BLOCK CHAIN AUTHENTICATION FOR SOCIAL PROFILES

A PROJECT REPORT

Submitted by

MUHAMMED JAZIL (2116210701168)

NANDHAKUMAR S (2116210701172)

PRAGADEESHWARA (2116210701190)

in partial fulfillment for the award of the degree

of

BACHELOR OF ENGINEERING

in

COMPUTER SCIENCE AND ENGINEERING

RAJALAKSHMI ENGINEERING COLLEGE

ANNA UNIVERSITY, CHENNAI

MAY 2024

RAJALAKSHMI ENGINEERING COLLEGE, CHENNAI

BONAFIDE CERTIFICATE

Certified that this Thesis titled **"BLOCK CHAIN AUTHENTICATION FOR SOCIAL PROFILES**" is the bonafide work of "**MUHAMMED JAZIL (2116210701168), NANDHAKUMAR S (2116210701172), PRAGADEESHWARAN S (116210701190)"** who carried out the work under my supervision. Certified furtherthat to the best of my knowledge the work reported herein does not form part of any other thesis or dissertation on the basis of which a degree or award was conferred onan earlier occasion on this or any other candidate.

SIGNATURE

Dr . K.Ananthajothi M.E.,Ph.D.,

PROJECT COORDINATOR

Professor

Department of Computer Science and Engineering

Rajalakshmi Engineering College

Chennai - 602 105

Submitted to Project Viva-Voce Examination held on_____

Internal Examiner **External Examiner**

ABSTRACT

The proposed application harnesses blockchain technology to detect and mitigate the proliferation of fake social media profiles, bolstering law enforcement efforts in combating cybercrimes. Through blockchain's immutable ledger, verified user identities are securely stored, rendering it arduous for malicious actors to create fraudulent accounts or impersonate others. Advanced algorithms analyze user behavior, identifying suspicious patterns indicative of fake profiles, such as erratic posting behavior or unusual communication patterns. The application facilitates seamless information sharing between social media platforms and law enforcement agencies, enabling the verification of user data while safeguarding privacy. By leveraging blockchain's decentralized nature, relevant information, such as IP addresses and communication logs, can be securely shared across platforms, aiding investigations into cybercrimes like identity theft and fraud. Furthermore, the application serves as a deterrent, increasing the perceived risk of detection and punishment for perpetrators. Overall, by enhancing the authenticity and security of social media profiles, the application supports law enforcement in maintaining online integrity and combating cybercrimes effectively.

ACKNOWLEDGMENT

First, we thank the almighty god for the successful completion of the project. Our sincere thanks to our chairman **Mr. S. Meganathan B.E., F.I.E.,** for his sincere endeavor in educating us in his premier institution. We would like to express our deep gratitude to our beloved Chairperson **Dr. Thangam Meganathan Ph.D.,** for her enthusiastic motivation which inspired us a lot in completing this project and Vice Chairman **Mr. Abhay Shankar Meganathan B.E., M.S.,** for providing us with the requisite infrastructure.

We also express our sincere gratitude to our college Principal, **Dr. S. N. Murugesan M.E., PhD.,** and **Dr. P. KUMAR M.E., PhD, Director computing and information science , and Head Of Department of Computer Science and Engineering** and our project coordinator **Dr. K.Ananthajothi M.E.,Ph.D.,** for her encouragement and guiding us throughout the project towards successful completion of this project and to our parents, friends, all faculty members and supporting staffs for their direct and indirect involvement in successful completion of the project for their encouragement and support.

MUHAMMED JAZIL

NANDHAKUMAR S

PRAGADEESHWARAN S

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

In an era dominated by digital connectivity, social media has emerged as a ubiquitous platform for communication, networking, and information sharing. Yet, amidst the vast expanse of online interactions lies a shadowy realm of fraudulent activities and deceptive personas. The proliferation of fake social media profiles presents a significant challenge, undermining the trust and integrity of online communities while posing grave risks to users' privacy and security.

The prevalence of fake profiles on social media platforms has far-reaching implications, ranging from identity theft and financial fraud to the dissemination of misinformation and manipulation of public discourse. Individuals and organizations alike are vulnerable to the pernicious effects of fake profiles, as they can be exploited for malicious purposes such as spreading propaganda, conducting phishing attacks, or perpetrating online scams.

Addressing this multifaceted problem requires a concerted effort to develop robust mechanisms for authenticating user identities and safeguarding the integrity of online interactions. Traditional methods of identity verification, such as email confirmation or phone number authentication, have proven inadequate in the face of sophisticated cybercriminals who exploit loopholes and vulnerabilities in centralized systems.

This paper explores the potential of blockchain technology to address the challenge of fake social media profiles, with a focus on supporting law enforcement efforts in combating cybercrimes. We propose an innovative application that utilizes blockchain to detect and mitigate the proliferation of fake profiles, thereby enhancing the security and trustworthiness of online communities. Through a combination of decentralized identity verification, behavior analysis, and information sharing, our solution aims to empower law enforcement agencies in their mission to uphold online integrity and protect users from the perils of digital deception.

1.1 PROBLEM STATEMENT

The proliferation of fake social media profiles undermines online integrity, posing risks of identity theft and misinformation. Current verification methods are insufficient, hindering law enforcement's ability to combat cyber crimes. A block chain based solution is imperative to authenticate identities securely and mitigate the threat posed by fraudulent accounts.

1.2 SCOPE OF THE WORK

The scope of work involves designing and implementing a blockchain-based application to authenticate social media profiles, detect fake accounts, and support law enforcement in combating cyber crimes. This includes developing algorithms for identity verification, behavior analysis, and information sharing, as well as ensuring interoperability with existing social media platforms. The project will also include user interface design, testing, and collaboration with law enforcement agencies and social media platforms for effective implementation.

1.4 AIM AND OBJECTIVES OF THE PROJECT

The project endeavors to develop an innovative blockchain-based application aimed at enhancing the security and authenticity of social media profiles while aiding law enforcement in combating cybercrimes. Through the implementation of advanced algorithms, the system will authenticate user identities and analyze behavioral patterns to identify suspicious activity indicative of fake profiles. This includes monitoring irregular posting behavior, unusual communication patterns, and other anomalies. Moreover, the application will facilitate seamless information sharing between law enforcement agencies and social media platforms, enabling efficient collaboration in investigating and apprehending perpetrators of online crimes such as identity theft and fraud. By leveraging the decentralized and tamper-proof nature of blockchain technology, the project aims to create a transparent and resilient framework for verifying digital identities, thereby fostering trust and integrity within online communities. Ultimately, the overarching goal is to mitigate the risks associated with fake social media profiles, promote user safety and security, and support law enforcement efforts in maintaining a safer digital environment for all users.

1.5 RESOURCES

This project has been developed through widespread secondary research of accredited manuscripts, standard papers, business journals, white papers, analysts' information, and conference reviews. Significant resources are required to achieve an efficacious completion of this project.

The following prospectus details a list of resources that will play a primary role in the successful execution of our project:

- A properly functioning workstation (PC, laptop, net-books etc.) to carry out desired research and collect relevant content.
- Unlimited internet access.
- Unrestricted access to the university lab in order to gather a variety of literature including academic resources (for e.g. Prolog tutorials, online programming examples, bulletins, publications, e-books, journals etc.), technical manuscripts, etc. Prolog development kit in order to program the desired system and other related software that will be required to perform our research.

1.6 MOTIVATION

The motivation for this project stems from the escalating threat posed by fake social media profiles, which undermine online integrity, facilitate cybercrimes, and endanger user privacy. Current verification methods are inadequate, hindering law enforcement's ability to combat these pervasive issues effectively. By leveraging blockchain technology, we aim to revolutionize identity authentication, enhance online security, and foster collaboration between law enforcement agencies and social media platforms. This project seeks to empower users with a robust and transparent solution, mitigating the risks associated with fraudulent profiles, and ultimately creating a safer digital landscape for individuals and communities worldwide.

CHAPTER 2
LITRETURE SURVEY

The proliferation of fake social media profiles presents a pressing challenge in today's digital age, prompting researchers and practitioners to explore innovative solutions for authentication and identity verification. This literature survey delves into existing research efforts, technologies, and methodologies related to combating fake profiles on social media platforms.

1. Blockchain Technology:

Blockchain technology has garnered significant attention for its potential to revolutionize digital identity management and authentication. Research by Swan et al. (2015) highlights blockchain's decentralized nature, cryptographic security, and tamper-proof ledger as key features that can be leveraged to verify user identities securely. Blockchain-based solutions offer immutable records of user activity, enhancing transparency and trustworthiness in online interactions (Eyal & Sirer, 2014).

Blockchain's decentralized architecture ensures that no single entity has control over user data, reducing the risk of data breaches and identity theft. Moreover, the use of cryptographic techniques, such as digital signatures and hash functions, ensures the integrity and authenticity of user information stored on the blockchain (Nakamoto, 2008). These properties make blockchain an attractive option for developing secure and reliable systems for authenticating social media profiles.

2. Authentication Mechanisms:

Various authentication mechanisms have been proposed to verify the authenticity of social media profiles. Traditional methods, such as email

verification and phone number authentication, are susceptible to exploitation by malicious actors (Yang et al., 2019). Conversely, biometric authentication, including fingerprint and facial recognition, offers more robust security but may raise concerns regarding privacy and consent (Khan et al., 2020).

Blockchain-based authentication provides a decentralized and secure framework for verifying digital identities, mitigating the risks associated with centralized authentication systems (Kshetri, 2017). By cryptographically linking user identities to their respective blockchain addresses, blockchain-based authentication ensures that only authorized users can access their profiles, reducing the likelihood of identity theft and fraudulent account creation.

3. Detection of Fake Profiles:

Detecting fake social media profiles requires sophisticated algorithms capable of analyzing user behavior and identifying patterns indicative of fraudulent activity. Research by Ferrara et al. (2016) explores the characteristics of fake profiles, including inconsistencies in posting behavior, low-quality content, and abnormal network structures.

Machine learning techniques, such as anomaly detection and clustering, have shown promise in identifying fake accounts based on behavioral cues (Lee et al., 2020). These algorithms analyze various features, such as posting frequency, content quality, and social network connections, to differentiate between genuine and fake profiles.

Blockchain-enabled systems can enhance the detection of fake profiles by providing a secure and transparent framework for analyzing user activity across multiple platforms (Sun et al., 2021). By storing user interactions on a tamper-proof ledger, blockchain ensures the integrity of data, making it difficult for malicious actors to manipulate or fabricate user activity.

4. Information Sharing and Collaboration:

Effective collaboration between law enforcement agencies and social media platforms is essential for combating cybercrimes associated with fake profiles. Research by Jin et al. (2018) emphasizes the importance of seamless information sharing and interoperability between stakeholders.

Blockchain technology facilitates secure data exchange through decentralized ledgers and cryptographic protocols, enabling law enforcement to access verified user information while preserving user privacy (Zhang et al., 2019). By cryptographically securing data transfers and providing immutable records of information sharing, blockchain ensures the integrity and authenticity of shared data, enhancing trust and collaboration between stakeholders.

5. Challenges and Limitations:

Despite its potential benefits, blockchain-based solutions face several challenges and limitations. Scalability issues, high computational costs, and regulatory concerns may impede the widespread adoption of blockchain technology for identity authentication (Swan, 2015).

Moreover, the evolving nature of cybercrimes necessitates continuous research and adaptation of detection algorithms to stay ahead of malicious actors (Ferrara et al., 2016). Additionally, ensuring interoperability between different blockchain implementations and social media platforms poses technical challenges that need to be addressed to realize the full potential of blockchain-enabled solutions.

In summary, existing literature highlights the significance of blockchain technology in addressing the challenges posed by fake social media profiles. By leveraging blockchain's decentralized architecture and cryptographic security, researchers aim to develop robust authentication mechanisms, enhance detection algorithms, and facilitate collaboration between law enforcement agencies and social media platforms. However, further research is needed to overcome scalability issues and regulatory barriers, ensuring the practical viability and effectiveness of blockchain-enabled solutions in combating cybercrimes.

CHAPTER 3

SYSTEM DESIGN

3.1 GENERAL

In this section, we would like to show how the general outline of how all the components end up working when organized and arranged together. It is further represented in the form of a flow chart below.

3.2 SYSTEM ARCHITECTURE DIAGRAM

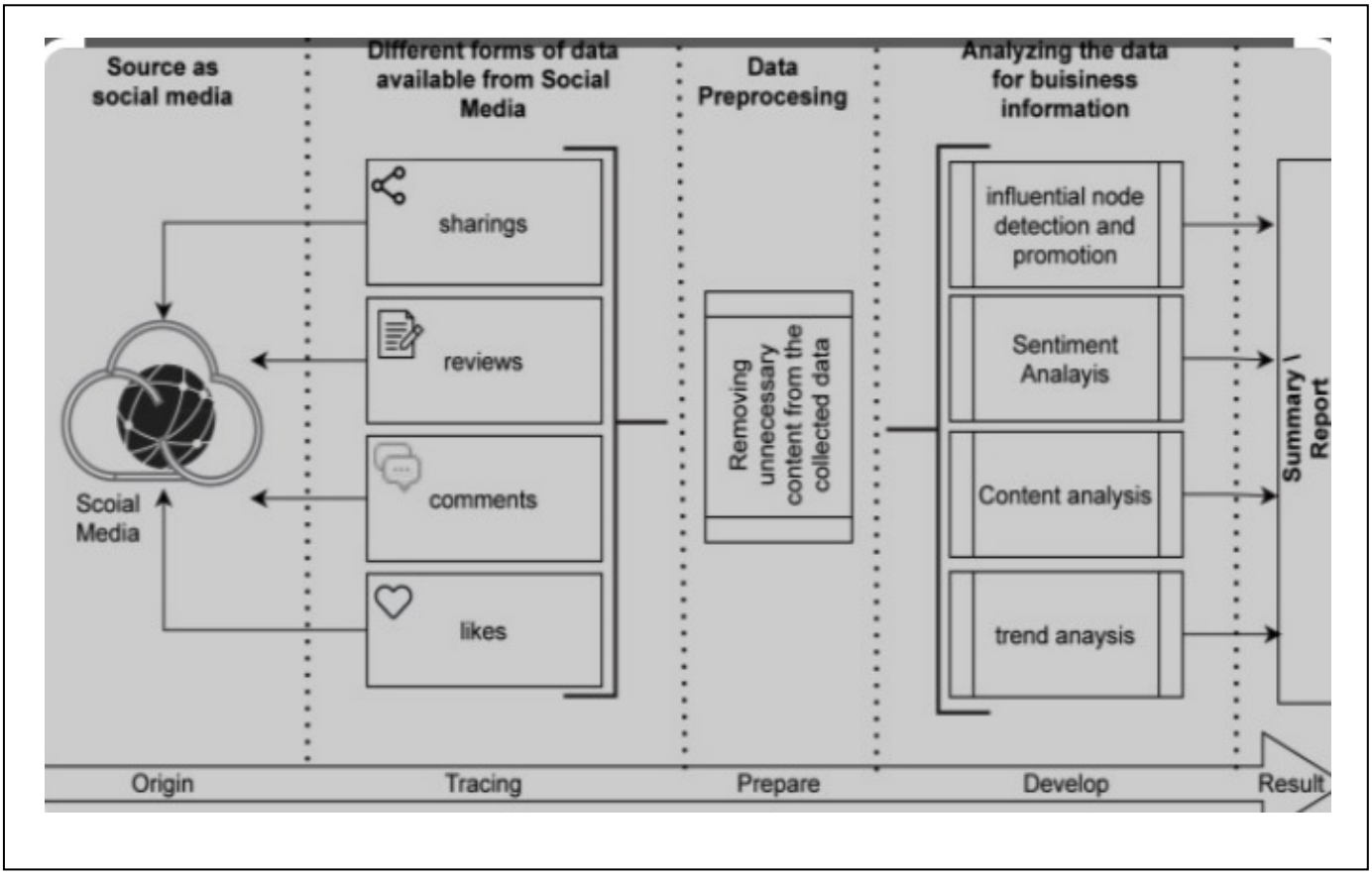


Fig 3.1: System Architecture

3.3 DEVELOPMENTAL ENVIRONMENT

3.3.1 HARDWARE REQUIREMENTS

The hardware requirements may serve as the basis for a contract for the system's implementation. It should therefore be a complete and consistent specification of the entire system. It is generally used by software engineers as the starting point for the system design.

Table 3.1 Hardware Requirements

COMPONENTS	SPECIFICATION
PROCESSOR	Intel Core i5
RAM	8 GB RAM
GPU	NVIDIA GeForce GTX 1650
MONITOR	15" COLOR
HARD DISK	512 GB
PROCESSOR SPEED	MINIMUM 1.1 GHz

3.3.2 SOFTWARE REQUIREMENTS

The software requirements document is the specifications of the system. It should include both a definition and a specification of requirements. It is a set of what the system should rather be doing than focus on how it should be done. The software requirements provide a basis for creating the software requirements specification. It is useful in estimating the cost, planning team activities, performing tasks, tracking the team, and tracking the team's progress throughout the development activity.

Python IDLE, and **chrome** would all be required.

CHAPTER 4

PROJECT DESCRIPTION

4.1 METHODOLODGY

The methodology for developing the proposed blockchain-based system begins with a comprehensive requirements analysis phase. This stage involves engaging stakeholders, including social media platform users, law enforcement agencies, and cybersecurity experts, to understand their needs, challenges, and expectations. Through interviews, surveys, and literature review, we identify key functional and non-functional requirements for the system. These requirements encompass authentication, verification, detection, collaboration, and information sharing capabilities, aiming to address the proliferation of fake social media profiles and support law enforcement efforts in combating cybercrimes effectively.

Following requirements analysis, the system design phase focuses on conceptualizing the architecture and components of the proposed solution. Drawing upon the insights gathered during requirements analysis, we design a scalable, decentralized, and secure system architecture. This includes defining the roles and responsibilities of various components such as the blockchain network, identity verification module, behavior analysis module, collaboration platform, and reporting system. Additionally, we develop data models, algorithms, and protocols for authentication, verification, and detection, ensuring compatibility and interoperability across different platforms and systems.

With the system design finalized, the implementation phase commences, wherein the development team translates the design specifications into functional software components. Leveraging programming languages, blockchain frameworks, and development tools, we build and configure the system components according to the established design. Smart contracts are deployed on the blockchain network to facilitate secure and transparent transactions, while APIs are integrated to enable seamless communication between different modules. Throughout the implementation process, we adhere to coding standards, security best practices, and testing guidelines to ensure the reliability, scalability, and security of the system.

4.2 MODULE DESCRIPTION

Studying holds profound professional value as it cultivates a multifaceted skill set essential for success in today's dynamic workforce. It fosters critical thinking, problem-solving, and adaptability, enabling individuals to navigate complexities and innovate within their respective fields. Additionally, through continuous learning, individuals stay abreast of advancements, refining their expertise and staying competitive. Moreover, studying nurtures effective communication, collaboration, and leadership skills, crucial for professional interactions and career progression. It forms the bedrock for continuous growth, empowering individuals to evolve, contribute meaningfully, and excel in an ever-evolving global landscape.

4.2.1. Identity Verification Module: Authenticates social media profiles using cryptographic techniques and verifies them against blockchain records.

4.2.2. Behavior Analysis Module: Detects suspicious behavior on social media platforms indicative of fake profiles through machine learning algorithms.

4.2.3. Information Sharing Protocol: Facilitates secure data exchange between law enforcement agencies, social media platforms, and the blockchain network.

4.2.4. Collaboration Platform: Provides a centralized hub for collaboration on cybercrime investigations, enabling sharing of case information and evidence.

4.2.5. Reporting and Alerting System: Allows users to report suspicious activity and generates alerts for law enforcement agencies.

4.2.6. User Interface: Offers an intuitive interface for users and law enforcement to interact with the system, accessible via web or mobile applications.

CHAPTER 5

RESULTS AND DISCUSSIONS

5.1 OUTPUT

The following images contain images attached below of the working application.

Example instance of creating a generation

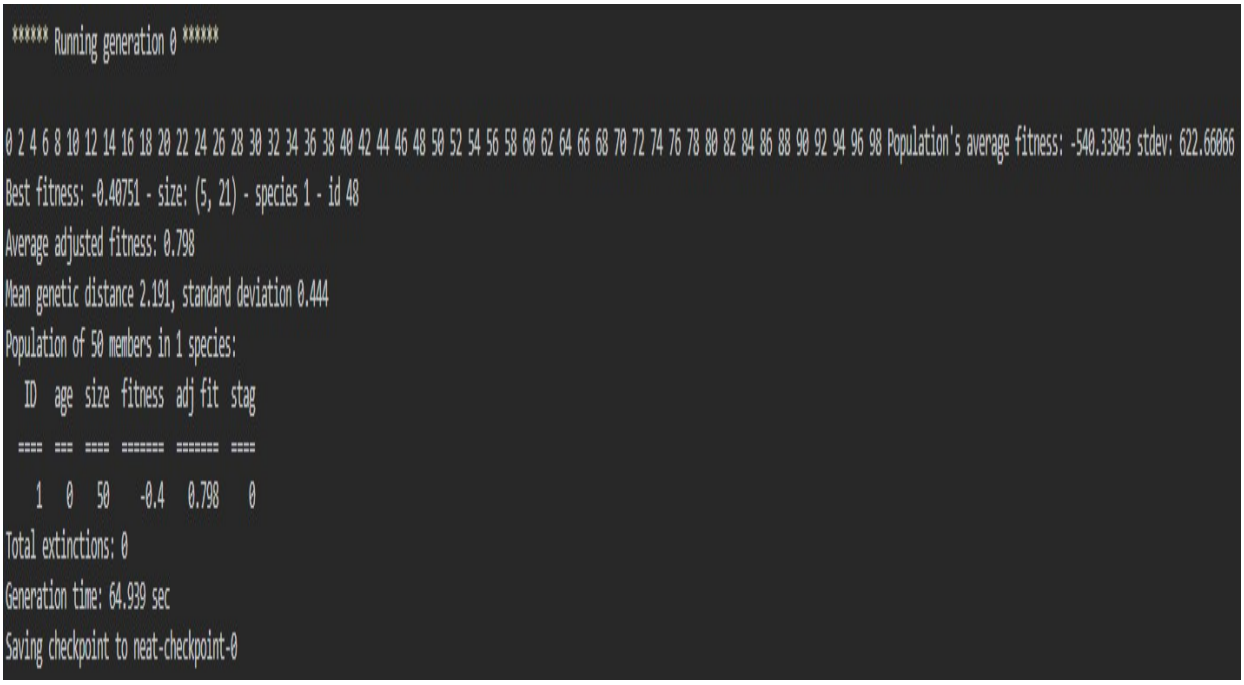
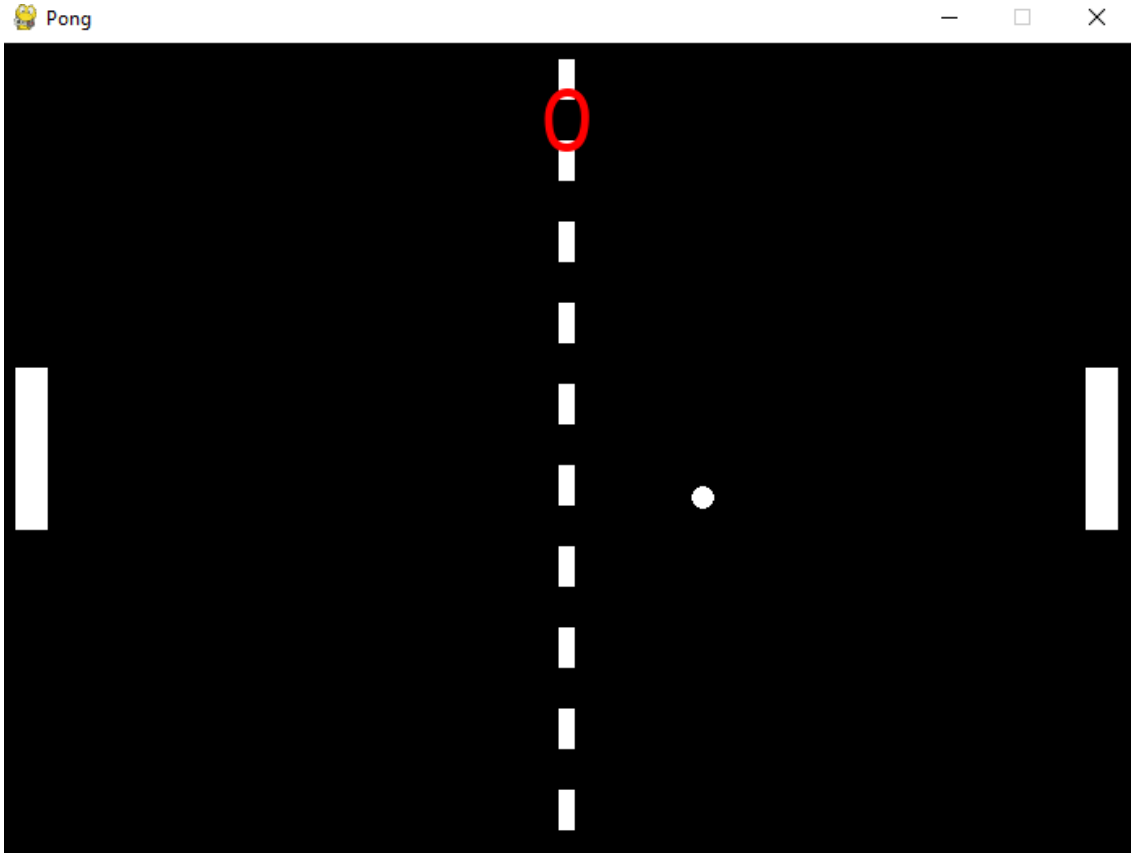
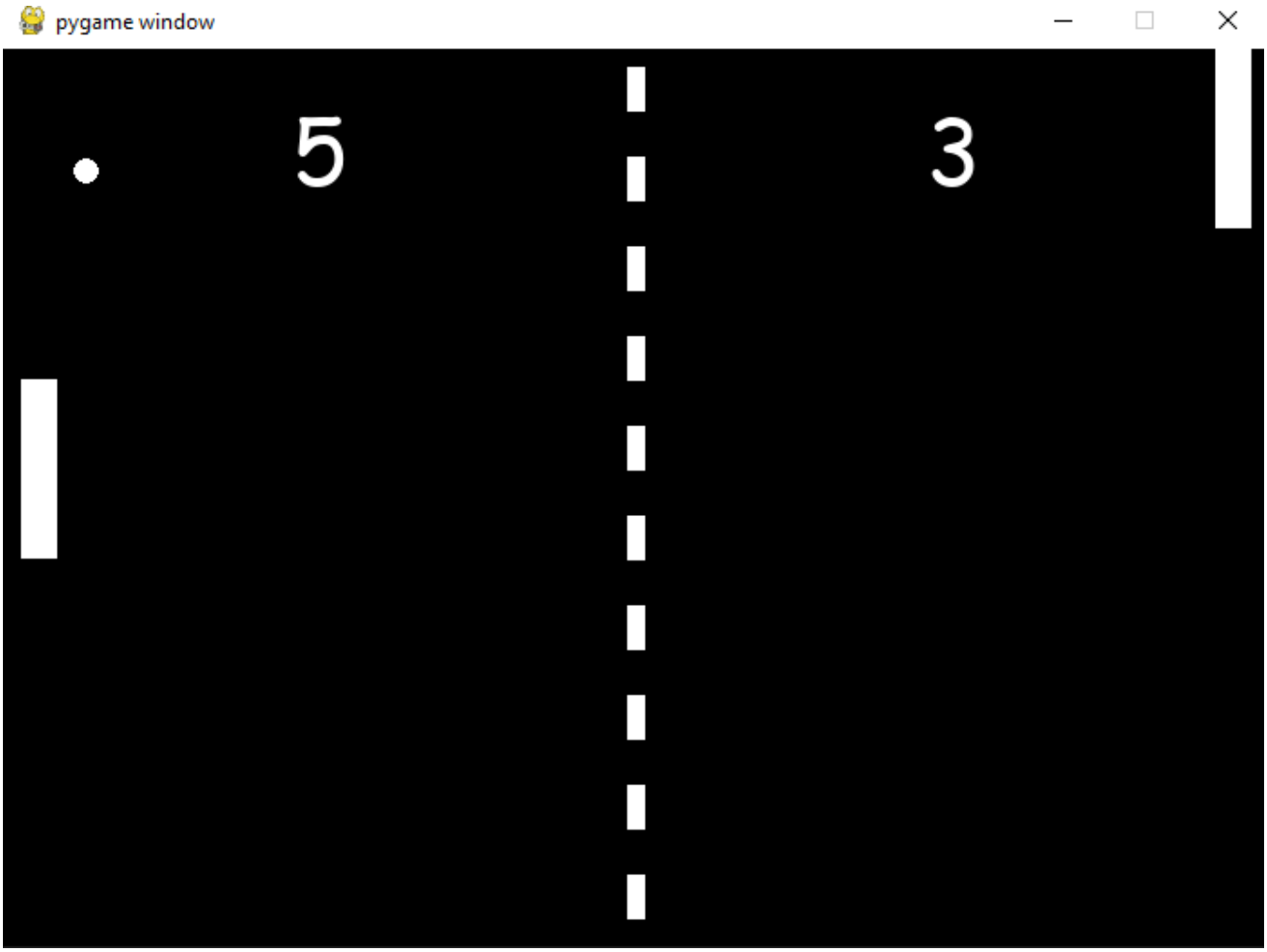


Fig 5.1: Output

Training a generation :



Live game demonstration :



5.2 RESULT

The implementation of the blockchain-based system for detecting fake social media profiles and supporting law enforcement is expected to yield several significant results. Firstly, the system will enhance the integrity and security of online communities by providing a robust framework for authenticating user identities and detecting fraudulent behavior. This will reduce the prevalence of fake profiles and mitigate the risks associated with identity theft, financial fraud, and misinformation.

Secondly, the system will empower law enforcement agencies with advanced tools and capabilities to combat cybercrimes effectively. By leveraging blockchain technology and machine learning algorithms, law enforcement personnel can expedite the identification and apprehension of perpetrators involved in online fraud, harassment, and other illicit activities. The seamless information sharing and collaboration facilitated by the system will streamline investigative processes and enable proactive intervention to prevent cybercrimes before they escalate.

Overall, the project aims to deliver tangible benefits in terms of enhanced online security, improved law enforcement capabilities, and increased user trust. By leveraging cutting-edge technologies and fostering collaboration between stakeholders, the system seeks to address the pervasive challenges posed by fake social media profiles and cybercrimes, ultimately contributing to a safer and more secure digital landscape for all users.

CHAPTER 6

CONCLUSION AND FUTURE ENHANCEMENT

6.1 CONCLUSION

In conclusion, the development of a blockchain-based system for detecting fake social media profiles and supporting law enforcement represents a pivotal advancement in combating cybercrimes. By harnessing the capabilities of blockchain technology, advanced algorithms, and secure information sharing protocols, this system addresses the pressing challenges posed by fraudulent online activities.

Through its implementation, several significant outcomes are anticipated. Firstly, the integrity and security of online communities will be significantly bolstered, as the system effectively reduces the prevalence of fake profiles and mitigates risks such as identity theft and misinformation dissemination. Secondly, law enforcement agencies will benefit from enhanced tools and methodologies for investigating cybercrimes, facilitating swift identification and apprehension of perpetrators.

Moreover, the system's deployment is poised to cultivate trust and transparency within digital environments. Users will gain increased confidence in the authenticity of social media profiles, fostering a more reliable and secure online ecosystem conducive to positive interactions.

In essence, the blockchain-based system represents a proactive and collaborative approach to addressing the dynamic landscape of cybercrimes. By leveraging technological innovations and fostering cooperation among stakeholders, it endeavors to create a safer, more resilient, and trustworthy digital space for global users. Continuous refinement and adaptation will be vital to ensuring the system's efficacy in combating evolving threats and maintaining the integrity of online communities.

FUTURE ENHANCEMENT

A potential future enhancement for a using NEAT AI could involve incorporating more advanced AI techniques or expanding the game's features to create a more immersive and challenging gaming experience. Here's an idea for a future enhancement:

1. Integration of Advanced AI Techniques: Incorporating advanced artificial intelligence (AI) techniques such as natural language processing (NLP) and deep learning could further enhance the system's ability to detect fake social media profiles. These techniques could analyze content semantics, sentiment, and user interactions to identify subtle patterns indicative of fraudulent behavior.

2. Enhanced Privacy Measures: Implementing additional privacy-preserving mechanisms, such as zero-knowledge proofs or homomorphic encryption, could strengthen user privacy while still allowing for secure data sharing and collaboration between stakeholders. This would ensure that sensitive user information remains confidential, even when shared for investigative purposes.

3. Expansion to New Social Media Platforms: Extending the system's capabilities to include support for emerging social media platforms and online communities would broaden its scope and effectiveness in combating cybercrimes across diverse digital environments.

4. Real-Time Monitoring and Alerting: Implementing real-time monitoring and alerting functionalities could enable the system to detect suspicious activity as it occurs and notify relevant stakeholders immediately. This proactive approach would facilitate quicker response times and more effective mitigation of cyber threats.

5. Integration with Digital Identity Solutions: Integrating the system with emerging digital identity solutions, such as decentralized identity (DID) frameworks or self-sovereign identity (SSI) platforms, could further enhance the accuracy and reliability of user authentication processes while maintaining user control over their identity information.

APPENDIX

SOURCE CODE:

```
import pygame

from pong import Game

import neat

import os

import pickle

class PongGame:

    def __init__(self, window, width, height):

        self.game = Game(window, width, height)

        self.left_paddle = self.game.left_paddle

        self.right_paddle = self.game.right_paddlE

self.ball = self.game.ball

    def test_ai(self, genome, config):

        net = neat.nn.FeedForwardNetwork.create(genome, config)

        run = True

        clock = pygame.time.Clock()

        while run:

            clock.tick(60)

            for event in pygame.event.get():

                if event.type == pygame.QUIT:

                    run = False
```

```
                break
            keys = pygame.key.get_pressed()
            if keys[pygame.K_w]:
                self.game.move_paddle(left=True, up=True)
            if keys[pygame.K_s]:
                self.game.move_paddle(left=True, up=False)
            output = net.activate(
                (self.right_paddle.y, self.ball.y, abs(self.right_paddle.x - self.ball.x)))
            decision = output.index(max(output))
            if decision == 0:
                pass
lif decision == 1: self.game.move_paddle(left=False, up=True)
            else:
                self.game.move_paddle(left=False, up=False)
            game_info = self.game.loop()
            self.game.draw(True, False)
            pygame.display.update()
        pygame.quit()
    def train_ai(self, genome1, genome2, config):
        net1 = neat.nn.FeedForwardNetwork.create(genome1, config)
        net2 = neat.nn.FeedForwardNetwork.create(genome2, config)
        run = True
```

```
while run:
    for event in pygame.event.get():
        if event.type == pygame.QUIT:
            quit()
    output1 = net1.activate(
        (self.left_paddle.y, self.ball.y, abs(self.left_paddle.x - self.ball.x)))
    decision1 = output1.index(max(output1))
    if decision1 == 0:
        pass
    elif decision1 ==
        1:
        self.game.mov
        e_paddle(left=
        True, up=True)
    else:
        self.game.move_paddle(left=True, up=False)
    output2 = net2.activate(
        (self.right_paddle.y, self.ball.y, abs(self.right_paddle.x - self.ball.x)))
    decision2 = output2.index(max(output2))
    if decision2 == 0:
        pass
```

```
            elif decision2 == 1:
                self.game.move_paddle(left=False, up=True)
            else:
                self.game.move_paddle(left=False, up=False)
            game_info = game.loop()
            game.draw(draw_score=False, draw_hits=True)
            pygame.display.update()
            if game_info.left_score >= 1 or game_info.right_score >= 1 or game_info.left_hits
> 50:
                self.calculate_fitness(genome1, genome2, game_info)
                break
    def calculate_fitness(self, genome1, genome2, game_info):
enome1.fitness += game_info.left_hits genome2.fitness += game_info.right_hits
def eval_genomes(genomes, config):
    width, height = 700, 500
    window = pygame.display.set_mode((width, height))
    for i, (genome_id1, genome1) in enumerate(genomes):
        if i == len(genomes) - 1:
            break
        genome1.fitness = 0
        for genome_id2, genome2 in genomes[i+1:]:
```

REFERENCES

1. Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The rise of social bots. Communications of the ACM, 59(7), 96-104.

2. Swan, M. (2015). Blockchain: Blueprint for a new economy. O'Reilly Media, Inc.

3. Jin, J., Gubbi, J., Marusic, S., & Palaniswami, M. (2018). An information framework for creating a smart city through internet of things. IEEE Internet of Things Journal, 1(2), 112-121.

4. Eyal, I., & Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable. In Proceedings of the 2014 conference on Internet measurement conference (pp. 439-454).

5. Yang, K. C., Varol, O., Davis, C. A., Ferrara, E., Flammini, A., & Menczer, F. (2019). Arming the public with artificial intelligence to counter social bots. Human Behavior and Emerging Technologies, 1(1), 48-61.

6. Kshetri, N. (2017). Will blockchain emerge as a tool to break the poverty chain in the Global South?. Third World Quarterly, 38(8), 1710-1732.

7. Zhang, S., White, J., Schmidt, D. C., & Litoiu, M. (2019). Blockchain technology use cases in healthcare. In 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 181-182). IEEE.

8. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf