ISSN No:-2456-2165

Securing Data Using Encryption and Blockchain Technology

Moona Olakara Mohammed
Dept of Computer Science Engineer
Nehru College of Engineering & Research Centre
Palakkad , India

Dr U.Vijay Sanker
Dept of Computer Science Engineer
Nehru College of Engineering & Research Centre
Palakkad , India

Shiji S
Dept of Computer Science Engineer
Nehru College of Engineering & Research Centre
Palakkad , India

Abstract:- Increasing the number of technologies in the modern world facing a major problem with the security issues. Most of the system providing a high level of security to ensure security from intruders'.But still, intruders were climbing to each technology to steal the authorized network. To avoid such a situation, new research has been done using encryption and blockchain technology. In this research, proposing an encrypting a part of the system with the blockchain and two authentication methods to provide high-security data. Hybrid encryption would be the first level of authentication using the RSA and Blowfish algorithm along with the face recognition method to provide authentication ad authorization. After enabling the system, using the blockchain technology method to store confidential information, data sharing will help the owner or organization from being unauthorized access and make data more reliable. All the information would be stored in an encrypted form inside the system. By disabling the system the files should unknown to others and cannot be viewed. These technologies provide more security for highly confidential information and protection from being attacked.

Keywords:- *Hybrid Encryption, Two Authentic Factor, Blockchain Technology, Face Recognition.*

I. INTRODUCTION

In recent years, security is one in all the key factors regarding in all technical fields. With the crucial development of technology in line with the human needments, the main issue lies behind the information security. Most of the technologies require the resources of hardware and software system needs. If any backdoor developed in any requirements of today's technology the intruders might climb upon theses technologies and take authorization access that they needed. within the case of many fields resembling banking transfer, non-public documents such as Aadhar Id, Debit, or mastercard all the kinds of transactions are done on a network. When the network isn't within the safe dealing or which will offer a backdoor the trespassers will simply access the network and steal the data for his or her benefits, considering in a very another case a corporation consists of consumers records, employees information, wind of the organization, sharing the information between the purchasers moreover as through the staffs. All the information perhaps saves in a server through the system. If the intruder may use some social engineering techniques to urge the small print of the server through it should access to each system of an organization. So, data security is that the main conception topic of the digital world.

The big usage of pc networks over all the world, computer security we have a tendency to as information security has become the foremost international a part of the world. a very important question for engineers and directors is regarding a way to shield the wizard world from attack and their main challenge to develop completely different techniques capable of sleuthing a shot to break the integrity and convenience of the network. This space we are called Intrusion Detection System(IDS). Definetly, there are continuously several solutions than expected within the field of technology to form a replacement outstanding invention and this results in a higher future. As well, there has been associate degree import to every invention moreover because the advancement of technology to make sure the diminution of risk beside the techniques becomes easier and faster.

The most task of methodology is providing high security to our system as well the to the confidential information. We all know that intruders are attempting their best to urge the network. therefore the answer is to use some method of coding algorithmic rule as well as blockchain technology to stop from being attacked. during this system 2 level of authentication is introduced beside blockchain technology. Hybrid coding is that the initial level of encryption for the user's authorization associate degreed authentication. Second level of authentication is the face recognition to notice the owner of system. when the fortunate of 2 authentication system begin to modify their feature then they may able to store wind moreover as data sharing through the system victimisation blockchain method. All the data saves in an encrypted form. whereas disabling the system an

outsider using the system couldnt able to decide an information that done the system. Combining these technologies offer the information integrity, confidentiality, authorization and complex security to the system. Main objective of this paper expecting to have associate degree high security that the third party couldn't access to the network while not the permission. This technique like the coding software system wherever a tiny low a part of computer system is encrypted. Implementing such strategies support numerous service in numerous domains like medical records, public services, company organizations etc. As the technologies are increasing the big scale data security enlarge with the explanation for security.

This next section shows the way to introduce this system by researching various material, section III introduce the idea of new system , section IV explains the overall and future of the system.

II. RELATED WORKS

The paper researched the technology of blockchain: its architecture, consensus, and future success of blockchain[1]. A blockchain is a group of blocks, which holds a complete list of transaction records like a conventional public ledger. Each block in a blockchain consists of the block header name, Merkle root hash, timestamp, nBits, nonce, parent hash block. A digital signature in the blockchain is part of security. It has its own private and public key on both sides of users.

To solve such a situation the researcher proposed efficient and privacy-preserving traceable attribute-based encryption in the blockchain[3].To maintain the privacy for traceability in blockchain, the author proposed the non-reputation and traceability blockchain and the digital content is the grantee[]. The problem lies in the issue of the secret key as the secret key does not hold the information of the user it is shared by any user. If the secret key is revealing the source of the key cannot be discovered. The bottleneck of the existing system leaks sensitive information in the access control system. Moreover, the addition of attribute-based encryption for privacy data is still secure for data. But the decryption does not improve efficiency.

To tackle this author research a blockchain-based security architecture for distributed cloud storage[4]: As per the security, the storage capacity of large-scale data increasing in creating more and more applications. To solve the issue supporting these limited nodes with cloud services thus resulting in the compromise in the cost-reducing and integrity of data and enlarge the storage capacity. The genetic algorithm method is used for the placement of replicate files between the multiple. But the decentralized storage platform such as file coin, storage, swarm ere not considered.

The researcher resolved the issue by proposing the decentralized PoD solutions for PoD digital assets[5]: The researcher overcomes the problem of proof of delivery using smart contract and Ethereum. Digital content is successfully delivered to the consumer sold by digital content and provider. After successful delivery, the download of content by the customer and the participating entities (owner and files) gives an incentive reward. The limitation of this research is the owner of content have the access right over the content through encryption of digital content and a review for the owner's authenticity and quality of data are not considered

III. METHODOLOGY

The architecture diagram of the system shown below. The system is mainly a type of encryption software where all users or an organization could able to use as personal. The description of the system is given:

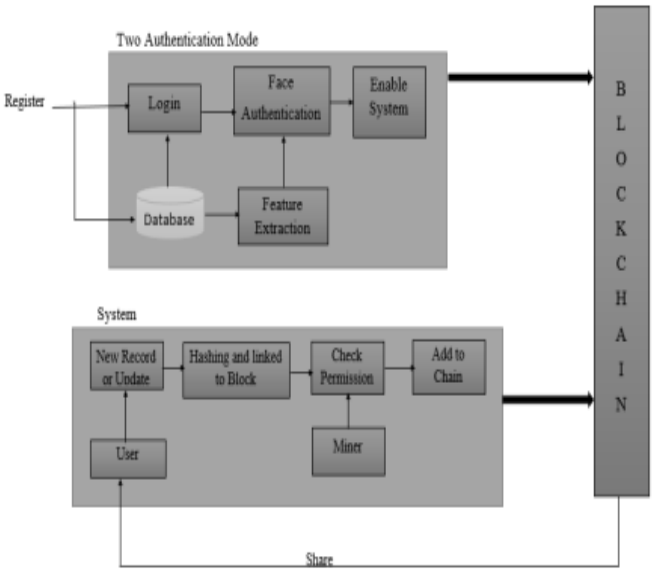

FIG 1 ARCHITECTURE

A. Two Authentication Mode

Two-factor validation (2FA), once in a while alluded to as two-venture confirmation or double factor verification, is a security cycle in which user give two diverse confirmation variables to check themselves. This cycle is never really ensure both the client's qualifications and the assets the client can get to. Two-factor validation gives a more significant level of safety than verification techniques that rely upon single-factor confirmation (SFA), in which the client gives just one factor ordinarily, a secret word or password. Two-factor verification techniques depend on a client giving a secret key, just as a subsequent factor, typically either a security token or a biometric factor, like a finger impression or facial sweep.

A.1 User Authentication

On dividing each phase of the system, the first phase comes under the login system where the user has to login to the system for his/ her work. As the system based on the security encryption the login system were designed with hybrid cryptosystem with combination of symmetric and asymmetric algorithm such as blow fish and RSA respectively.

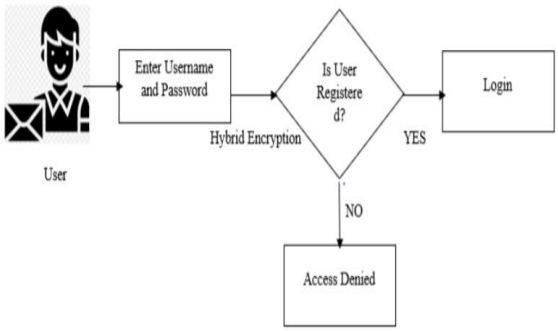

FIG 2 USER CREDENTIALS

The interaction begins with the asymmetric key exchange where random session key is produced by one of the gathering (initiator) in the correspondence. They utilize public key of that individual that they need to hash(encrypt) one time session key utilize the recipients public key.Now the session key is encoded it tends to be safely sends without a shift of somebody catching it and having the option to unscramble (decrypt) any resulting communication.Once the recipients gets the encoded information, they can decode it with their own private key and that they approach the symmetric encryption key that the sender was attempting to impart to them. They will at that point send a scrambled (encrypt) check message to affirm that they got right key and this is encoded utilizing a symmetric key. When the confirmation message back to the first sender they will unscramble it. On the off chance that they can effectively decode it they realize the interaction works accurately and secure the information.

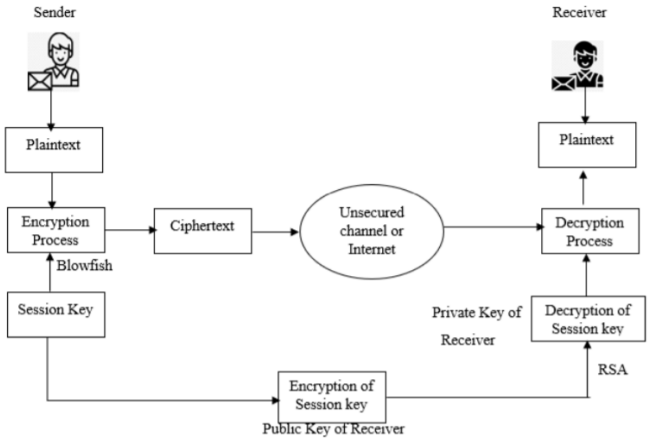

FIG 3 HYBRID ENCRYPTION

A.2 Face Authentication

The second phase of the system is face recognition to enable the system properly.In this phase system would identify the owner of the system is using the software for the working purposes.Face recognition is a bio metric tool which identifies a person based on specific aspects of their physiology.Though the software can vary the process of facial recognition trends follow three steps:

1. Face is captured with the webcam
2. The programming at that point estimates an assortment of facial highlights called milestone or nodal focuses on the face. This could incorporate the distance between the eyes, the width of the nose, profundity of eye attachment, distance from brow jawline. Each program utilizes diverse nodal focuses and may gather up to 80 distinct estimations a numerical equation which addresses your novel facial mark.
3. The facial mark is analyzes to a data set that is now enlisted. This would all be able to occur in merely second.

Facial acknowledgment framework where being consistently utilized by police to distinguish suspect in the field. A critical component of facial acknowledgment is in the space of wellbeing and security. Face acknowledgment frameworks can be utilized to distinguish individuals in photographs, video, or continuously. Law requirement may likewise utilize cell phones to recognize individuals during police stops. Face acknowledgment has been utilized to target individuals taking part in ensured discourse.

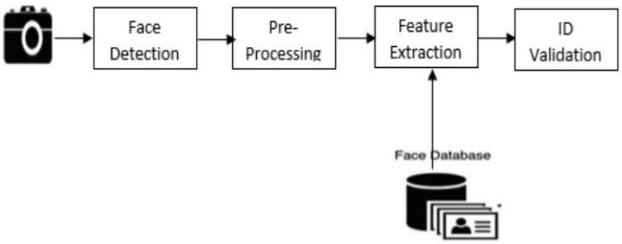

FIG 4 FACE RECOGNITION

B. Blockchain Technology

Blockchain is a shorthand for an entire set-up of appropriated legder advances that modified to record and track anything esteem from monetary transcation to clinical records or even a land titles.Blockchain might be a chain of squares that contain data .Blockchain might be a disseminated that is totally affable anybody..

Blockchain might be an advanced record that is acquiring huge loads of consideration and foothold as of late. Keeping record of information and exchanges are a significant piece of the business. Frequently, this data is taken care of in house or gifted an outsider like representatives, financiers, or legal advisors expanding time, cost, or both on the business. Luckily, Blockchain evades this long interaction and advances the quicker development of the exchange, through setting aside both time and cash.

B.1 Permissioned Blockchain

A Permissioned Blockchain might be an assortment of blockchain that has just related hubs that is every one of the members inside the organization are recognized. This gives a further layer of safety to the blockchain. Permissioned blockchains are blockchain networks that need admittance to be a part of. In these blockchain types, an effect layer runs on the top of the blockchain that coordinates the activities performed by the approved members. As you'll see, permissioned blockchains work totally unique in relation to that of individual and public blockchains. they're created to require the upside of blockchains without forfeiting the power

part of a unified framework. Permissioned blockchains additionally are not the same as private blockchains, which license just realized hubs to take an interest inside the organization. for example, a bank could likewise be running an individual blockchain worked through an appointed number of hubs interior to the bank. Interestingly, permissioned blockchains may permit anybody to hitch an organization once their character and job are characterized.

Permissioned blockchain upholds the property of Distributed Ledger, Immutability and Consensus system. The approval inside the organization is set among the individuals for permissioned blockchain. In any case, for a Permissioned blockchain, the data should be shared among the members inside the organization. Because of this, the topic of protection emerges. Since the information should be divided between the hubs, information security and protection could be settled.

FIG 5 PERMISSION BLOCKCHAIN

IV. ADVANTAGES

The basic advantage of blockchain technology provides security, immutability, traceability, and non-reputation. It allows authentication without the verification of a third party or completely processing between owner and user. Form the name itself, we get an idea of blockchain. Its small number of blocks connected in chain linked to one another by giving some hashing algorithms. The public key and private key in the blockchain are available as a partial to every authorized user. So, the system is not authorized by one person it is authorized by a different person in a link. For every technology, the main concept lies behind the security. If the security is poor, the success of technology is poor. In this system, the main task to develop high security through the combination of different methods like hybrid encryption, face recognition along blockchain technology. Various levels of authentication using hybrid encryption for user authentication and face recognition for authorization make the system complex thereby adding some other methods like blockchain technology by hashing some algorithms to make the data more secure. The data are stored in each block chaining to other blocks the keys are linked to previous blocks of the present with hashing algorithms' is crucial to crack the system easily. Bringing out this technology in different fields like companies, medical records, bank information would have successful data security and be relaxed.

V. CONCLUSION

Concluding the research, we have got an idea of today's modern technology developing the complex security. Finally, every technology uses the methods of cryptography to develop security. Encryption, key generation, and decryption is the most important part. In every encryption way of the method in each is different. This paper concept combines three methods were hybrid encryption and face detection authentication for authorization and authentication. Every technology starts with the level of authentication, how much complex we are developing on each phase that much data or confidential information are secured. In every aspect of the level, blockchain is the main trending technology. Along with the blockchain using some complex part of encryption methods like double or hybrid encryption, the system would be secured then we expected.

ACKNOWLEDGMENT

This examination is upheld extraordinarily from the direction of Nehru College of Engineering and Research Center. I'm additionally thankful to endless other people who gave help and exhortation all through the venture. Yet, chiefly I am obliged to the members in this examination, who were incredibly liberal with their time and information, and who made this exploration conceivable.

.REFERNCES

[1]. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology:Architecture, consensus, and future trends," in2017 IEEE international congress on bigdata (BigData congress). IEEE, 2017, pp. 557–564.

[2]. S. Hasavari and Y. T. Song, "A secure and scalable data source for emergency medical careusing blockchain technology," in2019 IEEE17th International Conference on Software Engineering Research, Management and Applications (SERA). IEEE, 2019, pp. 71–75.

[3]. A. Wu, Y. Zhang, X. Zheng, R. Guo, Q. Zhao, and D. Zheng, "Efficient and privacy-preserving traceable attribute-based encryption in blockchain,"Annals of Telecommunica-tions, vol. 74, no. 7-8, pp. 401–411, 2019.

[4]. J. Li, J. Wu, and L. Chen, "Block-secure: Blockchain based scheme for secure p2p cloudstorage,"Information Sciences, vol. 465, pp. 219–231, 2018.

[5]. H. R. Hasan and K. Salah, "Proof of delivery of digital assets using blockchain and smartcontracts,"IEEE Access, vol. 6, pp. 65 439–65 448, 2018

[6]. Holík, Filip, and Sona Neradova. "Vulnerabilities of modern web applications." In 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1256-1261. IEEE, 2017.
[7]. Alzahrani, M. E. "Auditing Albaha University Network Security using inhouse Developed Penetration Tool." In Journal of Physics: Conference Series, vol. 978, no. 1, p. 012093. IOP Publishing, 2018.
[8]. Ibrahim, Adamu Bin, and Shri Kant. "Penetration Testing Using SQL Injection to Recognize the Vulnerable Point on Web Pages." International Journal of Applied Engineering Research 13, no. 8 (2018): 5935-5942.
[9]. Donaldson, Scott, Natalie Coull, and David McLuskie. "A methodology for testing virtualisation security." In Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 2017 International Conference On, pp. 1-8. IEEE, 2017.
[10]. Hussain, Muhammad Zunnurain, Muhammad Zulkifl Hasan, and Muhammad Taimoor Aamer Chughtai. "Penetration testing in system administration." International Journal of Scientific & Technology Research 6, no. 6 (2017): 275-278.
[11]. Matheu-García, Sara N., José L. Hernández-Ramos, Antonio F. Skarmeta, and Gianmarco Baldini. "Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices." Computer Standards & Interfaces 62 (2019): 64-83.
[12]. G. J. Simon, H. Xiong, E. Eilertson and V. Kumar, "Scan detection: A data mining approach," In Proceedings of the Sixth SIAM International Conference on Data Mining, 2006, pp. 118–129.
[13]. P. A. Porras and A. Valdes, "Live traffic analysis of TCP/IP gateways," in NDSS, 1998,
[14]. C. Leckie and R. Kotagiri, "A probabilistic approach to detecting network scans," In Proceedings of the Eighth IEEE Network Operations and Management Symposium (NOMS 2002), 2002, pp. 359-372.
[15]. S. Staniford, J. A. Hoagland and J. M. McAlerney, "Practical automated detection of stealthy portscans," Journal of Computer Security, vol. 10, pp. 105-136, 2002.
[16]. J. Jung, V. Paxson, A. Berger and H. Balakrishnan, "Fast portscan detection using sequential hypothesis testing," In Proceedings of 2004 IEEE Symposium on Security and Privacy, 2004, pp. 211-225
[17]. Yang, Longzhi, Noe Elisa, and Neil Eliot. "Privacy and security aspects of E-government in smart cities." In Smart Cities Cybersecurity and Privacy, pp. 89-102. Elsevier, 2019.
[18]. Chandra, Yogesh, and Pallaw Kumar Mishra. "Design of Cyber Warfare Testbed." In Software Engineering, pp. 249-256. Springer, Singapore, 2019.
[19]. Kocher, Joshua E., and David P. Gilliam. "Self port scanning tool: providing a more secure computing environment through the use of proactive port scanning." 14th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise (WETICE'05). IEEE, 2005.
[20]. Rohrmann, R., Patton, M. W., & Chen, H. (2016, September). Anonymous port scanning: Performing network reconnaissance through Tor. In 2016 IEEE Conference on Intelligence and Security Informatics (ISI) (pp. 217-217). IEEE.