IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 6, June 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 6, June 2021 ||

|DOI:10.15680/IJIRSET.2021.1006183|

File Watermarking Using Hybrid Cryptography

Ms.Waje Ashwini R[1], Ms.Kadam Ashwini R[2], Ms.Shaikh Fariyal J[3], Prof.Mr.Hirave K.S[4]

Department of Computer Engineering, HSBPVT, Parikrama College of Engineering Kashti, Ahmednagar, Maharashtra, India[1,2,3]

HOD, Department of Computer Engineering, HSBPVT, Parikrama College of Engineering Kashti, Ahmednagar, Maharashtra, India[4]

ABSTRACT: Information and statistics safety is primary for maximum groups, army stations and even home computer users. consumer facts, transaction data, price statistics, private files, character files, financial account info - most of the people of this information can be tough to replace and conceivably dangerous at the off danger that it falls into the incorrect arms. statistics misplaced due to disasters, for instance, a flood or hearth is crushing, yet dropping it to hackers or a malware infection can have appreciably extra noteworthy outcomes. In block-chain generation, each page in a ledger of transactions bureaucracy a block. That block has an effect on the subsequent block or page through cryptographic hashing. In different words, when a block is finished, it creates a completely unique secure code, which ties into the following web page or block, developing a chain of blocks, or block-chain. In proposed device facts will be of healthcare facts want to relaxed. This paintings is designed the use of block chain idea and key-based totally cryptographic method. stores the hash tables of raw statistics and files on the block-chain, validates different copies by using going for walks a hashing technique, and then compares the facts stored in the block-chain, any interfere with the records will be speedy determined, because the original hash Tables are saved on millions of nodes. Proposed system paintings on records / records transmission. On net extra information of army protection machine is stored and that records want to stored securely.

KEYWORDS: Encryption, Decryption, Digital Hashing, File sharing, Key generation.

I. INTRODUCTION

The world got here to understand about the Block-chain concept nine years back when Satoshi Nakamoto conceptualized it in 2008; however it were given evolved a year later, using Bit-coin, a crypto-foreign money and virtual charge machine. The idea turned into later coming across to dispensed ledger that leverages the block-chain to verify and save transactions with out crypto-foreign money. The term block-chain is extensively used these days to symbolize a brand new disruptive era poised to be the subsequent massive issue throughout industries from healthcare to finance to retail. in step with Gartner, their consumer analysis on block-chain and related topics has quadrupled because August 2015. Block-chain is a divided database of facts or public ledger of virtual activities or transactions that got carried out and has been shared amongst related to events across a huge network of un-trusted individuals. It shops records in blocks that can affirm information and are very difficult to hack. A block-chain is a public ledger residing of ordered and time-stamped records of transactions arranged in statistics blocks which will use cryptographic validation to link themselves collectively. Block-chain is a path of recording data and transactions digitally.

Each file is a block connected chronologically together into a chain. A block of 1 or greater new transactions is composed into the transaction information part of a block. in keeping with the technique of cryptography, digital signature generates a hard and fast of information records representing the identification and information integrity of the signer, commonly appended to the records document.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 6, June 2021 ||

|DOI:10.15680/IJIRSET.2021.1006183|

II. RELATED WORK

Literature survey is the maximum important step in any type of research. earlier than begin developing we want to look at the preceding papers of our domain which we're running and on the basis of take a look at we can are expecting or generate the drawback and start running with the reference of previous papers.

on this section, we in short review the related paintings on statistics security.

R.Alvaro-Hermana, J. Fraile-Ardanuy, P. J. Zufiria, L. Knapen, and D. Janssens provided the concept between preparations of electrical cars, which essentially diminish the impact of the charging procedure on the power framework amid business hours. This buying and selling technique is also economically useful for all of the customers concerned inside the trading procedure. An activity-based method is used to predict the each day time table and journeys of a artificial population for Flanders (Belgium) [1].

Y. Xiao, D. Niyato, P. Wang, and Z. Han provide a study of the possible float and useful elements that enable DET in communication networks. diverse design troubles on the way to put in force DET in practice are mentioned. a really perfect approach is created for postpone-tolerant faraway controlled correspondence organizes in which each remote powered tool can masterminded its data transmission and power replacing activities as indicated via gift and destiny vitality accessibility [2].

N. Z. Aitzhan and D. Svetinovic gives a work that deal with the difficulty of supplying transaction safety in decentralized clever grid energy buying and selling with out self assurance on relied on 0.33 events. we've evolved a proof-of-idea for decentralized energy trading device using blockchain technology, multi-signatures, and nameless encrypted messaging flows, enabling peers to anonymously negotiate strength fees and securely carry out buying and selling transactions. [3]

M. Mihaylov, S. Jurado, N. Avellana, k. Van Moffaert, I. M. de Abril, and A. Now offers a piece that indicates decentralized automated coins, called NRG-coin. Prosumers in the clever grid framework exchange privately made sustainable electricity source utilizing NRG-coins, the estimation of which is indented on an open cash trade put it up for sale. Like Bit-coins, this money proposes various favorable occasions over fiat cash, however never like Bit-cash it is made by way of infusing vitality into the matrix, instead of giving power on computational have an impact on. Likewise, they make a novel exchanging worldview for getting and providing environmentally friendly energy power within the smart grid community. [4]

S. Barber et al offers a piece that Bit-coin is remoted computerized coins which has pulled in a large number of customers. They play out a top to backside examination to recognise what made Bit-coin so powerful, even as many years of research on cryptographic e-cash have not prompt a huge scale appropriation. They ask moreover how Bit-coin could turn into a respectable contender for seemingly perpetual stable cash. [5]

J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain presents a piece to accomplishes request reaction by giving motivating forces to liberating PHEVs to modify nearby strength request out in their own self-hobbies. Be that as it can, when you consider that exchange protection and safety coverage problems display genuine difficulties, they check out a promising consortium block-chain innovation to decorate alternate security with out dependence on a confided in outsider. A limited P2P electricity buying and selling framework with Consortium block- chain (PETCON) method is proposed to represent targeted activities of restricted P2P energy exchanging [6].

Jiafu Wan, Blockchain is characterized by means of its decentralized nature, integrity of the records saved within the chain and its openness. because of these characteristics, another vicinity in which Blockchain may be used is to launch government budget for a venture. usually whilst a task is allocated finances, there may be no expertise as to how those price range are getting used and a huge a part of it's far in no way shown in facts because of corruption. To resolve this problem, a system has been proposed using Blockchain to offer the transparency. [7]

Antonios Litke ,the writer propose an progressive blockchain-based totally IIoT architecture to help build a greater cozy and dependable IIoT device. by way of reading the fast-comings of the prevailing IIoT structure and the blessings of the Block-chain era. We decompose and reorganize the authentic IIoT architecture to form a brand new, multi-

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 6, June 2021 ||

|DOI:10.15680/IJIRSET.2021.1006183|

middle, partly decentralized structure. for this reason, the proposed architecture represents a vast improvement of the unique structure, which offers a brand new route for the IIoT development. [8]

I. Alqassem et al, offered a brand new information sharing scheme based totally on blockchain generation. customers can manipulate their statistics and understand the statistics being collected approximately them and a way to use it without trusting any 0.33 party. but, the scheme did no longer don't forget the opportunity of the business enterprise itself tampering with records. [9]

III. PROBLEM STATEMENT

.

A. Objectives

- To analyze the steps involved in the working of Block chain.
- To offer the security for important information.
- To use transportation statistics for secure transaction.

IV. PROPOSED METHOD

Data forms the foundation of the application system, and its integrity is the key to the data's value and the aim of data security technology prevention. According to the approach of cryptography, digital signature generates a set of data information representing the identity and data integrity of the signer, normally appended to the data file. The user validates the digital signature through the user's public key to verify the authenticity and integrity of the data information. In general, the intension of using a private key-based cryptography technique is for recipients or users to verify the origin of the data information.

For data security, this work is designed using block chain concept and key-based digital signature technology. In this work we stores the hash tables of raw data and files on the block-chain, validates other copies by running a hashing technique, and then checks the data stored in the block-chain, any interfere with the data will be quickly found, because the original hash Tables are stored on millions of nodes. In this military officers will store transportation data for different users.

Architecture

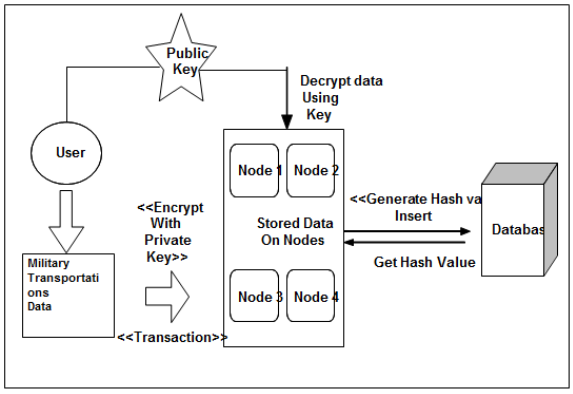

Fig.2 System Architecture

A. Modules

Module 1 - Sender (User):- Sender select the confidential file, encrypt them using encryption technique with unique private key.
Module 2 - Receiver (User):- Receiver select file, decrypt using unique private key belong to that file and download it.
Module 3 – Key Manager (Authority):- Key Manager have authority to give access to the user where they authorized or not. Key manager provides unique key to the users.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 6, June 2021 ||

|DOI:10.15680/IJIRSET.2021.1006183|

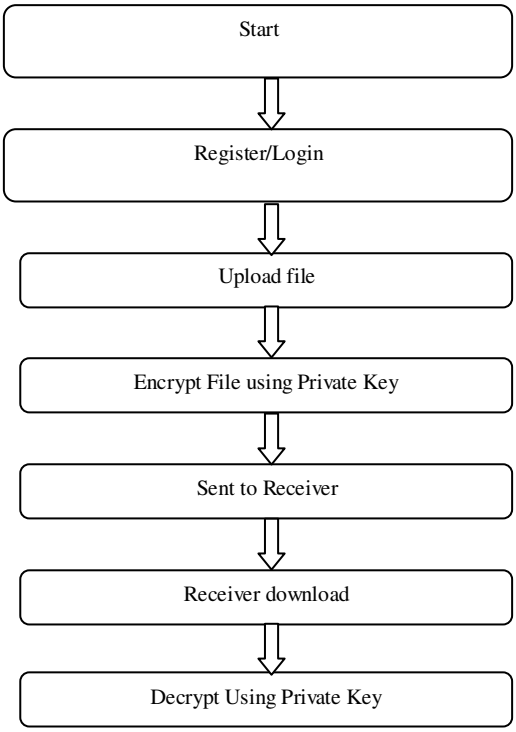

Fig: Flow Diagram

B. Mathematical model

S=
INPUT:
Identify the inputs
F= f1, f2, f3 ....., FN F as set of functions to execute commands
I= i1, i2, i3I sets of inputs to the function set
O= o1, o2, o3.O Set of outputs from the function sets,
S=I, F, O
I =upload file.
O = Output i.e. file encryption.
F= Functions implemented to get the output based on given Parameter

Space Complexity: The space complexity depends on Presentation and visualization of discovered patterns. More the storage of data more is the space complexity.

Time Complexity: Check No. of patterns available in the datasets= n If (n(1)) then retrieving of information can be time consuming. So the time complexity of this algorithm is O (nn). = Failures and Success conditions.

Failures:

- Huge database can lead to more time consumption to get the information.
- Hardware failure.
- Software failure.

Success:

- Search the required information from available in Datasets.
- User gets result very fast according to their needs.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 6, June 2021 ||

|DOI:10.15680/IJIRSET.2021.1006183|

V. CONCLUSION

When a sender want to send confidential data or file to another person / receiver or high level authority it uses several security methods. The digital signature algorithm is the scalable cryptographic solution for the secure retrieval of confidential data.

The proposed system to be developed for this project is better than any other systems the system uses encryption algorithm to protect the classified information.

REFERENCES

[1]. R. Alvaro-Hermana, J. Fraile-Ardanuy, P. J. Zufiria, L. Knapen, and D. Janssens, "Peer to peer energy trading with electric vehicles," *IEEE Intell. Transp. Syst. Mag.*, vol. 8, no., pp. 33–44, Fall 2016.

[2]. Y. Xiao, D. Niyato, P. Wang, and Z. Han, "Dynamic energy trading for wireless powered communication networks," *IEEE Commun. Mag.*, vol. 54, no. 11, pp. 158–164, Nov. 2016.

[3]. N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," IEEE Trans. Depend. Sec. Comput.

[4]. M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril, and A. Now, "Nrgcoin: Virtual currency for trading of renewable energy in smart grids," in *Proc. IEEE 11the Int. Conf. Eur. Energy Market*, 2014, pp. 1–6.

[5]. S. Barber *et al*, "Bitter to better-how to make bitcoin a better currency," in *Proc. Int. Conf. Financial Cryptography Data Security*, 2012, pp. 399–414.

[6]. J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[7]. Jiafu Wan, Jiapeng Li, Muhammad Imran, Di Li, Fazal-e-Amin, "A Blockchain-Based Solution for Enhancing Security and Privacy in Smart Factory",IEEE Transactions on Industrial Informatics Volume: 15 , June 2019.

[8]. Antonios Litke, Dimosthenis Anagnostopoulos, Theodora Varvarigou, "Blockchains for Supply Chain Management: Architectural Elements and Challenges Towards a Global Scale Deployment", MDPI January 2019.

[9]. I. Alqassem *et al.*, "Towards reference architecture for cryptocurrencies: Bitcoin architectural analysis," in *Proc. IEEE Internet Things, IEEE Int. Conf. Green Comput. Commun. IEEE Cyber, Physical Social Comput.* 2014, pp. 436–443.

[10]. K. Croman *et al.*, "On scaling decentralized blockchains," in *Proc. Int. Conf. Financial Cryptography Data Security*, 2016, pp. 106–125.

[11]. G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," in *Banking Beyond Banks and Money*. New York, NY, USA: Springer-Verlag, 2016, pp. 239–278.

[12]. L. Luu *et al.*, "A secure sharding protocol for open blockchains," *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2016, pp. 17–30.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details