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.2021.1006155|

Privacy Preserving Approach to Protect Location

Diksha Nagapure[1], Rajat Modokar[2], Neha Lad[3]

Students, Department of Computer Engineering, Sinhgad Institute of Technology, Lonavala, India

ABSTRACT: Advanced Encryption Standard (AES) algorithm is one on the most common and widely symmetric block cipher algorithm used in worldwide. This algorithm has an own particular structure to encrypt and decrypt sensitive data and is applied in hardware and software all over the world. It is extremely difficult to hackers to get the real data when encrypting by AES algorithm. Till date is not any evidence to crake this algorithm. AES has the ability to deal with three different key sizes such as AES 128, 192 and 256 bit and each of this ciphers has 128 bit block size. This paper will provide an overview of AES algorithm and explain several crucial features of this algorithm in details and demonstration some previous researches that have done on it with comparing to other algorithms such as DES, 3DES, Blowfish etc.

In a research community, data sharing is an essential step to gain maximum knowledge from the prior work. Existing data sharing platforms depend on trusted third party (TTP). Due to the involvement of TTP, such systems lack trust, transparency, security, and immutability. To overcome these issues, this paper proposed a blockchain-based secure data sharing platform by leveraging the benefits of interplanetary file system (IPFS)

KEYWORDS*:* location, AES, privacy, security , blockchain, IPFS, Ethereum, smart contracts.

I. INTRODUCTION

AES stands for Advanced Encryption Standard and is a majorly used symmetric encryption algorithm. It is mainly used for encryption and protection of electronic data. It was used as the replacement of DES(Data encryption standard) as it is much faster and better than DES. AES consists of three block ciphers and these ciphers are used to provide encryption of data. Internet communication is playing the important role to transfer large amount of data in various fields. Some of data might be transmitted through insecure channel from sender to receiver. Different techniques and methods have been using by private and public sectors to protect sensitive data from intruders because of the security of electronic data is crucial issue. Cryptography is one of the most significant and popular techniques to secure the data from attackers by using two vital processes that is Encryption and Decryption. Encryption is the process of encoding data to prevent it from intruders to read the original data easily. This stage has the ability to convert the original data (Plaintext) into unreadable format known as Cipher text. The next process that has to Cryptography and Network Security 2017 carry out by the authorized person is Decryption. Decryption is contrary of encryption. It is the process to convert cipher text into plain text without missing any words in the original text. To perform these process cryptography relies on mathematical calculations along with some substitutions and permutations with or without a key.

In the past decade, technological advancements have been made by research consortiums to adapt data sharing approaches. Data sharing is the fundamental step to gain maximum benefit from research innovations. However, it is very crucial to know the three W's for sharing purpose, such as what, when, and where. These questions need to be very much clear before initiating the data sharing process. There is still some scope to work on, how the data set owner should be given incentives or reward. This research provides secure sharing and selling of data by leveraging the benefits of blockchain [1]. Blockchain; a distributed ledger is a new trend in the world of information technology. A lot of financial and non financial applications have made use of blockchain. The consensus mechanism is considered as the most fundamental and significant invention as declared by one of the specialists of silicon valley. The current paper currency relies on third party, which means that there is a threat to security, trust, and privacy. The significant feature of blockchain is trust, which can be achieved by eliminating third party Ethereum is a decentralized open-source platform based on blockchain domain, used to run smart contracts i.e. applications that execute the program exactly as it was programmed without the possibility of any fraud, interference from a third party, censorship, or

| 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.2021.1006155|

downtime. It serves a platform for nearly 2,60,000 different cryptocurrencies. Ether is a cryptocurrency generated by ethereum miners, used to reward for the computations performed to secure the blockchain.
Solidity is a brand-new programming language created by the **Ethereum** which is the second-largest market of cryptocurrency by capitalization, released in the year 2015 led by Christian Reitwiessner.

A. Motivation

- Assumption of trusted entities .Anonymizer and trusted, non-colluding users. Considerable overhead for sporadic Maintenance of user locations No privacy guarantees especially for continuous queries Privacy
- Check-In Stress
- Many people are not keen on having everyone know their whereabouts all the time. Individuals are concerned about their privacy and services such as Foursquare can only enhance the problem.

II. LITERATURE SURVEY

Literature survey is the most important step in any kind of research. Before start developing we need to study the previous papers of our domain which we are working and on the basis of study we can predict or generate the drawback and start working with the reference of previous papers.
In this section, we briefly review the related work on location privacy system and their different techniques.
In this paper, author propose a trajectory privacy-preserving framework, named TrPF, for participatory sensing. Based on the framework, we improve the theoretical mix-zones model with considering the time factor from the perspective of graph theory. Finally, we analyze the threat models with different background knowledge and evaluate the effective-ness of our proposal on the basis of information entropy, and then compare the performance of our proposal with previous trajectory privacy protections [1].

Author propose user privacy protection for a mobile commerce alliance. They concentrate on mobile commerce model to study their anonymity models and privacy preserving algorithms. In their work, they exploit the centralized privacy-preserving system to support their methods [2].

Author introduces the three most common privacy-preserving architecture known as non-cooperation, centralized party, and peer-to peer [3].

Author introduces data sharing practices are much needed to maximize knowledge gain by researchers. However, when and what data should be shared with whom, and how credit should be awarded to the data owner needs to be clearly addressed to create an individual incentive for data owners to share their data[4].

In this paper, a blockchain-based privacy-preserving scheme is proposed, which realizes secure sharing of medical data between several entities involved patients, research institutions and semi-trusted cloud servers[5].

III. PROPOSED METHODOLOGY

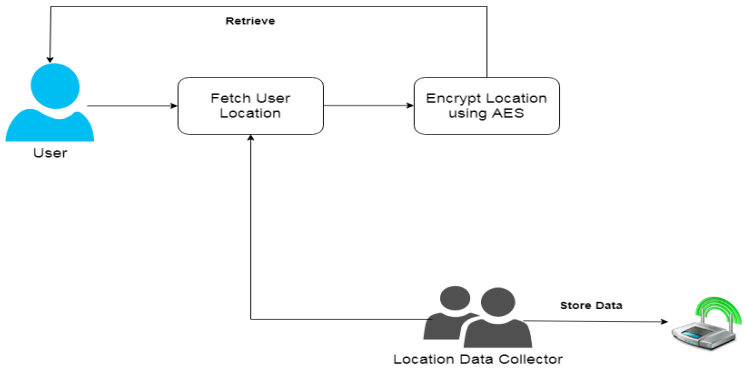

Fig. System Architecture

| 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.2021.1006155|

Algorithm:

1. AES Algorithm for Encryption.

AES (advanced encryption standard).It is symmetric algorithm. It used to convert plain text into cipher text .The need for coming with this algo is weakness in DES. The 56 bit key of des is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider asweak.AES was to be used128-bit block with128-bit keys.
Rijendeal was founder. In this drop we are using it to encrypt the data owner file.
Input:
128_bit /192 bit/256 bit input (0, 1)
Secret key (128_bit) +plain text (128_bit).
Process:
10/12/14-rounds for-128_bit /192 bit/256 bit input
Xor state block (i/p)
Final round:10,12,14
Each round consists: sub byte, shift byte, mix columns, add round key.
Output:
cipher text(128 bit)

2. Blockchain System Model.

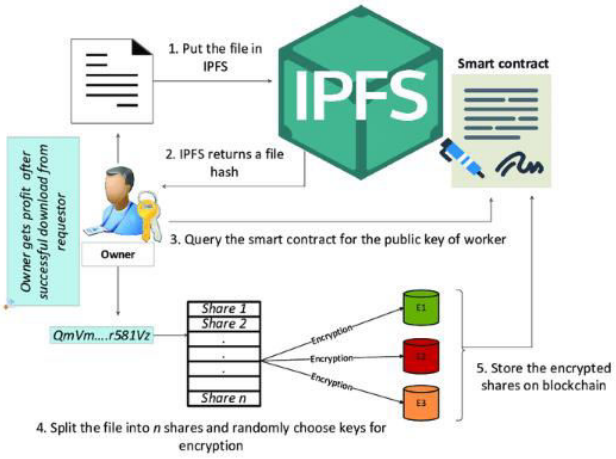

Fig. DATA SHARING ON IPFS BY OWNER.

The system model has the following entities :
Owner: It may be a person or organization which owns the data to be shared among customers. It can also control the query and access of data by filtering out the requestors.
Customer: Makes a Request for buying the data from the system. After receiving the desired content, the customer downloads the file from IPFS server by reconstructing the hash and registers his reviews about data on the review system.
Workers: It is the passive entity of system, provides decryption services on behalf of the customers. Authenticates the new customers through signatures and query the smart contract for requested data by customers.
Arbitrator: A trusted entity is responsible for solving disputes between the buyer and seller regarding the downloading of requested content. Based on the decision of arbitrator, a customer may be refunded the deposited amount.

3. Implementation

Creating metamask wallet account . Using ganache platform i.e ethereum platform , getting the private key.So basically we send the user address through IPFS and it gives an eth address when we give user address that is supposed to be made private. After IPFS we get a hash code which is then futher processed and the address is being mined in blocks . But for this there is energy consumption i.e gas limit for that we have to give a certain eth , so for that we take a private key, import a eth account into metamask and provide the necessary eth for making our location private by encrypting it into blockchain through smart contracts . The transaction of eth is the smart contract given to ethereum virtualmachine to secure Location.

| 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.2021.1006155|

Smart Contract : A contract in the sense of Solidity is a collection of code (its *functions*) and data (its *state*) that resides at a specific address on the Ethereum blockchain. To enter into a blockchain based smart contract, the parties first negotiate and agree to the terms of the agreement before memorialising the terms (either in part or entirely) in smart contract code that are stored inside the blockchain.

Transactions
A blockchain is a globally shared, transactional database. This means that everyone can read entries in the database just by participating in the network. If you want to change something in the database, you have to create a so-called transaction which has to be accepted by all others. The word transaction implies that the change you want to make (assume you want to change two values at the same time) is either not done at all or completely applied. Furthermore, while your transaction is applied to the database, no other transaction can alter it.
The Ethereum Virtual Machine or EVM is the runtime environment for smart contracts in Ethereum. It is not only sandboxed but actually completely isolated, which means that code running inside the EVM has no access to network, filesystem or other processes. Smart contracts even have limited access to other smart contracts.

III. CONCLUSION

Using internet and network are increasing rapidly. Everyday a lot of digital data have been exchanging among users. Some of data is sensitive that need to protect from intruders. Encryption algorithms play vital roles to protect original data from unauthorized access. Various kind of algorithms are exist to encrypt data. Advanced encryption standard (AES) algorithm is one of the efficient algorithm and it is widely supported and adopted on hardware and software.

A blockchain-based secure data sharing and delivery of digital assets framework is presented. The main aim of this proposed scenario is to provide data authenticity and quality of data to customer as well as a stable business platform for owner. A decentralized storage IPFS provides the solution for bloating problem at owner's end.

IV. ACKNOWLEDGMENT

Express my true sense of gratitude, sincere and sincere gratitude to my guide to the project Prof. Dr M.S. Chaudhari sir for his precious collaboration and guidance that he gave me during my research, to inspire me and provide me with all the laboratory facilities, This it allowed me to carry out this research work in a very simple and practical way. I would also like to express my thanks and thanks to our coordinator, Prof. V.S. Kadam HOD. Prof. Dr S.D .Babar and Principle Dr M.S. Gaikwad and all my friends who, knowingly or unknowingly, helped me during my hard work.

REFERENCES

1] Gao, S., Ma, J., Shi, W., Zhan, G., Sun, C.: TrPF: a trajectory privacy preserving framework for participatory sensing. IEEE Transactions on Information Forensics and Security, 8(6), 874–887 (2013).
2] Piao, C., Li, X., Pan, X., Zhang, C.: User privacy protection for a mobile commerce alliance. In Electronic Commerce Research and Applications, Vol. 18, 2016, 58-70 (2016) .
3]Mokbel, M.F.: Privacy in Location-based Services: State-of-the-Art and Research Directions. In Proceedings of the 8th International.
4]Shrestha, A.K.; Vassileva, J. Blockchain-Based Research Data Sharing Framework for Incentivizing the Data Owners. In International Conference on Blockchain; Springer: Cham, Switzerland, 2018; pp. 259–266.
5] Y. Deng, X. Chen, Z. Wang and D. Wang, "Blockchain-based Privacy Security Protection Feasibility Analysis," Software Guide, vol. 18, no. 1, pp. 166–168, Jun. 2019, DOI:10.11907/rjdk.181917.

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