DATA SECURITY WITH BLOCK CHAIN & AI

Anusha nallanagula [1], Dr. Deepak sukheeja [2], Dr. Bvkiranmayee [3]

[1] Student , Department of CSE, Vallurupalli Nageswara Rao Vignana Jyothi Institute of Engineering &Technology , Bachupally, Hyderabad, Telangana, India

Email- nallanagulaanusha444@gmail.com

[2]Associate Professor, Department of CSE, Vallurupalli Nageswara Rao Vignana Jyothi Institute of Engineering &Technology, Bachupally, Hyderabad,Telangana, India

[3]Professor,Department of CSE, Vallurupalli Nageswara Rao Vignana Jyothi Institute of Engineering &Technology , Bachupally, Hyderabad, Telangana, India

Email: Kiranmayee……..@ vnrvjiet.in

ABSTRACT

In today's digital world, Artificial Intelligence has provided ways of dealing with the ever-increasing cyber attacks and infections, privacy issues, and data breaches. Of course, the rise in cyber threats makes AI capable of infiltration into important areas, such as fraud detection and secure transactions, making our online life better and more reliable. AI technologies are also changing how we interact with the internet; from simple text searches to intuitive voice-based commands and experiences, like the voice assistant, Cortana.As tasks have been taken over by automation, the general trend has been for security to get smarter. AI is an integral component of today's data protection and enhanced monitoring systems in devices, smartphones, and more extensive surveillance networks. It's helping protect what matters most — our privacy and security.More specifically, though, this helps secure the digital world more with blockchain technology. In essence, it provides a decentralized and tamper-proof way of recording information, which guarantees that this information remains unaltered and trustworthy. When integrated into AI, blockchain creates systems that can quickly identify and address security threats while keeping transactions transparent and secure.The use of AI and blockchain together provides a means for enhancing data security. From facial recognition, to the security of blockchain's transparent ledger, we are creating new ways in which personal data and business data can be safeguarded against increased digital risks. Together, they provide a potent solution to these security challenges of today.

Keywords: Artificial Intelligence (AI) , Cybersecurity , Data Breaches , Privacy Protection, Blockchain Technology

I INTRODUCTION

With advancements in technology, it has brought down the older ways of securing entry into the electronic world such as keypads and passwords. The most exciting thing to pop up from these advancements has been the utilization of AI in voice recognition. Those who have even gotten a chance to use voice assistants such as Google Assistant or Amazon Alexa would agree that it is how easy it makes for humans to control their devices with words. Voice recognition will one day take away the older ways of locking a device or authentication.

However, with such advances, security comes into the question. Everything which is now in their hands needs to be ensured in order to guard sensitive information, so that nobody can get unauthorised access. Here is where blockchain helps in its role. Blockchain can give a guarantee regarding the

security as well as the non-tamperability of data, letting the user enjoy full control over his personal information. It's like an open digital ledger where anyone can have a view, but nobody can alter it.It integrates AI voice recognition capabilities and the power of blockchain. Such an integration allows it to establish a system where voice can be identified and confirmed in return and kept securely within a block in blockchain for long time preservation without potential changes and tampering, meaning voiceprints remain protected from possible invasion without any of the parties involved approval.

Our project is based on improvement in digital security. We are going to work on the system which authenticates your identity through voice but keeps your private data safe and secured. In this approach, the layers of blockchain place your information safely, and no one can tamper with it. It's much easier and dependable security due to our ever-growing online life.This project will demonstrate how the integration of AI and blockchain brings more strength in security while making it easier and more user-friendly for people to interact with digital systems.

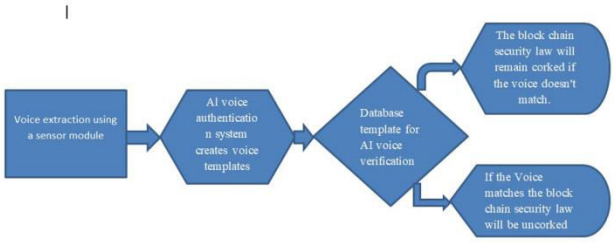

Fig 1 : The development of a block chain-based speech template for authentication.

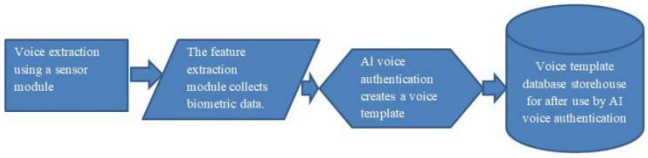

Fig 2 : speech verification using a Block chain databasetemplate.

II .LITERATURE SURVEY

Author(s) & Year	Title	Explanation
Kaur, P., Krishan, K., Sharma, S.K., and Kanchan, T. (2020)	Facial-Recognition Algorithms: A Literature Review	Provides a review of facial recognition algorithms, discussing their applications, methodologies, challenges, and ethical issues related to security and biometric authentication.
Internet Crime Complaints Center (2021)	Internet Crime Report 2021	Highlights trends in cybercrime, focusing on online fraud, ransomware, and other malicious activities, with data on common internet crimes and security protection strategies.
Novinson, M. (2021)	The 10 Biggest Data Breaches of 2021	Presents the top 10 data breaches of 2021, analyzing the causes, scale, impact, and lessons learned from these incidents.
Krasnokutsky, E. (2021)	Artificial Intelligence (AI) Biometric Authentication for Enterprise Security	Explores AI's role in improving biometric authentication technologies like facial recognition and fingerprint scanning to enhance enterprise security.
Wolfond, G. (2017)	Blockchain Ecosystem for Digital Identity	Discusses the use of blockchain for managing digital identities, emphasizing its security, decentralization, and potential for improving service delivery in various sectors.

III .IMPLEMENTATION

1.Collection and Preprocessing of Voice Data

The first step of the process would involve getting voice recordings from a user. These recordings will be used for forming a biometric voice template of them. The voice data should have factors such as pitch, loudness, tone, and even the language being spoken. All of these factors help in creating a distinct voice template for a different individual. The speech patterns it records should be totally clear and varied for the best accuracy.Now that the recordings have been gathered, preprocessing is conducted to clean and standardize the audio. Preprocessing includes cleaning the audio for background noise and normalizing volume levels. Finally, key features such as pitch, tone, cadence, and speech style are extracted.

2.Develop a unique voice template

A biometric voice template is created by using the preprocessed voice recording. The characteristics of the voice include pitch, loudness, tone, and speech patterns of the person. These characteristics will be useful in the authentication process.It analyzes some voice recordings, and it builds the best voice template by only selecting the most relevant and clearest features for the template.In this third step, it tries to construct a template with which it should be able to match any future range of inputs from the user.

3. Stores the Voice Template on the Blockchain

The moment the voice template is ready, it needs to be stored securely. This is where blockchain technology comes into play. The voice template is stored in a blockchain database, hence making it secure and immutable. Once saved on the blockchain, the voice template cannot be changed and hence ensures integrity and security.

As a decentralized process, it becomes impossible for some unauthorized change to happen in the voice template. Data, therefore, remains free from any form of tampering or breach.

4.Voice Authentication using AI

The voice input gets captured when the user tries to authenticate by speaking into the system. Then the AI takes real-time voice input and takes it for comparison with the voice template that is kept in the blockchain.The AI looks at different factors such as pitch, loudness, and tone and checks if they match the template. If the voice matches the stored template, the system recognizes the user as genuine and grants access.

5. Blockchain for Voice Verification

In the blockchain-based system, the process of voice authentication operates in a non-tamperable manner. The system will not unlock unless voice verification is successful. Blockchain ensures that the step of voice verification is safe and cannot be tampered with.After the AI ascertains that the input bears a likeness with the voice template, it further authenticates with a private key. This only those with an access code for entry to the system are permitted to do.

6. Immutability and Security Using Blockchain

Since blockchain technology is immutable, that is, it cannot be changed, the voice verification process ensures no one can tamper with voice data once stored. This makes the system very secure because if someone tries to alter the voice template, it will be impossible due to blockchain's decentralized and tamper-resistant nature.

IV.ALGORITHMS USED

1. Facial Recognition Algorithms

Facial recognition is one of the major areas under AI-driven security. There are various algorithms through which computers identify faces. A few of them are as follows:

Convolutional Neural Networks (CNNs)

CNNs are a type of neural network explicitly designed to handle image data. They work by discovering the patterns and features that exist in the image like eyes, nose, and mouths and then compares these features to some known face.

Formula: For every convolution layer, the output will be calculated using this formula:

$$Y = \sigma(W * X + b)$$

- W is the filter (or kernel),
- X is the input image,
- b is the bias term,
- $*$ represents convolution,
- σ is an activation function like ReLU (Rectified Linear Unit).

Local Binary Patterns (LBP)

LBP is used to describe the texture of facial features by comparing pixel values with their neighbors. It converts images into binary numbers, which can then be used to identify faces.

$$LBP = \sum_{i=0}^{P-1} s(g_i - g_c) \cdot 2^i$$

Where:

- P is the number of neighboring pixels,
- g_i is the intensity of each neighboring pixel,
- g_c is the center pixel's intensity,
- $s(x)$ is a threshold function that outputs 1 if $x > 0$, otherwise 0.

2. AI in Cybersecurity : AI plays a huge role in detecting and preventing cyber-attacks by analyzing patterns in network behavior, identifying malicious activities, and ensuring data integrity.

Anomaly detection is used to find unusual patterns in data. These patterns may indicate a security threat, such as an intrusion or malware.

$$\text{Error} = \|X - \hat{X}\|$$

Where:

- X is the input data,
- $\hat{X}$ is the reconstructed data (output from the autoencoder).

Support Vector Machines (SVM)

SVM is a supervised learning algorithm that works well in classification tasks, such as distinguishing between normal and malicious activities on a network.

Formula: The decision boundary is found by maximizing the margin between the two classes, which is represented by:

$$f(x) = w^T x + b$$

Where:

- w is the weight vector,
- x is the input feature vector,
- b is the bias term.

3. Blockchain Algorithms

Blockchain is widely known for its secure, tamper-proof structure, and several algorithms help ensure the integrity and security of the blockchain.

Proof of Work (PoW)

This is the consensus algorithm used in Bitcoin and other cryptocurrencies. It requires participants to solve a complex mathematical puzzle to validate transactions.

Formula: PoW requires participants to find a value NNN such that the hash of the block meets a certain condition (e.g., starts with a number of zeros). The hash function is typically something like **SHA-256**, represented as:

$$H(N) = \text{SHA-256}(N)$$

Where:

H(N) is the hash of N,

The goal is to find N such that the hash satisfies the difficulty target (e.g., begins with "0000").

Merkle Trees

Merkle Trees are used to efficiently and securely verify the integrity of large sets of data in blockchain. Each node in the tree contains the hash of its children, and this structure allows for quick verification of data integrity.

Formula: The Merkle root is the hash at the top of the tree and is calculated by combining hashes in pairs recursively:

$$H_{\text{root}} = H(H(H(A)||H(B))||H(H(C)||H(D)))$$

Where:

- $H(A)$, $H(B)$, etc., are hashes of the data,
- $||$ denotes concatenation.

CONCLUSION

Traditional security using keypads are slowly being replaced by advanced AI-powered speech technology with advancement in technology. AI voice technology is expected to be the next major breakthrough for privacy and security. Voice assistants, like Google Assistant, are now available, and certainly security systems will soon incorporate such inventions. However, blockchain for such purposes of privacy and decentralization will still be a discussion topic going forward. Until the right policies on rights and responsibilities are identified, public information will not serve the purpose of identity detection of crimes or criminals-and only if machines are designed such that they decide to do things on their own. Future efforts will be crucial in developing high-performance systems that integrate successfully blockchain and voice authentication using artificial intelligence, a step toward further decentralized and trusted solutions.

REFERENCES

[1] Kaur, P., Krishan, K., Sharma, S.K. and Kanchan, T. (2020) Facial-Recognition Algorithms:

A Literature Review. Medicine, Science and the Law, 60, 131-139. https://doi.org/10.1177/0025802419893168

[2] Internet Crime Complaints Center (2021) Internet Crime Report 2021. Federal Bureau of Investigations.

https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

[3]Novinson. M. (2021) The 10 Biggest Data Breaches of 2021. CRN.https://www.crn.com/slide-shows/security/the-10-biggest-data-breaches-of-2021

[4]UK Finance (2021) Half Year Fraud Update.https://www.ukfinance.org.uk/system/files/Half-year-fraud-update-2021-FINAL.pdf

[5] Krasnokutsky. E. (2021) Artificial Intelligence (AI) Biometric Authentication for Enterprise Security.MobiDev.

https://mobidev.biz/blog/ai-biometrics-technology-authentication-verification-security

[6]Dilek, S.H., Çakır, H. and Aydın, M. (2015) Applications of Artificial Intelligence Techniques to Combating Cybercrimes: A Review. International Journal of Artificial Intelligence & Applications (IJAIA), 6, 21-39.

https://doi.org/10.5121/ijaia.2015.6102

[7]ID R&D (n.d.) Frictionless Biometric Authentication Software. ID R&D.

https://www.idrnd.ai

[8] Wolfond, G. (2017) A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors. Technology Innovation Management Review, 7, 35-40.

https://doi.org/10.22215/timreview/1112

[9] Massaro, M., Dumay, J. and Guthrie, J. (2016) On the Shoulders of Giants: Undertaking a Structured Literature Review in Accounting. Accounting, Auditing & Accountability Journal, 29, 767-801.

https://doi.org/10.1108/AAAJ-01-2015-1939.