IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 9, September 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009015 |

Durable Biometric Authentication Scheme Using Blockchain

Nayankumar.B , Avinash N Rao, Dr.B.SShylaja

M. Tech, Dept. of Information Science & Engineering, DR.Ambedkar Institute of Technology, Bangalore, India

M. Tech, Dept. of Information Science & Engineering, DR.Ambedkar Institute of Technology, Bangalore, India

Professor, Dept. of Information Science & Engineering, DR.Ambedkar Institute of Technology, Bangalore, India

ABSTRACT: Composite biometrics is considered new and sustainable method to saveconfidential data. In modern society, biometric systems are widely used alternatively passwords authentication process with high security, which verycomplex when hackers infiltrate the system. At this point, blockchain give high-level security as a quick and efficient access process. Any validation action refers to the usual hashing policy for preparing digital signatures. same digital signature can be processed using blockchain techniques mention to the hashing approach discussed in this paper.

KEYWORDS: Blockchain, Hashing, SHA,AES,Fingerprint.

I. INTRODUCTION

Identity is receiving increasing recognition as it offers a encouraging ability to identify users using established authentication methods supported by passwords and adhara biometric identification card. learning is considered more reliable and practical. Furthermore, recognition adopted features in fingerprints, irises, leading patterns which can be collected from various sensors. The biometric identification system, the owner of database, federal bureau of investigation responsible for maintaining national fingerprint database. outsource large biometric data connected to server. cloud eliminate costly compute and storage cost. however maintain the security of biometric data must encrypted before outsourcing. Whenever an federal bureau of investigation partner (for example police station) wishes authenticate a person`s identity, federal bureau of investigation will turn generate a request for ID using the biometric characteristics of the person. individuals such as fingerprints, irises and voice patterns, faces, and so on. The federal bureau of investigation then encrypted the query and sends it to cloud. Therefore challenge is to design the protocol that enable efficient identification, privacy protection in the system of cloud. wide range of privacy-preserving identity verification solution is offered.

II. LITERATURE SURVEY

Digital payments transmitted from one party to another without passing betweenfinancial organizationif electronic cash was peer-to-peer. digital signatures contribute to the solution in some ways, but the primary advantages are lost if reliable third party is still necessary to stop double-spending. We offer apeer-to-peer network as a solution in double-spending issue. Network timestamps transactions being continuous chain of hash-based proof-of-work, insert record that cannot altered without performing a new proof-of-work.[1]

Many institutions have adopted biometrics as a security authentication tool due to its individuality. A central authority centralizes and administers these databases after processing the biometric data into templates that are saved on them. This type biometric data, fingerprint template, is asymmetric and vulnerable key security attacks. fake template input, template change or deletionand channel interception by an evildoer. This study, we use symmetric peer-to-peer network and symmetric encryption to protect a fingerprint template that has been encrypted. The fingerprint is encrypted using symmetric key scheme advanced encryption standard and then uploaded to the Interplanetary File system, a symmetrically distributed storage system.[2]

Data and the consensus-based method of recording and updating them via distributed nodes are key to enabling trustless multi-party transactions in a blockchain-based system. The degree of utility, performance, and cost of a blockchain-based application is thus ultimately determined by properly comprehending what and how the data are kept and modified. Blockchain technology improves the quality of the data by offering a transparent, immutable, and consistent data repository, but it also introduces new difficulties for data management. In this essay, we examine blockchains from the perspective of a developer to highlight key ideas and factors to take into account when integrating

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009015 |

a blockchain as a data repository into a broader software system. The project seeks to deepen knowledge of blockchain technology as a data repository.[3]

A growing field with promising developments, mobile ad hoc networks draw researchers with a variety of improvements and evolutions. These networks are autonomous, dynamic, and lack a clear structure. The Ad-hoc network's strength resides in its routing protocols, which make it a good option for transmission. Our focus is on the LGF (Location-based Geo-casting and Forwarding) protocol, which belongs to the position-based category, out of the several routing protocols that are accessible. With its low bandwidth usage and minimal routing overhead, LGF aims to catch people's attention, but at the expense of uninvited attacks that jeopardize data security. By combining LGF with k++ Means, we provide a method in our strategy to defeat powerful attacks like Wormhole and Blackhole.[4]

The Interplanetary File System is a distributed file system that aims to speed up and improve the web by decentralizing it. It makes use of well-known technologies like BitTorrent and Git to build an information-sharing swarm of computing units. IPFS has experienced significant advancements and adoption from both private persons and business entities since its launch in 2016. Users are able to share files and information globally because of its distributed network. Large files that could use a lot of bandwidth to upload or download over the Internet operate well with IPFS. This distributed file system has gained popularity quickly in part because IPFS is built to run on top of many protocols including FTP and HTTP.[5]

To CECS, they suggest the brand-new protected information searching as well as distribution system. This method has significant edge over earlier works throughout terms both safeguarding overall security for IoT Connected systems & customers' secret credentials as well as attaining Minimal savings for construct phrase searching passageways. information exchange with information seeking that is better secured as well as effective. With respect to privacy, this plan guarantees that privacy all information stored with that internet, protected information exchange among consumers as well as Internet of things, protected information searches among both access information centre with consumers, that permits for deployment of information facilities with a weaker level of confidence [6].

Researchers reviewed the threats on blockchain systems with permissions. Focusing upon these cyberattacks, they created indications that may be used whether strategically and responsively by such a specific organisation within a blockchain system can identify continuing threats. They suggested any viable computational framework that those parameters that was modelled after SIEM technologies [7].

This suggested method for privacy-preserving inspection on distributed information secures information kept on cloud servers that verifies its accuracy. Prior of saving all information within its clouds servers, its technology encrypts that information using using AES encryption algorithm. They employed the SHA1 technique that verifies the validity all the information so order that confirm storing accuracy [8].

Information from the authorized source is shared with your organization. This pairing key is generated by this files by utilizing DSS method. Every every blocks in that HARS system, a verified signatures is produced by utilizing publicly monitoring method. A Validation meta can always be generated by this team's member [9].

That cloud infrastructure that hosts this databases could not remain reliable. Every information controller must ensure ensure every services properly may use whatever portions in a public databases over whatever it has been granted permission. They provided the privacy-preserving distribution approach which ensures information held inside highly unreliable cloud remains secret & authentic [10].

Some features of varieties underlying information protection challenges throughout various phases various eras must be understood in its future of big data clouds technology in particular to assure data protection within that big data cloud computation system. In order to maintain the information privacy of an organisation as develop the sustainable big data clouds technology infrastructure, something that are required to investigate and develop effective privacy control techniques [11].

This problem of safely exchanging information through cloud technology has been overcome. With this research, several various strategies for protecting security while exchanging information securely were covered. Information security and information security are ensured through identification. Using that basis of this scientific review, they developed a hybrid approach. Combining the ABE & BRE algorithms may protect information security. These suggests how our suggested technique could being utilised for improve cloud service security protection [12].

Even if that information is transferred to clouds storage, a connection cryptography system can allow the users accessible management. Revocable Identity-based encrypting can stop systems customers whose membership has been terminated form accessing sharing information. Technologies including the meta-data files method and the periodical key managing approach have being employed in the suggested solution to increase privacy. This will assist in lowering that service's computationally expense [13].

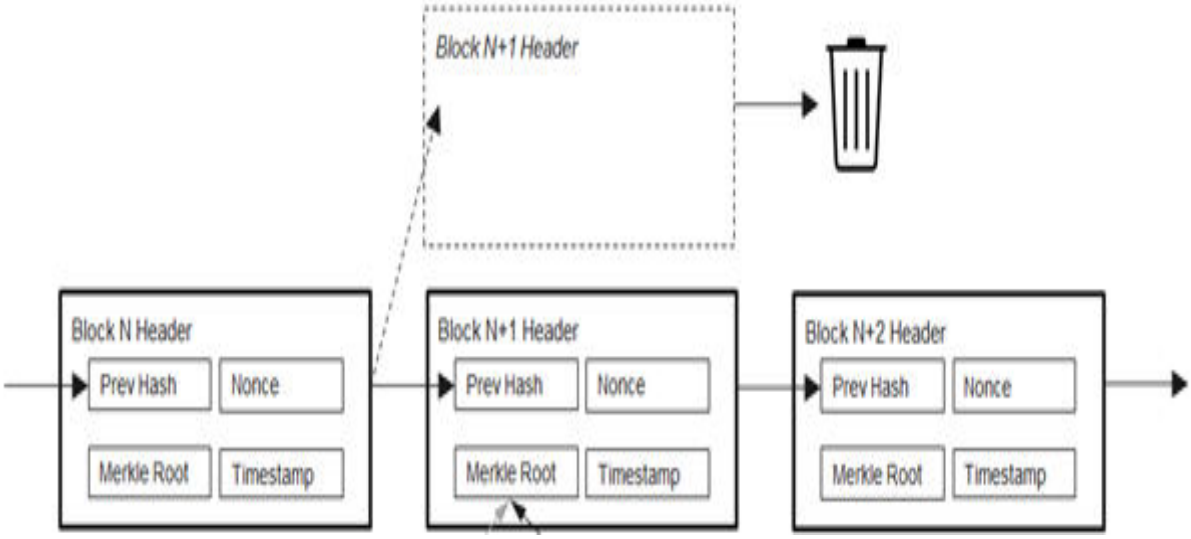
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009015 |

III. BLOCKCHAIN

Blockchain is extendof records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the formerstructure, a timestamp, and tradedata (generally indentify as merkel tree root hash).



IV. STRUCTURE

Blockchainis circulate, distributed, and public digital census use to record deals with computers so that the record can`tchangesubsequent without modification posterior blocks and agreement of network. This allows the actors examine deals sumptuously. blockchain is managed separately using peer-to-peer network and a distributed time-stamping. andauthenticated by mass collaboration powered by cooperative data. The outcomeis robust workflow where actors query concerning datasecurity framed. use of a blockchain removes the specific bottomless duplicatable digital asset. It confirms that each part value transferred only formerly, activelong standing problem of double spending. This block chain predicated swappingvalue can be completed hastily, secure, and cheaper than with traditional systems blockchain can assign title rights because when properly set up to detail the exchange agreement.

PROBLEM STATEMENT

In July 2018, Telecom unit of India Chairman R.S Sharma posted his Aadhaar card number on Twitter and challenged Aadhaar critics to hack if they're going to. Inside seven hours, the hacker posted screenshot of sending back to Sharma's bank account details, Aadhaar enabled services, and also they posted 14 details of his, including Sharma mobile number, date of birth,present address, phone number, PAN card number, Bank details, etc. Information don't seem to be welfare stored in cloud by the government of india creates an enormous security problem in preserving our privacy.

RELATED WORKS

The authentication process proposed withdiffrent authors is researched specify here for work related to Biometric Authentication based on Image Processing. The technique of processing and converting images into digital form plays a central role in generating the various hash codes when preparing a digital signature. We came up with the process of authentication via biometrics going through these articles.

Binary data in fingerprint:

grayscale image of the fingerprint is represented by pixel values of 0 for black and 1for white.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009015 |

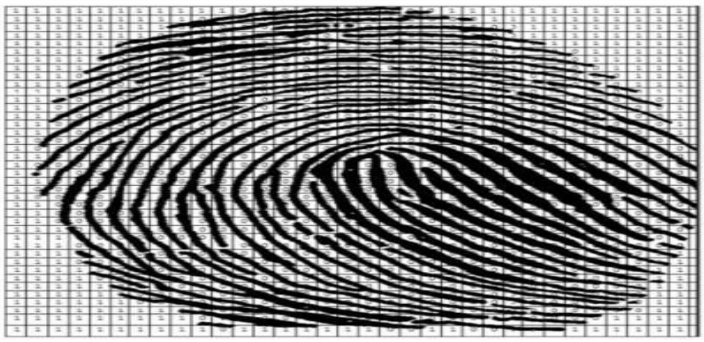


Figure I representation of fingerprints to matrix form

Figure I, model represent fingerprints in a matrix (mesh) of size 40 × 33 where the image elements represented as zero or one. The arcs, loops, or zigzags black and the rest are white. The same image can be represented on small to produce strong hash value. The md5 hash given below whose principle can be followed to generate hashes.

AES Algorithm

This algorithm used symmetric encryption .itmainly used for encryption and protection of electronic data. It because of relief for data encryption standard because of way hastily and further DES. AES consists of three block ciphers and these ciphers areused give encryption of knowledge.

SHA1 Algorithm

Secure hash algorithm is cryptographic hash algorithm.This hash value is understood as a communication condensation. This communication condensation is sometimes also rendered as a hexadecimal number which is 40 integers long. It'sAU.S. Civil information wisdom Standard and was designedBYU.s. National security Agency.5.6.2 point Algorithmic engineering, a characteristic algorithm could be procedure that maps an arbitrarily large data item(analogous computer train) way shorter bit string, its point, uniquely identifies the first data for all practical purposes indeed mortal fingerprints uniquely identify people for practical purposes. This point is also used for data reduplication purposes. This is constantly also remarked as train characteristic, data characteristic, or structured datafingerprinting. Fingerprints are generally avoid the comparison and transmission of big data. For illustration, an online cybersurfer or deputy garçon efficiently check whether a far- out train modified, by going point and comparing therewith to previously broughtcopy.

ANALYSIS

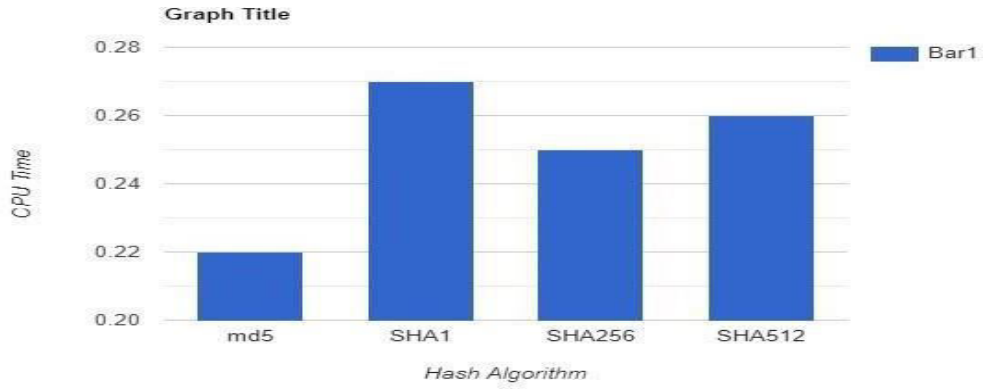


Fig 2 Hash algorithm comparison

Figure 2 technique among md-5, sha-1, sha-256, and sha-512 with a specified input size. speed can be considered based on cpu time limit, which prove md-5 to be fast. terms of security properties, sha-256 is better than others, higher level of security can be achieved with blockchain by referring to md-5. Of course, sha-256 can refer to the evolution of hashes to blockchain to achieve higher level of security.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009015 |

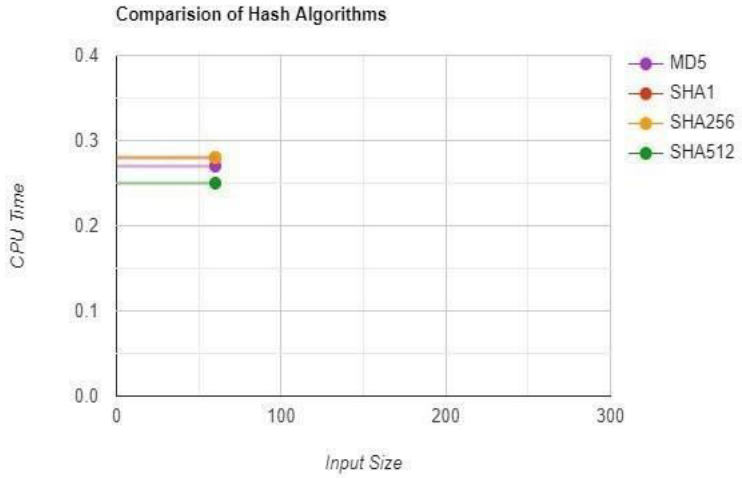


Figure 3 Hash algorithms with blockchain comparison and different input sizes

Fingerprint algoritham

Step1: Initialize colors
Step2: Open and make the softened image
Step3: produce the double picture
Step4: induce Greymap
Step5: double original Result
Step6: Remove Noise(Remove noise from the double picture using the mean algorithm)
Step7: Skeletonization(We skeletonize until there are not any changes between two duplications) Step8: Direction(Convert the direction matrix to a direction softened image)
Step9: Ramifications(corners- Extract crossroad points from the double image, which may be fairly ramifications)
Step10: Ramifications(endpoints- Extract endpoints from the double image, which could be nicely ramifications)

STORE DATA TO BLOCKCHAIN

In blockchain is include chain blocks, each block carrying some data. This amount is limited to the blockchain framework. That indicates size that can be uploaded to the blockchain is 1 MB. Save fingerprint images to block chain will be off limits of these images is little differentiate to other types of media files.

V. CONCLUSIONS AND FUTURE OF WORK

This article try to propose a new privacy scheme mention to blockchain with biometrics so that search fingerprints used to access a secure system. solve problem of digital signatures, highlight block chain emerging and promising plan on the internet of things and cloud servers. Fast and durable authentication policies handled by a composite of the suggested methods. In future this process can be done aadhara card to access registration unique identity authority of india server. indian server provide full security system.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009015 |

REFERENCES

1. Nakamoto S., "Bitcoin: A Peer-to-Peer Electronic Cash System" https://bitcoin.org/bitcoin.pdf.
2. Jaikaran C, "Blockchain: Background and Policy Issues", Congressional Research Service. https://www.americanvoiceforfreedom.org/wp-content /uploads/2018/03/Blockchain-Background-and-Policy-Issues.pdf.
3. Zhang R, Zheng Y "A Survey on Biometric Authentication: Towards Secure and Privacy-Preserving Identification". IEEE ACCESS, Vol.7, pp.5994-6009. DOI: 10.1109/ACCESS.2018.2889996.
4. Odelu V, "IMBUA: Identity Management on Blockchain for Biometrics- Based User Authentication".DOI: 10.1007/978-3-030- 23813-1_1.
5. Mohsin A.H, Zaidan A.A, Zaidan B.B, Albahri O.S, Albahri A.S, Alsalem M.A, Mohammad K.I, "Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions". Computer Standard & Interfaces, Vol.64, pp.41–60. doi.org/10.1016/j.csi.2018.12.002.
6. Tao, Y., Xu, P. and Jin, H., 2019. Secure data sharing and search for cloud-edge-collaborative storage.IEEE Access, 8, pp.15963-15972.
7. Putz, B. and Pernul, G., 2020, November. Detecting blockchain security threats. In 2020 IEEE International Conference on Blockchain (Blockchain) (pp. 313-320). IEEE
8. Ghutugade, K.B. and Patil, G.A., 2016, December. Privacy preserving auditing for shared data in cloud. In 2016 International Conference on Computing, Analytics and Security Trends (CAST) (pp. 300-305). IEEE.
9. Trueman, T.E. and Narayanasamy, P., 2015, November. Ensuring privacy and data freshness for public auditing of shared data in cloud. In 2015 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM) (pp. 22-27). IEEE.
10. Ulybyshev, D., Bhargava, B., Villarreal-Vasquez, M., Alsalem, A.O., Steiner, D., Li, L., Kobes, J., Halpin, H. and
11. Ranchal, R., 2017, June. Privacy-preserving data dissemination in untrusted cloud. In 2017 IEEE 10th International Conference Cloud Computing (CLOUD) (pp. 770-773). IEEE.
12. Wang, F., Wang, H. and Xue, L., 2021, March. Research on data security in big data cloud computing environment. In 2021
13. IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) (Vol. 5, pp. 1446- 1450). IEEE.
14. More, P., Chandugade, S., Rafiq, S.M.S. and Pise, P., 2018, February. Hybrid encryption techniques for secure sharing of a sensitive data for banking systems over cloud. In 2018 International Conference on Advances in Communication and Computing Technology (ICACCT) (pp. 93-96). IEEE.
15. Pathare, K.G. and Chouragade, P.M., 2017, July. Reliable Data Sharing Using Revocable-Storage Identity-Based Encryption in Cloud Storage. In 2017 International Conference on Recent Trends in Electrical, Electronics and Computing Technologies (ICRTEECT) (pp. 173-176). IEEE.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details