IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Blockchain Enabled Proxy Chaining Algorithm For Enhanced Security and Privacy

[1]Mr.Mohd Shoaib Shaikh, [2]Mr.Sayyad Shah Hussain, [3]Mr.Faiz Ali Sayyed, [4]prof.Sneha Sankhe

[1 2 3]UG student, [4]Assistant Professor

[1 2 3 4]Department of Information Technology,

[1 2 3 4]Theem college of engineering, Boisar, India

Abstract: In an era where digital privacy and cybersecurity are major concerns, the development of innovative solutions becomes imperative. This system presents a pioneering approach to address these concerns through the integration of blockchain technology with proxy chaining, creating a robust and secure system for enhancing online security and privacy. The core objective of this system is to design and analyze a blockchain-enabled proxy chaining algorithm that ensures a higher level of security and privacy for users navigating the internet. This innovative algorithm leverages blockchain's inherent features, including decentralization, transparency, and immutability, to establish a trustless environment for proxy chaining. Key elements of the proposed algorithm include decentralized proxy node management, automated proxy selection and rotation through smart contracts, secure data transmission, and auditability through blockchain's transparent ledger. By decentralizing proxy services and enhancing user control, the algorithm reduces reliance on centralized entities, thereby minimizing the risk of data breaches and unauthorized access. Moreover, the system ensures robust security measures, safeguarding user data from threats such as man-in-the-middle attacks, data leaks, and privacy infringements. Data encryption, secure key management, and consistent security standards are integral components of this algorithm. Privacy is a fundamental concern addressed through IP address obfuscation, user identity protection, and data minimization, in compliance with applicable privacy regulations.

***Keywords* – Encryption, Decryption, Proxy, chat application, Server.**

I. INTRODUCTION

In an increasingly interconnected digital world, ensuring security and preserving privacy are major concerns. To deal with the major concern a cutting-edge solution, a Blockchain-Enabled Proxy Chaining Algorithm, designed to elevate the levels of security and privacy in online communication and data transmission. This innovative approach leverages blockchain technology to enhance the effectiveness of proxy chaining, making it a robust solution for safeguarding sensitive information and user identities. the applicable criteria that follow. The aim of the Blockchain Enabled Proxy Chaining Algorithm for Enhanced Security and sequestration is to Empower individualities and associations with an innovative and slice- edge result that leverages the power of blockchain technology and deputy chaining to establish a new standard for online security and sequestration. Our thing is to produce a robust and decentralized system that not only defends against cyber pitfalls but also ensures stoner obscurity, unrestricted access to information, and control over particular data. By achieving this end, we seek to establish a safer and further private digital terrain, where druggies can confidently engage in online conditioning without compromising their security or privacy.

II. LITERATURE SURVEY

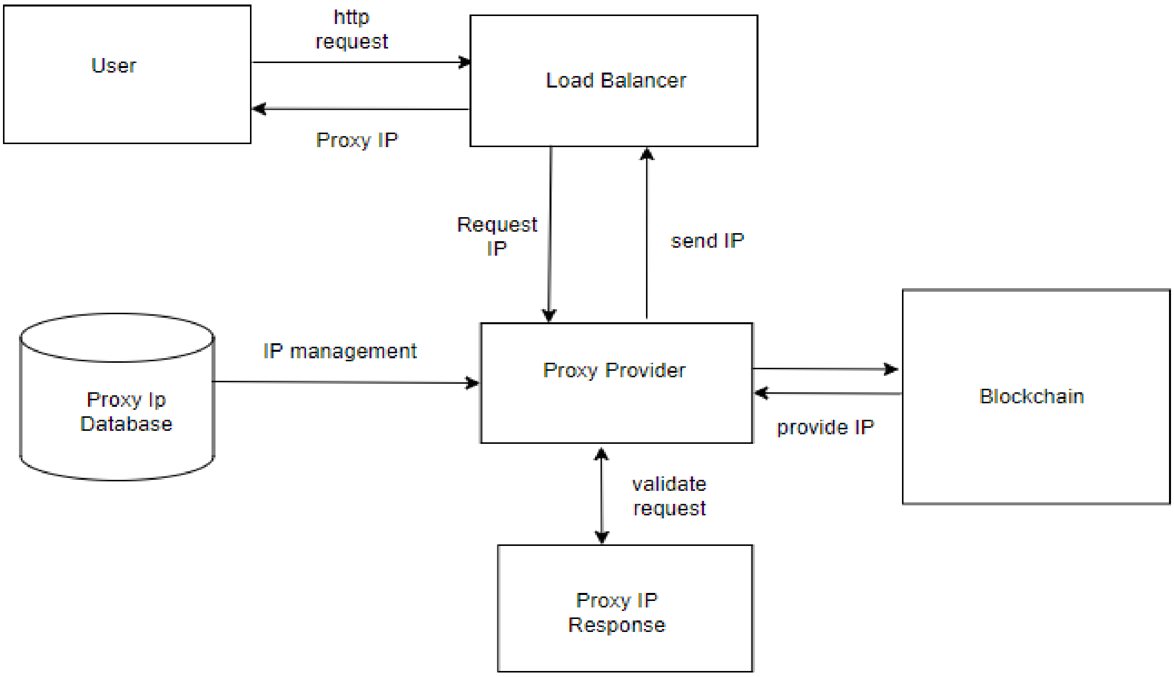
A efficient writing survey may be a of assessing and translating all accessible inquire about important to a specific inquire about address, point or wonder of intrigued. The logical databases with full content paper, and the other accessible logical articles within the field of social sciences were utilized within the inquire about. All logical and other papers and works written within the time span from 2009 to Walk 2020 are taken into consideration within the comes about selection.

Sr no.	Paper Title (Reference)	Author Name	Advantages	Disadvantage
[1]	A Blockchain Proxy for Lightweight IoT Devices.	Gero Dittman, J	By delivering trustworthy readings to the blockchain, the proxy service enhances the reliability of data transmitted from IoT devices.	support only the most common programming language for lightweight IoT devices, potentially limiting

				accessibility to developers using other languages.
[2]	Analysis blockchain solutions for IoT: A systematic literature review.	S.K. Lo, Y. Liu, S.Y. Chia	A summary of the existing IoT issues and the roles blockchain played to address the issues; Investigation of IoT management that covers both data and Things aspects.	But these are two different technologies having different nature thus having certain limitations and challenges like data storage.
[3]	Security threats and solutions to IOT using blockchain.	Shireen Rafat Alam, Saurabh Jain, Rajesh Doriya	By leveraging blockchain technology, the integration with IoT could potentially resolve challenges related to identification, authentication, scalability, and data security.	Need to address open issues and challenges in the integration of blockchain with IoT, providing a basis for future research directions to overcome these limitations.
[4]	Equipment Data Sharing Method Based on Block-chain.	Shaofeng lin, Xiao Wang, Shaotao Nie	Overall Framework method of data sharing using block-chain is presented	There are many short-coming such as unclear data, leakage of share data, and difficulty in traceability which effects the development of mechanisms.
[5]	On blockchain and its integration with IoT. Challenges and opportunities	A. Reyna, C. Martín, J. Chen	Study of challenges, potential benefits and open issues of the integration of blockchain and IoT. Study of existing blockchain–IoT platforms and applications.	Storing capacity and scalability, lawful issues, and consequences.

III. SYSTEM ARCHITECTURE

The System architecture revolves around several key components working in tandem to facilitate secure and efficient proxy services. At the forefront, users initiate requests for proxy IP addresses through a user interface or application. These requests are then directed to a load balancer, which distributes the incoming traffic evenly across multiple proxy providers to ensure optimal performance and reliability. The proxy providers, equipped with a pool of available IP addresses, respond to these requests by dynamically allocating proxy IPs to users as needed. Central to the system's integrity is the integration of blockchain technology. The blockchain serves as a decentralized ledger, recording every transaction and interaction within the system. When a user requests a proxy IP and it is allocated by a provider, this transaction is securely recorded on the blockchain, ensuring transparency and immutability of the process. Additionally, the blockchain facilitates trust among all parties involved, as the transaction history can be verified by anyone accessing the distributed ledger.



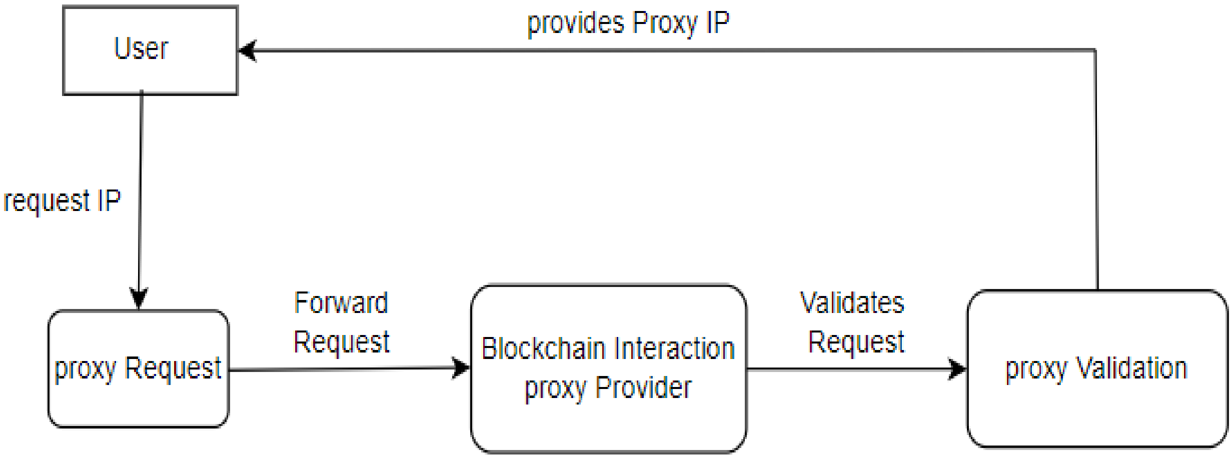
3.1 Requirement Analysis

For any software project there are different kinds of requirements to be fulfilled in order to ensure smooth running of the processes. Clearly defined requirements are important markers on the road to a successful project. They establish a formal agreement between the customer and the service provider that both are working towards the same goal. The following are the different kinds of requirement for our project.

Software Requirements	Hardware Requirements
Proxy Server Software	Windows 11 or latest version
Block Chain Platform	8 GB RAM
Encryption Software	Intel core processor i3
Decentralized Identity	Wi-Fi Router

3.2 PROPOSED SYSTEM

We propose a proxy system and a terminal for typing was developed to secure the communication process between User and public server. This makes the users to connect internet more securely along with data privacy. In a blockchain-enabled proxy IP system, the setup revolves around four key players: the user, proxy provider, proxy validator, and blockchain interaction module First up, we have the user - they're the ones in need of a proxy IP address, which they request from the system. Once the user sends off their request, it lands in the hands of the proxy provider, acting as the middleman. Now, the proxy provider's job is to check if the request is genuine and if there's a suitable proxy IP available. This process of checking is what we call validation. If everything checks out, the proxy provider gives the green light, and the requested IP gets assigned.



IV. PROBLEM DEFINITION

The Blockchain Enabled Proxy Chaining Algorithm proposal intends to bolster security and confidentiality through the utilization of blockchain technology and proxy chaining. Key objectives include bolstering data security, safeguarding user privacy, countering censorship, and diminishing centralization. Through the resolution of these challenges, the proposed algorithm aims to equip individuals and entities with the necessary means to traverse the digital realm securely and privately, fostering a more open and robust online environment.

V. RESULT

A blockchain-enabled proxy system goes beyond traditional security measures by offering an unprecedented level of trust and transparency. By recording access requests and data validations on a public ledger, it creates an immutable history of transactions, making it virtually impossible for bad actors to manipulate or forge records. This audit trail not only enhances security but also bolsters privacy. Users can be confident that their data remains confidential and unaltered throughout the process. Furthermore, this system's decentralized architecture reduces the risk of a single point of failure. In a traditional proxy system, a compromised central authority could result in significant security breaches. However, with blockchain, the absence of a central entity ensures that no single entity can compromise the system. This distributed structure also helps protect user privacy, as data is not concentrated in one location or controlled by a single entity.

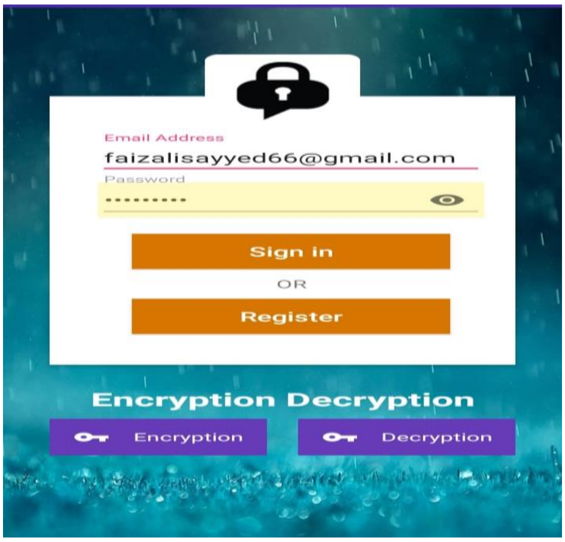

Email Address
faizalisayyed66@gmail.com
Password
•••••••••

Fig1: Login Panel

This is A login panel is a user authentication interface commonly found in websites and applications. It typically consists of fields for entering a username or email address and a password, allowing registered users to securely access their accounts. Users must provide valid credentials to gain entry, ensuring privacy and security. Login panels are a fundamental component of user access control in the digital realm. Additionally, the login page may incorporate additional security measures such as two-factor authentication or biometric verification to further enhance the system's security posture. Overall, the login page plays a crucial role in ensuring that only authorized users can utilize the advanced security and privacy features offered by the blockchain-enabled proxy chaining algorithm.

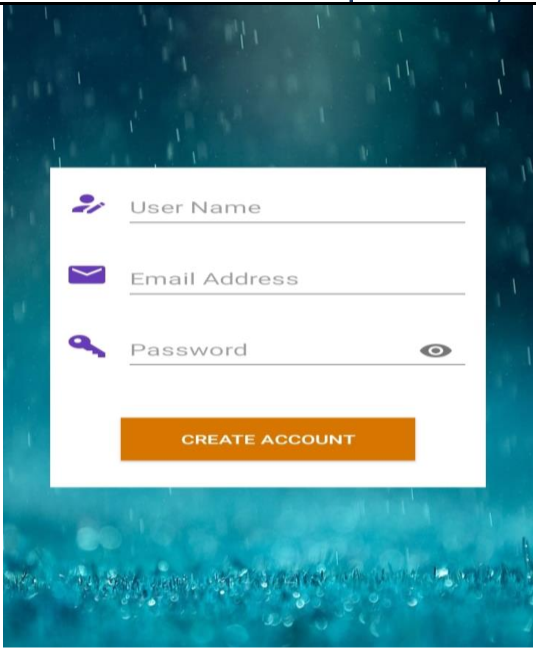


Fig2: Sign Up Panel

A sign-up panel is a user registration interface often featured in websites and apps. It typically includes fields for users to input their information, such as name, email address, and password, to create a new account. Successful registration grants users access to the platform's features and services. Sign-up panels are crucial for onboarding new users and expanding a digital community.

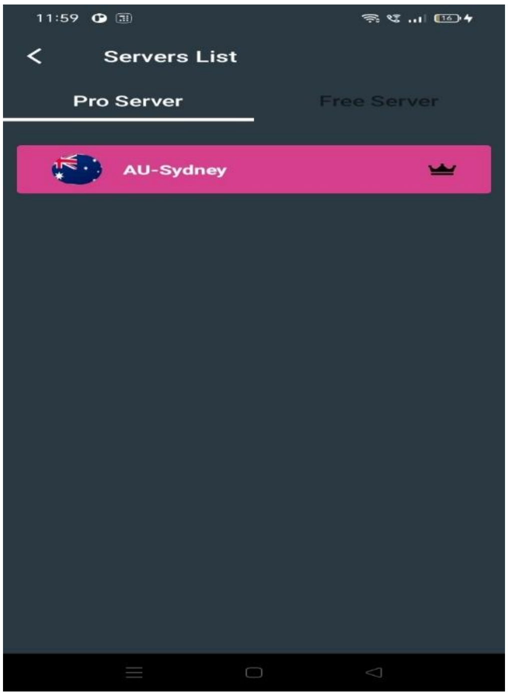


Fig3: Proxy Pro Server

The Proxy Pro Server is like a guardian for your internet data in the Blockchain-Enabled Proxy Chaining Algorithm for Enhanced Security and Privacy. It works by using a special kind of technology called blockchain to make sure your data stays safe and private. Here is how it works: Imagine you are sending a secret message online. Instead of sending it directly to the recipient, the message first goes through a series of secure "middlemen" called proxy servers. Each proxy server adds an extra layer of protection to your message.

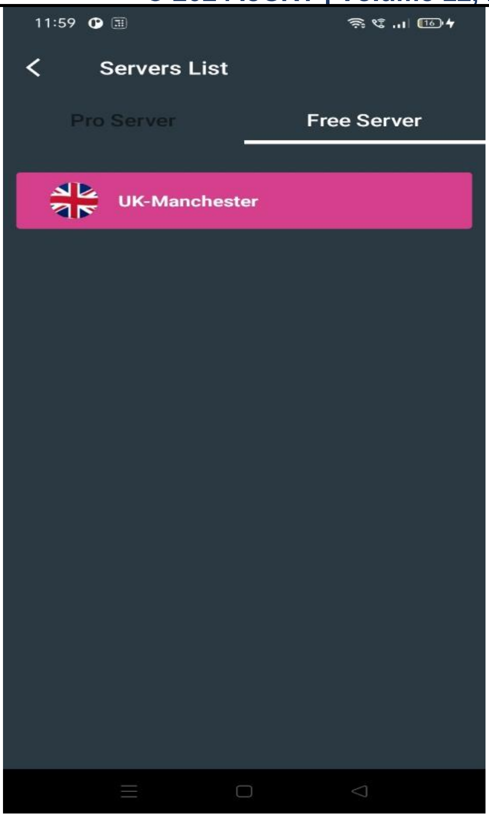


Fig4: Proxy Free Server

The proxy-free server plays a pivotal role in ensuring seamless functionality and heightened protection. Unlike traditional proxy servers that act as intermediaries between users and the internet, the proxy-free server operates without reliance on intermediary nodes. Instead, it leverages blockchain technology to establish a direct and secure connection between users and online resources. The proxy-free server functions by utilizing a blockchain-enabled proxy chaining algorithm, which dynamically routes user requests through a series of decentralized nodes. Each node in the chain validates and encrypts the data before passing it along to the next node, thereby creating a multi-layered shield against potential threats.

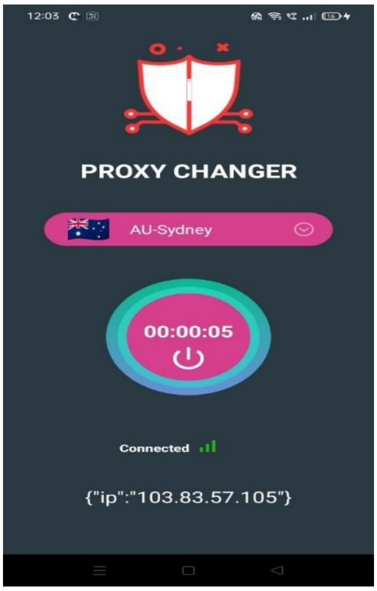


Figure5: Activated Proxy Ip

Activated proxy IP refers to the functionality where Internet Protocol (IP) addresses are actively engaged within the blockchain-based proxy chaining process. When an IP address is activated within this system, it becomes a crucial element in the chain of proxies, facilitating secure and private communication between users and the internet. The activated IP works by securely routing data packets through a series of proxy nodes, each recorded and validated on the blockchain ledger. This process ensures that each step in the communication pathway is transparent and tamper-proof, reducing the risk of interception or manipulation by malicious actors.

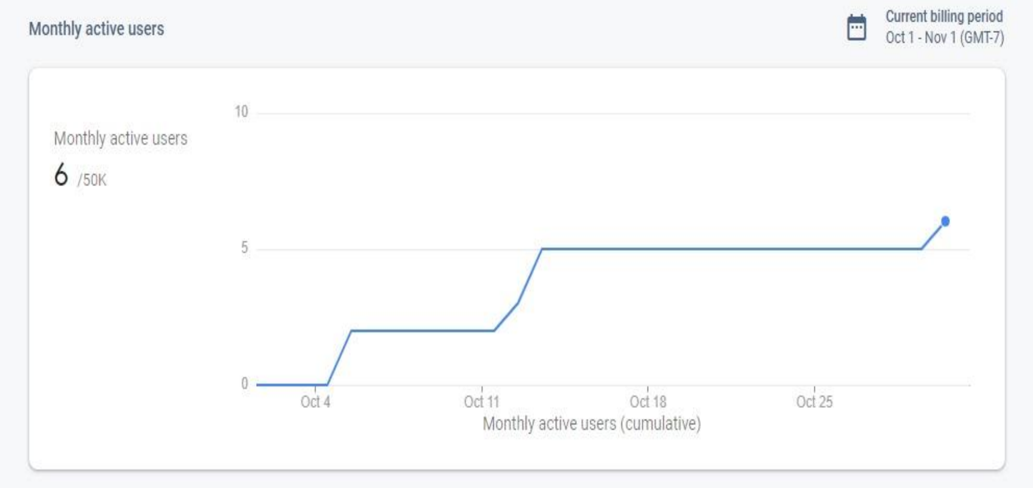
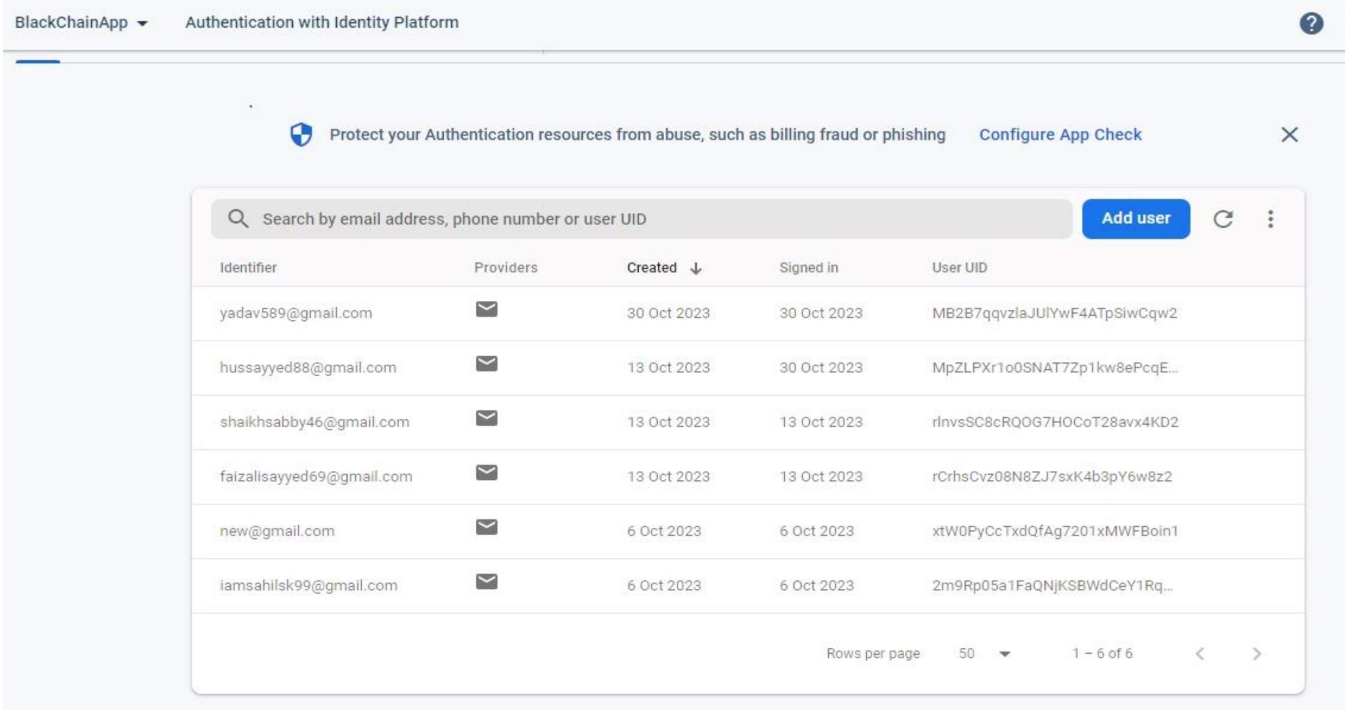


Figure6: Firebase User Activity

Firebase offers user activity tracking through Firebase Analytics, which records user behavior, screen views, and events. You can also use Cloud Fire store or the Realtime Database to log and manage user-specific data. Firebase Cloud Functions enable server-side processing in response to user actions, while Firebase Authentication tracks sign-ins and user account activity. Together, these tools help you analyze and respond to user activity, enhancing your app's performance and user engagement.


BlackChainApp
Authentication with Identity Platform
Protect your Authentication resources from abuse, such as billing fraud or phishing
Configure App Check
Search by email address, phone number or user UID
Add user

Identifier	Providers	Created ↓	Signed in	User UID
yadav589@gmail.com	✉	30 Oct 2023	30 Oct 2023	MB2B7qqvzlaJUlYwF4ATpSiwCqw2
hussayyed88@gmail.com	✉	13 Oct 2023	30 Oct 2023	MpZLPXr1o0SNAT7Zp1kw8ePcqE...
shaikhsabby46@gmail.com	✉	13 Oct 2023	13 Oct 2023	rlnvsSC8cRQOG7HOCoT28avx4KD2
faizalisayyed69@gmail.com	✉	13 Oct 2023	13 Oct 2023	rCrhsCvz08N8ZJ7sxK4b3pY6w8z2
new@gmail.com	✉	6 Oct 2023	6 Oct 2023	xtW0PyCcTxdQfAg7201xMWFBoin1
iamsahilsk99@gmail.com	✉	6 Oct 2023	6 Oct 2023	2m9Rp05a1FaQNjKSBWdCeY1Rq...

Rows per page 50 1 – 6 of 6

Figure7: User Authentication Panel

Firebase Authentication is commonly integrated into apps to enable secure access control and user management. Developers can easily customize and control authentication flows through Firebase's APIs and SDKs, making it a popular choice for building user authentication systems in various applications.

VI. CONCLUSION

In the ever-evolving landscape of cybersecurity and privacy concerns, the blockchain-enabled proxy system stands out as a trailblazing solution. By anchoring access and data verification in a tamper-proof ledger, it not only secures online interactions but also offers users an unshakable assurance that their digital footprints are protected. This technology transcends geographical and jurisdictional boundaries, providing a shield against data breaches and unauthorized surveillance. Its promise lies in the ability to reestablish control over personal data, enabling individuals to navigate the digital world with peace of mind, knowing their information remains confidential and unaltered. With its decentralized architecture and cutting-edge encryption techniques, the blockchain-enabled proxy system is poised to be a cornerstone in the ongoing quest for robust security and privacy in the digital age.

VII. FUTURE SCOPE

In the future, we can explore making the algorithm even smarter and more efficient. This means finding ways to make it work faster while keeping everything super secure. We could also look into adapting it for different devices and platforms, so people can use it on all their gadgets, like phones and tablets. Plus, we can keep improving how user-friendly it is, making it simple for anyone to use, even if they are not tech whizzes. With these advancements, we can continue to make the internet a safer place for everyone.

REFERENCES

[1] Lo, S.K.; Liu, Y.; Chia, S.Y.; Xu, X.; Lu, Q.; Zhu, L.; Ning, H. Analysis of blockchainsolutions for IoT: A systematic literature review. IEEE Access 2019, 7, 58822–58835.

[2] Ye, C.; Cao, W.; Chen, S. Security challenges of blockchain in Internet of things: Systematicliterature review. Trans. Emerg. Telecommun. Technol. 2020, 32, e4177

[3] El-Masri, M.; Hussain, E.M.A. Blockchain as a mean to secure Internet of Things ecosystems–a systematic literature review. J. Enterp. Inf. Manag. 2021, 34, 1371–1405.

[4] Patil, P.; Sangeetha, M.; Bhaskar, V. Blockchain for IoT access control, security and privacy: DOI: Wirel. Pers. Commun. 2021, 117, 1815–1834

[5] Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT.

[6] M. Blaze, G. Bleumer, and M. Strauss, ``Divertible protocols and atomic proxy cryptography, &#39;&#39; in Advances in Cryptology-EUROCRYPT. Berlin, Germany: Springer, 1998, pp. 127144.