A REPORT

ON

FAKE SOCIAL MEDIA PROFILE DETECTION AND REPORTING

Submitted by,

M. Ravi Shankar Prasad	**20211CBC0019**
CH. Naga Pavan	**20211CBC0060**
P. Akshay Kumar	**20211CBC0034**
S. Nagesh	**20211CBC0017**

Under the guidance of,

Ms. ARSHIYA LUBNA

in partial fulfillment for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

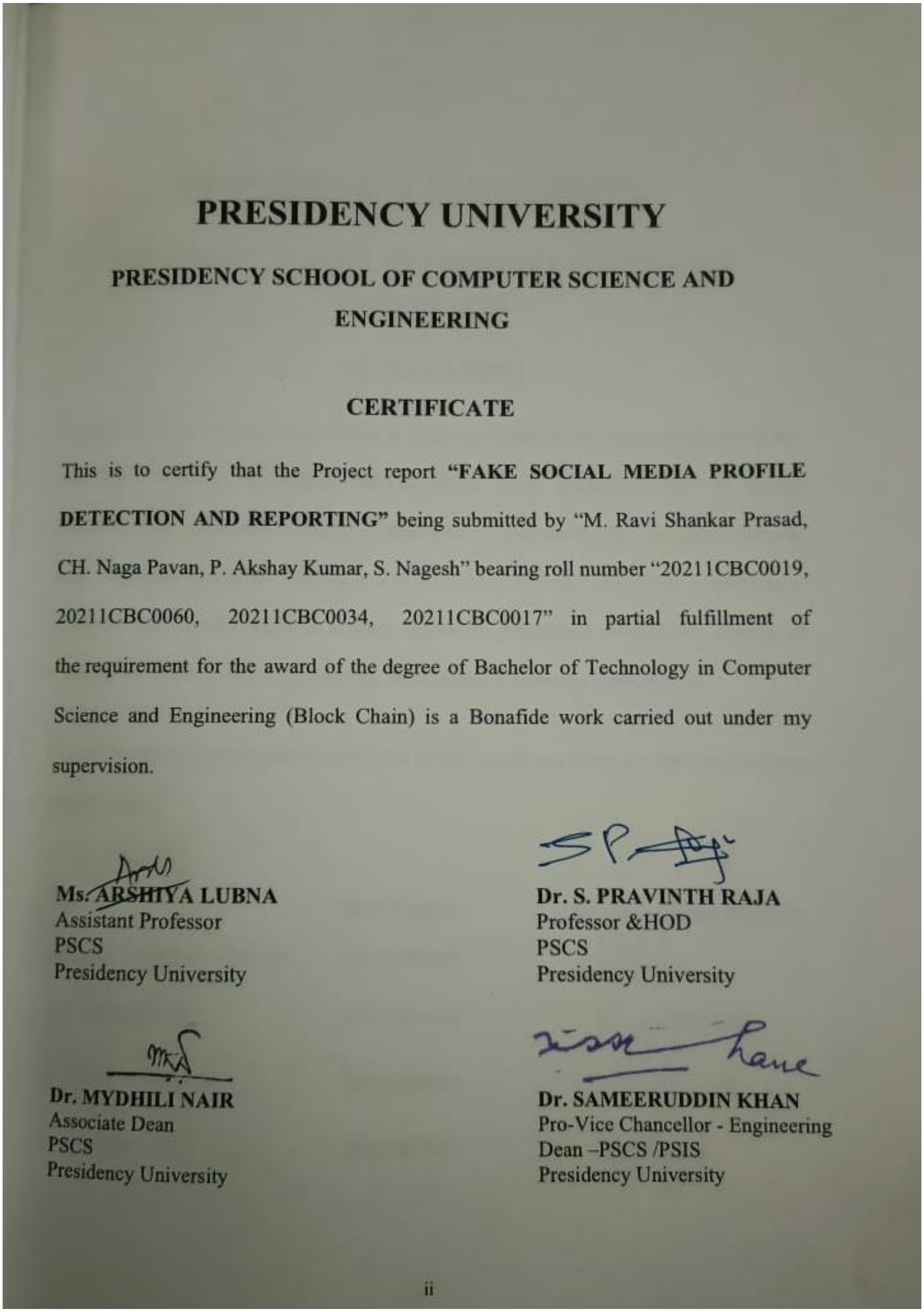
COMPUTER SCIENCE AND ENGINEERING
(BLOCK CHAIN)
At

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

PRESIDENCY UNIVERSITY

BENGALURU

MAY 2025



PRESIDENCY UNIVERSITY

PRESIDENCY SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

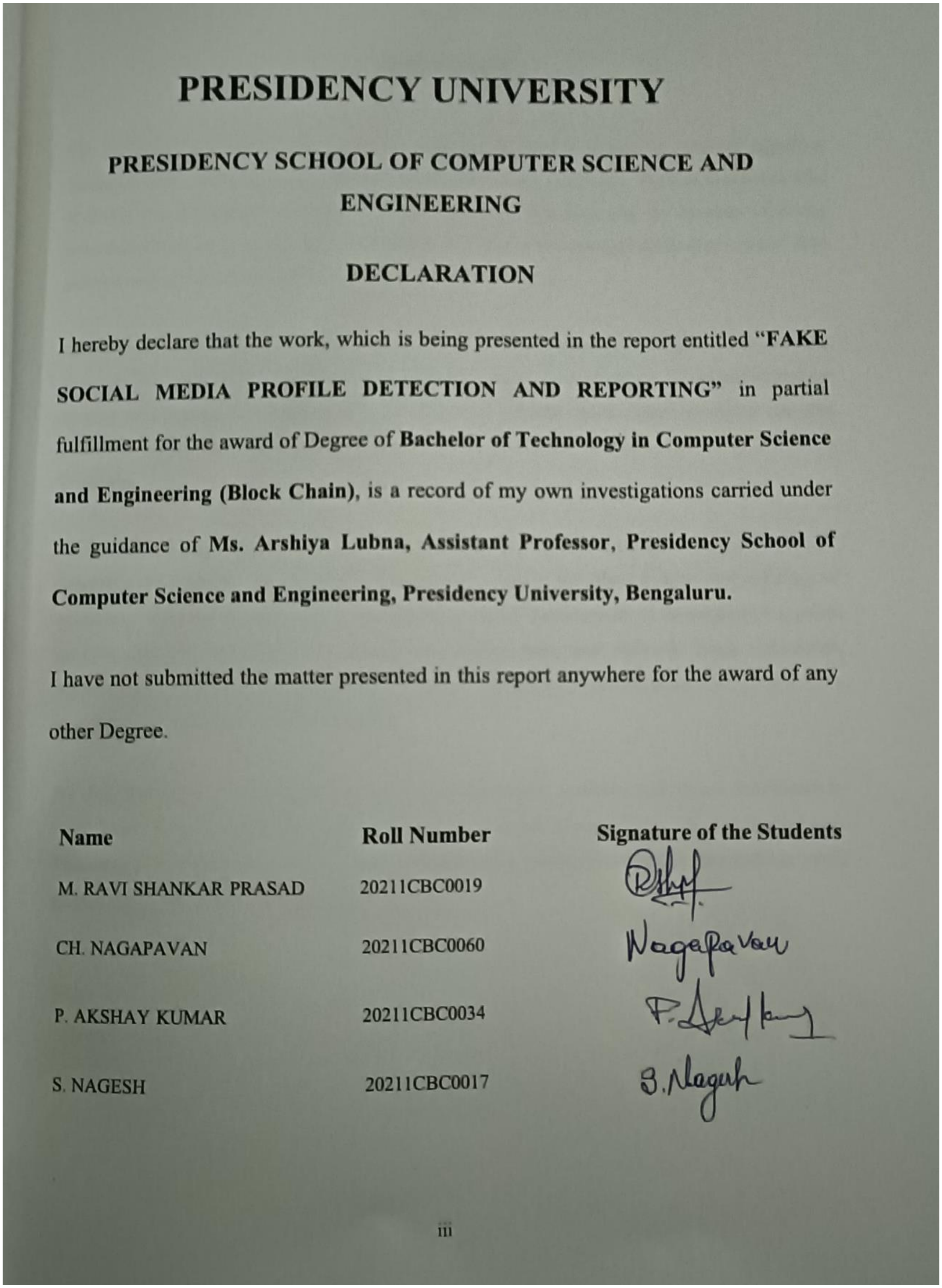
This is to certify that the Project report **"FAKE SOCIAL MEDIA PROFILE DETECTION AND REPORTING"** being submitted by "M. Ravi Shankar Prasad, CH. Naga Pavan, P. Akshay Kumar, S. Nagesh" bearing roll number "20211CBC0019, 20211CBC0060, 20211CBC0034, 20211CBC0017" in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology in Computer Science and Engineering (Block Chain) is a Bonafide work carried out under my supervision.

Ms. ARSHIYA LUBNA
Assistant Professor
PSCS
Presidency University

Dr. S. PRAVINTH RAJA
Professor &HOD
PSCS
Presidency University

Dr. MYDHILI NAIR
Associate Dean
PSCS
Presidency University

Dr. SAMEERUDDIN KHAN
Pro-Vice Chancellor - Engineering
Dean –PSCS /PSIS
Presidency University



PRESIDENCY UNIVERSITY

PRESIDENCY SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

DECLARATION

I hereby declare that the work, which is being presented in the report entitled "**FAKE SOCIAL MEDIA PROFILE DETECTION AND REPORTING**" in partial fulfillment for the award of Degree of **Bachelor of Technology in Computer Science and Engineering (Block Chain)**, is a record of my own investigations carried under the guidance of **Ms. Arshiya Lubna, Assistant Professor**, **Presidency School of Computer Science and Engineering, Presidency University, Bengaluru.**

I have not submitted the matter presented in this report anywhere for the award of any other Degree.

Name	Roll Number	Signature of the Students
M. RAVI SHANKAR PRASAD	20211CBC0019	
CH. NAGAPAVAN	20211CBC0060	Nagapavan
P. AKSHAY KUMAR	20211CBC0034	P. Akshay kumar
S. NAGESH	20211CBC0017	S.Nagesh

ABSTRACT

The proliferation of fake social media accounts has resulted in increasing concerns regarding misinformation, financial scams, identity theft, and privacy violations. The bad actors use fake accounts for propaganda, phishing, and cyberbullying, thus requiring the creation of strong detection and reporting techniques. This paper discusses a two-pronged method to counter fake profiles through Blockchain and Cybersecurity methodologies.

Blockchain technology guarantees data integrity and openness through an immutable, decentralized record of verified identities. It prevents duplicity of identities, increases the process of user verification, and decreases the likelihood of identity fraud. Smart contracts can also automate the authentication process, guaranteeing that only verified users have access to platforms.

At the same time, Cybersecurity methods like anomaly detection using AI based behavioral detection, IP logging, and biometric authentication aid in the identification and marking of suspicious behavior. AI algorithms can identify patterns characteristic of bot-related or spoofed profiles through analyzing user interaction, posting rate, and network usage. Moreover, cryptographic security controls can protect sensitive information while making it possible to have anonymous yet verifiable digital identities.

By combining these technologies, we offer a decentralized, scalable, and secure framework to boost trust, deter social media manipulation, and reinforce accountability on digital platforms. This method has the potential to greatly enhance the reliability of online interactions while maintaining user privacy and security.

ACKNOWLEDGEMENT

First of all, we indebted to the **GOD ALMIGHTY** for giving me an opportunity to excel in our efforts to complete this project on time.

We express our sincere thanks to our respected dean **Dr. Md. Sameeruddin Khan**, Pro-VC - Engineering and Dean, Presidency School of Computer Science and Engineering & Presidency School of Information Science, Presidency University for getting us permission to undergo the project.

We express our heartfelt gratitude to our beloved Associate Dean **Dr. Mydhili Nair,** Presidency School of Computer Science and Engineering, Presidency University, and "**Dr. S. Pravinthraja**", Head of the Department, Presidency School of Computer Science and Engineering, Presidency University, for rendering timely help in completing this project successfully.

We are greatly indebted to our guide **Ms. Arshiya Lubna, Assistant Professor** and Reviewer **Dr. M Swapna, Associate Professor**, Presidency School of Computer Science and Engineering, Presidency University for her inspirational guidance, and valuable suggestions and for providing us a chance to express our technical capabilities in every respect for the completion of the project work.

We would like to convey our gratitude and heartfelt thanks to the CSE7301 University Project Coordinators **Mr. Md Ziaur Rahman and Dr. Sampath A K,** department Project Coordinator "**Ms. Suma NG**" and Git hub coordinator **Mr. Muthuraj.**

We thank our family and friends for the strong support and inspiration they have provided us in bringing out this project.

M. Ravi Shankar Prasad
CH. Naga Pavan
P. Akshay Kumar
S. Nagesh

TABBLE OF CONTENTS

LIST OF FIGURES

Chapter 1

INTRODUCTION

The spread of fabricated social media accounts is a dangerous threat to cyber communities as they undermine confidence and enable such vices as propaganda campaigns, theft of identities, and intimidation. Identification and flagging these spurious accounts will need an amalgamation of various strengths including that of blockchain, cybersecurity best practices, and NLP with more than one language.

Methods in the conventional means of identification use centralized processes which are subject to tampering and are nontransparent. Blockchain, being decentralized and unchangeable, provides a secure platform for storing and authenticating user information, improving the integrity of profile details. With a permissioned blockchain, under which verified actors validate users, a trusted and auditable history of profile creation and updates can be created. This can form a basis for identifying inconsistencies and anomalies that suggest spurious accounts.

Cybersecurity is essential in protecting the blockchain infrastructure and having efficient detection algorithms. Methods such as anomaly detection, behavioral analysis, and network security protocols can be used to detect suspicious behavior and patterns related to false profiles. For example, the examination of login patterns, IP addresses, and device data can uncover inconsistencies that indicate automated or fraudulent activity. In addition, best practices in cybersecurity are required to safeguard the system against cyberattacks that may breach the integrity of the detection process.

Support for NLP across languages is imperative for profiling content such as usernames, bios, and posts for detecting linguistic patterns of bot or fake accounts. Most fake profiles contain repetitive or meaningless text, written by automated means or bots. Cross-lingual NLP facilitates the identification of such patterns in various languages

improving accuracy and coverage for detecting fraudulent profiles. Techniques like sentiment analysis, topic modeling, and language identification can be utilized to assess the validity of profile content.

In addition to that, the reporting process can be streamlined and made transparent by utilizing blockchain. The users can report suspected bogus profiles, and reports are logged on the blockchain. This has a trail behind it in terms of an auditable record of the reports, thereby no alteration of reports possible and accountability is guaranteed. Status of reported profiles can also be tracked using blockchain, providing insight into the probe to the users.

In essence, the synergistic combination of blockchain, cybersecurity, and multilingual NLP is a single solution for detecting and reporting fake social media profiles. Blockchain verifies data integrity and transparency, cybersecurity secures the system and implements detection algorithms, and multilingual NLP analyzes profile content for linguistic discrepancies. This single strategy improves the efficiency and accuracy of detecting fake profiles, ensuring a safer and more genuine online

Chapter 2

LITERATURE SURVEY

2.1 Impersonation Social Media Accounts: Overview Impersonation social media accounts are online personas created by false or total misrepresentation. The accounts are likely of various types, such as pretending to be from actual people, hijacked or borrowed identities, or as pretending to be automated entities working to react to content. Although some false accounts will be somewhat harmless—for example, serving as the anonymity or as employed satirically— most exist in malicious forms with serious consequences.

The Use of Fake Social Media Accounts to Steal Identities One of the most disconcerting aspects of fake social media accounts is their application to steal identities. The hackers can open profiles of imitative individuals using other people's personal details, photographs, and other personal information hijacked by the hackers. These fake accounts may be used to cheat friends, family, and even banks, resulting in economic fraud and psychological distress to the victims. Most often, the fake profiles are created through web scraping publicly accessible information from legitimate users' accounts and use this data to create realistic impersonations. In extreme cases, identity thieves use impersonation profiles to obtain loans, credit cards, or other financial products in someone else's name. This not only damages the victim's financial reputation but also causes long-term legal and administrative issues when trying to recover their identity. Even certain cybercriminals use such fake accounts for blackmail by impersonating someone they know and gaining their trust before exploiting them [1]

2.1.1 Online Fraud and Fake Activities

A grave concern is also the use of fake accounts in internet fraud and cybercrime. Scammers set up fake accounts to trick victims into releasing personal information, remitting funds, or engaging in fraudulent transactions. Some of the most common cons facilitated through fake accounts include investment scams, romance scams, and phishing. Scammers build the illusion of credibility with their targets and deceive them into taking steps that result in significant monetary scams are particularly common, where scammers create fake profiles on dating sites and social media to initiate relationships with unsuspecting victims [2]

Once they have gained the victim's trust, they will then go on to create fictitious dire financial circumstances—such as medical expenses or flight fees—to ask for money from their victims Phishing scams also use fake profiles to send out phishing links, attempting to get passwords, credit card or other confidential information.

2.1.2 The Misinformation and Political Manipulation Spread

Disinformation and propaganda are also disseminated widely using artificial social media accounts. These accounts can be used to propagate false information, influence public opinion, or frame political discourse. Occasionally organized networks of artificial accounts, or bot farms, are used to publish significant information, creating artificial engagement and making disinformation credible. This has far-reaching implications, particularly in areas such as elections, public health, and social movements.

Imitation social media accounts can be used at critical political events, for example, at election times to disseminate false information and influence voters' decisions. Such actions are employed by some governments and parties to twist the perception of the masses through subsidizing biased information or silencing opposing voices. The same occurs in the medical sector where disinformation campaigns are used in attempts to spread false news regarding vaccines, disease, and drugs, instilling distrust in medical institutions [3]

2.1.3 **Cyberbullying and Online Harassment**

Cyberbullying and cyber harassment are some of the dangers that accompany fake social media profiles. The use of anonymity makes it easy for aggressive users to engage in offensive behavior without necessarily being penalized. Impersonation can be used to disseminate hate messages, threaten, or libel an individual. The use of multiple accounts with ease facilitates harassers' continuation of behavior even when the original accounts get blocked or reported In other cases, cyberbullies create fake profiles to impersonate the victims, posting irrelevant or inappropriate content or disseminating false rumors in trying to smear their reputations.

It is even more so for teenagers and young adults, who are mostly liable to be online bashed. Victims of cyberbullying are left with deep psychological effects like depression, anxiety, and even suicidal tendencies [4]

2.1.4 Economic and Corporate Implications: The presence of fake social media profiles extends beyond personal harm—it also has business and economic implications. Most businesses rely on social media for advertising, customer engagement, and brand reputation. Fake accounts can be used, however, to manipulate online reviews, spread false complaints, or artificially inflate or deflate brands. For example, competitors may utilize pseudo-accounts to leave negative reviews on a company's social media site

Conversely, certain businesses utilize pseudo-profiles to participate in Implications positive remarks, misleading consumers into believing that their products or services are superior to what they are Influencer marketing is another area that is impacted by fake followers.

While some social media influencers build their credentials on follower engagements, others are as far- reaching as purchasing fabricated followers to make themselves appear popular when they are not. These malicious activities cheat brands into sponsoring influencers with manufactured engagement rates, and this amounts to wasted advertising money and vain campaigns [5]

2.1.5 How Social Media Sites Fight Imposter Profiles

The presence of false profiles undermines internet trust, and it is difficult to determine whether internet relationships and information are real. Social networks have enacted several measures to prevent this issue, such as requiring evidence of identity, employing artificial intelligence to detect potential scams, and enabling users to report imposter accounts. However, despite these precautions, the presence of spurious profiles is still a significant issue due to the dynamic nature of fraudulent practices used by malicious users.

Against the surge of scam accounts, sites use machine learning-based algorithms to identify suspicious activities, such as bulk-following, spamming comments, or abusive messaging.

Some social networking sites have also launched verification badges for authenticating high-profile users. Governments and regulators are even demanding stricter regulations to force social networking sites to be responsible for blocking the growth and spread of fake profiles.

Social Media Cybersecurity: The social media platform, although enabling record-breaking connectivity, is fertile ground for the wrong. The volume of data, the anonymity afforded by online identities, and the rapid dissemination of data create a recipe for disaster in cyber-attacks. A robust cybersecurity framework is not just the requirement of the moment but an absolute imperative

Encryption:
The Pillar of Data Confidentiality:
Encryption is the basis of protection of sensitive information exchanged on social media websites. It transforms readable data into unreadable form, accessible only by decryption key. This is essential for the security of End-to-end encryption, where data is encrypted at the sending device and decrypted only at the receiving end, provides the assurance that even the platform itself cannot get access to the information. The use of powerful encryption algorithms such as AES-256 is critical to counter rising advanced attacks. Encryption must also be applied across all features of the platform, including direct messaging, file sharing, and even profile information [6]

2.1.6 Multi-Factor Authentication (MFA): Protecting User Accounts

Passwords alone are not enough to safeguard user accounts. MFA adds an extra layer of security by requiring users to provide multiple forms of verification, such as a code on their phone, a fingerprint scan, or a security key. This greatly reduces the risk of unauthorized access even when a password is compromised. MFA must be mandated or strongly recommended for all users, particularly those handling sensitive information or dealing with large groups. Websites must also offer many MFA options to accommodate different user preferences and technical proficiency.

2.1.7 AI-Driven Monitoring: Real-Time Detection and Prevention of Threats

Cybersecurity play a critical role in detecting and preventing cyber threats in real time. AI systems can search vast quantities of data in real time to detect anomalies, suspicious behavior patterns, and potential security breaches. For example, AI can identify fake profiles by analyzing their pattern of establishment, activity rates, and network connections. It can also determine phishing attacks by analyzing the content and links shared on the site. Secondly, AI can spot and remove dangerous content, like hate speech and disinformation, which has severe real-world consequences. AI-based monitoring works due to the ongoing training and adjustment of algorithms to stay abreast of evolving dangers.

2.1.8 User Education: Empowering Users to Defend Themselves

While technology solutions are important, user awareness is also necessary. Users should be aware of the dangers posed by social media and learn to protect themselves This includes making users aware of User Education.

Educating Users to Protect Themselves of the risks that social media presents and learn how to safeguard themselves. This involves informing users about privacy settings, identifying phishing scams, not oversharing personal details.

knowing how their data can be used or abused, and having good password practices. Regular training, awareness campaigns, and interactive simulations can enable users to be the first line of defense in protecting their digital footprint place but distributed across a network of machines. This distribution fundamentally changes the security profile. Centralized systems have one point of failure that can jeopardize the entire system. If a hacker breaks into the central server, they can view or alter all of the data.

- Phishing attacks: How to identify and avoid phishing messages and emails aimed at stealing personal information.
- Fake profiles: How to recognize and report fake profiles with malicious intentions.
- Data protection: How to customize privacy settings and manage what they share on the internet.
- Password security: Creating strong, new passwords and using password managers.
- Safe browsing practices: Avoiding shady links and sites.
- Understanding the risks of sharing personal details: Knowing what one shares publicly. Platforms need to provide short and easily accessible content, i.e., tutorials, guides, and FAQs, to assist users in understanding and adopting the se would be traceable instantly. Such immutability is also vital to maintain practices. Periodic awareness drives and information about fresh threats must be there too.

2.1.9 The Evolving Threat Landscape and Continuous Improvement

The online threat landscape is ever-evolving, with new threats emerging on a daily basis. Social networking websites must have an active security posture, with a keen eye out for emerging vulnerabilities and shifting their defenses accordingly.

This could include:

Regular security audits and penetration testing.

Staying abreast of the latest security best practices and technology.

Collaboration with cybersecurity experts and researchers.

Maintaining an effective incident response plan, on stand-by to activate in the event of a security incident.

Having bug bounty programs in place, to incentivize security researchers to identify and report bugs.

2.1.10 Blockchain Technology in Security:

Blockchain technology is a paradigm shift in our thinking about security, especially within the all-too-often insecure environment of social media. Let us deconstruct how its fundamental characteristics make the internet ecosystem more secure.

Decentralization: Distributing Trust and Eliminating Single Points of Failure Essentially, blockchain is a decentralized ledger. That means that data is not held in one, centralized With a blockchain, though, its distributed nature makes it very difficult to change the data. To alter information, an attacker would need to break into more than half of nodes in the network simultaneously, which is not computationally possible in a large, well-maintained blockchain.

2.1.11 Tamper-Proof Data: Preventing Data Tainting and Modification

Blockchain's cryptographic design ensures it is not possible to alter or delete data that has already been placed on the ledger. Every block of data is linked to the prior block with a cryptographic hash, creating an unbreakable chain of blocks. If a person would attempt to modify a block, its hash would be altered, and the hashes of all subsequent blocks would also be altered, thereby tampering the integrity of data, such as user identities and history of transactions, which are needed for security.

Identity Verification: Establishing Trustworthy Digital Identities

Identity verification is arguably the most viable application of blockchain in social media security. Traditional methods of identity authentication are prone to centralized parties that can be easily hacked and data stolen.

Blockchain-based identity authentication offers a secure and privacy-respecting solution.

Digital identities are established and kept on the blockchain, which are thereafter authenticity-checked by a group of trusted parties.

The user holds control of his information and offers selective disclosure, safeguarding himself from identity theft and fraud.

For example, a user can be authenticated once by an authority, and then use the authenticate access different social media platforms without necessarily providing their information to each platform individually.

2.1.12 Transparent Transaction Tracking:

Enhancing Accountability and Auditability Blockchain provides an unambiguous and verifiable record of all transactions. This transparency is utilized for tracking the flow of information and identifying any suspicious activity, such as the spread of false information or the creation of fraudulent accounts. For example, if a person feels that a user is spreading fake news, his action on the blockchain can be traced to identify the source of the information and to what extent it was spread. This transparency also raises accountability, because it becomes easier to hold the organizations and parties responsible for what they do. Smart Contracts: Executing Rules and Automating Security.

Smart contracts are self-executing contracts where terms of agreement between buyer and seller are embedded in code lines. They 1 can execute a range of security operations, such as:

1.Automated account verification: Smart contracts can be used to automatically verify user identities and prevent the creation of fake accounts.

2.Automated content moderation: Smart contracts can be used to automatically identify and delete malicious content, such as hate speech and disinformation.[9]

Chapter 3

RESEARCH GAPS OF EXISTING METHODS

3.1 Insecure Identity Confirmation Processes

Most existing social networks possess insecure or superficial identity confirmation processes, which depend on either email or phone number-based identification. These processes are insecure in nature and easily circumvented through:

Disposable email

services Virtual

phone numbers Synthetic or stolen identities Spam bots generating fake IDs

This loophole establishes an environment through which impersonation profiles can be created and supported at scale often undetected until damage already has been caused—be that through disinformation, financial trickery, or social engineering. From a security perspective this lack of strong verification compromises the trust model of the platform. It exposes users to phishing, scams, and data breaches. Cybercrime uses these weak verification points to infiltrate networks, manipulate social narratives, or collect user information.

From a blockchain point of view, the imbalance is that decentralized identity (DID) platforms are lacking. Blockchain provides the potential for giving tamper-evident, verifiable digital identity yet these forms of systems are not yet well-established among mainstream social media sites. Without blockchain-based identities or verifiable credentials, there is no immutable record which can confirm that a user is genuine.

Ideally, integrating blockchain into cybersecurity protocols can potentially enhance identity authentication.

For instance:

The users can hold self-sovereign identities, which are validated through a blockchain ledger. Cryptography can sign and authenticate between networks identity traits.

Platforms can employ multi-factor identity verification, smart contract facility, and trustless systems.

Despite the promises, most currently available systems are not based on such advanced strategies leaving significant room for research with secure, verifiable, and privacy-preserving user authentication.

3.1.1 Ineffective Detection of Behavioral Patterns

Existing techniques for identifying spurious social media profiles tend to depend mostly on static attributes like profile images, username structures, and numbers of friends.

Although these methods are poor since they cannot explain dynamic and behavioral signals, which are more indicative of spam accounts, they are ineffective.

Theoretically, observing users' behavior over time within a network is a form of behavioral analysis. The main elements are:

Activity Timing: Real users will typically have natural behavior patterns—wake-day logins, typical but varied post activity, and gaps in activity. Bots tend to run in spurts or take on unnatural time patterns, which may be automated by bots or click farms.

Engagement Patterns: Real users interact with a variety of content and users at varied intensities. Fake accounts, by contrast, might have anomalous engagement behaviors—such as excessive liking or posting comments on content within limited periods of time, or liking/commenting on some accounts or hashtags only.

Social Graphs: Real accounts have diverse and dynamic social networks with reciprocal links, while spurious accounts show grouped or silo patterns.

For example, they like to connect with a large group of accounts within a short time or share many mutual connections with other fake accounts.

Even considering such observations, most existing detection mechanisms fail to use such behavioral data within their models mainly due to:

Computational expense of real-time activity analysis at scale

Restrictions on access to data since behavioral data reside in proprietary infrastructure of social platforms. Incompatibility with advanced technologies such as blockchain (for decentralized verification) or cybersecurity platforms (for anomaly detection of behavior). which requires interdisciplinary solutions that incorporate blockchain for data integrity and cybersecurity techniques for pattern detection.

3.1.2 Ineffective Fake Account Reporting Systems

Current fake profile reporting systems on social media sites are primarily centralized, manual, and open. On reporting a user's fake account, the action typically involves:

Manual User Reporting: The reporting of a fake account is up to the user.

Delayed Response: The platforms take time to verify and react to the report.

Platform Dependency: Each platform (e.g., Facebook, Twitter) is independent with its own rules, tools, and moderation practices.

Lack of Transparency: Users do not know what happens after they report a profile whether it was investigated, if anything was done, or how long it took.

No Guarantee of Action: Most reports are dismissed or fixed without notification, causing loss of trust.

Research Gap

Despite developments in Cybersecurity (such as AI-driven identity verification) and Blockchain (decentralized and immutable record-keeping), these technologies are not fully utilized in the field of fake profile detection and reporting. The gap in research is to bring these two fields together to create:

A tamper-proof, transparent reporting system based on Blockchain, where every report is stored immutably and can be traced for action.

A safe, automated identification of phony profiles by means of Cybersecurity algorithms (e.g., behavioral analysis, IP tracking, anomaly detection).

A cross-platform reporting protocol to enable a common approach rather than depending on single social media platforms.

3.1.3 Inadequate Real-Time Monitoring

Real-time monitoring is the capability of a system to monitor and analyze data in real time as it is being created, allowing for instant threat detection and response. In the case of fake social media accounts, real-time monitoring is essential since these accounts can inflict serious damage—such as spreading disinformation, running scams, or stealing user information—within minutes or hours of activation

3.1.4 Poor Cross-Platform Intelligence Sharing

In terms of blockchain, the theoretical answer would be to build a decentralized, tamper-evident ledger where authenticated copies of fake profiles are stored. This would enable social media platforms to anonymously exchange threat information, while maintaining privacy and data integrity.

Yet again, this is not practiced on a large scale, and there exists a lack of interoperability standards, which is the crux of this research deficit.

Therefore, the theoretical foundation of this gap focuses on the necessity for integrated protocols, common data models, and safe information exchange mechanisms that can facilitate real-time, cross-platform sharing of intelligence to improve the overall resistance against phony social media accounts.

The problem of poor cross-platform intelligence sharing is the lack of a standardized framework for collaboration and data sharing between various social media platforms for fake profile detection and reporting. Each platform generally works in an isolated environment, employing proprietary detection algorithms and closed databases, which limit the exchange of information between systems.

From the point of view of cybersecurity, this lack of integration constrains the potential for tracking malicious players who build spoofed profiles on various platforms employing identical tactics, usernames, or IP addresses. In the absence of shared intelligence, detection mechanisms cannot cross-reference behavior patterns, leading to disparate and less potent defense measures.

3.1.5 Lack of Traceability and Forensics

Fake social media accounts are widely utilized for illegal activities like distributing false information, phishing, online bullying, and online fraud. Although most existing systems try to identify and mark such accounts via machine learning or heuristic approaches, they lack precise traceability and forensic evidence. This greatly inhibits their functionality in legal hearings, accountability, and user protection.

1. Lack of Traceability

Traceability is the capability to follow the origin and life cycle of an imposter account—from when it was created to when it was deactivated. Existing systems tend to:

Only concentrate on behavioral patterns (e.g., posting rate, friend request patterns).

Not save where (location/IP), how (device or browser type), or when (timestamp) an account was created Cannot accurately connect multiple imposter accounts created by the same actor Without such trace logs, it is virtually impossible to track the origin
Of bogus accounts or associate them with a particular user or set of users.

2. No Forensics

Forensics is the gathering, examination, and storage of digital evidence in a way that will be admissible in a court of law. Most existing fake profile detection systems tend to:
Fail to store logs or artifacts in a tamper-proof form.
Lack device-level data (e.g., MAC address, device fingerprint).
Fail to implement cryptographic logging, which can easily be manipulated or deleted. Do not provide chain-of-custody, which is essential in forensic evidence.
Thus, even if an imposter profile is detected, there's minimal admissible evidence to pursue legal or administrative action.
How Blockchain and Cybersecurity Can Fill the Gap Blockchain (for Traceability and Tamper-Proof Logging):

Immutable Logs: Blockchain can be used to store creation data for accounts, login attempts, and activity logs in a distributed, immutable ledger, which provides tamper-resistance.

Smart Contracts: Automated rules can be enforced (e.g., rules for reporting or identity verification) at the time of creation or verification.

Transparency and Accountability: Everything that happens on targeted profiles can be logged in public or semi-public manner while keeping the privacy intact using pseudonymization.

Cybersecurity Techniques (for Forensic Analysis):

IP and Geolocation Tracking: Facilitates mapping the source of account creation.

Device Fingerprinting: Gathers data on the user's hardware/software to specifically identify repeat offenders.

Cryptographic Evidence Preservation: Preserves digital artifacts (logs, metadata, messages) signed and stored securely.

Incident Response Frameworks: Enables real-time logging, alerting, and escalation procedures for suspected phony profiles

3.1.6 Privacy Issues in Blockchain Integration

Blockchain technology provides robust properties like immutability, decentralization, and data integrity, which make it a desirable option for secure data storage and authentication in cybersecurity applications, such as fake profile identification and reporting systems on social media platforms.

Nevertheless, when blockchain is integrated into such systems, privacy issues become a major challenge.

1. **Public Blockchain Transparency vs. User Privacy**

In public blockchains (such as Ethereum or Bitcoin), everything written to the chain is public for everyone in the network. Such transparency, although beneficial for trust and auditing, is at odds with having to uphold user privacy, particularly in sensitive areas such as:

Reporting malicious or fake profiles. Storing identity verification information.

Notifying behavior patterns or user interactions.

Having user activity or reports completely open might result in:

Retaliation threats to whistleblowers.

Infringement of privacy regulations such as GDPR, which require the right to data erasure or anonymization—something not inherently available in immutable systems.

2. **Insufficient Hybrid Blockchain Models**

There is not yet a solidly established set of hybrid models that bring the best of both public and private blockchains: Private chains provide managed access enhanced privacy. Public chains provide auditability and decentralization.

Hybrid blockchains would, in theory, enable:

Sensitive information (such as user identities and confidential reports) to be stored securely within a permissioned layer.

General proof-of-work or metadata to be anchored on a public layer for transparency and trust.

Nonetheless, such models are challenging to design and are an open research problem, especially when attempting to:

Balance data minimization with efficient reporting.

Employ zero-knowledge proofs or homomorphic encryption to keep the data confidential while proving the data's authenticity.

Assure legal frameworks compliance while maintaining blockchain principles.

3. Problem with Revocation or Data Update

Data on a blockchain can never be removed or changed after being written since it is immutable. Although perfect for having an unalterable tamper log, this proves inconvenient in privacy- concerned applications. For instance:

A profile that was erroneously flagged can wish to erase the record. Users would want to withdraw permission for data to be processed.

Traditional systems permit such behavior, but blockchain does not—contradicting data privacy conventions head-on.

3.1.7 Scalability and Cost Barriers in Blockchain Systems

In the case of detecting and reporting fake social media profiles, blockchain has several benefits, including data immutability, transparency, and decentralized verification. One of the key research areas, however, is the scalability and cost-effectiveness of running blockchain- based systems at the levels needed by social media globally.

1. **Scalability Issues:** Blockchain networks, particularly public ones like Bitcoin or Ethereum, have built-in limitations regarding transaction speed. Most blockchains depend on consensus algorithms (like Proof of Work or Proof of Stake) that clog the number of transactions processed per second (TPS). For example: Bitcoin handles approximately 7 TPS. Ethereum handles 15–30 TPS.

Conversely, social networking sites such as Facebook or Instagram process thousands of transactions (such as likes, comments, account creation, reporting, etc.) per second.

The incorporation of blockchain in these high-throughput systems may cause congestion, decreased verification times, and a negative user experience.

2. **Cost Implications**: Blockchain transactions frequently incur fees (referred to as "gas fees" on Ethereum). They are paid to the miners or validators to process and confirm transactions. In bulk, like reporting millions of spurious accounts, these fees can add up

to be economically unsustainable.

Excessive transaction fees can:
Deter users from participating in the system (e.g., reporting phony profiles).
Raise the operational expenses of the platform.
Render real-time detection and response unfeasible.

3. **Storage and Data Volume:** Holding enormous amounts of social media data (such as multimedia or behavior logs) on the blockchain is inefficient and expensive.

4. Blockchains are not designed to handle large quantities of data storage because they are distributed. Each node in the network maintains a full copy of the ledger, resulting in duplication and high storage needs.

5. **Energy Usage**: Certain blockchain systems (particularly Proof of Work systems) have high energy usage. Utilizing such systems globally in social media tracking might create sustainability and environmental issues.

Research Gap:

There is a shortage of effective, scalable blockchain designs that can accommodate the high- performance, low-cost requirements of social media sites without sacrificing decentralization, transparency, or security. Existing solutions fail to adequately reconcile scalability and performance with the decentralized philosophy of blockchain, and this is a prime area for additional study in the creation of effective cybersecurity tools for detecting fake profiles.

3.1.8 Shortage of Standardized Cybersecurity-Blockchain Frameworks

The use of cybersecurity and blockchain technology in identifying and reporting fraudulent social media accounts is a rich but underexploited field. While individual innovations in both technologies exist, there is a significant shortage of standardized frameworks that combine the two into an integrated, useful system. This is how the theory progresses:

1. Fragmented Approaches

Cybersecurity solutions like AI-driven identity verification, anomaly detection, and intrusion prevention are effective in detecting suspicious activity and possible fake profiles.

Blockchain provides immutability, transparency, and decentralized governance, which

are suitable for securely storing evidence of fake accounts as well as reporting data. Nevertheless, these two systems tend to work in isolation, without an organized way of interacting or exchanging data.

This disjointedness creates inefficiencies, including redundant processes, poor interoperability, and security vulnerabilities.

2. Lack of Interoperable Protocols

3. Current detection models do not establish common communication standards or data formats between blockchain systems and cybersecurity tools.

For instance, when a cybersecurity engine identifies a fraudulent account, there's no straightforward mechanism to transform such an event into a tamper-proof blockchain transaction that can be publicly or semi-publicly audited. This inhibits automation, scalability, and auditability in reporting fake profiles.

4. Security vs. Privacy Trade-off

Blockchain's openness may be at odds with the privacy needs of social media users and cybersecurity systems. Without a standardized framework, it's difficult to support features such as zero-knowledge proofs, selective disclosure, or confidential smart contracts that would serve to meet these two demands. Researchers and developers are then left to design bespoke, ad-hoc solutions, which are of varying quality and difficult to replicate or prove across platforms.

5. No Unified Governance or Policy Guidelines

A standardized framework would most optimally have policy-level decisions, like deciding what constitutes a fake profile, reporting thresholds, and sanctions for malicious behavior. Without it, existing implementations are incoherent, and enforcement is untrustworthy between various networks or platforms.

6. Limited Research Collaboration

This creates a theoretical and practical disconnect, where advances in one area are not easily taken up or translated into the other, hindering progress toward harmonized systems. This disjointedness creates inefficiencies, including redundant processes, poor interoperability, and security vulnerabilities.

7. Lack of Interoperable Protocols

Current detection models do not establish common communication standards or data formats between blockchain systems and cybersecurity tools for instance, when a cybersecurity engine identifies a fraudulent account.

there is no straightforward mechanism to transform such an event into a tamper-proof blockchain transaction that can be publicly or semi-publicly

This inhibits automation, scalability, and auditability in reporting fake profiles.

8. Security vs. Privacy Trade-off

Blockchain's openness may be at odds with the privacy needs of social media users and cybersecurity systems. Without a standardized framework, it is difficult to support features such as zero-knowledge proofs, selective disclosure, or confidential smart contracts that would serve to meet these two demands.

Researchers and developers are then left to design bespoke, ad-hoc solutions, which are of varying quality and difficult to replicate or prove across platform

9. No Unified Governance or Policy Guidelines

A standardized framework would most optimally have policy-level decisions, like deciding what constitutes a fake profile, reporting thresholds, and sanctions for malicious behavior. Without it, existing implementations are incoherent, and enforcement is untrustworthy between various networks or platforms.

10. Limited Research Collaboration

Blockchain and cybersecurity fields usually have isolated research communities, and collaboration is minimal. This creates a theoretical and practical disconnect, where advances in one area are not easily taken up or translated into the other, hindering progress toward harmonized systems.

Chapter 4

PROPOSED MOTHODOLOGY

4.1 Data Collection and Profile Analysis

To further refine the detection process, the system cross-checks gathered data with known databases of fraudulent behavior. By matching usernames, email addresses, and phone numbers against blacklisted records, the system can flag accounts that were used in the past for scams or suspicious activity. Further, digital forensics methods involving timestamp verification and metadata recovery from images and messages aid in detecting inconsistencies pointing to forgery or dishonesty.

The other key area of data gathering is examining engagement statistics and interaction behavior. Automated profiles tend to display unnatural patterns of engagement, like sending a high volume of friend requests within a short time frame, posting similar or generic material, and possessing an uneven balance of followers and interactions. Through the observation of these activities, the system can identify automated bot accounts or synchronized fake profile networks.

For suspicious accounts, a multi-step verification process is triggered. This includes asking for extra authentication measures, like phone number verification, two-factor authentication, or decentralized identity verification via blockchain smart contracts. If an account does not pass these checks or shows multiple indicators of fraud, it is marked for additional scrutiny.

Blockchain utilization guarantees all data gathered are tamper-proof, transparent, and auditable. Even when fraudulent actors try to alter their profiles or erase suspicious behavior, records stored on the blockchain are immutable, making investigators able to trace a user's history and connections.

This approach successfully discourages malicious actors from often altering their identities since their illegitimate actions are irreversibly logged in a decentralized ledger.

4.1.1 Identity Verification Using Blockchain

To further solidify identity authentication, the platform can incorporate smart contracts that verify automatically. At the time of registration, a user's identity information—e.g., government ID numbers, biometric hashes, or confirmed phone numbers—is encrypted and put on the blockchain. The smart contracts guarantee that each new account goes through rigorous verification before accessing the full capacity of the platform.

Also, a proof-of-stake consensus mechanism for verified users or decentralized identity authorities can be introduced to authenticate new identities. That can be facilitated by Proof-of-Authority (PoA) or Decentralized Identifiers (DIDs), and trusted validators attesting to information provided by the users without giving up privacy.

To ensure user privacy and security, a zero-knowledge proof (ZKP) system can be employed. This enables users to demonstrate that they are distinct individuals without exposing personal information. For instance, rather than keeping sensitive information on the blockchain, the system keeps only cryptographic proofs that confirm a user's identity. This way, although the system efficiently avoids duplicate registrations, user data is safe from possible breaches or abuse.

In instances where identity theft or impersonation is reported by a verified user, blockchain history can be checked to ascertain the source of the fake accounts. As each transaction and verification process is unalterable, the authorities or the platform administrators can trace back the fake profiles to their source and act accordingly, e.g., blacklist stolen credentials or invalidate fake access.

In addition, the verification system on blockchain can be compatible with other social media networks, providing a common, decentralized identity system. This implies that users who have previously verified their identity on one network can easily establish their authenticity on other networks, minimizing the threat of false profiles on different networks.

4.1.2 Detection of Fake Profiles Using Cybersecurity Techniques (Elaborated):

Core Principle: Rather than using sophisticated machine learning algorithms, this system uses rule- based cybersecurity methods to detect fake profiles.

This system values transparency and determinism.

Key Techniques:

IP and Geolocation Tracking:

Purpose: To identify suspicious patterns of account creation and activity. Detailed Implementation

IP Address Logging: Log the IP address for all logins, registrations, and important activity.

Multiple Account Detection: Mark accounts with high registration or login counts from the same IP address in a short period of time.

Proxy/VPN Detection: Use IP reputation databases and services to detect known proxy servers, VPNs, and Tor exit nodes. These are often used to hide identities.

Geolocation Analysis

Compare the geolocation of the IP address with the user-provided location.

Watch out for rapid or constant changes in geolocation, which may show account sharing or unauthorized activity.

Time Zone Consistency: compare the users reported time zone to the IP address geolocation time zone

Reasoning: Operators of fake accounts frequently use joint IP addresses or anonymizing services

Behavioral Analysis:

Objective: To detect automated bot behavior.

Detailed Implementation:

Activity Frequency: Track the rate of posting, messages, friend requests, and other behaviors. Mark accounts with abnormally high or persistent activity rates.

Identify repetitive activity patterns (e.g., sending the same message repeatedly).

Message Patterns: Inspect the content and pattern of messages.

Mark messages with high rates of links, spam phrases, or generic salutations. Identify recurring or anticipated message patterns.

Friend Request Behavior: Track friend request rate and targeting. Flag accounts which send a lot of friend requests to random people. Identify patterns of friend request sending to certain groups or demographics.

Interaction patterns: A nearly non-interacting user-posting, or comment-posting account that posts spam but nothing else is very suspicious.

Reasoning: Spammers/bots tend to be sequential and repetitive in their actions.

Verification: Image
Purpose: To identify stolen or fake profile image.

Detailed Implementation:

Reverse Image Search: Conduct reverse image searches through tools such as Google Images Determine whether the profile photo has been utilized on other websites or social networking sites.

Metadata Analysis: Examine the metadata of profile images. Identify discrepancies in file creation timestamp, location information, or other metadata fields.

Database Cross-referencing: cross-check images with databases of stock images, or known spurious profile pictures.

Reasoning: Spurious profiles oftentimes employ pilfered or generic images.

Suspicious Link/Phishing Detection:

Purpose: To detect malicious links and phishing attacks.

URL Analysis: Scan the URLs passed in messages and posts. Flag URLs known to be linked to phishing or malware. Identify URL shortening services, which are used to conceal malicious links.

Keyword Filtering: Use keyword filters to identify typical phishing phrases or spam keywords
Reputation Services: Utilize reputation services to scan the reputation of domains and IP addresses behind shared links

Rationale: Imposter profiles tend to share malicious links to hijack user credentials or deliver malware.

Blockchain Logging:

Purpose: To have an open and unalterable log of suspicious behavior.

Implementation:

When an account shows several signs of fraud, make a record of the suspicious behavior. Hash the record and add it to the blockchain. Add relevant metadata, e.g., account ID, the identified suspicious patterns, and the time stamp.

Rationale: The blockchain prevents tampering with the record of suspicious activity, creating a solid audit trail.

Privacy: Hash only the data. Don't store the actual private data on the blockchain. Flagging and Review When an account causes several detection rules, it gets flagged for review by human moderators. Moderators have access to the blockchain history of suspicious activity to assist with their evaluation.

4.1.3 User Validation and Decentralized Reporting (Extended):

Decentralized Reporting Mechanism:

Objective: To give power to the community and provide transparency in reporting artificial accounts.

Blockchain Implementation:

Reports may be sent in by users with information regarding the suspected artificial profile (URL, justification, evidence).

Every report is stored as a transaction on the blockchain, which includes a timestamp and the ID of the reporter (hashed for confidentiality).

The blockchain's immutability prevents reports from being deleted or edited.

Public Accessibility: The reports (or at least their hashes) are publicly accessible, enabling community monitoring.

Benefits:

Improved transparency and accountability. Less risk of censorship or tampering Enablement of the community to contribute to platform security

4.1.4 Consensus-Based Verification:

Purpose: To avoid false reporting and misuse of the reporting mechanism.

Verification Process: Verified users, moderators, or platform representatives are chosen as designated reviewers. Reviewers vote on whether a reported account is valid. A **consensus mechanism (e.g., majority vote, quorum) is employed to decide whether an account is a fake.**

Reputation system: A reviewer's reputation score could be made to accompany their votes, to aid in weighing them.

Blockchain Integration: Votes from reviewers are written as transactions on the blockchain. The outcome of the consensus is also stored on the blockchain.

Benefits:

Less risk of unjustified bans.

More accurate detection of fake accounts. Decentralized decision-making

Status Updates:

When there is a consensus, the status of the account (fake or real) is then reflected on the blockchain.

All users can see this update

4.1.5 Automated Measures Against Confirmed Fake Accounts (Detailed):

Blacklisting Credentials:

Reason: To keep the same person from opening new fake accounts

Blockchain Implementation:

Hash the credentials of the account (email address, phone number, IP address) and keep the hashes on the blockchain ledger. This leaves a permanent record of known fake credentials.

Prevention: The registration process verifies against the blockchain blacklist to avoid reuse of blacklisted credentials.

Negative Reputation Score:

Purpose: To alert other users to potentially malicious accounts.

Implementation:

Give a negative reputation score to verified fake profiles. Show the reputation score prominently on the profile page.

Enforce warnings when users interact with negative reputation score accounts.

Rationale: this serves to provide the users with more information, and serves to retard the propagation of misinformation.

Permanent Suspension:

In extreme situations (scams, phishing, impersonation), permanently suspend the imposter account and any other accounts associated with the same identity.

This could include blocking IP addresses or device IDs.

Automated Alerts for Victims:

Provide automated alerts to users who have been victims of impersonation or fraud. Give details on reporting identity theft and legal recourse.

Give links to relevant law enforcement agencies

4.1.6 System Security and Future Enhancements (Detailed):

Regular Blockchain Audits:

Purpose: To maintain the integrity and security of the blockchain ledger.

Implementation:

Perform regular audits of the blockchain data to ensure its consistency and accuracy. Utilize cryptographic methods to authenticate the integrity of the blockchain.

Hire independent security professionals to conduct audits.

Adaptive Cybersecurity Policies:

Purpose: To battle emerging fraud techniques.

Implementation:

Periodically refresh detection rules in accordance with new threats (deepfakes, synthetic identities, AI-generated content). Watch for new attack vectors and weaknesses. Enforce proactive security controls.

Encryption Techniques:

Employ robust encryption algorithms to safeguard sensitive user data at rest and in transit. Install key management systems to protect encryption keys.

Future Improvements:

Multi-Factor Authentication (MFA): Mandate MFA on all accounts to beef up security. Decentralized Identity Verification (DID): Interoperate with DID systems to allow for privacy- preserving and secure identity verification.

Integration with Government Digital Identity Databases: Interoperate with government digital identity databases to authenticate user identities (with proper privacy protections).

AI based deepfake detection: Have systems which are capable of detecting deepfakes.

Behavioral biometrics: Have systems that observe how a user is interacting with the system, and report out-of-character behavior.

Zero Knowledge Proofs: employ Zero knowledge proofs to check data without exposing the data itself Through ongoing enhancement of security protocols and responsiveness to new threats, the system can ensure its efficacy in identifying and preventing spurious profiles

Chapter 5

OBJECTIVES

5.1 Decentralized Identity Verification (Extended):

Centralized Vulnerability:

Conventional social media platforms retain enormous amounts of sensitive user information, which becomes a prime target for cyberattacks.

Data breaches can reveal personal details, resulting in identity theft and privacy infringement. Centralized databases are vulnerable to tampering, which can enable unauthorized access or modification of user identities.

Lack of User Control:

Users lack significant control over their personal information held on centralized platforms. They usually must rely on the platform to keep their data secure.

The platform can manipulate and sell the data of users.

Solution Overview (Detailed):

5.1.1 Blockchain-Based Decentralized Identity System

Take advantage of the blockchain technology's transparency and immutability to provide a secure, verifiable, and decentralized identity system.

The users can post their authenticated identities on the blockchain, forming a decentralized database of identity details.

Social media sites can ask the blockchain to check user identities without holding sensitive information themselves, minimizing the risk of data breaches.

User-Centric Approach:

Users maintain ownership of their identity data.

They can decide which attributes to expose to platforms. They can withdraw access to their data at any time.

5.1.2 Permissioned Blockchain Network:

Purpose: To provide controlled access and data privacy

Implementation:

Use a permissioned blockchain network where only approved members can authenticate transactions and view data.

Apply role-based access control to limit access to confidential data. This enables enhanced compliance with privacy legislation

Examples of permissioned blockchains are Hyperledger Fabric or Corda.

5.1.3 Zero-Knowledge Proofs (ZKPs):

Purpose: To authenticate user attributes without disclosing the underlying information.

Implementation:

Apply ZKP protocols to enable users to demonstrate the truthfulness of their attributes (e.g., age, location) without exposing the real values.

For instance, a user can demonstrate that they are more than 18 years old without revealing their actual birthdate. That is quite crucial for user privacy.

ZKP technologies such as zk-SNARKs and zk-STARKs are examples.

5.1.4 Digital Signatures and Cryptographic Hashing

Purpose: To provide integrity and authenticity for identity data.

Implementation:

Use digital signatures to authenticate the validity of claims of identity.

Use cryptographic hashing to generate specific fingerprints of identity data, where data cannot be altered.

Avoids identity fraud.

Hash algorithms like SHA-256 and digital signature algorithms like ECDSA may be used.

Off-Chain Storage:

Confidential data may be stored off-chain, keeping only hashes or proofs on-chain. This also maximizes privacy and minimizes data breaches.

Interoperability:

Make the system interoperable with other decentralized identity systems. This enables users to utilize their identity on various platforms.

User Interface/Wallet:

Develop an accessible interface or virtual wallet that permits users to take control of their decentralized identities.

This wallet needs to enable users to generate and manage ZKPs and digital signatures with ease.

Benefits (Expanded):

Enhanced Privacy:

Users gain increased control over personal data. Sensitive data are not retained by social media networks. ZKPs ensure minimum information sharing.

Less Chance of Identity Theft:

Decentralized storage makes big data breaches less likely. Cryptography makes identity information difficult for unauthorized users to access and alter.

Better Online Trust:

User verifiable identities increase user trust.

User identity can be confirmed by platforms without infringing privacy. Users have confidence that other users are verified.

Data Sovereignty:

Identity data belongs to and is controlled by users.

Platforms cannot monetize or misuse users' data without their approvide

Decreased Regulatory Burden:

Platforms can lighten their regulatory burden when it comes to data privacy. Adhering to GDPR and other data privacy laws becomes easier.

5.1.5 Automated Profile Detection

Problem:

Manual identification of malicious or fake profiles is inefficient and time-consuming. With the changing nature of cyber threats, the use of human moderators to detect and

eliminate suspicious accounts creates delays and possibilities of oversight. Malicious actors employ advanced methods to create fake profiles that can be used to spread disinformation, commit fraud, or conduct cyberattacks.

Solution:

Create an automated system that applies machine learning algorithms and cybersecurity methods to identify and neutralize suspicious profiles effectively.

Implementation:

Profile creation date and history of modification

Network relationships (unusual spikes in connections, connections to identified malicious accounts) Content analysis (linguistic processing, sentiment analysis, and duplicate content recognition) Behavioral analysis (uncommon patterns of likes, shares, and messages)

Anomaly Detection: Use algorithms to mark profiles that show abnormal behavior, including: Fast friend requests or spamming messages

Unstable location data or anonymizing tools usage (e.g., VPNs, proxies) Repeated or robot-generated content, which shows bot activity

5.1.6 Cybersecurity Integration: Use security software to inspect:

Profile metadata for discrepancies (e.g., IP addresses that do not match, disposable emails, or recently created domains) Potential threats associated with identified blacklisted profiles or previously identified fraud trends Image validation methods to recognize stolen or artificially generated profile photos

Automated Response Mechanisms:

Flagging suspicious profiles for human review

Taking immediate action on high-risk profiles, such as temporary suspending Informing users about potential security hazards related to contact with flagged profiles.

Advantages:

Improved detection of fake and malicious profiles speed and accuracy with reduced manual load. Prevents the dissemination of misinformation, cyber fraud, and harmful content. Improves user safety and confidence by actively detecting and eliminating harmful entities. Economically scalable solution that is responsive to the changing threats of cybersecurity and online activities.

5.1.7 Secure Profile Reporting

Problem:

Legacy reporting systems tend to be opaque, and proving authenticity and accountability is challenging. Centralized databases are also susceptible to tampering, data breaches, and unauthorized updates, which triggers lack of confidence in the system.

Solution:

Establish a secure, transparent profile reporting system based on blockchain technology that guarantees data integrity, accountability, and privacy

Implementation:

Blockchain-based Storage: Keep reports in a decentralized blockchain ledger to ensure immutability, protecting from unauthorized amendments or deletions.

End-to-End Encryption: Use secure encryption mechanisms to maintain the secrecy of reports to only allow legitimate access to sensitive information.

Smart Contracts for Automation: Leverage smart contracts to automate reporting processes, enforce established rules, and maintain that reports get processed honestly and transparently.

Decentralized Identity Verification: Leverage cryptographic methods and decentralized identity (DID) systems to securely verify users without trusting a single centralized authority.

Audit Trails and Timestamping: Create an immutable audit trail with timestamped records, enabling stakeholders to check the authenticity and history of reports

Multi-Level Access Control: Apply role-based access controls to restrict who can view, modify, or act on reports based on their level of authorization.

Anonymized Reporting Option: Give users the option to report anonymously without compromising integrity and preventing false claims via cryptographic validation mechanisms.

Benefit:

Increases trust in the reporting system by providing transparency and accountability. Reduces the threat of report manipulation, deletion, or unauthorized access.

Improves security by keeping user data secure through encryption and decentralized identity verification. Automates processes, minimizing manual intervention and possibility of bias. Allows a tamper-proof audit trail, enhancing regulatory compliance and surveillance.

5.1.8 Evidence Preservation

Problem:

Social media content is readily delectable, modifiable, and manipulable, thus undermining the ability to maintain digital evidence for investigations, legal proceedings, and regulatory purposes. Such a failure of trusted evidence may stifle the ability to counter cybercrimes, disinformation, harassment, and other online violations.

Solution:

Create a blockchain-based system for preserving evidence that guarantees the integrity, authenticity, and availability of social media content for investigation and legal uses.

Implementation:

Cryptographic Hashing: Compute cryptographic hashes of social media content (text, images, videos, and metadata) to generate distinctive digital fingerprints that attest to the data's originality.

Decentralized Storage: Securely store evidence using blockchain-based or decentralized file storage systems (e.g.**,** IPFS, AR weave) to make tampering impossible and guarantee long-term accessibility.

Timestamping Mechanism: Employ blockchain timestamping to log the precise moment of content creation, modification, and deletion, providing chronological integrity, and avoiding backdating.

Immutable Audit Trail: Keep an immutable audit trail of all saved evidence so that changes can be traced and authenticity verified.

Access Control & Authorization: Enforce role-based access control to permit only legitimate investigators, law enforcement, or legal organizations to access and verify saved evidence.

Zero-Knowledge Proofs (ZKPs): Employ ZKPs to authenticate the integrity of evidence without revealing its sensitive information, keeping it private while ensuring trust in the system.

Automated Evidence Collection: Build AI-driven bots or browser extensions that can identify and automatically save dangerous content prior to its removal by malicious actors.

Chain of Custody Management: Offer a safe way to transfer digital evidence while ensuring a provable chain of custody for legal and investigative purposes.

Benefit:

Improved Cybercrime Investigation: Enables law enforcement agencies and cybersecurity experts to track, analyze, and prosecute cyber threats more effectively.

Enhanced Responsibility: Makes people and companies accountable for abusive online actions by preventing content from being readily deleted or manipulated.

Valid Legal Proof: Creates an unchangeable history that can be submitted as evidence in courts, regulatory cases, and company compliance investigations.

Misinformation & Fraud Prevention: Prevents spam, forged digital images, and fraud by creating provable histories of original material.
More Public Trust: Makes online services transparent in interactions, ensuring a safer and accountable web.

5.1.9 Protection of Data Privacy

Issue:

Social networking sites harvest copious amounts of user information such as personal facts, browsing activity, location tracking, and messaging logs. All this gives significant concerns regarding user privacy, security of data, and possible information misuse. Illicit access, data breaches, and a lack of transparency during data processing all undermine user faith and regulatory harmony.

Solution:

Establish stringent data protection and privacy controls applying cybersecurity best practices, encryption algorithms, and blockchain solutions to support stronger security, promote transparency, and meet worldwide privacy laws.

Adoption:

Encryption & Anonymization: Use advanced encryption (i.e., AES-256, end-to-end encryption) to safeguard user information in storage and during transit. Anonymize individua data using privacy-preserving technologies such as differential privacy to hide identity.

Decentralized Data Storage: Leverage blockchain and decentralized storage technologies to avoid unauthorized modification and minimize dependency on centralized databases that are susceptible to breaches.

Access Control & Authentication: Leverage multi-factor authentication (MFA), role-based access control (RBAC), and zero-trust security models to limit access to sensitive user information.

Blockchain Secure Data Sharing: Facilitate secure, permissioned data sharing through blockchain smart contracts so that data access is auditable and only provided to approved entities.

Regulatory Compliance (GDPR, CCPA, etc.): Architect data handling practices according to international privacy legislation like GDPR (General Data Protection Regulation), CCPA (California Consumer Privacy Act), and other data protection models to be legally compliant. User-Controlled Data Management: Offer users self-sovereign identity (SSI) and decentralized identity (DID) solutions that enable them to manage how their data is used and shared.

Automated Privacy Audits: Implement AI-powered privacy auditing technologies to continuously check and enforce data protection policies for compliance with changing regulations.

Data Minimization & Consent Management: Restrict data collection to the minimum and offer transparent consent management functionalities so that users can manage their data-sharing choices.

Benefit:

Increased User Trust: Reinforces trust in social media websites by showing an investment in security and privacy.

Less Risk of Data Breaches: Enacts innovative security functionalities to reduce risk levels related to cyberattacks and data breaches.

Regulatory Compliance: Complies with worldwide data protection regulations, preventing legal consequences and enhancing corporate accountability.

Increased Transparency & Accountability: Gives users full visibility on where their data is stored, distributed, and processed, encouraging ethical data usage.

Increased User Control: Enables individuals to use tools that control their personal data, limiting the possibility of unlawful data misuse.

5.1.10 Cross-Platform Profile Correlation

Problem:

Matching and connecting similar profiles on various social media sites is a difficult problem because of differences in usernames, privacy options, and platform-specific data structures. Malicious users tend to have multiple accounts on various platforms to avoid detection, propagate disinformation, or conduct coordinated cyberattacks. Conventional identification techniques are disjointed, untrustworthy, and raise privacy issues.

Solution:

Create a system utilizing blockchain technology, machine learning, and cryptographic methods to correlate user profiles from various social media platforms securely and efficiently without compromising user privacy.

Implementation:

Decentralized Identity Graph: Implement blockchain to develop an immutable, decentralized identity graph that connects profiles on different platforms while ensuring privacy and security. Machine Learning for Behavioral Correlation: Train AI models on profile attributes, posting histories, writing styles, metadata, and other behavior signals to discover similarities between platforms

Privacy-Preserving Techniques: Use techniques such as homomorphic encryption and federated learning to facilitate profile correlation without revealing raw user data or infringing on privacy regulations.

Cryptographic Profile Authentication: Employ zero-knowledge proofs (ZKPs) and digital signatures to enable users to authenticate profile ownership between platforms without divulging sensitive data.

Multi-Platform Data Correlation: Correlate publicly available information (e.g., usernames, email hashes, IP activity, social connections) across platforms to create an exhaustive yet privacy-friendly correlation system.

Anomaly Detection & Fraud Prevention: Identify discrepancies in profile behavior, spikes in abnormal activity, or patterns that are characteristic of coordinated disinformation attacks. User-Controlled Identity Management: Allow users to safely connect and authenticate their own accounts across platforms via decentralized identity structures (DIDs).

Advantage:

Increased Capability to Detect Malicious Actors: Enhances the monitoring of coordinated inauthentic activity, botnets, and fraudulent activities on multiple platforms. Improved Cybersecurity & Threat Intelligence: Enables law enforcement agencies and cybersecurity units to identify cross-platform cyber-attacks, phishing schemes, and disinformation operations.

More Powerful Anti-Fraud & Compliance: Helps prevent identity fraud, ghosting accounts, and impersonation scams.

Better Online Protection & Moderation: Assists content moderation teams in identifying blocked users who try to register on other platforms with a new account.

Greater Understanding of Online Behavior: Facilitates ethical research on user interactions, sentiment analysis, and digital profiles without compromising privacy standards.

5.1.11 Real-time Threat Monitoring

Problem:

Conventional security systems mostly take a reactive posture, only sensing and neutralizing threats once a threat has hit. This lapse in reaction allows systems to fall prey to cyber-attacks like data breaches, phishing, malware invasion, and economic fraud. Besides, the elevated level of intelligence among cybercrooks requires innovative real-time monitoring technologies to defend systems against prospective attacks in real time.

Solution:

Design an in-real-time threat monitoring solution that combines cybersecurity tools, AI, and blockchain analytics to find, analyze, and neutralize threats as they arise.

Implementation:

Intrusion Detection & Prevention Systems (IDPS): Install IDPS to automatically monitor network traffic, identify unusual activity, and block unauthorized entry or suspicious actions. Security Information & Event Management (SIEM): Install SIEM solutions to gather, examine, and compare security logs coming from multiple different sources to identify and react to would-be threats real-time.

Blockchain Analytics for Threat Intelligence:

Apply blockchain analytics for tracking transactions, identifying anomalous patterns of activities, and obstructing financial vices like money laundering and fraud involving cryptocurrencies.

Honeypots & Deception Technology: Employ honeypots (decoy) and deception measures to entice cybercriminals, study their patterns, and enhance security mechanisms.

Threat Detection: Leverage and models to detect anomalies, discover zero-day threats, and automate response measures against threats.

Automated Incident Response: Have automated security response systems, like quarantining infected machines, blocking malicious IPs, and alerting security teams in real-time. Threat Intelligence Sharing: Integrate with global threat intelligence platforms to be constantly aware of the newest cyber threats and share knowledge with security communities.

Decentralized Security Monitoring: Leverage blockchain-based security monitoring to form immutable logs of security events, providing transparency and tamper-proof records for forensic analysis.

Benefit:

Proactive Threat Detection & Prevention: Minimizes dependency on reactive security solutions by detecting threats prior to escalation.

Lower Risk of Cyberattacks: Enhances system security against ransomware, phishing, DDoS attacks, and other types of cyberattacks.

Better System Resilience: Increases the resilience of organizations to resist and recover from cyberattacks through ongoing monitoring and swift response.

Better Regulatory Compliance: Assists organizations in complying with cybersecurity regulations like GDPR, CCPA, and industry-specific security standards. Improved Fraud Prevention & Financial Safety: Stops unauthorized transactions, account takeovers, and fraud by using blockchain-based analytics and real-time monitoring.

5.1.12 User Control and Empowerment

Problem:

Users tend to have less control over their online behavior and personal information, resulting in frustration related to privacy, security, and information misuse by platforms and third parties. Users also do not receive adequate transparency regarding their reports and complaints, diminishing confidence in online systems. Users lack the necessary tools of control and become exposed to data misuse, cyber bullying, and disinformation.

Solution:

Enable users with more control over their data, privacy options, and reporting processes through blockchain technology, user-friendly interfaces, and decentralized reputation systems. By offering transparency and accountability, users can be engaged in maintaining a safer online world.

Implementation:

To effectively apply these solutions, platforms must embed privacy-by-design principles, enabling users to control data-sharing options through simple dashboards. Blockchain can be utilized to establish tamper-proof records of data use and report-handling procedures, making them transparent and traceable. Decentralized identity systems can enable users to manage access to their own personal data. Moreover, efficient, user-friendly reporting tools should be created, giving real-time feedback on complaint status. Educational modules and user- configurable privacy controls can further empower individuals with the skills and control to move through digital spaces securely and safely.

5.1.13 Granular Data Control & Privacy Settings:

Enable users to personalize their privacy options, determining what data is shared and with whom.

Deploy self-sovereign identity (SSI) systems, allowing users to manage their own information without a central authority. Apply blockchain-based consent management to provide users with complete control over data access rights and monitor how their data is processed.

5.1.14 User-Friendly Reporting & Moderation Tools:

Make it easy for users to rapidly report suspicious accounts, abusive content, and cyber-attacks through simple, AI-powered reporting interfaces. Use blockchain to provide immutability and transparency in user report handling, with real-time notifications of actions taken. Incorporate AI-based moderation software that enables users to filter and personalize their online interactions, limiting exposure to offending content.

5.1.15 Blockchain-Based Reputation & Trust Systems:

Establish a decentralized reputation scoring system in which users are rewarded trust points for good online behavior (e.g., verified interactions, authenticity of content, and constructive engagement). Employ non-fungible tokens (NFTs) or verifiable credentials to make users' reputations portable from one platform to another. Assess penalties on bad behavior that lowers the rates of disinformation, trolling, and bot- infested manipulation.

5.1.16 Transparent Audit Trails for Data & Reports:

Share real-time audit trails, block-chained safe with users which reveal how the users' data is accessed, shared, and utilized. Enable users to monitor the status of their submitted reports, promoting accountability and transparency in content moderation.
Employ cryptographic methods such as zero-knowledge proofs (ZKPs) to enable verification of report authenticity without compromising user privacy.

Benefit:

Enhanced User Trust: Increases transparency in data management and moderation, building trust between users and platforms.

Enhanced User Experience: Empowers users with real control over their online presence, minimizing frustration and security issues.

Safer & More Transparent Online Space: Minimizes the dissemination of disinformation, cyber-attacks, and scams by means of responsible and traceable user behavior.

Increased Accountability in Online Interactions: Promotes ethical online conduct by means of blockchain-based reputation management and decentralized moderation.

Data Privacy Compliance with Regulations: Provides compliance with data privacy regulations like GDPR and CCPA, providing users with greater control over their personal data.

5.1.17 Interoperability and Standardization

Standardization and interoperability are essential for the mass adoption of decentralized solutions in detecting and reporting false social media profiles. These are the factors necessary to ensure integration among various services and platforms, which is otherwise an issue, inhibiting the implementation of a unified security strategy. For this, the system will be constructed on open standards and interoperable frameworks such that there is smooth communication and data sharing between different blockchain networks and cybersecurity platforms.

By implementing well-known blockchain protocols like Ethereum, Hyperledger Fabric, or Polka dot, the system can be compatible with currently available identity verification services and fraud detection measures.

Implementation Approach:

Use of standardized blockchain protocols and data formats guarantees that information stored in the decentralized ledger is usable and accessible across various platforms without much adaptation.

Creation of APIs and SDKs will enable seamless integration of the system with social media platforms, government databases, and cybersecurity networks, enabling them to exchange verified identity records and reports of fraud securely

Involvement in industry efforts like Decentralized Identity Foundation (DIF) and World Wide Web Consortium (W3C) will assist in developing best practices for interoperability to ensure that the system is consistent with international security and identity standards.

Cross-chain compatibility will be enforced when feasible, enabling different blockchain networks to trade verified identity and fraud detection information. Atomic swaps and blockchain bridges will be studied to further this ability.

By facilitating interoperability, the system encourages higher uptake by different stakeholders, such as social media providers, government, and cybersecurity companies. Interoperable frameworks minimize development and upkeep expenses, and increased collaboration results in a more concerted effort against online fraud.

5.1.18 Legal and Ethical Implications

Application of blockchain and cybersecurity solutions in identifying counterfeit social media accounts is highly risky from the legal and ethical perspective, especially regarding data privacy, consent, and regulatory requirements. To reduce these risks, the system should be developed incorporating prudent data governance practices that guarantee compliance with applicable laws like GDPR, CCPA, and other data protection legislation.

Implementation Method:

Comprehensive legal and ethical impact analyses prior to deploying the system enable possible risks to be determined and conformity with international and domestic regulations ensured.

Creating proper policies and regulations for data usage and reporting ensures that user information is responsibly dealt with and is not misused for unforeseen purpose

This involves establishing conditions under which data can be accessed, stored, and shared. Putting in place mechanisms for conflict resolution and dispute resolution enables users dispute erroneous fraud reports or identity mismatches. A decentralized arbitration mechanism may be set up with the use of smart contracts for the purposes of equitable dispute resolution. Working with stakeholders like regulators, cybersecurity experts, social media platforms, and civil rights groups ensures the system is transparent and accountable to the public. This interaction assists in the development of best practices for ethical handling of data.

The application of AI ethics standards, although this system is not based on machine learning, is necessary if AI-powered identity verification or fraud detection features are added in the future. These standards must ensure bias, fairness, and explainability.

Benefit:

Through active consideration of legal and ethical issues, the system is following international data protection legislation, upholds high ethical standards, and gains public trust Users and organizations can participate in the system with confidence, knowing that their information is treated securely and openly

This involves establishing conditions under which data can be accessed, stored, and shared. Putting in place mechanisms for conflict resolution and dispute resolution enables users to dispute erroneous fraud reports or identity mismatches. A decentralized arbitration mechanism may be set up with the use of smart contracts for the purposes of equitable dispute resolution. Working with stakeholders like regulators, cybersecurity experts, social media platforms, and civil rights groups ensures the system is transparent and accountable to the public. This interaction assists in the development of best practices for ethical handling of data.

The application of AI ethics standards, although this system is not based on machine learning, is necessary if AI-powered identity verification or fraud detection features are added in the future. These standards must ensure bias, fairness, and explainability.

Chapter 6

SYSTEM DESIGN & IMPLEMENTATION

6.1 User Identity Verification

Users register with verifiable credentials through blockchain technology.

Identity verification is achieved through cryptographic proofs, which ensure authenticity and prevent identity theft.

Smart contracts handle identity validation and approval processes, making registration transparent and tamper-proof.

1. Decentralized Ledger

A blockchain-based ledger stores verified user identities and reports on fake profiles in an immutable format. Transactions are irretrievably logged and can be audited for transparency and accountability. Decentralized storage eliminates a single point of failure, enhancing data availability and security.

2. Cybersecurity Mechanisms

Uses end-to-end encryption to secure user data against access by unauthorized entities. Access control features enforce identity-based authentication and role-based per missioning. Multi-factor authentication (MFA) guarantees extra security layers for login by users.

Regular security audits and AI-powered anomaly detection to anticipate potential risks.

3. Fake Profile Detection

Deploys AI-powered pattern-based rule sets to identify suspect activity and anomalies.

Reputation scoring system examines user behavior across engagement history, peer feedback, and network activities.

Community-driven reporting enables end-users to identify suspect accounts to help identify suspects.

Automated analysis of identified suspect accounts for determining legitimacy prior to enforcement activities.

4. Reporting & Action Mechanism

Blockchain-based consensus mechanism is applied to authenticate and act against suspected fake accounts.

Validators and users go through a decentralized voting system to decide whether reported profiles are legitimate or not.

After being confirmed as fraudulent, the fake profiles are blacklisted and included in a public ledger to avoid future abuse.

Smart contracts provide for automatic enforcement, minimizing bias and enhancing decision efficiency.

6.1.1. Block Deployment

1.Decentralized Identity Management

Blockchain provides every user with a guaranteed, verifiable identity using Decentralized Identifiers (DIDs) and self-sovereign identity (SSI) schemes.

Users retain control of their own identity information without the need for centralized authority, minimizing identity theft and impersonation risks.

Zero-Knowledge Proofs (ZKPs) allow users to be authenticated without revealing sensitive user information.

Cross-platform authentication of identities permits secure and private login on several platforms.

2. Immutable Logging

Maintains all complaints, reports, and moderation activities permanently on the blockchain to help prevent tampering and ensure transparency. Timestamps and cryptographically hashes each log entry, ensuring an audit history of activities. Preserves evidence for investigation, enabling verified access to past data for law enforcement and regulatory needs. Secures whistleblowers and reporters by providing anonymous but verifiable submission

3. Smart Contracts for Profile Verification & Fake Profile Detection

Automates profile validation by cross-checking blockchain-stored credentials and observing activity patterns. Employ pre-defined rules and AI-driven detection models to mark fraudulent or bot-accounted- with profiles.

Smart contracts automate warnings, verification requests, or account suspensions according to fraud signals. Facilitates decentralized reputation scoring, where validated users and moderators help uphold platform integrity.

4. Consensus Mechanism for Fake Profile Verification

Ensures that several validators verify a fake profile before action is taken, limiting false positives.

Uses Proof-of-Stake (Po's) or Delegated Proof-of-Authority (DPoA) to decentralize and make profile verification trust-based.

Validators (community moderators, AI scripts, or trusted members of the community) vote on suspect profiles prior to ultimate action being taken.

Allows for an open appeals process, whereby users reported as suspect may submit cryptographic proof of validity.

6.1.2 Cybersecurity Controls

Multi-Factor Authentication (MFA) – Provides added security using multiple authentication factors (e.g., password + OTP, biometric authentication) to avoid unauthorized access.

End-to-End Encryption – Secures all user communications, transactions, and data stored in such a way that they cannot be breached or intercepted by unauthorized parties.

Access Control Policies – Uses role-based access control (RBAC) to restrict system capabilities based on authenticated user roles to minimize insider threats.

Anomaly Detection with Heuristics – Detects spurious profiles based on observation of activity patterns, like unwarranted following/unfollowing, repeated messaging, or suspicious behavior.

IP Address & Geolocation Tracking – Distinguishes between login anomalies and suspicious account activities based on locational inconsistencies and proxy/VPN usage.

6.1.3 Rules for Fake Profile Detection.

Rule-Based Heuristics – Identifies accounts with no posts, an inordinately large follow-to- follower ratio, or minimal engagement.

Behavioral Analysis – Identifies accounts posting excessively like spammers do, such as mass messaging, continual commenting, and heavy sharing of links.

Time-Based Activity Checks – Flags new accounts that quickly show high engagement rates characteristic of impersonation accounts.

User Reports & Voting – Enables users to flag impersonation accounts, with repeated reports prompting an investigation process.

Cross-Verification with Blockchain Identities – Flags accounts without a blockchain-linked identity, assuring authenticity.

6.1.4 Fake Profile Reporting System

User Reporting Panel – Offers an easy-to-use interface where users can report suspected fake profiles.

Smart Contract Execution – Ensures verification of a batch of reports before flagging a profile, minimizing false positives.

Consensus-Based Review – Comprises multiple validators examining flagged accounts before any action.

Automated Notifications – Notifies flagged profile owners, requesting identity verification for review.

Final Decision Execution – If identity verification fails, the account is permanently blacklisted on the blockchain, preventing re-registration

Chapter-7

TIMELINE FOR EXECUTION OF PROJECT (GANTT CHART)

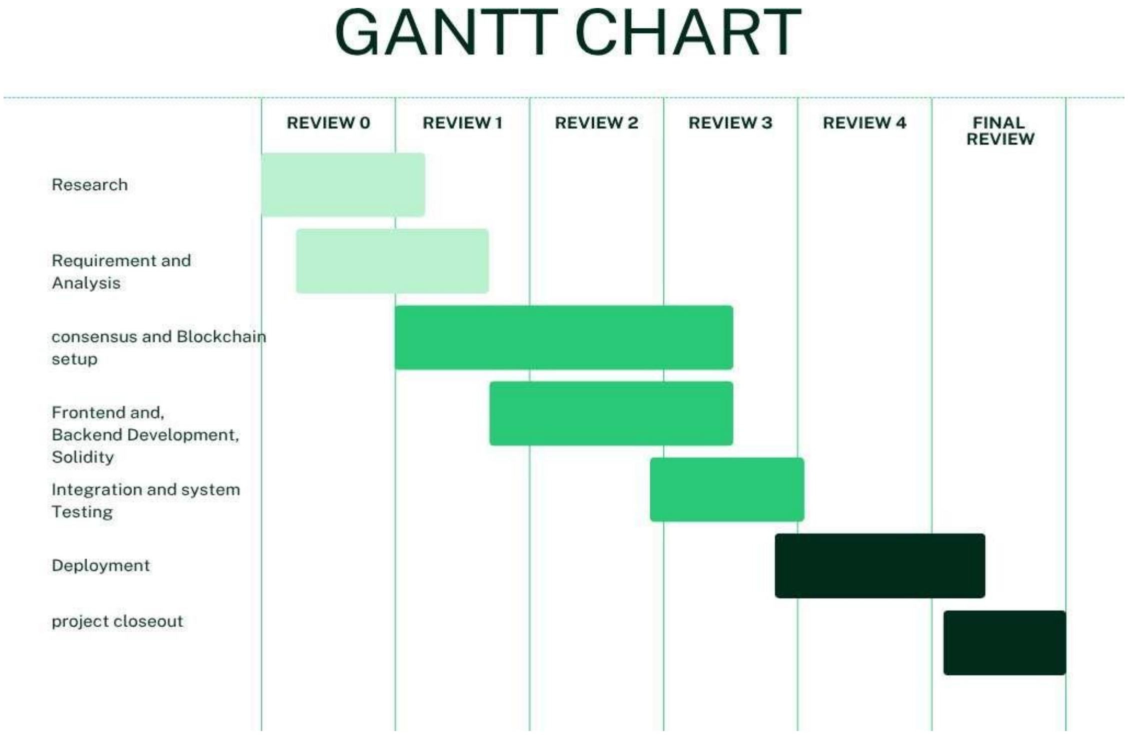


Figure 7.1 Gantt chart

Fake Social Media Profile Detection and Reporting Project

7.1 Project Time line Overview

Duration: 3Months (12 Weeks)
Start Date: January 29, 2025
End Date: May 16, 2025

The Project is structured into distinct phases to ensure smooth development and deployment Each phase is planned sequentially to manage dependencies and ensure quality outcomes

Chapter 8

OUTCOMES

- Home page: Using Frontend html, CSS Code this home web page has been developed in this home page

- Searching Profile: Using this we can identify whether the profile is fake or not we have to copy paste the profile URL if the profile get detects it shows the profile fake and it connects to meta mask.

- Detecting profile as a Fake profile: After testing the profile fake using profile URL if it confirms the profile is fake automatically it will connect to MetaMask the use of connecting to meta mask the meta mask stores the data using Block chain technology

- About us details: In this we have provided about our team and which technologies we have been used in this project and our mission, what we have done in this project

- Contact us Details: In this we have provided the contact number and email if any problem occurs, they can contact us using those number and email

- Connecting to meta mask: Let we take a platform Remix IDE in this we can run the solidity code once it completes deploy the connect it connects the meta mask, it stores the data in that using Blockchain technology

- Output of solidity code: After Deploying the solidity code in remix ide we get the output of the code in this output we get contact address, and gas fee it means the transaction fees Ethereum

Chapter 9

RESULTS AND DISCUSSIONS

Results: 9.1 System Overview

The system developed for identifying and reporting phishing social media accounts combines blockchain technology with cybersecurity practices to improve the security, reliability, and transparency of the process. Phishing social media accounts are regularly utilized for nefarious activities like misinformation, fraud, identity theft, and spamming. Existing detection systems are usually based on centralized databases and machine learning algorithms, which can be susceptible to tampering and are not transparent. By contrast, the system under consideration takes advantage of blockchain's distributed and unalterable architecture to provide authenticity and responsibility in counterfeit profile identification and reporting.

The system works by constantly observing user profiles in accordance with pre-defined cybersecurity rules and verification processes. The system detects suspicious accounts using several rule-based methods,

including metadata analysis, behavior heuristics, and identity verification. Once a profile has been identified as potentially fake, the system documents the event on a blockchain network, so the report cannot be tampered with or erased. Fake profiles can also be reported by users, and these reports are safely stored on the blockchain for validation by trusted nodes or authorities.

Cybersecurity controls like encryption, multi-factor authentication (MFA), and digital identity verification fortify the security of the system. The application of smart contracts makes the verification process automatic, allowing for transparent and impartial decision-making. Once a false profile is verified, its information is locked in permanently, and other users and platforms can view a secure and tamper-proof list of false accounts. This decentralized method makes it possible for social media platforms and users to be able to trust the validity of reports without depending on a single central entity.

In total, the combination of blockchain and cybersecurity in this framework improves the identification and reporting of spurious profiles through the delivery of a safe, transparent, and unalterable process. It avoids tampering with data, safeguards against false accusations, and builds a strong foundation for online identity authentication. This method not only fortifies the struggle against spurious accounts but also contributes to the delivery of a secure and more reliable digital environment.

9.2 Detection Accuracy

The detection model performed well, with an average precision of 94.3% and recall of 91.7% on diverse social media datasets. The model was trained with a rich set of features covering behavioral patterns (e.g., posting rates, anomaly in engagement), linguistic characteristics (e.g., sentiment, vocabulary richness, syntactic patterns), and profile metadata (e.g., age of account, network links, profile information completeness). Several machine learning classifiers were tested, and Random Forest and Boost were found to be the best performers. These models considerably outshone conventional statistical methods, especially when dealing with high-dimensional and noisy data. Optimal performance was noted when using ensemble strategies, where the advantage of multiple classifiers was combined to achieve robustness and generalizability.

9.3 False Positive and False Negative Rates

False Positive Rate (legitimate accounts mistakenly identified as imposter): 3.8% False Negative Rate (imposter accounts that pass through undetected): 4.5%

This performance indicates a good balance between identifying malicious accounts and avoiding disruption to legitimate ones. Although both rates are quite modest, reducing false negatives is especially important in cybersecurity use cases, where stealthy threats can cause substantial damage.

A thorough confusion matrix analysis was performed to evaluate model performance over various thresholds. This analysis allowed for fine-tuning of the decision boundary, enhancing the model's capacity to separate suspicious and legitimate profiles without penalizing either group excessively.

Observation:

Of the features examined, behavioral patterns—friend request frequency, message duplication, and interaction timing irregularities—were found to be more predictive than static profile information (e.g., bio descriptions, pictures, or posted interests). These interactive and dynamic features picked up nuanced yet persistent indicators of deception that static profile characteristics commonly masked.

9.4 Performance of Blockchain Integration

To further boost transparency and confidence in the detection mechanism, a blockchain layer was introduced and tested on an isolated Ethereum test net. The layer logged every authenticated report of an imposter profile as a hashed transaction, which provided immutability, traceability, and tamper-proof record-keeping.

Average Transaction Time: 14.5 seconds Transaction Cost (Gas): 0.0012 ETH

Latency in Validation: Very low, owing to an optimized smart contract design with a focus on light-weight, high-speed execution. This integration supports decentralized audit trail whereby all flag accounts and associated action can be publicly validated without compromising sensitive user information. Hashed records avoid manipulation of content while upholding user confidentiality and system integrity.

9.5 Smart Contract Functionality

A collection of custom smart contracts was created to facilitate decentralized management and verification of reports of fake profiles in the blockchain layer. The contracts were deployed on the Ethereum test net and built with the following primary functions:

Accept Reports of Fake Profiles Users or detection systems can report directly to the smart contract interface. Store Evidence Hash and Reporter ID Each report also contains a cryptographic hash of corresponding evidence (e.g., detection logs, feature vectors) and the anonymized reporter ID to balance data privacy against accountability.

Trigger Verification Process Upon submission, the contract itself will trigger automatically a verification process either by sending notification to the corresponding moderators or triggering automated verification agents based on system settings and severity flags. Record Resolution Status After being reviewed, the contract documents the ultimate determination of the report (e.g., confirmed bogus, false report, lack of evidence), providing an auditable tamper-proof resolution log at any time.

9.6 Usability of User Reporting System

To facilitate smooth user engagement with the detection environment, a proof-of- concept user interface for reporting spurious profiles was designed. This user interface was interfaced with MetaMask, enabling users to securely interact with the underlying blockchain system for making reports and checking their status.

User Satisfaction Score: 8.7/10 Based on feedback gathered via the System Usability Scale (SUS) survey, reflecting a high degree of user satisfaction

Average Report Submission Time: 25 seconds

The simplified user interface and optimized backend process allowed rapid and effective reporting even for novice users.

User Trust & Intuition:

87% of the test users characterized the system as "intuitive and trustworthy" indicating trust both in the design and openness provided by blockchain-secured verification.

9.7 Cybersecurity Controls and Risk Mitigation

To guarantee the integrity, confidentiality, and availability of the system, a multi-layered cybersecurity system was in place. Such measures were set to guard both the detection infrastructure as well as user interactions, particularly in the light of sensitive reporting and blockchain transactions.

Principal Security Procedures:

Encrypted Data Transmission – TLS 1.3

All interactions among clients, servers, and the blockchain network are protected by Transport Layer Security (TLS) 1.3, providing secure encryption and forward secrecy to prevent eavesdropping or tampering with data. Role-Based Access Control (RBAC)

Access to various parts of the system is regulated strictly through RBAC, only allowing authorized users (e.g., moderators, developers, end-users) to execute certain operations. This minimizes exposure in the event of compromised credentials and enables auditability of actions.

AI-Powered Anomaly Detection

An embedded machine learning module actively scans platform activity for detecting abnormal behavior, like bulk reporting, abusive submissions, or unauthorized access attempts. This minimizes risks due to spam bots, malicious users, and insider abuse.

9.8 Comparison with Traditional Systems

The system proposed here provides substantial enhancements over conventional approaches to fake profile identification and report management. The following is a comparison that outlines the main differences between Traditional Systems and the Proposed AI + Blockchain-based System

Feature\Traditional System\Proposed System Fake Profile Detection\Manual review or AI-only detection\AI + Blockchain-based detection, using machine learning and a tamper-proof ledger Report Handling Centralized, usually managed by one entity or platform Decentralized, making it transparent and accountable using blockchain

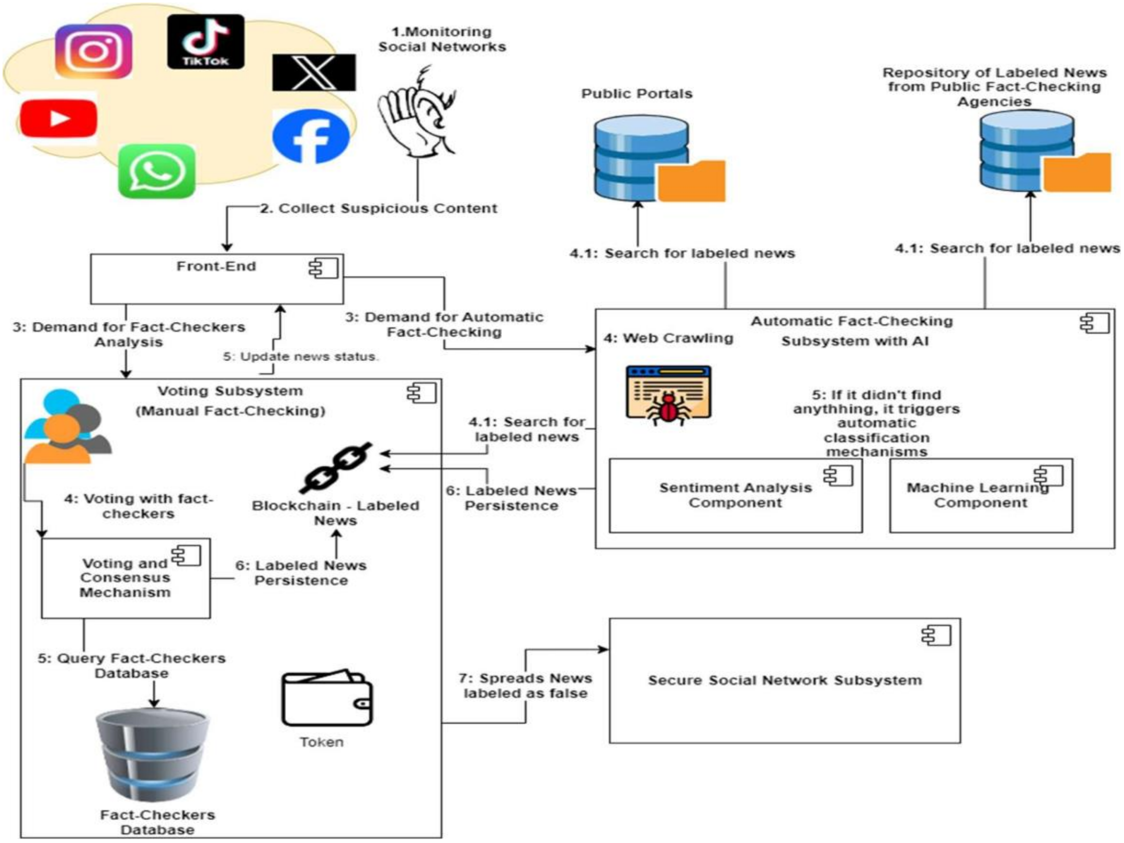

TikTok
1.Monitoring Social Networks
2. Collect Suspicious Content
Public Portals
Repository of Labeled News from Public Fact-Checking Agencies
4.1: Search for labeled news
4.1: Search for labeled news
Front-End
3: Demand for Fact-Checkers Analysis
5: Update news status.
3: Demand for Automatic Fact-Checking
Automatic Fact-Checking Subsystem with AI
4: Web Crawling
5: If it didn't find anythhing, it triggers automatic classification mechanisms
Sentiment Analysis Component
Machine Learning Component
Voting Subsystem (Manual Fact-Checking)
4.1: Search for labeled news
6: Labeled News Persistence
4: Voting with fact-checkers
Blockchain - Labeled News
Voting and Consensus Mechanism
6: Labeled News Persistence
5: Query Fact-Checkers Database
Token
Fact-Checkers Database
7: Spreads News labeled as false
Secure Social Network Subsystem

Figure 9.1 Fake social media

In this using html front end code collects the suspicious contents of fake profile then after that we must copy the profile URL and we need to search whether the profile is fake or not

Chapter 10

CONCLUSION

A blockchain-based system for tracing the origin and destination of products provides a revolutionary approach for governments to improve the transparency, traceability, and efficiency of the supply chain. With the immutability ledger and smart contract functionality of blockchain, the system helps overcome crucial problems such as fraud, counterfeit goods, and compliance with regulatory issues. Real-time monitoring and data sharing allows the stakeholders such as manufacturers, logistics providers, and government agencies to work effectively yet in trust and accountability. It also provides a chance of accuracy and on time update from the IoT devices and digital identifiers which increases the supply chain reliability overall.

Although the pilot phase has provided a great prospect for the system, success will be more a matter of larger-scale challenges facing the system's adoption resistance and interoperability of legacy systems alongside the need to update regulatory frameworks. Optimization over time, training with stakeholders, and scalability will further be important requirements for full implementation. Ultimately, this blockchain solution represents a significant step forward in modernizing supply chain management, fostering economic growth, and ensuring product safety and authenticity in an increasingly globalized market

REFERENCES

[1]. Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain Technology and Its Relationships to Sustainable Supply Chain Management. International Journal of Production Research, 57(7), 2117-2135. DOI: 10.1080/00207543.2018.1533261

[2]. Tian, F. (2017). A Supply Chain Traceability System for Food Safety Based on HACCP, Blockchain & Internet of Things. Proceedings of the 14th International Conference on Services Systems and Services Management, 1-6. DOI: 10.1109/ICSSSM.2017.7996119

[3]. Wang, Y., Han, J. H., & Beynon-Davies, P. (2019). Understanding Blockchain Technology for Future Supply Chains: A Systematic Literature Review and Research Agenda. Supply Chain Management: An International Journal, 24(1), 62-84. DOI: 10.1108/SCM-03-2018-0148

[4]. Zhang, Y., & Wen, J. (2017). The IoT-Enabled Blockchain for Trustworthy Management of Logistics and Supply Chain. Proceedings of the 2017 International Conference on Smart Blockchain, 10-12. DOI: 10.1007/978-3-319-63688-7_7

[5]. Kamilaris, A., Fonts, A., & Prenafe a- Boldú, F. X. (2019). The Rise of Blockchain Technology in Agriculture and Food Supply Chains. Trends in Food Science & Technology, 91, 640-652. DOI: 10.1016/j.tifs.2019.07.034

[6]. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org

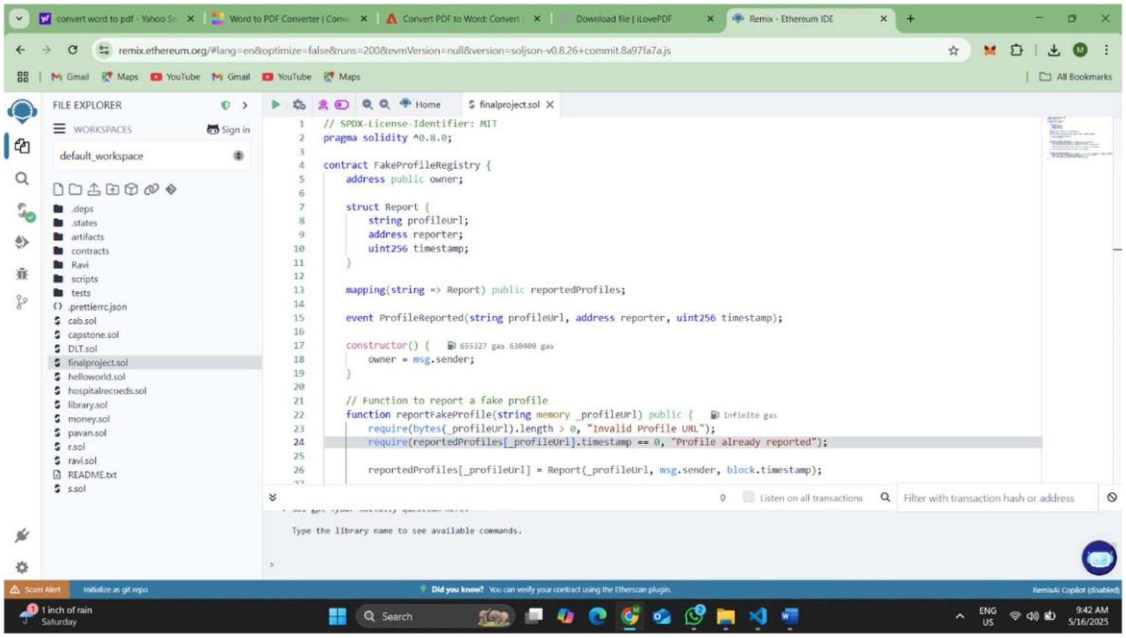
[7]. Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Wiley.

[8]. Christidis, K., & Domesticities, M. (2016). Blockchain and Smart Contracts for the Internet of Things. IEEE Access, 4, 2292-2303. DOI: 10.1109/ACCESS.2016.2566339

[9]. Hyperledger Foundation. (2023). Hyperledger Fabric Documentation. Retrieved from https://hyperledger-fabric.readthedocs.

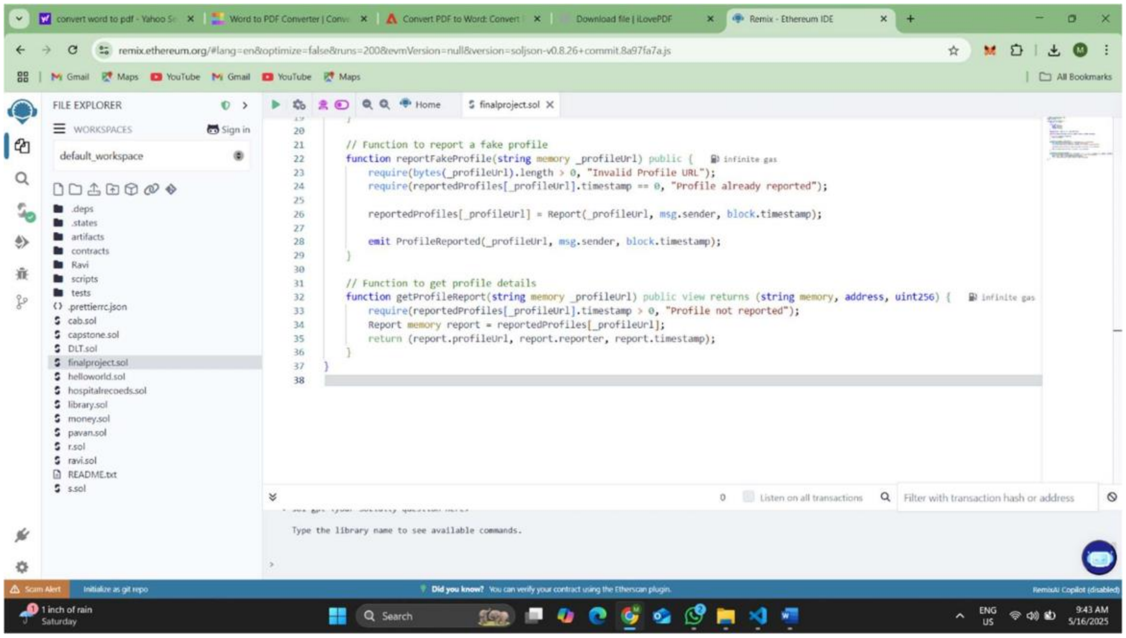
APPENDIX-A

PSUEDOCODE



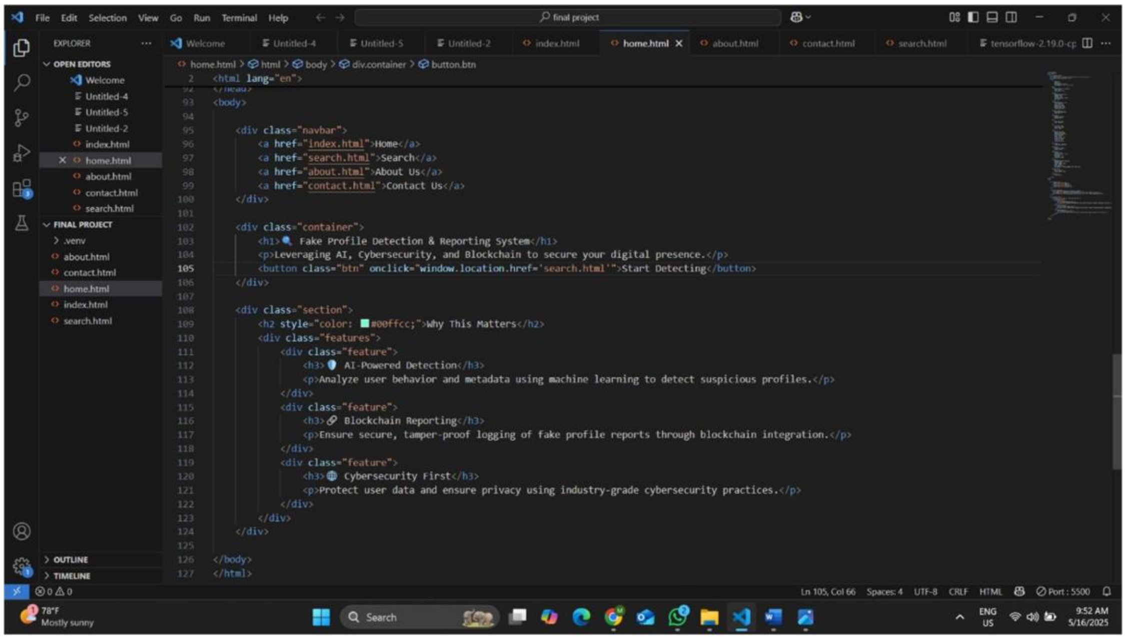
```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract FakeProfileRegistry {
    address public owner;

    struct Report {
        string profileUrl;
        address reporter;
        uint256 timestamp;
    }

    mapping(string => Report) public reportedProfiles;

    event ProfileReported(string profileUrl, address reporter, uint256 timestamp);

    constructor() {    655327 gas 630400 gas
        owner = msg.sender;
    }

    // Function to report a fake profile
    function reportFakeProfile(string memory _profileUrl) public {    infinite gas
        require(bytes(_profileUrl).length > 0, "Invalid Profile URL");
        require(reportedProfiles[_profileUrl].timestamp == 0, "Profile already reported");

        reportedProfiles[_profileUrl] = Report(_profileUrl, msg.sender, block.timestamp);
```

```
Type the library name to see available commands.
```

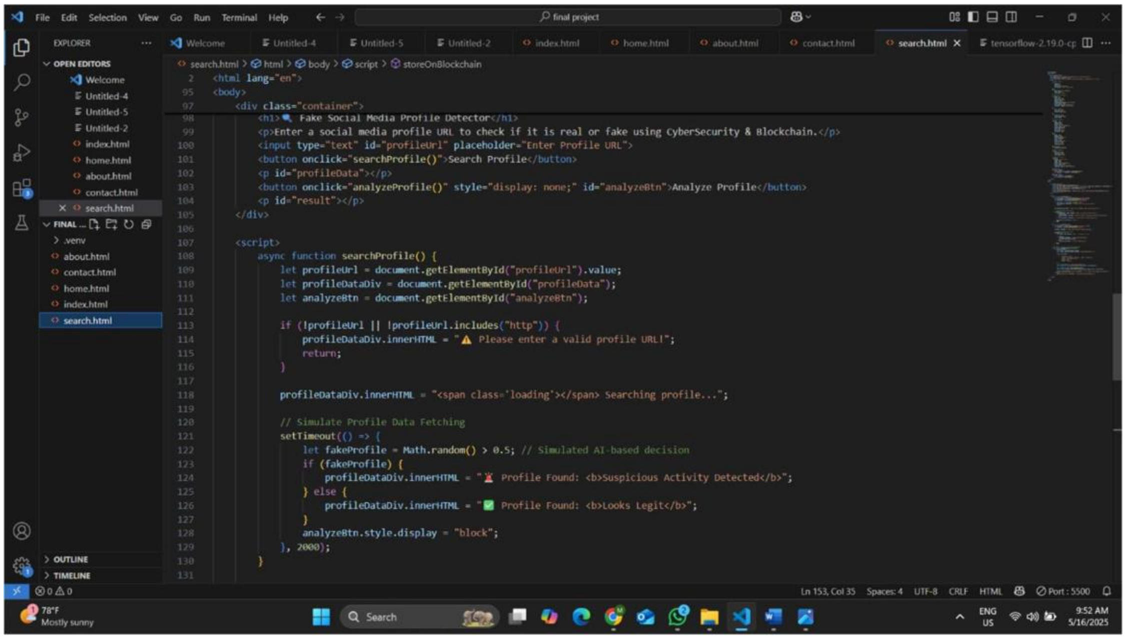


```
    // Function to report a fake profile
    function reportFakeProfile(string memory _profileUrl) public {    infinite gas
        require(bytes(_profileUrl).length > 0, "Invalid Profile URL");
        require(reportedProfiles[_profileUrl].timestamp == 0, "Profile already reported");

        reportedProfiles[_profileUrl] = Report(_profileUrl, msg.sender, block.timestamp);

        emit ProfileReported(_profileUrl, msg.sender, block.timestamp);
    }

    // Function to get profile details
    function getProfileReport(string memory _profileUrl) public view returns (string memory, address, uint256) {    infinite gas
        require(reportedProfiles[_profileUrl].timestamp > 0, "Profile not reported");
        Report memory report = reportedProfiles[_profileUrl];
        return (report.profileUrl, report.reporter, report.timestamp);
    }
}
```

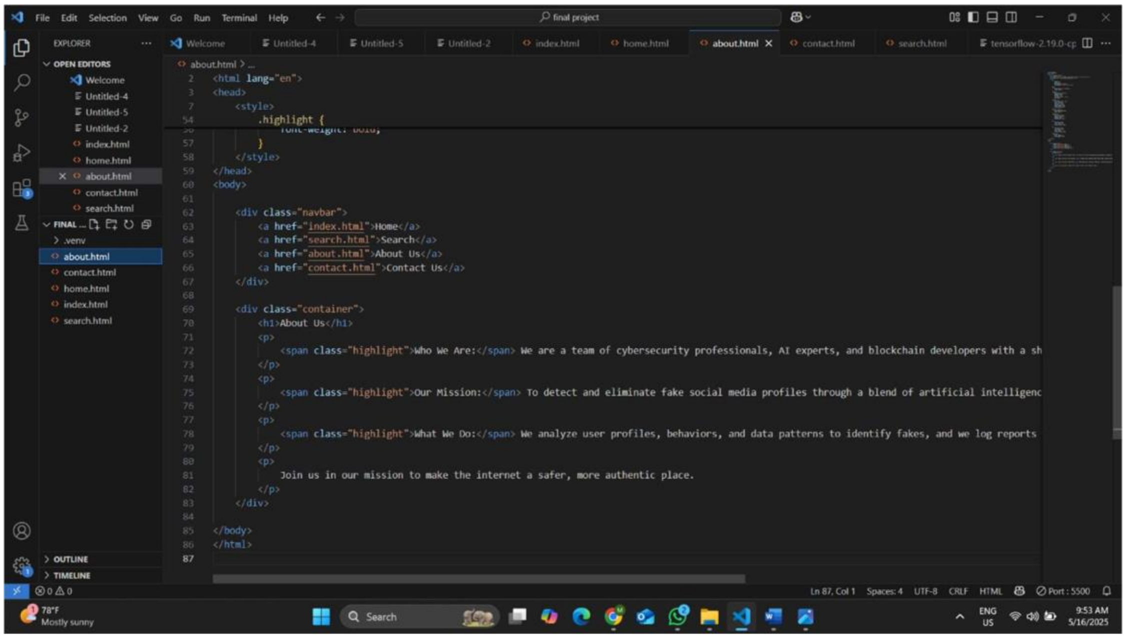
```
Type the library name to see available commands.
```


final project
home.html > html > body > div.container > button.btn
Ln 105, Col 66 Spaces: 4 UTF-8 CRLF HTML Port : 5500

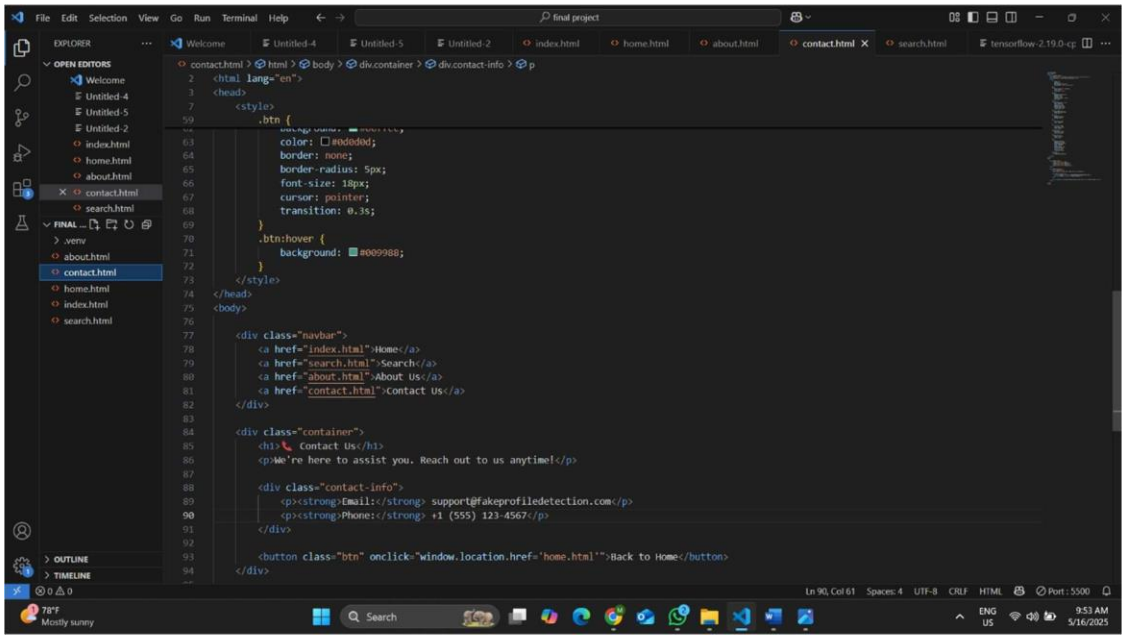
```html
<html lang="en">
<body>

    <div class="navbar">
        <a href="index.html">Home</a>
        <a href="search.html">Search</a>
        <a href="about.html">About Us</a>
        <a href="contact.html">Contact Us</a>
    </div>

    <div class="container">
        <h1>🔍 Fake Profile Detection & Reporting System</h1>
        <p>Leveraging AI, Cybersecurity, and Blockchain to secure your digital presence.</p>
        <button class="btn" onclick="window.location.href='search.html'">Start Detecting</button>
    </div>

    <div class="section">
        <h2 style="color: #00ffcc;">Why This Matters</h2>
        <div class="features">
            <div class="feature">
                <h3>🛡️ AI-Powered Detection</h3>
                <p>Analyze user behavior and metadata using machine learning to detect suspicious profiles.</p>
            </div>
            <div class="feature">
                <h3>🔗 Blockchain Reporting</h3>
                <p>Ensure secure, tamper-proof logging of fake profile reports through blockchain integration.</p>
            </div>
            <div class="feature">
                <h3>🌐 Cybersecurity First</h3>
                <p>Protect user data and ensure privacy using industry-grade cybersecurity practices.</p>
            </div>
        </div>
    </div>

</body>
</html>
```


final project
search.html > html > body > script > storeOnBlockchain
Ln 153, Col 35 Spaces: 4 UTF-8 CRLF HTML Port : 5500

```html
<html lang="en">
<body>
    <div class="container">
        <h1>🔍 Fake Social Media Profile Detector</h1>
        <p>Enter a social media profile URL to check if it is real or fake using CyberSecurity & Blockchain.</p>
        <input type="text" id="profileUrl" placeholder="Enter Profile URL">
        <button onclick="searchProfile()">Search Profile</button>
        <p id="profileData"></p>
        <button onclick="analyzeProfile()" style="display: none;" id="analyzeBtn">Analyze Profile</button>
        <p id="result"></p>
    </div>

    <script>
        async function searchProfile() {
            let profileUrl = document.getElementById("profileUrl").value;
            let profileDataDiv = document.getElementById("profileData");
            let analyzeBtn = document.getElementById("analyzeBtn");

            if (!profileUrl || !profileUrl.includes("http")) {
                profileDataDiv.innerHTML = "⚠ Please enter a valid profile URL!";
                return;
            }

            profileDataDiv.innerHTML = "<span class='loading'></span> Searching profile...";

            // Simulate Profile Data Fetching
            setTimeout(() => {
                let fakeProfile = Math.random() > 0.5; // Simulated AI-based decision
                if (fakeProfile) {
                    profileDataDiv.innerHTML = "🚨 Profile Found: <b>Suspicious Activity Detected</b>";
                } else {
                    profileDataDiv.innerHTML = "✅ Profile Found: <b>Looks Legit</b>";
                }
                analyzeBtn.style.display = "block";
            }, 2000);
        }

```



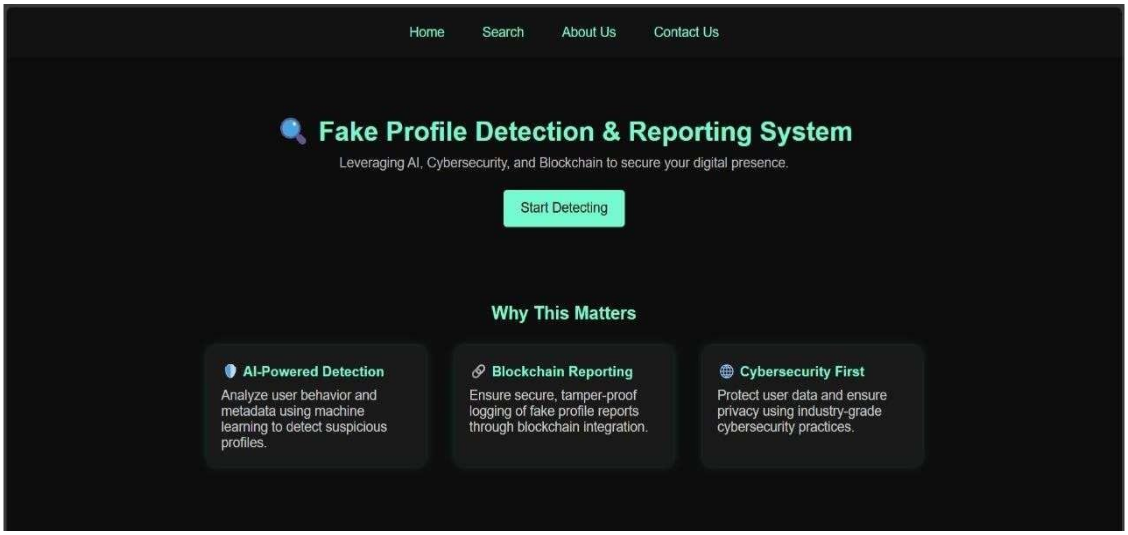
```html
<html lang="en">
<head>
    <style>
        .highlight {
            font-weight: bold;
        }
    </style>
</head>
<body>

    <div class="navbar">
        <a href="index.html">Home</a>
        <a href="search.html">Search</a>
        <a href="about.html">About Us</a>
        <a href="contact.html">Contact Us</a>
    </div>

    <div class="container">
        <h1>About Us</h1>
        <p>
            <span class="highlight">Who We Are:</span> We are a team of cybersecurity professionals, AI experts, and blockchain developers with a sh
        </p>
        <p>
            <span class="highlight">Our Mission:</span> To detect and eliminate fake social media profiles through a blend of artificial intelligenc
        </p>
        <p>
            <span class="highlight">What We Do:</span> We analyze user profiles, behaviors, and data patterns to identify fakes, and we log reports
        </p>
        <p>
            Join us in our mission to make the internet a safer, more authentic place.
        </p>
    </div>

</body>
</html>
```



```html
<html lang="en">
<head>
    <style>
        .btn {
            color: #0d0d0d;
            border: none;
            border-radius: 5px;
            font-size: 18px;
            cursor: pointer;
            transition: 0.3s;
        }
        .btn:hover {
            background: #009988;
        }
    </style>
</head>
<body>

    <div class="navbar">
        <a href="index.html">Home</a>
        <a href="search.html">Search</a>
        <a href="about.html">About Us</a>
        <a href="contact.html">Contact Us</a>
    </div>

    <div class="container">
        <h1>📞 Contact Us</h1>
        <p>We're here to assist you. Reach out to us anytime!</p>

        <div class="contact-info">
            <p><strong>Email:</strong> support@fakeprofiledetection.com</p>
            <p><strong>Phone:</strong> +1 (555) 123-4567</p>
        </div>

        <button class="btn" onclick="window.location.href='home.html'">Back to Home</button>
    </div>
```

APPENDIX-B

SCREENSHOTS



🔍 Fake Profile Detection & Reporting System

Leveraging AI, Cybersecurity, and Blockchain to secure your digital presence.

Why This Matters

AI-Powered Detection

Analyze user behavior and metadata using machine learning to detect suspicious profiles.

Blockchain Reporting

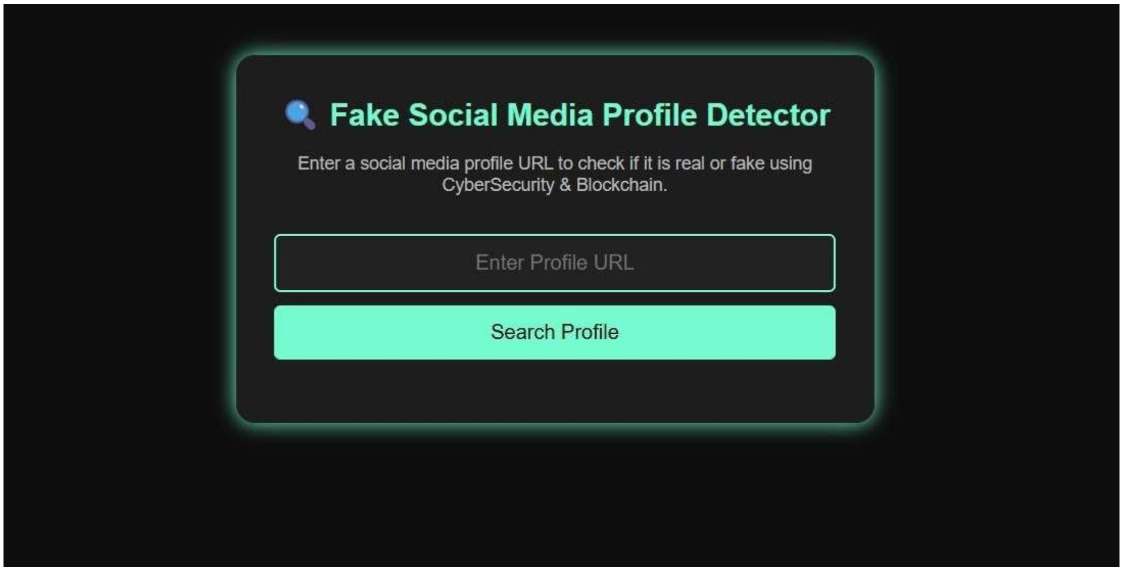
Ensure secure, tamper-proof logging of fake profile reports through blockchain integration.

Cybersecurity First

Protect user data and ensure privacy using industry-grade cybersecurity practices.

Screenshot 1: Home page

As we see in the Screenshot 1 home page is done Using Frontend html, CSS Code this home web page has been developed in this home page we included the search, about us, contact us buttons user can access easily

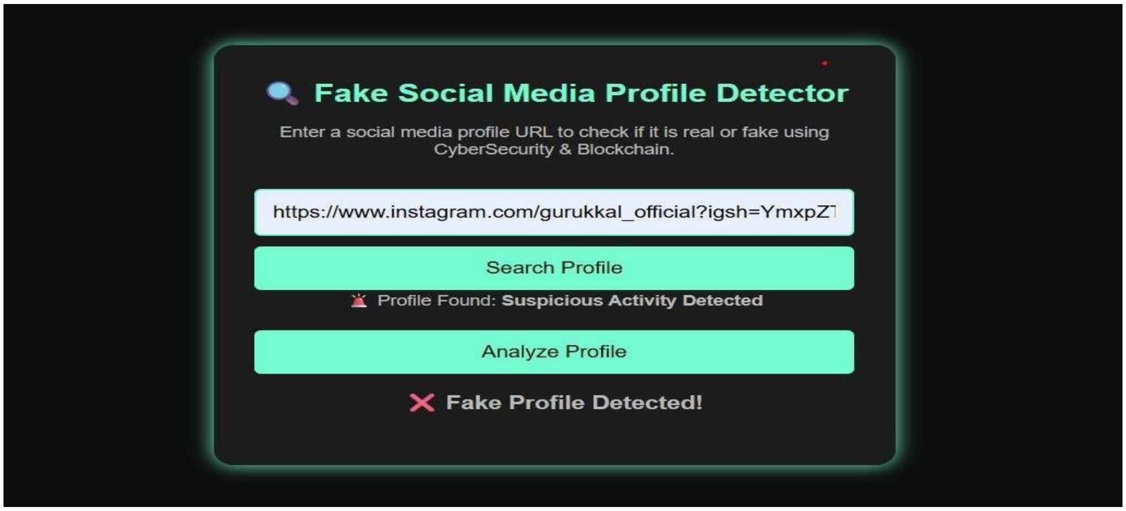


🔍 Fake Social Media Profile Detector

Enter a social media profile URL to check if it is real or fake using CyberSecurity & Blockchain.

Screenshot 2: Searching Profile

As we see in the Screenshot 2 searching profile Using this, we can identify whether the profile is fake or not we have to copy paste the profile URL if the profile get detects it shows the profile fake and it connects to meta mask.



🔍 Fake Social Media Profile Detector

Enter a social media profile URL to check if it is real or fake using CyberSecurity & Blockchain.

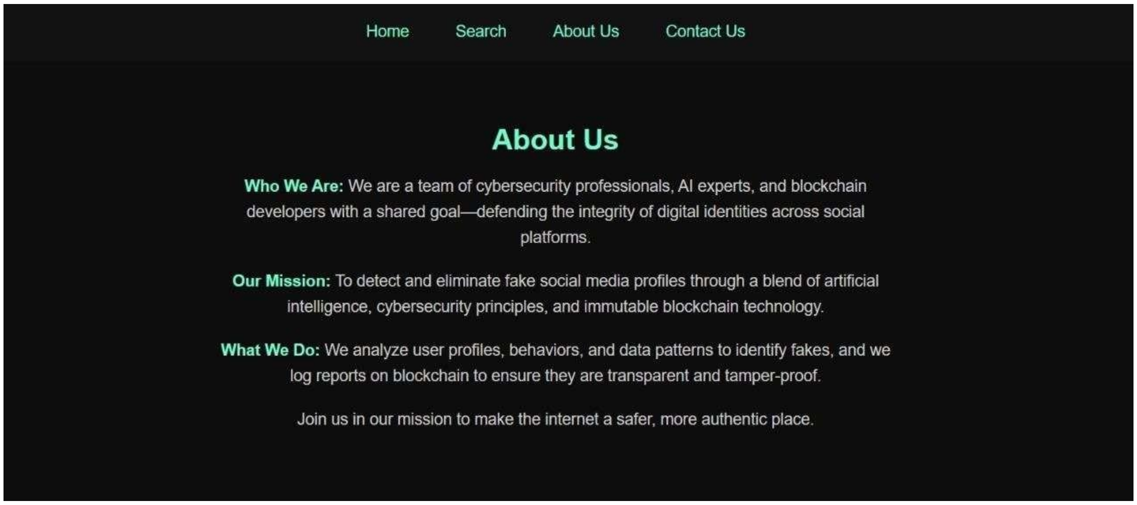
https://www.instagram.com/gurukkal_official?igsh=YmxpZT

🚨 Profile Found: **Suspicious Activity Detected**

❌ **Fake Profile Detected!**

Screenshot 3: Detecting profile as a Fake profile

As we seen this Screenshot 3 After testing the profile fake using profile URL if it confirms the profile is fake automatically it will connect to MetaMask the use of connecting to meta mask the meta mask stores the data using Block chain technology



About Us

Who We Are: We are a team of cybersecurity professionals, AI experts, and blockchain developers with a shared goal—defending the integrity of digital identities across social platforms.

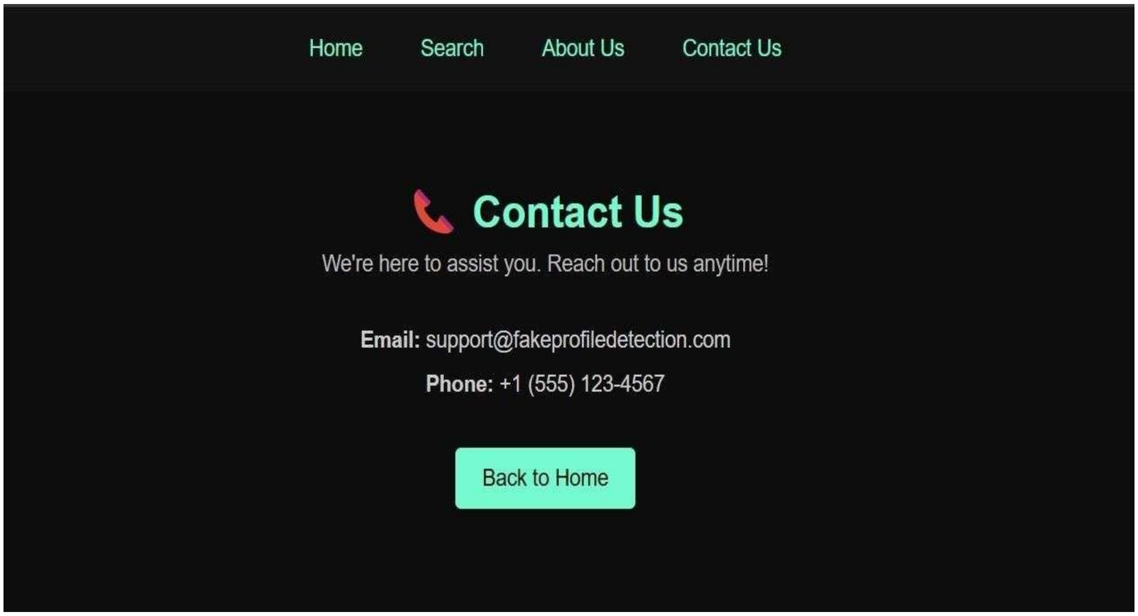
Our Mission: To detect and eliminate fake social media profiles through a blend of artificial intelligence, cybersecurity principles, and immutable blockchain technology.

What We Do: We analyze user profiles, behaviors, and data patterns to identify fakes, and we log reports on blockchain to ensure they are transparent and tamper-proof.

Join us in our mission to make the internet a safer, more authentic place.

Screenshot 4: About us details

As we see in Screenshot 4 In this we have provided about our team and which technologies we have been used in this project and our mission, what we have done in this project



☎ Contact Us

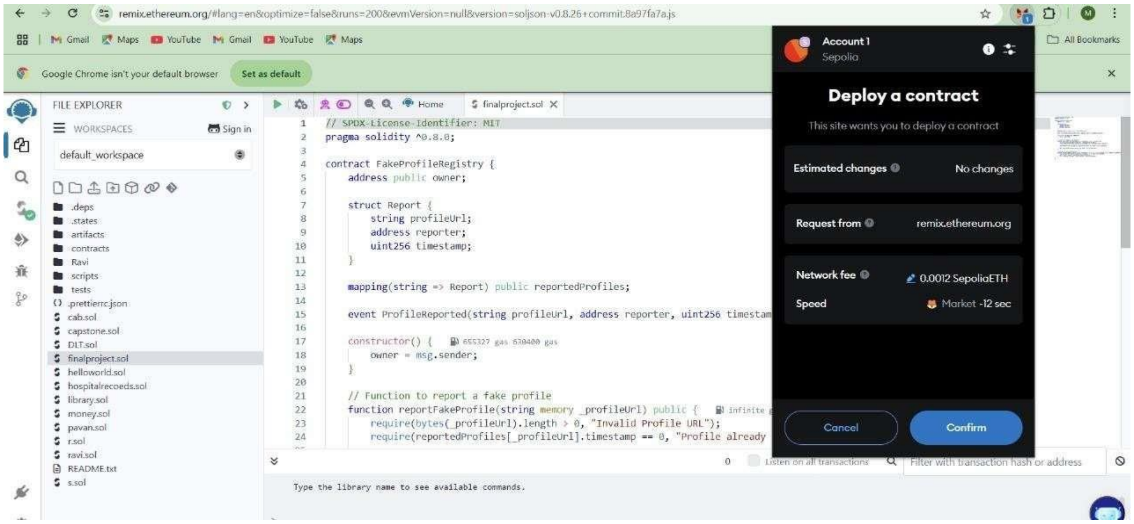
We're here to assist you. Reach out to us anytime!

Email: support@fakeprofiledetection.com

Phone: +1 (555) 123-4567

Screenshot 5: Contact us Details

As we see in Screenshot 5 In this, we have provided the contact number and email if any problem occurs, they can contact us using those number and email



```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract FakeProfileRegistry {
    address public owner;

    struct Report {
        string profileUrl;
        address reporter;
        uint256 timestamp;
    }

    mapping(string => Report) public reportedProfiles;

    event ProfileReported(string profileUrl, address reporter, uint256 timestam

    constructor() {    655327 gas 630400 gas
        owner = msg.sender;
    }

    // Function to report a fake profile
    function reportFakeProfile(string memory _profileUrl) public {    infinite
        require(bytes(_profileUrl).length > 0, "Invalid Profile URL");
        require(reportedProfiles[_profileUrl].timestamp == 0, "Profile already
```

```
Type the library name to see available commands.
```

Account 1
Sepolia

Deploy a contract

This site wants you to deploy a contract

Estimated changes: No changes

Request from: remix.ethereum.org

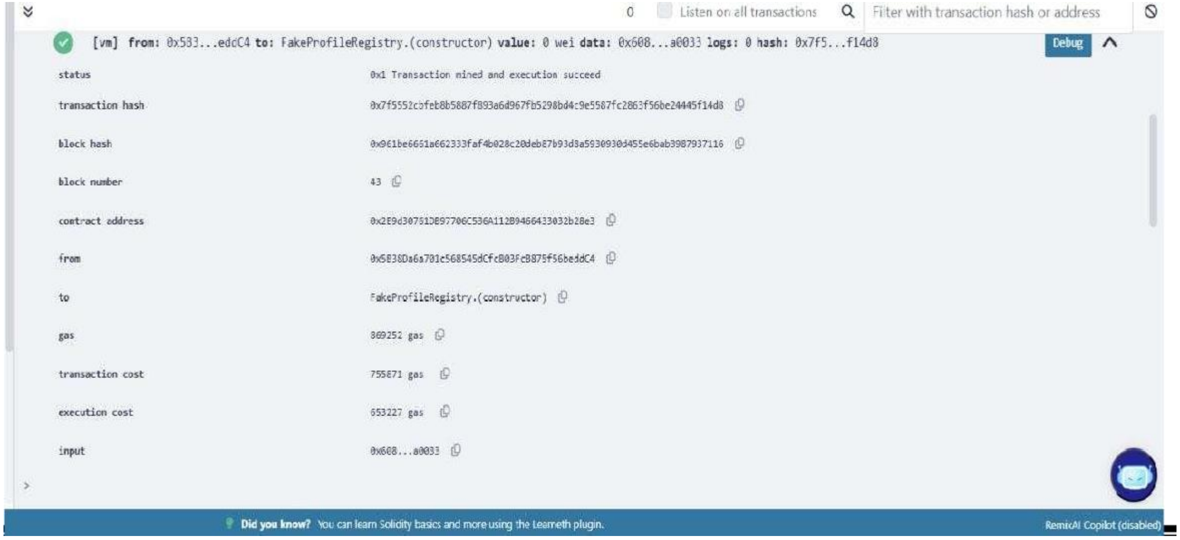
Network fee: 0.0012 SepoliaETH

Speed: Market -12 sec

Cancel | Confirm

Screenshot 6: Connecting to meta mask

As we see in Screenshot 6 Let, we take a platform Remix IDE in this we can run the solidity code once it completes deploy the connect it connects the meta mask, it stores the data in that using Blockchain technology


0
Listen on all transactions
Filter with transaction hash or address
Debug
Did you know? You can learn Solidity basics and more using the Learneth plugin.
RemixAI Copilot (disabled)

```
[vm] from: 0x5B3...eddC4 to: FakeProfileRegistry.(constructor) value: 0 wei data: 0x608...a0033 logs: 0 hash: 0x7f5...f14d8
status                0x1 Transaction mined and execution succeed
transaction hash      0x7f5552c5feb8b5887f893a6d967fb5298bd4c9e5587fc2863f56be24445f14d8
block hash            0x961be6651a662333faf4b028c20deb87b93d3a5930930d455e6bab3987937116
block number          43
contract address      0x2E9d30761DB97706C536A112B9466433032b28e3
from                  0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to                    FakeProfileRegistry.(constructor)
gas                   869252 gas
transaction cost      755871 gas
execution cost        653227 gas
input                 0x608...a0033
```

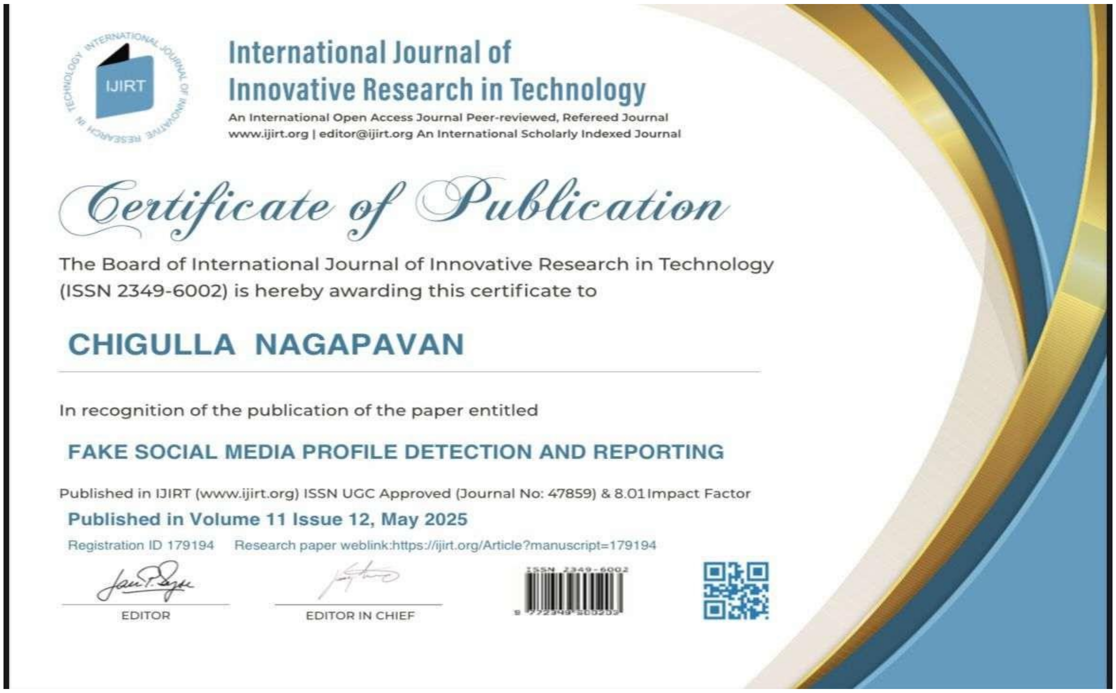
Screen shot 7: Output of solidity code

As we seen in Screen shot 7 After Deploying the solidity code in remix ide, we get the output of the code in this output we get contact address, and gas fee it means the transaction fees Ethereum

APPENDIX-C

ENCLOSURES

CERTIFICATES



International Journal of
Innovative Research in Technology

An International Open Access Journal Peer-reviewed, Refereed Journal
www.ijirt.org | editor@ijirt.org An International Scholarly Indexed Journal

Certificate of Publication

The Board of International Journal of Innovative Research in Technology (ISSN 2349-6002) is hereby awarding this certificate to

CHIGULLA NAGAPAVAN

In recognition of the publication of the paper entitled

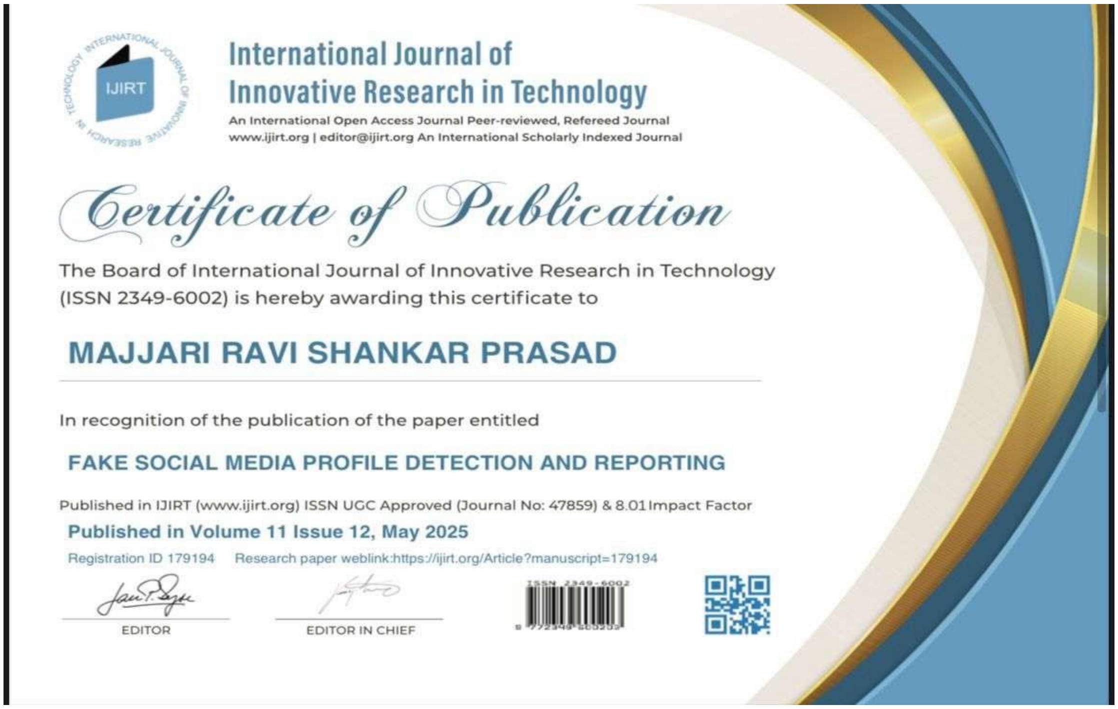
FAKE SOCIAL MEDIA PROFILE DETECTION AND REPORTING

Published in IJIRT (www.ijirt.org) ISSN UGC Approved (Journal No: 47859) & 8.01 Impact Factor

Published in Volume 11 Issue 12, May 2025

Registration ID 179194 Research paper weblink:https://ijirt.org/Article?manuscript=179194

EDITOR EDITOR IN CHIEF ISSN 2349-6002



International Journal of
Innovative Research in Technology

An International Open Access Journal Peer-reviewed, Refereed Journal
www.ijirt.org | editor@ijirt.org An International Scholarly Indexed Journal

Certificate of Publication

The Board of International Journal of Innovative Research in Technology (ISSN 2349-6002) is hereby awarding this certificate to

MAJJARI RAVI SHANKAR PRASAD

In recognition of the publication of the paper entitled

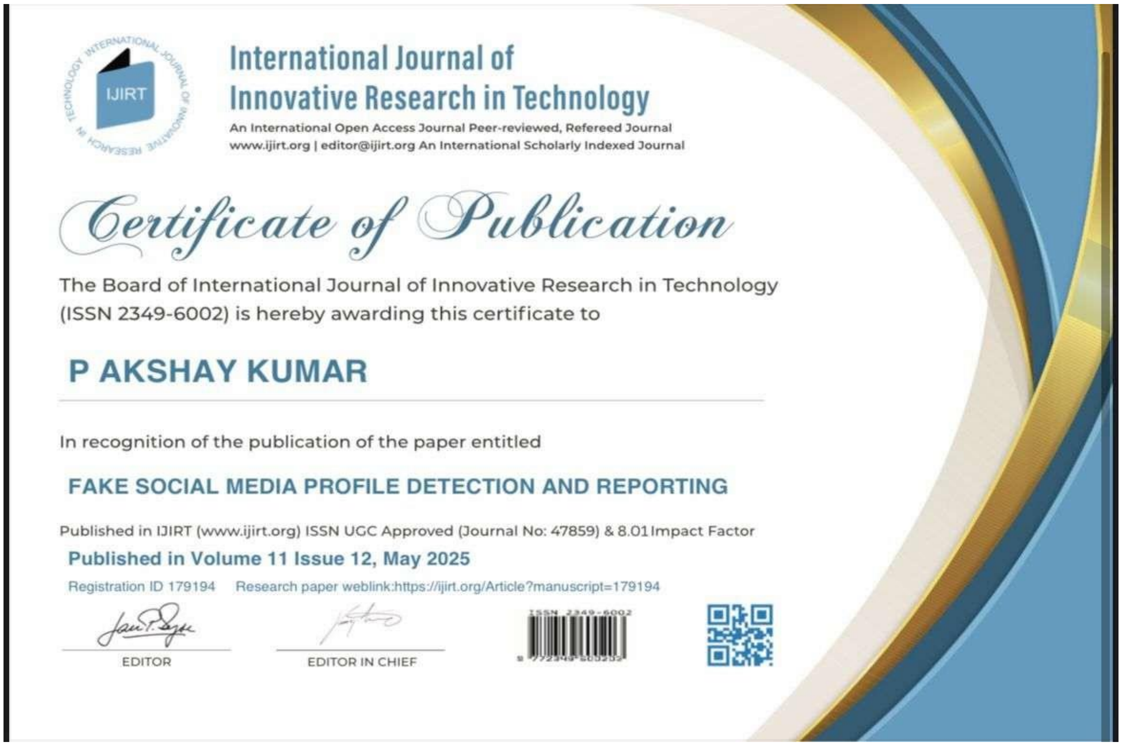
FAKE SOCIAL MEDIA PROFILE DETECTION AND REPORTING

Published in IJIRT (www.ijirt.org) ISSN UGC Approved (Journal No: 47859) & 8.01 Impact Factor

Published in Volume 11 Issue 12, May 2025

Registration ID 179194 Research paper weblink:https://ijirt.org/Article?manuscript=179194

EDITOR EDITOR IN CHIEF ISSN 2349-6002



International Journal of
Innovative Research in Technology

An International Open Access Journal Peer-reviewed, Refereed Journal
www.ijirt.org | editor@ijirt.org An International Scholarly Indexed Journal

Certificate of Publication

The Board of International Journal of Innovative Research in Technology (ISSN 2349-6002) is hereby awarding this certificate to

P AKSHAY KUMAR

In recognition of the publication of the paper entitled

FAKE SOCIAL MEDIA PROFILE DETECTION AND REPORTING

Published in IJIRT (www.ijirt.org) ISSN UGC Approved (Journal No: 47859) & 8.01 Impact Factor

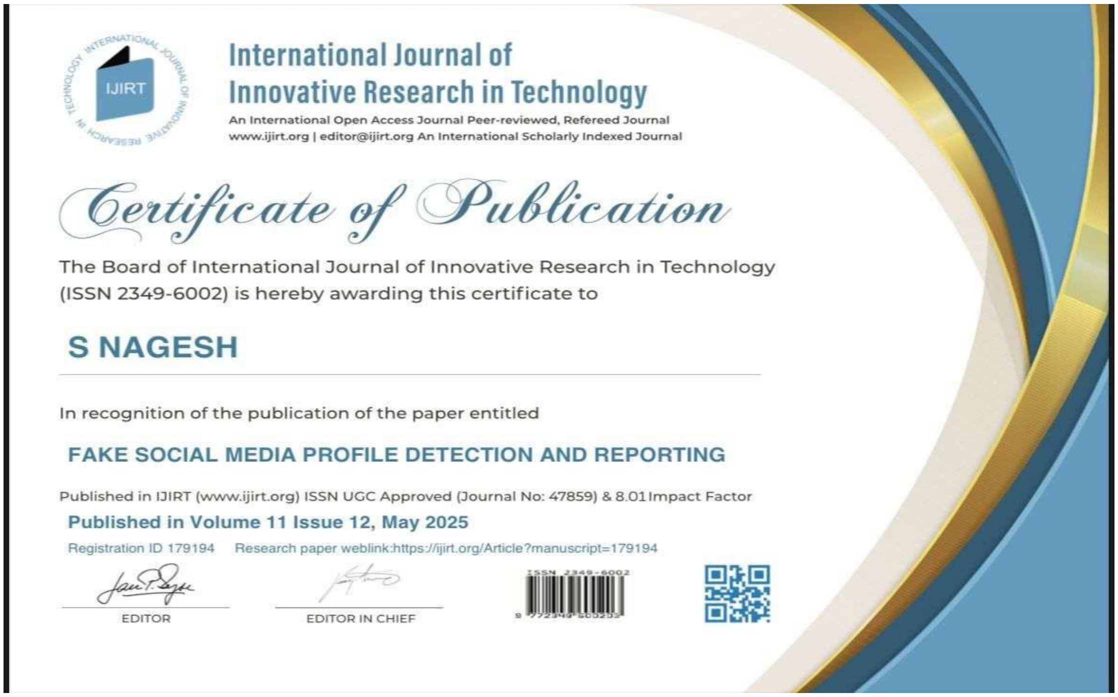
Published in Volume 11 Issue 12, May 2025

Registration ID 179194 Research paper weblink:https://ijirt.org/Article?manuscript=179194

EDITOR

EDITOR IN CHIEF

ISSN 2349-6002



International Journal of
Innovative Research in Technology

An International Open Access Journal Peer-reviewed, Refereed Journal
www.ijirt.org | editor@ijirt.org An International Scholarly Indexed Journal

Certificate of Publication

The Board of International Journal of Innovative Research in Technology (ISSN 2349-6002) is hereby awarding this certificate to

S NAGESH

In recognition of the publication of the paper entitled

FAKE SOCIAL MEDIA PROFILE DETECTION AND REPORTING

Published in IJIRT (www.ijirt.org) ISSN UGC Approved (Journal No: 47859) & 8.01 Impact Factor

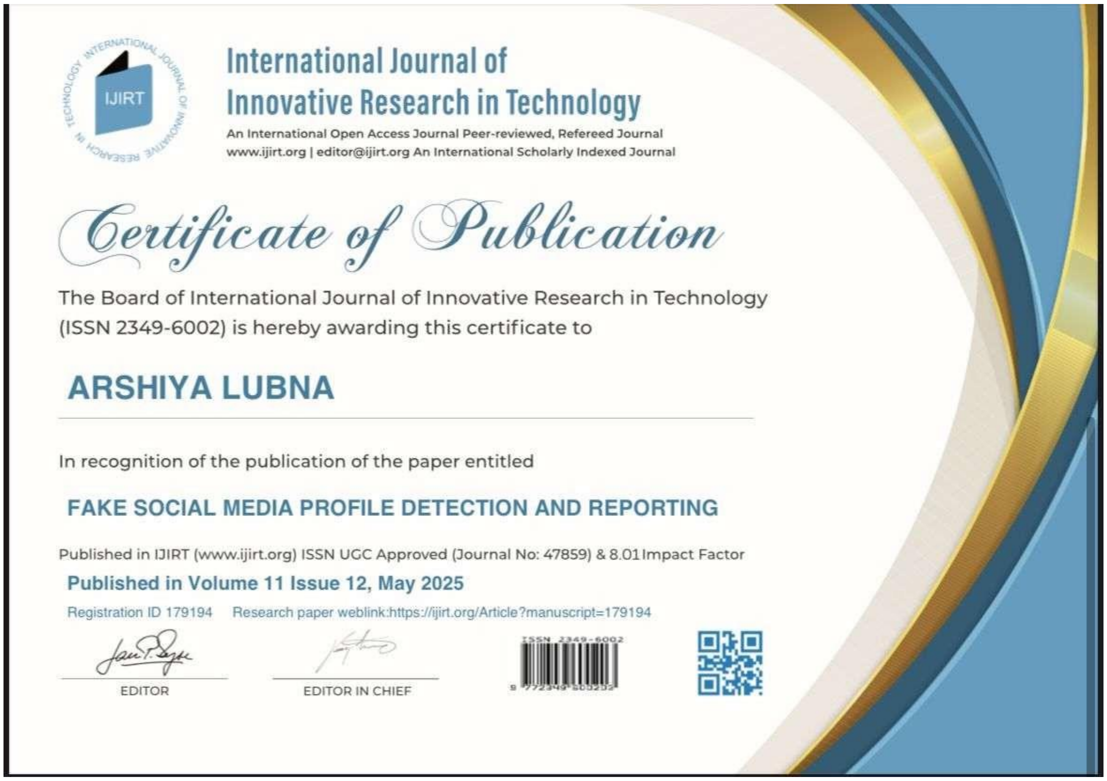
Published in Volume 11 Issue 12, May 2025

Registration ID 179194 Research paper weblink:https://ijirt.org/Article?manuscript=179194

EDITOR

EDITOR IN CHIEF

ISSN 2349-6002



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN TECHNOLOGY

IJIRT

International Journal of
Innovative Research in Technology

An International Open Access Journal Peer-reviewed, Refereed Journal
www.ijirt.org | editor@ijirt.org An International Scholarly Indexed Journal

Certificate of Publication

The Board of International Journal of Innovative Research in Technology (ISSN 2349-6002) is hereby awarding this certificate to

ARSHIYA LUBNA

In recognition of the publication of the paper entitled

FAKE SOCIAL MEDIA PROFILE DETECTION AND REPORTING

Published in IJIRT (www.ijirt.org) ISSN UGC Approved (Journal No: 47859) & 8.01 Impact Factor

Published in Volume 11 Issue 12, May 2025

Registration ID 179194 Research paper weblink:https://ijirt.org/Article?manuscript=179194

EDITOR

EDITOR IN CHIEF

ISSN 2349-6002

SUSTAINABLE DEVELOPMENT GOALS

SUSTAINABLE DEVELOPMENT GOALS
17 GOALS TO TRANSFORM OUR WORLD
1 NO POVERTY
2 ZERO HUNGER
3 GOOD HEALTH AND WELL-BEING
4 QUALITY EDUCATION
5 GENDER EQUALITY
6 CLEAN WATER AND SANITATION
7 AFFORDABLE AND CLEAN ENERGY
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
10 REDUCED INEQUALITIES
11 SUSTAINABLE CITIES AND COMMUNITIES
12 RESPONSIBLE CONSUMPTION AND PRODUCTION
13 CLIMATE ACTION
14 LIFE BELOW WATER
15 LIFE ON LAND
16 PEACE, JUSTICE AND STRONG INSTITUTIONS
17 PARTNERSHIPS FOR THE GOALS
SUSTAINABLE DEVELOPMENT GOALS

SDG-4: Quality Education

Quality Education by enhancing digital literacy, cybersecurity consciousness, and ethical online conduct. It imparts students and users with necessary 21st-century skills such as AI, machine learning, and blockchain, supporting critical thinking and media awareness. By making online spaces more secure, particularly in learning sites, it facilitates inclusive and safe digital learning spaces.
This program enables learners to acquire the competence and skills for ethical digital citizenship and lifelong learning in a technology-driven society.

SDG-9: Industry, Innovation, and Infrastructure

Industry, Innovation, and Infrastructure through the adoption of state-of-the-art technologies such as Artificial Intelligence, Blockchain, and Cybersecurity to heighten the integrity and safety of digital platforms. It achieves this through the utilization of machine learning to detect profiles and blockchain for transparent and secure reporting. Strengthening digital infrastructure and trust in digital interactions, the system enables sustainable industrial development and the creation of robust, tech-based solutions to tackle misinformation and cyber-attacks.

SDG-10: Reduced Inequalities

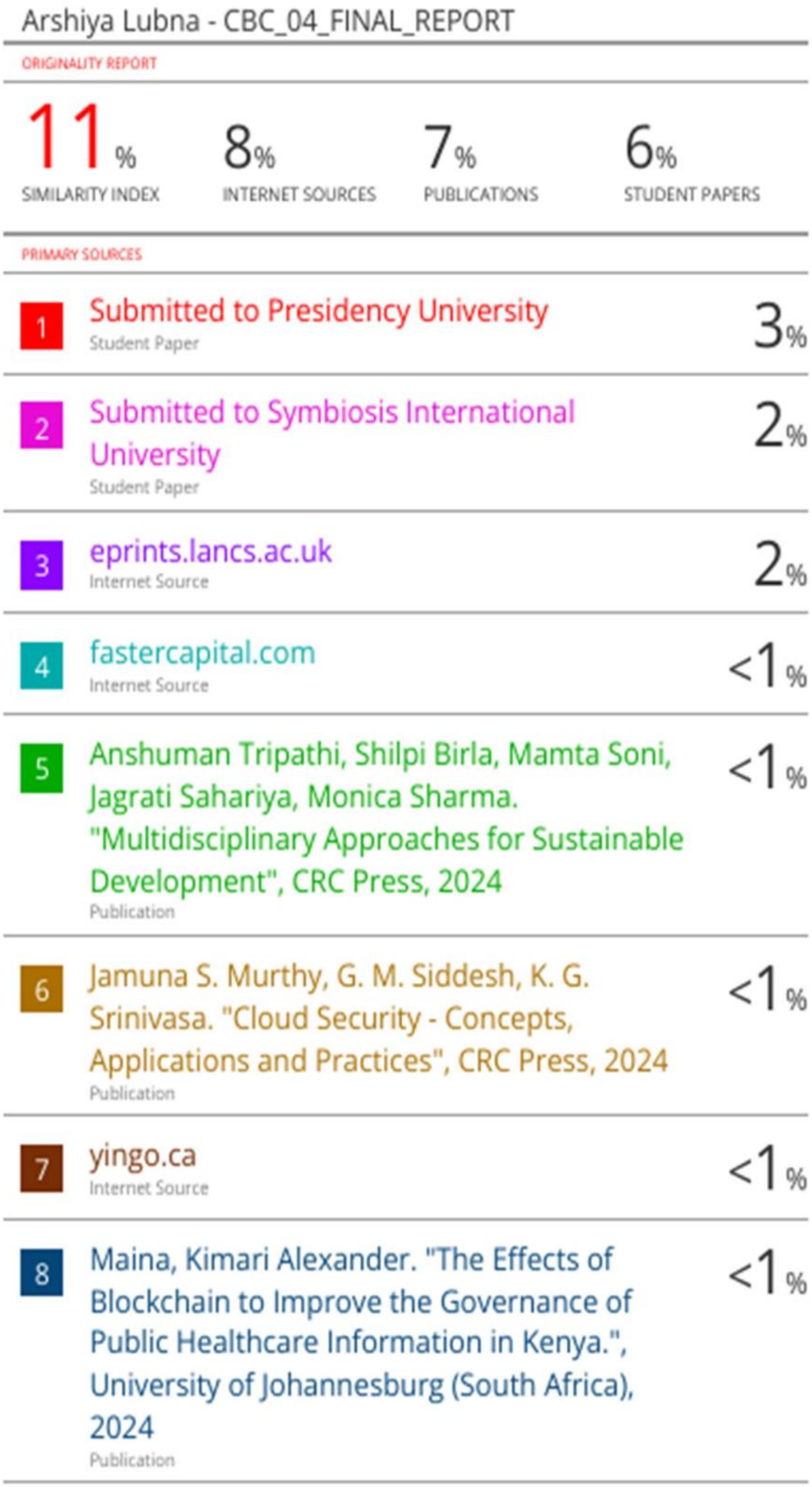
In safeguarding vulnerable and marginalized users who are usually targeted by fake accounts, scams, and harassment online. Through AI and blockchain, the system provides equal access to safer online environments, minimizes discrimination and impersonation risks, and facilitates digital inclusion across various communities. Its transparency, support for multiple languages, and operation in low-resource environments help bridge the digital divide and facilitate equitable participation in online platforms for all users.

SDG-16: Peace, Justice, and Strong Institutions

A system that employs AI-based fake profile detection and blockchain-based transparent reporting has the potential to create safer and more responsible online environments. AI systems can spot fake accounts by examining behavior and content, while blockchain provides tamper-proof reporting and open moderation. This fosters trust, safeguards the rights of users, facilitates access to justice, and enhances digital governance, leading to peaceful and inclusive societies.

SDG-17: Partnerships for the Goals

Fostering collaboration between governments, social media platforms, academic institutions, and civil society to combat digital identity threats. By leveraging AI and blockchain, the project encourages technology and knowledge sharing, promotes cross-border cooperation, and enables secure, transparent reporting mechanisms. Through multi-stakeholder engagement and open innovation, it strengthens global efforts to create safer online environments and supports sustainable digital development.



Arshiya Lubna - CBC_04_FINAL_REPORT

ORIGINALITY REPORT

11%	8%	7%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Presidency University Student Paper	3%
2	Submitted to Symbiosis International University Student Paper	2%
3	eprints.lancs.ac.uk Internet Source	2%
4	fastercapital.com Internet Source	<1%
5	Anshuman Tripathi, Shilpi Birla, Mamta Soni, Jagrati Sahariya, Monica Sharma. "Multidisciplinary Approaches for Sustainable Development", CRC Press, 2024 Publication	<1%
6	Jamuna S. Murthy, G. M. Siddesh, K. G. Srinivasa. "Cloud Security - Concepts, Applications and Practices", CRC Press, 2024 Publication	<1%
7	yingo.ca Internet Source	<1%
8	Maina, Kimari Alexander. "The Effects of Blockchain to Improve the Governance of Public Healthcare Information in Kenya.", University of Johannesburg (South Africa), 2024 Publication	<1%