Based on Hybrid Neural Networks

The paper [12] discusses the use of blockchain technology and its potential for improving transparency and efficiency in transactions. It highlights the concept of blockchain, which was initially introduced by Satoshi Nakamoto in 2008 with the creation of Bitcoin, a decentralized monetary network.

Blockchains are classified into two main types: permissioned and permissionless (public). In a permissionless blockchain, anyone can participate in mining and conducting transactions, while in a permissioned blockchain, only registered users are allowed to carry out transactions and participate in the consensus process.

The advantages of the unspent transaction output (UTXO) mechanism used in Bitcoin as discussed in [12], treating each transaction as a token rather than a closed balance, providing improved

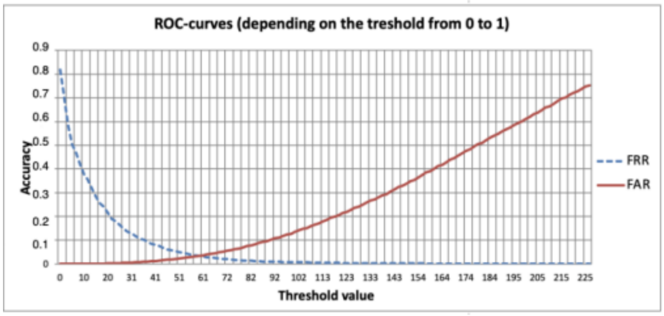


Figure 4.12: ROC curve. Source: [12]

security and the ability to handle multiple transactions from the same payer simultaneously.

To prevent attacks like the 51% or Sybil attacks and double spending, permissionless blockchains employ the proof of work (PoW) consensus mechanism. However, PoW is energy-intensive and contributes to increased CO2 emissions and global warming. In contrast, permissioned blockchains do not require energy-intensive consensus techniques for network security. Instead, blocks are certified by a group of authorities, enabling fraud detection and voting out of bad nodes.

The concept of Decentralized Identifiers (DIDs), which are cryptographic identifiers for decentralized digital identity verification is mentioned in [12]. DIDs enable self-managed authentication and are essential for access control in blockchain and peer-to-peer networks. The World Wide Web Consortium (W3C) is working on standardizing DIDs, but the protocol implementation is left open.

[12] discusses the proposed system's throughput limit of 15 transactions per second (TPS), which is significantly lower than regular Visa's 1700 TPS. Blockchain networks typically have lower transaction throughput due to decentralized consensus, leading to an expanding MemPool for pending transactions if TPS is insufficient.

In conclusion, the text emphasizes the importance of DIDs for decentralized, self-managed identity verification, ensuring secure authentication independent of centralized control. DIDs can adapt to a wide range of application cases and subjects. However, transaction speed remains a challenge, and hardware improvements and the effectiveness of PoA consensus nodes are crucial for ensuring adequate transaction throughput.

4.2.3 AI-Assisted Risk Based Two Factor Authentication Method (AIA-RB-2FA)

[13] proposes a new AI-assisted risk-based two-factor authentication (AIA-RB-2FA) method to enhance user authentication security. It provides background on authentication methods like username/password, multi-factor authentication, biometrics, certificates, and tokens, commonly used in web applications today.

Two-Factor Authentication (2FA) relies on two factors – a password and a second factor, typically a one-time code sent to the user's phone. After entering their credentials, users must enter a one-time access code sent to their device. If both factors are verified, access is granted, otherwise, failed attempts are tracked, and the account gets locked.

Risk-Based Two-Factor Authentication (RB-2FA) aims to reduce the cost and delays of 2FA by estimating login risk based on past activity. It stores a list of safe devices and requires 2FA only for new devices, reducing costs and delays compared to 2FA.

The proposed AIA-RB-2FA method enhances RB-2FA security by using AI to model user login behavior based on selections from a multi-option login form. An AI algorithm, currently the KNN algorithm, models user preferences and distinguishes between legitimate user logins and attackers.

If the AI model predicts the login as a user, access is allowed; otherwise, 2FA is required. The method aims to balance usability, security, and cost by adaptively using 2FA based on AI-assessed risk.

In conclusion, the AIA-RB-2FA method proposes a novel way to strengthen existing risk-based two-factor authentication by using AI to model user behavior. More research is needed to test and improve the method further.

In conclusion, the AIA-RB-2FA method proposes a novel way to strengthen existing risk-based two-factor authentication by using AI to model user behavior. Preliminary analysis with sample data shows potential, but more research is needed, especially around the selection of optimal AI algorithms for this use case. If effective, it can meaningfully improve authentication security.

The in-depth analysis yielded an understanding of the core solution, quantitative security evaluation, assessment of innovations and limitations, and a high-level synthesis of the advances presented and future directions needed. This provides a model for deeply analyzing a technical paper to extract

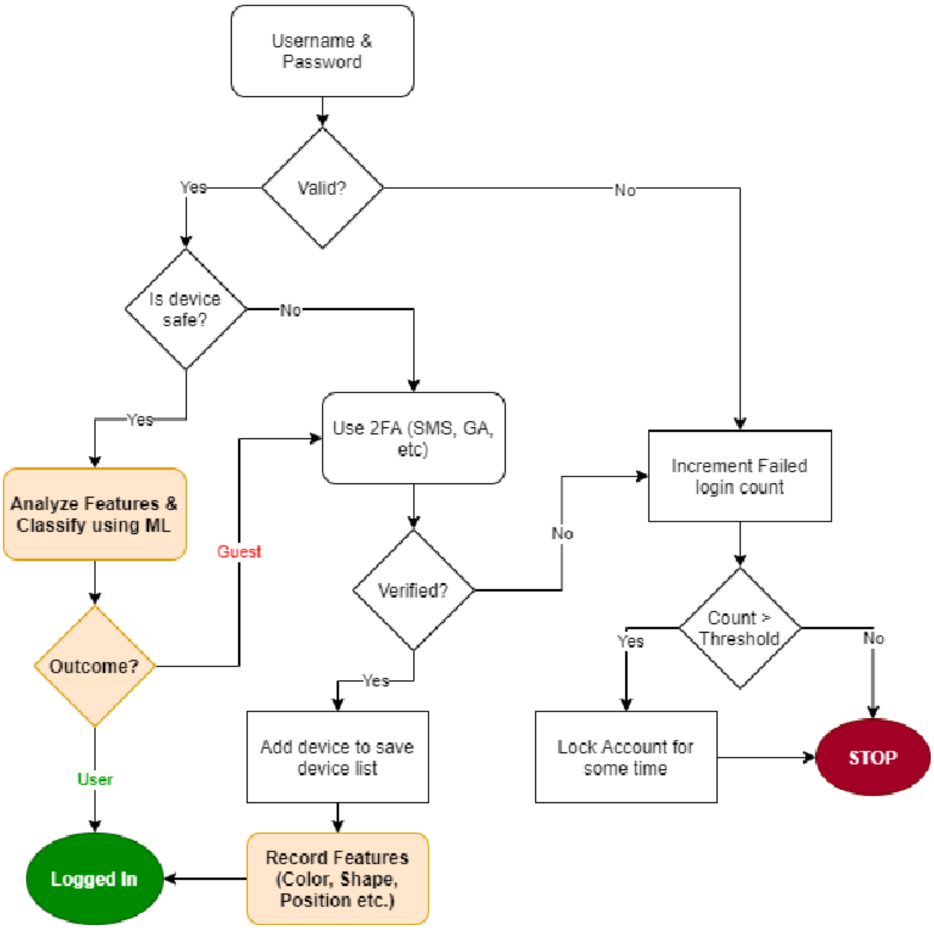

Username & Password
Valid?
Yes
No
Is device safe?
No
Yes
Use 2FA (SMS, GA, etc)
Increment Failed login count
Analyze Features & Classify using ML
Guest
No
Verified?
Outcome?
Count > Threshold
Yes
No
Yes
Add device to save device list
Lock Account for some time
STOP
User
Logged In
Record Features (Color, Shape, Position etc.)

Figure 4.13: AIA-RB-2FA methodology. Source: [13]

key knowledge contributions.

4.2.4 Social Media User's Safety Level Detection through Classification via Clustering Approach

The paper [14] presents a model for classifying social media users into three categories - safe, medium safe, and risky - based on their account security practices, privacy settings, posting behavior, and potential exposure to phishing incidents. The goal is to provide personalized safety assessments by combining unsupervised and supervised machine learning techniques.

The methodology begins with data collection through a closed-ended questionnaire containing 30 multiple-choice questions designed after studying prior research on social media user behavior and security risks. These questions capture various aspects such as account security habits, privacy settings, posting patterns, and instances of phishing attacks. Survey responses were gathered from 1,000 Facebook users.

To build the predictive model, the 12 most relevant features were used for further analysis. The data was clustered into three groups using a hierarchical agglomerative clustering approach. The cluster statistics were then manually analyzed to create labels for the three clusters: safe, medium safe, and risky.

Logistic Regression achieved the highest accuracy of 97.4% based on metrics like Accuracy, Area Under the Curve (AUC), Precision, Recall, and F1-Score. The trained Logistic Regression model can then be used to provide safety classification for new user data in the prediction stage. The core techniques employed in this study include data collection through a closed-ended question survey and label encoding, feature selection using Gain Ratio, hierarchical clustering for data segmentation, and various classification algorithms for building the predictive model. Model evaluation was performed using metrics such as Accuracy, AUC, Precision, Recall, and F1-Score.

The key advantages of this approach are providing personalized safety assessments, combining unsupervised and supervised techniques, and comparing multiple classifiers to choose the optimal model. However, limitations include the dataset's potential lack of global representation, the absence of more rigorous privacy-sensitive features, the need for continuous retraining as new threats emerge, and limited details on the survey methodology and analysis.

Overall, this safety assessment model is highly relevant for analyzing authentication risks in social media platforms. By extracting user features and activity patterns that can compromise account security, the combined clustering and classification approach could be adopted for predicting authentication risks in social media and other online platforms.

4.2.5 Experimental Face Recognition System Based On Improved Artificial Intelligence Model

The study [15] introduces a state-of-the-art AI model for facial recognition tailored for high performance in wireless multimedia networks. This improved model integrates Blind Feature Learning (BFL) and Lightweight Physical Layer Authentication (LPLA), exploiting neural networks for analyzing and interpreting complex multimedia data. Through these technologies, the model significantly enhances both security and efficiency compared to traditional methods.

The proposed model streamlines the face recognition process, starting from data collection to the final authentication step, using a sophisticated recognition server and database server for storing and managing facial data. The utilization of a video accelerator and a developer's ARM module aids in refining the AI models and algorithms, ensuring real-time face recognition capabilities, as depicted in Figure 4.14.

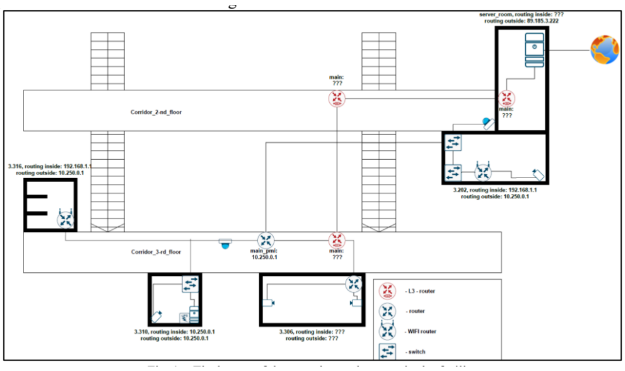

server_room, routing inside: ???
routing outside: 89.185.3.222
main:
???
Corridor_2-nd_floor
main:
???
3.316, routing inside: 192.168.1.1
routing outside: 10.250.0.1
3.202, routing inside: 192.168.1.1
routing outside: 10.250.0.1
Corridor_3-rd_floor
main_pmi:
10.250.0.1
main:
???
3.310, routing inside: 10.250.0.1
routing outside: 10.250.0.1
3.306, routing inside: ???
routing outside: ???
- L3 - router
- router
- WIFI router
- switch

Figure 4.14: Schematic of the data collection and authentication process in the face recognition system. Source: [15]

In comparison to conventional systems, the AI-based system demonstrates superior accuracy in facial recognition, alongside increased efficiency and strengthened security protocols. This system excels in its real-time processing speed and its ability to provide flexible solutions across various challenging environments, marking it as a more adaptable and robust alternative.

Challenges such as ensuring high-quality training data, privacy concerns, and adapting to environmental factors are addressed through innovative approaches like data augmentation and adaptive algorithms. This ensures that the system remains effective and reliable under diverse conditions, safeguarding user privacy and maintaining recognition accuracy.

In conclusion, [15] presents a compelling advancement in facial recognition technology, showcasing an AI-assisted system that stands out for its accuracy, adaptability, and real-time efficiency. This research indicates a significant step forward in security authentication, with implications for enhancing the integrity of social media platforms and other digital services that require reliable identity verification.

4.2.6 Determination of Performance to Verify the Synthetic Identity Theft by Training the Neural Networks

[16] Synthetic identity theft is a complex and growing financial crime that involves creating new identities by combining real and fake information. This fraudulent method is used to open credit accounts, qualify for benefits, or live or work in the U.S. Fraudsters blend fictitious details, such as fabricated names, with actual data, like a child's Social Security number, to create fraudulent accounts. Detecting and preventing synthetic identity theft is challenging due to its intricate nature and the absence of clear victims.

Fraudsters typically start by pilfering information from unsuspecting individuals to construct synthetic identities. They steal Social Security numbers (SSNs) and pair them with false details like names, addresses, and birthdates. With these synthetic identities, criminals open accounts and behave responsibly to build credit scores and history. A higher credit score allows for more substantial fraudulent gains. Some criminals accumulate fraudulent charges and then pose as victims to restore their credit lines. With restored credit, they exploit additional credit lines for further theft.

Detecting synthetic identity theft is challenging due to its complexity. Financial institutions' filters may not catch it, and since there is no clear victim, institutions struggle to identify the fraud. The types of synthetic identity fraud vary, including cases where criminals aim to steal money from creditors or cases involving undocumented immigrants using invented or stolen SSNs to access financial services.

Preventing and recovering from synthetic identity theft require advanced techniques and vigilance from financial institutions. Detecting synthetic identity theft requires sophisticated methods, and financial institutions must remain vigilant to prevent and recover from this pervasive crime.

In conclusion, synthetic identity theft remains a significant financial challenge, affecting millions of people and costing billions of dollars. Detecting and preventing it require advanced techniques and vigilance from financial institutions. The intricate nature of synthetic identity theft, coupled with the absence of clear victims, makes it a formidable adversary. As technology evolves, continuous enhancements in detection mechanisms are crucial to combat this growing threat.

This in-depth analysis provides an understanding of a method for analyzing various user identities to detect synthetic identity theft, a type of fraud that involves creating a new identity by combining real and fake information. The paper uses three types of data (Input, Normal, and Target) containing text or string data related to different identities, such as name, date of birth, address, and document numbers. The identities are categorized as High, Medium, or Low based on the accuracy of the information. Neural networks are trained using this data, and their performance is evaluated in terms of epoch values, time, gradient, and validation checks.

4.2.7 Deep Face Recognition for Biometric Authentication

The paper [17] presents a convolutional neural network (CNN) based face recognition system for biometric authentication. Facial recognition is widely used for human identity authentication due to its seamless process and versatility across domains like security, access control, and social media. However, traditional methods struggle with varying conditions like illumination and facial expressions, requiring innovative approaches for robust performance.

Facial recognition faces challenges like processing speed, image quality, and lighting variations. Despite these, its speed and user independence make it compelling for applications like security and attendance management. To overcome these challenges, the paper proposes using CNNs, creating a diverse dataset, and employing the Viola Jones algorithm for face detection. Choosing the right pre-trained CNN model, such as Squeezenet, is crucial for performance. The training process involves fine-tuning the model on an augmented dataset. The paper highlights the importance of deep learning in advancing facial recognition technology and its potential in real-world applications. Continued research

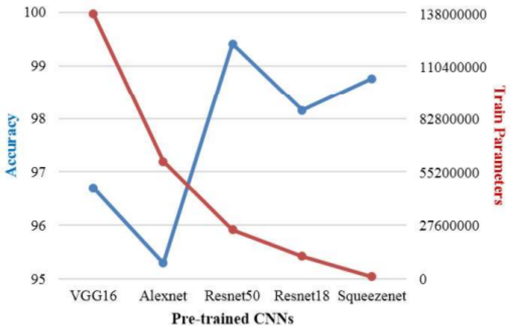


Figure 4.15: Performance comparison of pre-trained CNNs. Source: [17]

and integration with emerging technologies are key to enhancing biometric authentication systems.

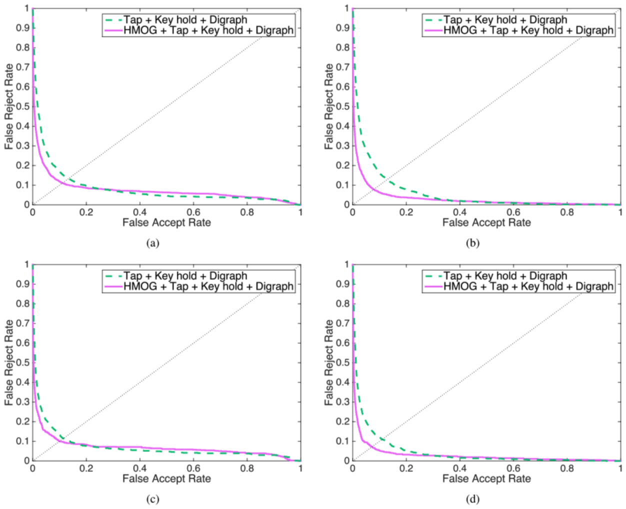
The outcomes of the study reveal the promising potential of deep learning-based facial recognition systems in overcoming traditional limitations. By leveraging CNNs and augmented datasets, the proposed system achieves impressive accuracy rates while addressing challenges such as varying illumination and facial expressions. The robust performance of the system underscores its viability for deployment in diverse real-world scenarios, ranging from security to attendance management and beyond. These outcomes highlight the transformative impact of deep learning in enhancing biometric authentication systems and pave the way for future advancements in facial recognition technology.

4.2.8 HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users

[18] presents an innovative approach to smartphone security with the introduction of Hand Movement, Orientation, and Grasp (HMOG) as behavioral biometric features for authentication. This method utilizes the sensors within smartphones, such as accelerometers, gyroscopes, and magnetometers, to capture the unique ways in which a user interacts with their device. By analyzing these interactions, the system continuously authenticates the user, ensuring a high level of security without any active input from the user, which is a considerable enhancement over traditional static authentication methods.

The key techniques explored in [18] include HMOG feature extraction and biometric key generation. The unique patterns in hand movements and orientation during phone use are translated into a form of continuous authentication, which is both secure and user-friendly. Moreover, the paper explores the feasibility of generating cryptographic keys based on HMOG features, providing a new dimension to security in mobile computing. An energy efficiency analysis ensures that these advanced authentication methods do not compromise the device's battery life, striking an optimal balance between security and usability, as demonstrated in Figure 4.16.

While the study indicates that the HMOG-based system outperforms traditional authentication methods, it also identifies challenges such as data quality, environmental factors, and adaptability over time. These areas present opportunities for further research to enhance the effectiveness and reliability



(a) (b) (c) (d)

Figure 4.16: DET curves for fusion of all feature types including and excluding HMOG. Source:[18]

of HMOG-based authentication systems.

In conclusion, the research in [18] is a significant stride towards a new era of mobile security. It illustrates the vast potential of behavioral biometrics in creating more secure, efficient, and unobtrusive authentication mechanisms for smartphone users, which aligns with the ongoing efforts to improve authentication in social media applications using AI and blockchain.

4.3 USING BLOCKCHAIN TO HELP PERFORM SECURE AUTHENTICATION

4.3.1 Decentralized Dynamic Identity Authentication System Based on Blockchain

[19]introduces a decentralized dynamic identity authentication system leveraging blockchain technology to overcome the limitations of centralized systems. It aims to enhance security against forgery and unauthorized access, particularly against replay and dictionary attacks, by utilizing public keys with nonce for sign-in authentication. The proposed system operates on a public chain model, enabling any organization or individual to join as a verifier.

Key features of the system include the incorporation of nonce arrays within the block structure, facilitating dynamic updates to user identities, and ensuring independence across the blockchain. A limit of 100 authentications per block is imposed to manage system efficiency.

The system offers three main interfaces: Account Registration, Nonce Query, and Identity Authentication. Account registration involves generating public and private keys, hashing them, and broadcasting the new block to the network. Identity authentication is carried out through nonce query, where the client signs the nonce with their private key and compares it with the cached value, ensuring secure login procedures.

Security measures include the utilization of blockchain for tamper-proof identity management, smart contracts for access control, digital signatures for data integrity, and dynamic identity attributes for user control. Decentralization eliminates single points of failure, while pseudonymity protects user privacy.

The system allows users to update their attributes without central authority involvement, ensuring transparency and auditability. It addresses the inefficiencies and security vulnerabilities of traditional centralized systems, offering fine-grained access control and efficient revocation mechanisms for compromised identities.

Compared with traditional systems, the proposed solution offers superior security, user control, and efficiency in managing dynamic identity changes. Notably, it ensures non-tamperable authentication through public-private key mechanisms and utilizes a modified block structure for nonce-based authentication. Additionally, the inclusion of both light and heavy nodes reduces space complexity and enhances security and network participation.

4.3.2 A distributed biometric authentication scheme based on blockchain

This paper[20] presents a novel distributed biometric authentication scheme leveraging blockchain technology, aimed at addressing the challenges of traditional centralized authentication methods. The proposed scheme eliminates the need for a central node storing users' biometric templates, thereby enhancing privacy and security. Instead, it utilizes the Ethereum blockchain and IPFS distributed file system, combined with homomorphic encryption, to securely store and manage users' biometric data.

The registration phase involves users generating encrypted transformed templates of their biometric data, which are then uploaded to IPFS and linked to an Ethereum smart contract. These templates are securely stored and managed without exposing sensitive biometric information. During authentication, users authenticate themselves against third-party services using their biometric data, which is transformed and encrypted locally before being sent for verification. The third-party service retrieves the encrypted template from IPFS, calculates the distance between the templates, and makes an authentication decision without accessing the user's actual biometric data.

The paper[20] provides insights into the technical implementation of the proposed scheme, including the setup of private Ethereum and IPFS networks, as well as the development of client and service implementations. Experimental results demonstrate the efficiency of the scheme, with minimal time overhead for template preparation and authentication procedures.

Overall, the proposed scheme offers a secure and privacy-preserving biometric authentication solution suitable for various applications. Future research directions include exploring hardware security mechanisms for biometric sensor devices and further optimizing the homomorphic encryption algorithm for improved security.

4.3.3 A Minimal Disclosure Signature Authentication Scheme Based on Consortium Blockchain

[21]introduces the Minimal Signature Authentication (MDSA) scheme, utilizing consortium blockchain technology to address limitations in traditional identity authentication methods. It identifies centralized systems' vulnerabilities, such as single points of failure and privacy breaches, contrasting them with the decentralized and immutable nature of blockchain. The concept of Self-Sovereign Identity (SSI), granting individuals control over their digital identities, is explored, though detailed implementation architectures are lacking, prompting the proposal of MDSA.

Background information covers blockchain-based identity authentication, emphasizing distinctions between public, consortium, and private blockchains. Standards like Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) are discussed, alongside authentication models and zero-knowledge proof techniques for privacy preservation.

The MDSA framework consists of credential generation, transaction, and minimal disclosure authentication stages. Credential creation involves Merkle Tree structures and cryptographic algorithms, ensuring comprehensive and verifiable identity representations. Smart contracts on the consortium blockchain facilitate secure interactions, while minimal disclosure authentication and zero-knowledge range proofs maintain privacy during attribute validation.

Performance evaluation demonstrates MDSA's feasibility, scalability, and efficiency, with linear overhead increases as attribute volumes scale. The comparative analysis highlights its superiority over traditional methods in signing and verification speeds.

Performance analysis underscores MDSA's efficacy in privacy, security, and efficiency. Its emphasis on user-controlled identities and minimal disclosure ensures data protection while enabling seamless authentication. Merkle Trees' robustness and zero-knowledge proofs' efficiency reinforce MDSA's viability.

Related work contextualizes MDSA within decentralized authentication, Merkle Tree applications, and selective disclosure schemes, offering insights into the field's evolution.

In conclusion, MDSA presents a pioneering approach to decentralized, privacy-preserving identity authentication. Future research avenues include optimizing overhead and exploring broader applications beyond identity authentication.

The study suggests applying MDSA to social media authentication, addressing rising mobile device use, and ensuring security while preventing information leakage and privacy breaches.

4.3.4 Blockchain-enabled secure and efficient data sharing scheme for trust management in healthcare smartphone network

This paper [22] presents a blockchain-enabled secure and efficient data-sharing scheme for trust management in healthcare smartphone networks (HSNs). The Internet of Medical Things (IoMT) is utilized within the HSN framework for remote patient monitoring, and smartphones play a crucial role in collecting and sharing patient data among IoMT nodes. However, security concerns arise due to potential attacks targeting IoMT nodes, leading to compromised patient data and network integrity.

To address these challenges, the paper [22] proposes a solution based on Hyperledger blockchain technology combined with a Clustered Hierarchical Trust Management System (CHTMS). The Hyperledger blockchain ensures tamper-proof ledger distribution among IoMT nodes without the need for a centralized authority, thereby enhancing data security and integrity. The CHTMS helps identify compromised IoMT nodes at the cluster level and integrates an Intrusion Detection System (IDS) to block malicious nodes.

Furthermore, the proposed methodology employs Elliptic Curve Cryptography (ECC) to protect sensitive health records and mitigate Denial-of-Service (DoS) attacks. The evaluation results demonstrate improved detection performance compared to existing solutions, indicating enhanced security and reliability in data sharing within HSNs.

The paper [22] also discusses the concept of smartphone-powered IoMT devices, which enable instant monitoring of various health parameters and facilitate data collection for the HSN platform. Trust management in HSNs involves distinguishing between benign and malicious nodes based on communication patterns and prior interactions. The proposed scheme operates in both intragroup and intergroup topologies, allowing centralized and distributed trust management among healthcare organizations.

Overall, the proposed methodology aims to enhance the security and efficiency of data sharing in healthcare smartphone networks through blockchain technology, trust management systems, and cryptographic techniques, thereby improving patient confidentiality and network resilience against malicious attacks.

4.3.5 Blockchain Technology for Authentication and Validation of Social Network Accounts

[23] In the evolving landscape of social media, the imperative for robust authentication mechanisms is paramount, given the rising incidences of identity misrepresentation and account falsification. The study [23] presents a groundbreaking approach utilizing blockchain technology to fortify the authentication and validation processes of social network accounts. This methodology not only enhances the security framework of social media platforms but also instills a higher degree of trust among users, thereby mitigating the risks associated with fraudulent accounts and enhancing overall platform integrity.

The research elucidates the deployment of blockchain as a decentralized ledger that irrevocably records user data, thereby establishing a verifiable and immutable point of trust. Through the creation of encrypted blocks containing users' data, the system ensures the authenticity and non-repudiability of user identities, making unauthorized data alterations practically unfeasible. The proposed model signifies a paradigm shift in how social media platforms could leverage cryptographic blocks to authenticate user profiles, thus ensuring that the real identity behind an account is verifiable and secure.

Moreover, the integration of blockchain into social media frameworks addresses significant challenges like the ease of creating counterfeit profiles and the proliferation of misinformation. By enabling a straightforward verification mechanism through blockchain's transparent yet secure ledger, users can independently verify the authenticity of the profiles they interact with, thereby fostering a safer social media environment. The system's resilience against alterations ensures that once a user's data is encoded into a blockchain block, it remains an unalterable point of reference for the account's authenticity.

Figures integrated into the study, such as the blockchain validation process and the subsequent authentication flow, provide a clear visualization of the operational framework. These illustrations are pivotal in understanding the seamless integration of blockchain technology into the user verification process, offering a comprehensive view of the potential transformations in social media security protocols.

In conclusion, the research presented in [23]. underscores the significant potential of blockchain technology in redefining the authenticity of social network accounts. By employing a decentralized, transparent, and secure method of user validation, the study heralds a new era in social media usage, where the assurance of identity integrity becomes a cornerstone of digital interactions. Future directions might include exploring the scalability of this model and its adaptability across various social media platforms, potentially setting a new standard for online identity verification and trust.

4.3.6 Blockchain-based biometric identity management

[24]aims to revolutionize authentication on social media platforms by combining AI-based biometric identification with blockchain-based identity management. The system utilizes deep learning models to analyze facial features for user authentication while storing biometric data securely on a blockchain. Key components include user-friendly interface design, regulatory compliance, risk management strategies, interoperability with existing systems, user adoption campaigns, and cost/resource

estimations.

Ethical considerations are paramount, addressing consent, autonomy, discrimination, and societal impact. The system offers enhanced security through biometric uniqueness, immutable records on the blockchain, and a decentralized architecture. Dynamic identity updates enable users to modify biometric data as needed.

Compared to traditional systems, the proposed solution offers heightened security, improved user experience, and reduced identity theft risk. Challenges such as biometric data security, scalability, regulatory compliance, and interoperability are mitigated through encryption, scalability solutions, compliance frameworks, and adherence to standards.

User experience considerations focus on usability, accessibility, feedback mechanisms, transparency/control, error handling, performance optimization, mobile responsiveness, aesthetics/branding, training/education, and continuous improvement.

Expected outcomes include increased security, enhanced user experience, and greater platform trust. Users can trust their identities are securely managed, leading to improved engagement and satisfaction with social media platforms.

4.3.7 Two Factor Authentication Framework Using OTP-SMS Based on Blockchain

This paper [25] discusses the need for more secure two-factor authentication (2FA) schemes, particularly focusing on the vulnerabilities of traditional OTP-SMS-based methods. It proposes a novel 2FA framework utilizing blockchain technology to address these vulnerabilities.

The paper outlines various attacks on 2FA schemes, including man-in-the-middle attacks and exploits targeting third-party OTP providers. It provides background on blockchain technology, highlighting its transparency, security, and resilience against single points of failure, along with an overview of Ethereum blockchain and smart contract functionality.

Reviewing related works, the paper cites instances of blockchain being used for authentication purposes in different contexts.

The proposed 2FA framework involves users logging in with a username and password, followed by interaction with a smart contract on the Ethereum blockchain to generate and authenticate OTPs.

Comparing with other blockchain-based 2FA schemes, the paper highlights the simplicity and effectiveness of its proposed framework in preventing common attacks.

In conclusion, the paper asserts that its blockchain-based 2FA framework enhances security by thwarting common attacks like MITM and third-party compromises, offering a flexible and secure alternative to traditional 2FA methods [25].

4.3.8 Authentication Protocol for Cloud Databases Using Blockchain Mechanism

[26] The exploration of enhancing data security in cloud environments, especially in the context of authentication protocols, is critically examined in [26]. The paper presents a novel Blockchain-based Authentication Mechanism (BAM) that addresses the profound security vulnerabilities posed by both insider and outsider threats in cloud databases. The authors illuminate the growing concern over data breaches, emphasizing the imperative need for robust authentication mechanisms that preempt unauthorized access and ensure the integrity of stored data.

Central to their discourse is the innovative use of blockchain technology as a bulwark against the multifaceted threats compromising cloud databases. By integrating a blockchain framework, the proposed authentication protocol fortifies the security barriers against malicious entities, ensuring that user credentials are inviolably stored and verified across a decentralized ledger. This approach not only mitigates the risks of data tampering but also enhances transparency and auditability, essential attributes in maintaining rigorous data security standards.

The paper delineates a comprehensive methodology wherein the blockchain's immutable and transparent nature is harnessed to develop an authentication system resilient to a spectrum of cybersecurity threats, including perilous insider attacks. The experimental results, validated using the Scyther formal system tool, substantiate the protocol's resilience against common cyber threats such as offline guessing, replay, and Denial of Service (DoS) attacks, confirming its robustness and efficacy.

Moreover, the research insightfully compares the proposed BAM with existing schemes, underscoring its superior capability in thwarting insider and outsider attacks, a testament to the innovative amalgamation of blockchain technology with traditional security paradigms. The findings advocate for a paradigm shift towards adopting distributed ledger technologies in safeguarding cloud databases, highlighting the potential of blockchain in revolutionizing the authentication landscape.

In conclusion, the study presented in [26]. contributes significantly to the ongoing discourse on enhancing cloud database security, offering a cogent, blockchain-oriented solution that promises to elevate the standards of data protection in cloud environments. Their work not only paves the way for future research in blockchain applications for security but also aligns seamlessly with the overarching goal of our project, which seeks to leverage cutting-edge technologies like AI and blockchain in fortifying authentication processes in social media applications.

4.3.9 Data Security in Healthcare Using Blockchain Technology

In this paper[27], a thorough examination is conducted on the critical issue of data security within the healthcare sector, with a particular focus on the application of blockchain technology. This study delves into the urgent need for robust data protection measures in healthcare, given the sensitive nature of patient information stored in Electronic Health Records (EHRs).

To address the escalating threat of cyber attacks targeting healthcare organizations, this paper[27] explores the potential of blockchain technology, which offers inherent security features grounded in cryptographic principles. The decentralized and immutable ledger architecture of blockchain ensures data integrity and transparency, making it an ideal solution for securing patient records and medical transactions.

One of the key challenges identified in healthcare data security is the prevalence of cyber attacks, with phishing emails accounting for a significant portion of security breaches. Regulations such as the Healthcare Insurance Portability Act (HIPAA) underscore the importance of implementing proactive security measures to safeguard patient information.

This paper[27] proposes a system that integrates blockchain technology with data management frameworks tailored for healthcare, such as EdgeMediChain, to ensure efficient and secure data sharing among authorized users. By leveraging blockchain's distributed ledger and cryptographic features, the system enhances interoperability and collaboration while minimizing the risk of data breaches.

Figure 4.17 illustrates the workflow of blockchain technology in healthcare, showcasing how each digital transaction is recorded, verified, and added to the blockchain. The decentralized nature of blockchain ensures that patient records can be securely accessed and shared across different healthcare providers, thereby improving care coordination and decision-making.

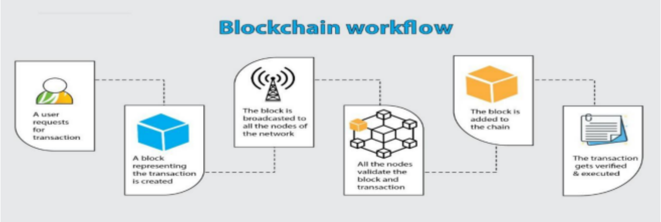

Blockchain workflow
A user requests for transaction
A block representing the transaction is created
The block is broadcasted to all the nodes of the network
All the nodes validate the block and transaction
The block is added to the chain
The transaction gets verified & executed

Figure 4.17: Workflow of blockchain. Source: [27]

Furthermore, the proposed blockchain-based architecture (Figure 4.18) outlines the components and relationships involved in securing patient medical records. Users play a central role in the architecture, with data security achieved through authentication mechanisms such as one-time passwords (OTP) or biometrics linked to social security numbers.

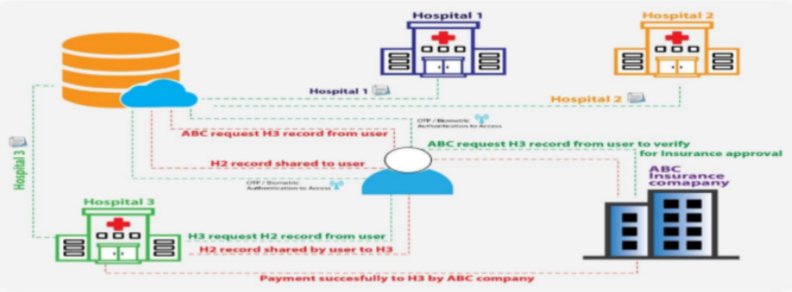

Hospital 1
Hospital 2
Hospital 1
Hospital 2
OTP / Biometric Authentication to Access
ABC request H3 record from user
ABC request H3 record from user to verify for Insurance approval
H2 record shared to user
ABC Insurance comapany
Hospital 3
OTP / Biometric Authentication to Access
Hospital 3
H3 request H2 record from user
H2 record shared by user to H3
Payment succesfully to H3 by ABC company

Figure 4.18: Proposed Blockchain Framework. Source: [27]

In conclusion, this paper[27] underscores the potential of blockchain technology to enhance data security and privacy in healthcare. While challenges such as scalability and implementation persist, continued research and development in blockchain-based healthcare systems hold the promise of revolutionizing the industry, providing patients and practitioners with secure and interoperable data management solutions.

4.4 PROPOSED SOLUTION

To enhance social media authentication effectively, integrating Artificial Intelligence (AI) and Blockchain technology presents a promising solution that addresses several existing challenges in digital identity verification and user privacy. The proposed system aims to leverage the strengths of both technologies to create a more secure, privacy-preserving, and user-friendly authentication process.

AI-driven continuous authentication forms the cornerstone of the proposed solution, utilizing advanced algorithms to analyze and learn from user behavior patterns, such as typing speed, login times, and interaction habits. This continuous monitoring enables the system to dynamically authenticate users based on their unique behavior patterns, offering a personalized and adaptive security layer. This method significantly improves security by identifying potential unauthorized access in real-time, based on deviations from established user behavior norms.

In parallel, the integration of Blockchain technology provides a robust framework for immutable user identity verification. By recording user credentials and authentication transactions on a decentralized ledger, the system ensures the integrity of data and prevents unauthorized access, all while maintaining transparency and auditability. Blockchain's inherent characteristics, such as decentralization, immutability, and transparency, make it an ideal technology for securing sensitive authentication data against tampering and breaches.

Smart contracts on the Blockchain further automate access control decisions, streamlining the authentication process and minimizing the potential for human error. These self-executing contracts can enforce access policies based on predefined criteria, such as user role, behavior, and authentication history, enhancing the system's efficiency and reliability.

To address privacy concerns associated with biometric authentication methods, the proposed system employs privacy-preserving techniques. AI enhances the accuracy and efficiency of biometric methods like facial recognition or fingerprint scanning, while Blockchain secures biometric data, ensuring it remains encrypted and only accessible through secure channels.

A user-centric approach to identity management is another pivotal feature of the proposed system. It empowers users with greater control over their digital identities, allowing them to manage their authentication credentials securely on the Blockchain. This approach not only enhances user privacy by giving individuals control over their data but also facilitates a trust-based relationship between users and social media platforms.

The system also incorporates adaptive multi-factor authentication (MFA), dynamically adjusting authentication requirements based on real-time risk assessments conducted by AI algorithms. This flexibility ensures that additional authentication factors are only requested when necessary, such as during login attempts from new devices or locations, thereby balancing security with user convenience.

Finally, a decentralized application (DApp) interface allows users to interact with their authentication settings, view access logs, and receive alerts for suspicious activities. This transparency and control mechanism further reinforces the security and user-centric nature of the proposed system.

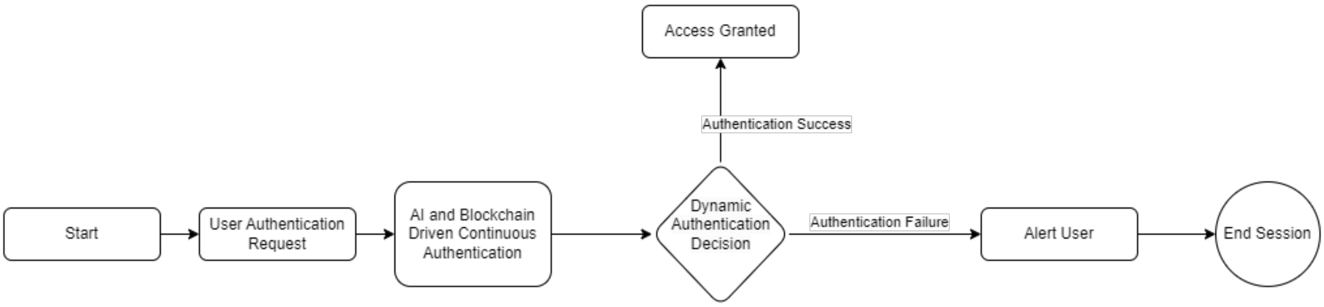

Access Granted
Authentication Success
Start
User Authentication Request
AI and Blockchain Driven Continuous Authentication
Dynamic Authentication Decision
Authentication Failure
Alert User
End Session

Figure 4.19: Flowchart of the Proposed Solution

Figure 4.19 depicts the flow of the proposed authentication process in a Social Media Authentication situation, where the Continuous Authentication is now composed of the following technologies and methodologies:

- AI-driven Continuous Authentication
- Blockchain Integration
  - Recording of User Credentials and Transactions
  - Data Integrity and Security Mechanisms
  - Smart Contracts for Access Control
- Automated Authentication Decisions

- Privacy-Preserving Biometric Authentication with Encrypted and Secure Biometric Data
- User-Centric Identity Management and User-Controlled Authentication Credentials
- Trust-Based User-Platform Relationship
- Adaptive Multi-Factor Authentication (MFA)
- Real-Time Risk Assessment by AI
- Dynamic Adjustment of Authentication Factors
- Decentralized Application (DApp) Interface
- User Interaction with Authentication Settings
- Access Log Viewing and Suspicious Activity Alerts

By combining AI's analytical capabilities with Blockchain's security features, the proposed solution offers a comprehensive approach to tackling the challenges of social media authentication. This integration not only enhances the security and privacy of digital identities but also sets a new standard for user experience in the ever-evolving landscape of social media platforms.

Chapter 5

CONCLUSIONS AND RECOMMENDATIONS

5.1 CONCLUSIONS

Our investigation into the integration of Artificial Intelligence (AI) and blockchain technologies within social media platforms has yielded significant insights. These technologies, both powerful in their own right and, when synergistically combined, offer robust solutions to the pervasive challenges of digital identity authentication and user data security. Below, we encapsulate our primary findings, implications for future research, and the broader impact on digital security and user privacy.

- Identity theft remains a concern within the realm of large-scale social applications, demanding steadfast attention from organizations to uphold user safety and security [5], [28], [29]. Safeguarding against identity theft is paramount, necessitating proactive measures to thwart potential breaches.

- Harnessing the prowess of artificial intelligence (AI), organizations can fortify user security through innovative authentication mechanisms [1]–[3], [30], [31]. These mechanisms, rooted in AI technologies, are instrumental in identifying, preempting, and reclaiming compromised user accounts by scrutinizing anomalous activities. Real-time implementations leverage a spectrum of AI techniques, including facial recognition [32]–[37], speech recognition [38], [39], generative adversarial networks [40], recurrent neural networks [41], AI-hard password authentication [42], and sentiment analysis [43], to swiftly discern potential threats to user identities.

- Blockchain technology emerges as a stalwart solution for validating transactions within a distributed ledger, extending its utility to authentication processes [4], [11], [44]–[50]. Employing blockchain, organizations bolster authentication integrity through techniques such as notarization

[51] and modified authentication protocols [19], [24], [52]–[56]. These protocols encompass innovative approaches like Honeytoken authentication, decentralized dynamic identity authentication, adaptive Multi-Factor authentication (MFA), biometrics, smart contracts, and cross-domain authentication. By integrating these methodologies into real-world scenarios, users can confidently engage with systems, free from the looming threat of identity theft.

- Identity theft is a persistent concern for large-scale social applications, demanding constant vigilance from organizations to ensure user safety. Proactive security measures are vital to thwart potential breaches and uphold user trust.

- Artificial intelligence (AI) empowers organizations to bolster user security through innovative authentication methods. Leveraging AI technologies, these mechanisms swiftly identify and mitigate compromised user accounts by analyzing anomalous activities. Techniques such as facial recognition, speech recognition, and sentiment analysis enable real-time threat detection.

- Blockchain technology's decentralized nature enhances authentication and data integrity. By maintaining a tamper-proof ledger of user activities, blockchain fosters transparency and trust in digital interactions, providing a secure framework for online engagements.

- The integration of AI and blockchain technologies marks the advent of a new era in digital security. This synergistic approach combats fraud and unauthorized access by evolving in response to emerging threats, thereby ensuring the security and trustworthiness of social media platforms.

- Collaborative efforts within the community are crucial for advancing social media security. Sharing knowledge and resources fosters innovation and refines security measures, collectively safeguarding users against evolving digital threats.

5.2 RECOMMENDATIONS

To enhance the security, efficiency, and user experience of social media platforms through the integration of Blockchain and AI technologies, the following detailed recommendations are proposed:

1. **Comprehensive Integration of AI and Blockchain:** Develop and deploy a hybrid model merging AI's real-time authentication with blockchain's decentralized verification. Collaborate with tech providers to ensure seamless integration and address technical hurdles.

2. **Extensive User Education and Engagement Programs:** Launch targeted educational campaigns to educate users on robust authentication practices, AI, and blockchain's role in online security. Utilize interactive guides, tutorials, and gamification to enhance engagement.

3. **Advanced Privacy Protection Mechanisms:** Implement blockchain-based privacy mechanisms like Zero-Knowledge Proof (ZKP) protocols to minimize personal data exposure. Regular audits and updates are crucial for adapting to evolving privacy challenges.

4. **Global Standards and Protocols Development:** Partner with international standards organizations to set global standards for AI and blockchain integration in social media authentication. These standards should cover technical specifications, privacy considerations, and ethical guidelines.

5. **Dedicated Research and Innovation Labs:** Invest in R&D initiatives and innovation labs to prototype new authentication technologies. Foster collaboration among experts in AI, blockchain, cybersecurity, and social media to stay ahead of emerging threats.

5.3 FUTURE OF SOCIAL MEDIA AUTHENTICATION WITH BLOCKCHAIN AND AI

The convergence of Blockchain and AI technologies heralds a new era in social media authentication, characterized by enhanced security, user privacy, and seamless authentication experiences. In the foreseeable future, we anticipate the development of sophisticated AI algorithms capable of learning and adapting to users' unique behavioral patterns, providing continuous, passive authentication. Concurrently, blockchain will solidify its role as a foundational technology for secure, decentralized identity management. This synergy will not only fortify defenses against traditional cyber threats but also pave the way for addressing more sophisticated attacks leveraging AI-generated deepfakes and synthetic identities. As these technologies mature, we expect to see broader adoption across social media platforms, driven by user demand for greater security and privacy and regulatory pressures for improved data protection.

5.4 CHALLENGES IN IMPLEMENTING BLOCKCHAIN AND AI IN A SOCIAL MEDIA ENVIRONMENT

While the integration of Blockchain and AI into social media platforms offers substantial benefits, several significant challenges must be navigated:

1. **Technical and Scalability Challenges:** The inherent complexities of blockchain and AI technologies pose substantial technical challenges, especially in terms of scalability. Ensuring that blockchain networks can handle the vast volumes of transactions generated by millions of users without compromising speed or efficiency is crucial. Similarly, AI models must be capable of processing and analyzing large datasets in real time to provide accurate, continuous authentication.

2. **Integration and Compatibility Issues:** Seamlessly integrating blockchain and AI with existing social media infrastructure requires overcoming compatibility issues. This involves not only technical integration but also ensuring that the user experience

Chapter 6

REFERENCES

[1] E. Holm, “Social networking and identity theft in the digital society,” Mar. 2014.

[2] H. Uygun and R. Gujrati, *Role of artificial intelligence and machine learning in social media*, 2022.

[3] X. Qiu, Z. Du, and X. Sun, “Artificial intelligence-based security authentication: Applications in wireless multimedia networks,” *IEEE Access*, vol. 7, pp. 172 004–172 011, 2019. DOI: 10.1109/ACCESS.2019.2956480.

[4] M. A. Hisseine, D. Chen, and X. Yang, “The application of blockchain in social media: A systematic literature review,” *Applied Sciences*, vol. 12, no. 13, p. 6567, Jun. 2022, ISSN: 2076-3417. DOI: 10.3390/app12136567. [Online]. Available: http://dx.doi.org/10.3390/app12136567.

[5] F. Cremer, B. Sheehan, M. Fortmann, *et al.*, “Cyber risk and cybersecurity: A systematic review of data availability,” *The Geneva Papers on Risk and Insurance - Issues and Practice*, vol. 47, no. 3, pp. 698–736, Feb. 2022, ISSN: 1468-0440. DOI: 10.1057/s41288-022-00266-6. [Online]. Available: http://dx.doi.org/10.1057/s41288-022-00266-6.

[6] M. Shahria, M. nazim uddin, and M. Ahmed, “Social media security: Identity theft prevention,” *International Journal of Innovative Science and Research Technology*, vol. 5, pp. 1656–1662, Sep. 2020. DOI: 10.38124/IJISRT20AUG762.

[7] L. Cheng, F. Liu, and D. D. Yao, “Enterprise data breach: Causes, challenges, prevention, and future directions: Enterprise data breach,” *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 7, e1211, Jun. 2017. DOI: 10.1002/widm.1211.

[8] J. Á. Concepción-Sánchez, J. Molina-Gil, P. Caballero-Gil, and I. Santos-González, "Fuzzy logic system for identity theft detection in social networks," in *2018 4th International Conference on Big Data Innovations and Applications (Innovate-Data)*, 2018, pp. 65–70. DOI: 10.1109/Innovate-Data.2018.00017.

[9] M. Gomez-Barrero, C. Rathgeb, G. Li, R. Ramachandra, J. Galbally, and C. Busch, "Multi-biometric template protection based on bloom filters," *Information Fusion*, vol. 42, pp. 37–50, 2018, ISSN: 1566-2535. DOI: https://doi.org/10.1016/j.inffus.2017.10.003. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1566253516301233.

[10] C. Wang, B. Yang, and J. Luo, "Identity theft detection in mobile social networks using behavioral semantics," in *2017 IEEE International Conference on Smart Computing (SMARTCOMP)*, 2017, pp. 1–3. DOI: 10.1109/SMARTCOMP.2017.7947016.

[11] Amitkumar, M. I. Sanni, and D. Apriliasari, "Blockchain technology application: Authentication system in digital education," *Aptisi Transactions On Technopreneurship (ATT)*, vol. 3, no. 2, pp. 37–48, Sep. 2021, ISSN: 2655-8807. DOI: 10.34306/att.v3i2.209. [Online]. Available: http://dx.doi.org/10.34306/att.v3i2.209.

[12] S. S. Zhumazhanova and I. D. Tatarinov, "User authentication by face thermograms based on hybrid neural networks," in *2021 Dynamics of Systems, Mechanisms and Machines (Dynamics)*, 2021, pp. 1–3. DOI: 10.1109/Dynamics52735.2021.9653694.

[13] S. Pappu, D. Kangane, V. Shah, and J. Mandwiwala, "Ai-assisted risk based two factor authentication method (aia-rb-2fa)," in *2021 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES)*, 2021, pp. 1–5. DOI: 10.1109/ICSES52305.2021.9633937.

[14] M. K. A. Chy, S. A. Ahmed, A. H. Doha, A. K. M. Masum, and S. I. Khan, "Social media user's safety level detection through classification via clustering approach," in *2019 International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2)*, 2019, pp. 1–4. DOI: 10.1109/IC4ME247184.2019.9036489.

[15] P. Anufriiev, Y. Bashkov, and D. Khoma, "Experimental face recognition system based on improved artificial intelligence model," in *2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT)*, 2022, pp. 181–186. DOI: 10.1109/ATIT58178.2022.10024248.

[16] K. Veena and K. Meena, "Determination of performance to verify the synthetic identity theft by training the neural networks," in *2017 IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)*, 2017, pp. 246–250. DOI: 10.1109/ICSTM.2017.8089161.

[17] M. Zulfiqar, F. Syed, M. J. Khan, and K. Khurshid, "Deep face recognition for biometric authentication," in *2019 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*, 2019, pp. 1–6. DOI: 10.1109/ICECCE47252.2019.8940725.

[18] Z. Sitová, J. Šeděnka, Q. Yang, *et al.*, "Hmog: New behavioral biometric features for continuous authentication of smartphone users," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 877–892, 2016. DOI: 10.1109/TIFS.2015.2506542.

[19] J. Zhu, Y. Wei, and X. Shang, "Decentralized dynamic identity authentication system based on blockchain," in *2021 International Conference on Networking Systems of AI (INSAI)*, 2021, pp. 1–4. DOI: 10.1109/INSAI54028.2021.00012.

[20] F. Toutara and G. Spathoulas, "A distributed biometric authentication scheme based on blockchain," in *2020 IEEE International Conference on Blockchain (Blockchain)*, 2020, pp. 470–475. DOI: 10.1109/Blockchain50366.2020.00068.

[21] Z. Yang, H. Ma, M. Ai, M. Zhan, G. Wu, and Y. Zhang, "A minimal disclosure signature authentication scheme based on consortium blockchain," in *2022 IEEE International Conference on Blockchain (Blockchain)*, 2022, pp. 516–521. DOI: 10.1109/Blockchain55522.2022.00079.

[22] R. Bhan, R. Pamula, P. Faruki, and J. Gajrani, "Blockchain-enabled secure and efficient data sharing scheme for trust management in healthcare smartphone network," *The Journal of Supercom-*

puting, vol. 79, no. 14, pp. 16 233–16 274, Apr. 2023, ISSN: 1573-0484. DOI: 10.1007/s11227-023-05272-6. [Online]. Available: http://dx.doi.org/10.1007/s11227-023-05272-6.

[23] Z. Althero, J. Syahreza, and A. Ortiz, *Blockchain technology for authentication and validation social network accounts*, 2023. DOI: 10.34306/bfront.v3i1.358.

[24] S. H. G. Salem, A. Y. Hassan, M. S. Moustafa, and M. N. Hassan, "Blockchain-based biometric identity management," *Cluster Computing*, Nov. 2023, ISSN: 1573-7543. DOI: 10.1007/s10586-023-04180-x. [Online]. Available: http://dx.doi.org/10.1007/s10586-023-04180-x.

[25] E. Alharbi and D. Alghazzawi, "Two factor authentication framework using otp-sms based on blockchain," *Transactions on Engineering and Computing Sciences*, vol. 7, Jun. 2019. DOI: 10.14738/tmlai.73.6524.

[26] G. Deep, R. Mohana, A. Nayyar, P. Sanjeevikumar, and E. Hossain, "Authentication protocol for cloud databases using blockchain mechanism," *Sensors*, vol. 19, no. 20, p. 4444, Oct. 2019, ISSN: 1424-8220. DOI: 10.3390/s19204444. [Online]. Available: http://dx.doi.org/10.3390/s19204444.

[27] S. Baskar, K. Ramar, and H. Shanmugasundaram, "Data security in healthcare using blockchain technology," in *2021 International Conference on Decision Aid Sciences and Application (DASA)*, 2021, pp. 354–359. DOI: 10.1109/DASA53625.2021.9682300.

[28] S. Irshad and T. Soomro, "Identity theft and social media," vol. 18, Feb. 2018.

[29] A. Mohammed, S. Kumar, H. G. Mu'Azu, *et al.*, "Data security and protection: A mechanism for managing data theft and cybercrime in online platforms of educational institutions," in *2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON)*, vol. 1, 2022, pp. 758–761. DOI: 10.1109/COM-IT-CON54601.2022.9850702.

[30] N. Aljohani, J. Shelton, and K. Roy, "Authentication based on touch patterns using an artificial immune system," in *2021 IEEE Symposium Series on Computational Intelligence (SSCI)*, 2021, pp. 1–8. DOI: 10.1109/SSCI50451.2021.9660096.

[31] A. Lo, *Towards Privacy-Preserving Social Media Networks: Protecting the Facial Privacy of Images Uploaded On Social Media — repository.fit.edu*, https://repository.fit.edu/etd/1266/, [Accessed 19-03-2024].

[32] U. Ahmad, A. Baqir, F. u. Mustafa, S. Malik, S. A. Sani, and S. Z. H. Shah, "Enhancing the authentication mechanism of social media websites using face detection," in *2019 4th International Conference on Emerging Trends in Engineering, Sciences and Technology (ICEEST)*, 2019, pp. 1–5. DOI: 10.1109/ICEEST48626.2019.8981692.

[33] S. Girmay, F. Samsom, and A. M. Khattak, "Ai based login system using facial recognition," in *2021 5th Cyber Security in Networking Conference (CSNet)*, 2021, pp. 107–109. DOI: 10.1109/CSNet52717.2021.9614281.

[34] T. Pinthong, W. Yimyam, N. Chumuang, and M. Ketcham, "Face recognition system for financial identity theft protection," in *2020 15th International Joint Symposium on Artificial Intelligence and Natural Language Processing (iSAI-NLP)*, 2020, pp. 1–6. DOI: 10.1109/iSAI-NLP51646.2020.9376826.

[35] Y. Mohialden, N. Mahmood Hussien, and D. Muhsin, "Enhancing user authentication with facial recognition and feature-based credentials," vol. 4, p. 2023, Dec. 2023. DOI: 10.37899/journallamultiapp.v4i6.903.

[36] M. G. Sonkusare, H. A. Meshram, A. Sah, and S. Prakash, "Detection and verification for deepfake bypassed facial feature authentication," in *2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, 2022, pp. 646–649. DOI: 10.1109/ICAIS53314.2022.9742980.

[37] S. Mohan and N. Z. Harun, "Jeev time: Secure authentication using integrated face recognition in social media applications," *Journal of Soft Computing and Data Mining*, vol. 3, no. 2, Aug. 2022, ISSN: 2716-621X. DOI: 10.30880/jscdm.2022.03.02.003. [Online]. Available: http://dx.doi.org/10.30880/jscdm.2022.03.02.003.

[38] C. Sanderson, S. Bengio, H. Bourlard, *et al.*, “Speech and face-based biometric authentication at idiap,” in *2003 International Conference on Multimedia and Expo. ICME ’03. Proceedings (Cat. No.03TH8698)*, vol. 3, 2003, pp. III–1. DOI: 10.1109/ICME.2003.1221233.

[39] D. R. Chandran, “Use of ai voice authentication technology instead of traditional keypads in security devices,” *Journal of Computer and Communications*, vol. 10, no. 06, pp. 11–21, 2022, ISSN: 2327-5227. DOI: 10.4236/jcc.2022.106002. [Online]. Available: http://dx.doi.org/10.4236/jcc.2022.106002.

[40] C. S. Vorugunti, P. Mukherjee, and V. Pulabaigari, “Online signature profiling using generative adversarial networks,” in *2020 International Conference on COMmunication Systems and NETworkS (COMSNETS)*, 2020, pp. 894–896. DOI: 10.1109/COMSNETS48256.2020.9027369.

[41] J. Ackerson, R. Dave, and N. Seliya, “Applications of recurrent neural network for biometric authentication &amp; anomaly detection,” *Information*, vol. 12, no. 7, p. 272, Jul. 2021, ISSN: 2078-2489. DOI: 10.3390/info12070272. [Online]. Available: http://dx.doi.org/10.3390/info12070272.

[42] T. V. Raghavasimhan, S. Manoj, J. D. Sweetlin, and S. Rakshit, “Preventing cryptographic attacks using ai-hard password authentication,” in *2023 International Conference on Networking and Communications (ICNWC)*, 2023, pp. 1–6. DOI: 10.1109/ICNWC57852.2023.10127557.

[43] “Ai-powered text analysis tool for sentiment analysis,” Ph.D. dissertation, 2023. [Online]. Available: https://urn.kb.se/resolve?urn=urn:nbn:se:mdh:diva-63059.

[44] S. Choudhari, S. K. Das, and S. Parasher, “Interoperable blockchain solution for digital identity management,” in *2021 6th International Conference for Convergence in Technology (I2CT)*, 2021, pp. 1–6. DOI: 10.1109/I2CT51068.2021.9418220.

[45] W. L. Sim, H. N. Chua, and M. Tahir, “Blockchain for identity management: The implications to personal data protection,” in *2019 IEEE Conference on Application, Information and Network Security (AINS)*, 2019, pp. 30–35. DOI: 10.1109/AINS47559.2019.8968708.

[46] X. LI, “A blockchain-based verifiable user data access control policy for secured cloud data storage,” *Computational Intelligence and Neuroscience*, vol. 2022, K. Demertzis, Ed., pp. 1–12, Apr. 2022, ISSN: 1687-5265. DOI: 10.1155/2022/2254411. [Online]. Available: http://dx.doi.org/10.1155/2022/2254411.

[47] S. Shorman and M. Allaymoun, “Authentication and verification of social networking accounts using blockchain technology,” *International Journal of Computer Science and Information Technology*, vol. 11, pp. 01–13, Dec. 2019. DOI: 10.5121/ijcsit.2019.11601.

[48] S. Patwe and S. Mane, “Blockchain enabled architecture for secure authentication in the metaverse environment,” in *2023 IEEE 8th International Conference for Convergence in Technology (I2CT)*, 2023, pp. 1–8. DOI: 10.1109/I2CT57861.2023.10126452.

[49] Z. Gao, L. Xu, G. Turner, *et al.*, “Blockchain-based identity management with mobile device,” Jun. 2018, pp. 66–70. DOI: 10.1145/3211933.3211945.

[50] H. Nusantoro, R. Supriati, N. Azizah, N. P. Lestari Santoso, and S. Maulana, “Blockchain based authentication for identity management,” in *2021 9th International Conference on Cyber and IT Service Management (CITSM)*, 2021, pp. 1–8. DOI: 10.1109/CITSM52892.2021.9589001.

[51] G. Song, S. Kim, H. Hwang, and K. Lee, “Blockchain-based notarization for social media,” in *2019 IEEE International Conference on Consumer Electronics (ICCE)*, 2019, pp. 1–2. DOI: 10.1109/ICCE.2019.8661978.

[52] V. Papaspirou, L. Maglaras, I. Kantzavelou, N. Moradpoor, and S. Katsikas, *A blockchain-based two factor honeytoken authentication system*, 2023. arXiv: 2307.05047 [cs.CR].

[53] Y. Xu, X. Jian, T. Li, S. Zou, and B. Li, “Blockchain-based authentication scheme with an adaptive multi-factor authentication strategy,” *Mobile Information Systems*, vol. 2023, P. Zhang, Ed., pp. 1–13, Nov. 2023, ISSN: 1574-017X. DOI: 10.1155/2023/4764135. [Online]. Available: http://dx.doi.org/10.1155/2023/4764135.

[54] P. Kamboj, S. Khare, and S. Pal, “User authentication using blockchain based smart contract in role-based access control,” *Peer-to-Peer Networking and Applications*, vol. 14, Sep. 2021. DOI: 10.1007/s12083-021-01150-1.

[55] L. Chen, W. Wu, G. Kou, and L. Zhang, “Blockchain-based supervised anonymous cross-domain authentication scheme,” in *2021 7th International Conference on Computer and Communications (ICCC)*, 2021, pp. 1565–1569. DOI: 10.1109/ICCC54389.2021.9674287.

[56] Y. E. Oktian, S.-G. Lee, and H.-J. Lee, “Twochain: Leveraging blockchain and smart contract for two factor authentication,” in *2020 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, 2020, pp. 187–191. DOI: 10.1109/ISRITI51436.2020.9315514.