International Journal for Multidisciplinary Research (IJFMR)

E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Access Control System Using AI and Blockchain

Saqib Ahad Khan[1], Sona Mohammad Idrees Shamshuddin[2], Dr. N. Srinivasan[3], Dr. G Kalaiarasi[4], Dr. M Selvi[5]

[1,2]Student, Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai

[3,4,5]Associate Professor, Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai

ABSTRACT

The demands of a hyperconnected society that demand increased security, transparency, and user autonomy cause traditional access control to crumble. This abstract investigates how combining blockchain technology with artificial intelligence could revolutionize access control systems. By removing single points of failure and increasing accountability, blockchain's distributed ledger technology (DLT) creates irreversible trust via a shared, tamper-proof database of rights and transactions. By automating policies, smart contracts give people command over their digital assets. AI adds intelligence and flexibility. Real-time machine learning systems detect anomalies, dynamically assess behavior, and modify policy. Access requests are filtered by AI-driven risk assessment, and sensitive resources are protected by improved identity verification. The combination of AI's dynamic powers and blockchain's unchangeable base opens the door to a future where safe, user-focused access is commonplace.

1. INTRODUCTION

Protecting sensitive data has become a top priority in the constantly changing world of digital communication. Access Control Systems (ACS) are essential for data security because they manage user rights and restrict access to vital resources. The increasing prevalence of intricate cyber threats has made it difficult for conventional access control systems to adjust to ever-changing and intricate security environments. This introduction examines the paradigm shift in the field of access control systems that results from the combination of two cutting-edge technologies: blockchain and artificial intelligence (AI).

Artificial Intelligence in Access Management:

Artificial intelligence introduces a paradigm shift in access control systems, moving away from static rule-based systems and toward adaptive, learning models. AI algorithms, especially those powered by machine learning, enable the system to do a thorough analysis of user behavior patterns. The system learns what constitutes normal and aberrant user actions through ongoing study. The Access Control System can change over time and respond more precisely to new security risks thanks to its adaptive learning.

AI aids in the early identification of anomalies in the system. The system can detect changes from typical user behavior patterns and alert users to possible security breaches by using advanced analytics.

Blockchain Technology for Access Control:

Blockchain adds a new level of security to decentralized and transparent ledgers, which gives Access Control Systems a fresh perspective. The vulnerability of a single point of failure, when a breach in one area of the system threatens the entire network, exists in a typical centralized arrangement. This danger is reduced by the decentralized structure of blockchain, which disperses access control data among several nodes. Because each node has a copy of the access control data, there is redundancy and the vulnerability to attacks is decreased.

The security and effectiveness of the access control procedure are further improved by smart contracts, which are self-executing contracts containing coded rules. By automating the implementation of access controls, these contracts lessen the need for middlemen and the possibility of manipulation or human error.

2. RELATED WORKS

a. "Intelligent Access Control System Using Machine Learning"

Authors: Chen, L.

Summary: The work of Dr. Chen, L is based on the application of machine learning algorithms in conventional access control systems. The study utilizes the use of Artificial Intelligence to analyze the behavior and access control policies based on previous historical data. The authors have a unique approach to building a smart access control system that has the ability of self-learning and which can dynamically adjust to the change in security requirements.

b. "Blockchain and Artificial Intelligence Integration: A Survey"

Authors: Kumar, P.

Summary: This work focuses on the latest advancements in the integration of artificial intelligence and blockchain. It showcases numerous use cases, including the access control systems, where the integrated capabilities of artificial intelligence and blockchain contribute to enhanced adaptability and security. The paper provides the drawbacks, current trends, and future directions for research in this vast field.

c. "Secure Access Control System Using Ethereum Smart Contracts"

Authors: Wang, Y.

Summary: This survey paper primarily focuses on the secured access control system using Ethereum smart contracts for practical implementation of blockchain technology. The authors focus on the design and deployment of a complete decentralized access control framework which emphasizes on the use of smart contracts to automate the security and access policies. The research also includes evaluation of system's performances and the security capabilities of smart contracts.

d. "Adaptive Access Control System Using Reinforcement Learning"

Authors: Li, H.

Summary: This research-based article emphasizes the integration of reinforcement learning in access control systems. The word introduces a new concept of adaptive access control model that requires the usage of reinforcement learning algorithms to optimize access policies based on real-time feedback. The authors showcase how this method increases the system's ability to adapt to the behavior of the user and evolving security threats.

3. EXISTING SYSTEM

Even though conventional access control systems have been useful for many years, they are finding it more and more difficult to meet the needs of the hyperconnected digital world. Let's examine a few of these systems' main shortcomings:

a. Single points of failure and centralized control

Imagine having just one vault containing all of your access keys. That's basically how traditional systems work, with access and permissions managed by centralized servers and administrators. This leads to a significant vulnerability whereby an attacker can access everything if they manage to break the central server.

b. Absence of Accountability and Transparency:

It can be challenging to keep track of who accessed what and when there is centralized control. Accountability is hampered by this lack of openness, which also makes it more difficult to find and fix security vulnerabilities.

c. Static and Inflexible Policies:

It is difficult for traditional systems to adjust to dynamic contexts because access requirements are always changing. Strict, predetermined rules frequently result in cumbersome access restrictions or security flaws because of out-of-date permits.

d. Limited Integration and Scalability:

Traditional systems may become unwieldy and ineffective when user and resource numbers increase. It might be difficult to integrate older technology with a variety of platforms, which limits adaptability and creativity.

e. Privacy and User Control Issues:

Users' control over their data and privacy is frequently restricted by traditional systems, which force them to rely on centralized authority for access. Furthermore, insufficient protection for sensitive data can result in its exposure through data breaches.

f. Vulnerability to Phishing and Social Engineering Attacks:

Simple authentication techniques, like passwords, are frequently used by centralized systems and are readily breached by phishing or social engineering attacks. Resources and sensitive data are in danger because of this. These shortcomings show how stronger and more reliable access control systems are required. Blockchain and artificial intelligence (AI) are two emerging technologies that can overcome these constraints and bring in a new era of safe, open, and user-focused access control. Recall that while conventional methods are still useful in some situations, adopting cutting-edge solutions that more effectively safeguard our digital assets and provide users more power in today's linked society requires an awareness of their limitations.

4. PROPOSED SYSTEM

An access control system that incorporates blockchain technology and artificial intelligence (AI) has various benefits over conventional systems, including increased security, privacy, transparency, and adaptability. The following are some significant ways that an AI and blockchain-based access control system can outperform existing ones:

a. Anomaly detection and adaptive learning:

Current System: Static rules and preset policies are frequently the foundation of traditional access control systems. They can find it difficult to adjust to growing risks and shifting user habits. Blockchain System with AI: Adaptive learning made possible by AI integration enables the system to recognize abnormalities and comprehend typical user behavior. By continuously analyzing trends, machine learning algorithms enhance the system's capacity to recognize and react to new security threats instantly.

b. Decentralized Systems and Adaptability

Existing System: Single points of failure can occur in centralized access control systems. A single system vulnerability can jeopardize the network as a whole. Blockchain and AI: Blockchain decentralizes by sharing access control information among several nodes. This lowers the possibility of unwanted access or manipulation while enhancing system resilience. Blockchain's decentralized structure reduces the possibility of a single point of failure.

c. Immutable and Open Documentation:

Current System: The integrity of access logs may be jeopardized by tampering or unauthorized adjustments to audit trails in traditional systems. Blockchain Technology with Artificial Intelligence: The immutability of blockchain guarantees the security and resistance to tampering of access logs. Every access event is transparently and irrevocably recorded, creating a trail that can be independently verified.

d. AI-Powered Smart Contracts for Automated Compliance:

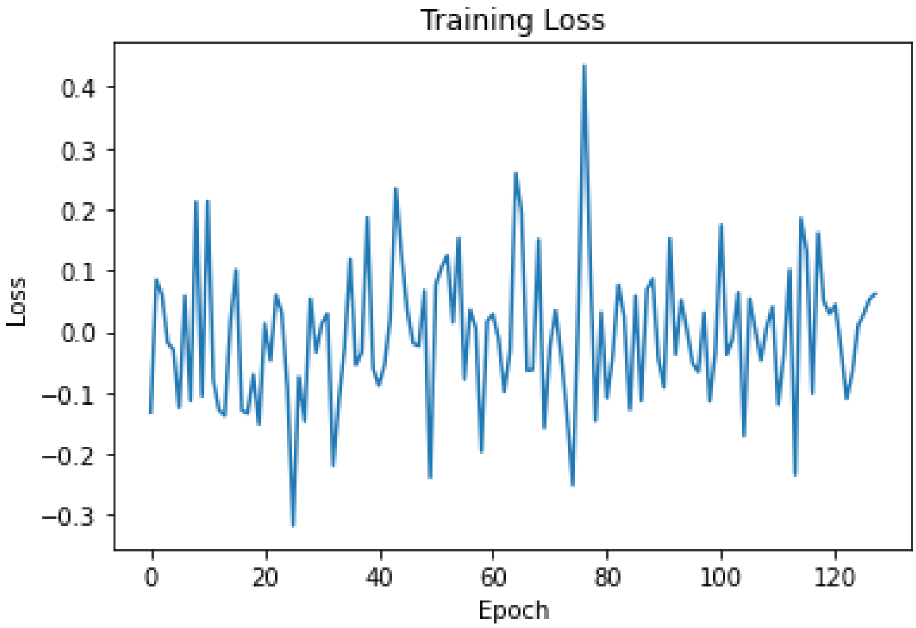
Current System: Manual procedures may be used in traditional systems to enforce access controls, which can cause delays, mistakes, and extra administrative work. Blockchain Technology with Artificial Intelligence: Blockchain smart contracts automate the application of access controls. By enforcing rules without the need for middlemen, these self-executing contracts lower the possibility of human error and guarantee that access permissions are implemented consistently and automatically.

e. Improved Control and Privacy for Users:

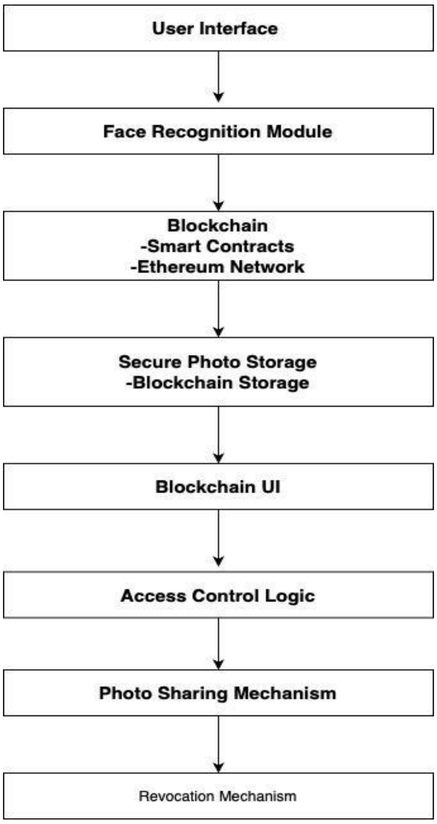
Existing System: Concerns regarding data privacy may arise from traditional systems' potential to centrally store user credentials and access rights. AI and Blockchain System: The cryptography methods used by Blockchain protect user credentials and access authorization. The decentralized structure of the system gives users more control over their data and lowers the possibility of unwanted access.

f. Active Mitigation of Threats:

Current System: Reactive measures may be used by traditional systems to address security incidents after they happen. Blockchain technology and AI: Proactive threat detection is made possible by the incorporation of AI. Unusual patterns or deviations can be recognized by the system, which prompts quick reactions to possible security risks. In a cyber threat scenario that is constantly changing, this proactive strategy is essential. In conclusion, compared to conventional solutions, an access control system that leverages AI and Blockchain provides a more reliable, flexible, and privacy-focused solution. A system that is more capable of handling the difficulties of cybersecurity is produced by combining blockchain technology for decentralized, secure record-keeping with machine learning for intelligent analysis.



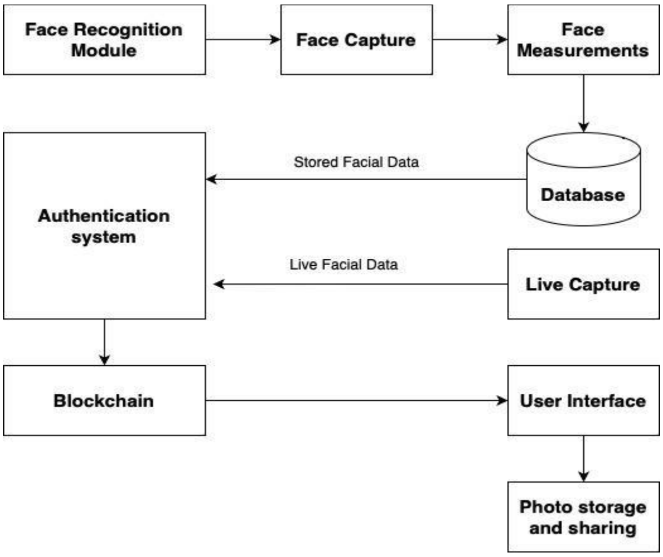
5. SYSTEM ARCHITECTURE



6. METHODOLOGY

a. Decentralized Access Control Utilizing Blockchain Technology:

Important Components: Policies and permissions for access are kept on a blockchain. Decisions about access restriction and policy enforcement are automated using smart contracts. Not a single control or point of failure. Secure audit records to ensure accountability and openness.



b. Attribute-Based Access Control (ABAC) Enabled by AI:

Important components: Judgments about access depend on resource and user characteristics. AI algorithms decide which access points to use by dynamically evaluating attributes. Fine-grained privacy and data sharing management.

c. AI-Powered Anomaly Detection and Risk Assessment:

Important components: AI examines network activities, access patterns, and user behavior. detects abnormalities and possible dangers instantly. Activates risk-reducing adaptive access control procedures.

d. Identity management that is decentralized (DID):

Important components: Users are in charge of their access credentials and digital identities. Blockchain gives DIDs access to a safe and unchangeable register. Not dependent on central identity suppliers.

e. AI-Powered Biometric Verification:

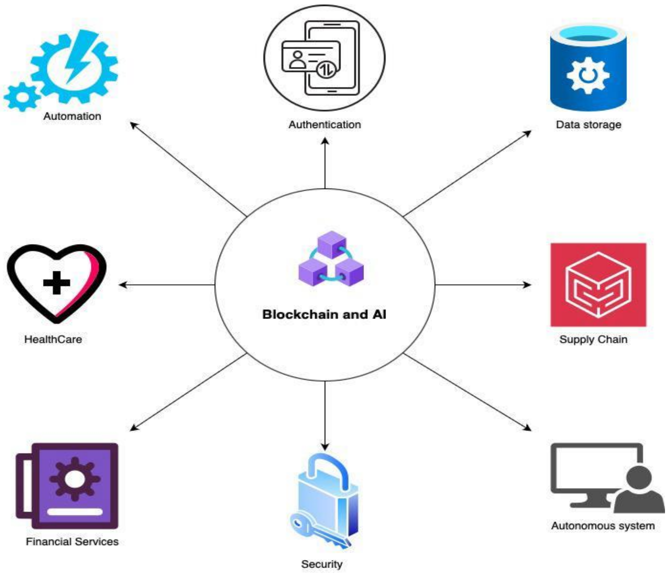
Important components: speech recognition, fingerprint scanning, and facial recognition enabled by AI. Stronger authentication than that of standard passwords. Lowers the possibility of phishing and social engineering scams.

f. Federated Learning for AI That Protects Privacy:

Important components: AI algorithms are developed with dispersed data without sacrificing privacy. Permits group model development without requiring the disclosure of private information. Ideal for industries where anonymity is a concern, such as healthcare and finance.

g. Blockchain and AI integration:

Important components: Blockchain offers an open, transparent, and safe platform for access control. Intelligent, flexible, and dynamic decision-making are enhanced by AI. The synergistic method tackles the shortcomings of conventional solutions.



7. RESULT AND DISCUSSION

The result that we have obtained after integrating Artificial Intelligence with Blockchain technology has been peerless. The first step of our project is the utilization of Artificial Intelligence where the new user registers his/her photo via a camera and an access key on the User Interface, then the photo gets saved as a pickle file as a python object structure in the database. Next is the part where the camera detects the image of the person trying to log into the system or any facility that requires authorized access, if the person’s image is not saved in the database or if the person tries to trick the system by using the photo of a registered person then his/ her access will be denied and the system will log him out instantly. Thus, the access control system will only allow a registered person to access the system by recognizing his/her facial features using deep learning technology like convolutional neural network (CNN) and haar cascade, which is an algorithm that detects objects like eyes, nose, lips, and ears irrespective of their scale and location and which can run in real-time.

The second part is the utilization of Blockchain technology where smart contract gets integrated into NodeJS. We use the Ethereum network as a medium for running the smart contracts on the website using Hardhat (truffle). We utilize Metamask for the transaction of photo storing, sharing, and revocation**.** This image is stored in a decentralised database and can never be changed, altered or deleted.

8. CONCLUSION

To sum up, the incorporation of Artificial Intelligence (AI) and Blockchain technology into access control systems is a revolutionary development in the field of digital security. This creative combination creates a dynamic solution that strengthens security measures and adapts in ways that conventional systems are unable to.

Blockchain's decentralized architecture provides resilience against single points of failure, while AI's adaptive learning allows real-time danger detection. By automating access policies, smart contracts remove risks associated with central authority. Accountability and compliance are promoted by the system's transparency and unchangeable audit trails. Additionally, blockchain's cryptographic methods improve privacy and conform to changing data protection laws. Scalability, user-friendliness, proactive threat mitigation, and a dedication to ongoing development highlight the system's all-encompassing approach to digital security.

Looking ahead, the integration of AI and Blockchain promises not just evolution but a revolution in safeguarding sensitive information, laying the foundation for the future of access control in the digital age.

9. FUTURE WORK

Blockchain and artificial intelligence (AI) combined with access control systems of the future promise to revolutionize the field of digital security. Deep learning models and other AI algorithmic advancements offer more adaptive security by identifying subtle trends in user behavior. The combination of AI with multi-modal biometrics will improve user authentication and strengthen system security as a whole. The widespread use of edge AI will speed up real-time processing and enable prompt reactions to security events. Standardization and interoperability will become essential for a cohesive security ecosystem. Blockchain developments will handle privacy issues while preserving transparency, such as privacy-focused protocols. Users will have more control over their information thanks to the rise in popularity of decentralized identification solutions. Features related to regulatory compliance will change to conform to international data protection laws. The Internet of Things (IoT) integration will increase the breadth and device-awareness of access control. On-premises and hybrid cloud solutions will provide resilience and flexibility. User interfaces will emphasize simplicity, offering experiences that are clear and focused on the user. Fundamentally, a dynamic combination of security, flexibility, and user privacy will drive access control powered by AI and Blockchain in the future, changing the face of digital security in a networked world.

References

1. Blockchain-Based Access Control Systems: State of the Art and Challenges by Md. Asif Rahman et al. (2022)
2. AI-Enabled Blockchain-Based Access Control for Malicious Attacks Detection and Mitigation in IoE

by Md. Touhiduzzaman et al. (2022)

3. Blockchain-based Access Control and Data Sharing Systems for Smart Devices by Md. Touhiduzzaman et al. (2021)
4. A Scalable Multilabel-Based Access Control as a Service for the Cloud (SMBACaaS) by P. Chinnasamy and P. Deepalakshmi (2018)
5. Blockchain-Based Access Control Techniques for IoT Applications by Md. Touhiduzzaman et al. (2020)
6. Blockchain-Based Access Control for Healthcare Systems by M. A. Khan et al. (2022)
7. AI-Enabled Blockchain-Based Access Control for Secure Smart Industry Management Systems by A. Pribadi et al. (2023)
8. Blockchain-Based Access Control for Secure and Efficient Data Sharing in IoT by M. A. Khan et al. (2023)
9. A Decentralized Access Control System Based on Blockchain and AI by Y. Zhang et al. (2022)
10. AI-Enabled Blockchain-Based Access Control for Secure and Efficient Data Sharing in Vehicular Networks by S. Zhao et al. (2023)
11. Outchakoucht, A., Es-Samaali, H., & Philippe, J. (2017). Dynamic Access Control Policy based on Blockchain and Machine Learning for the Internet of Things
12. Enhancing Data Security in Cloud Computing Using Blockchain and Attribute-Based Encryption Xuyun Zhang, Ke Zhang, Yue Zhang, et al.