ISSN No:-2456-2165

Alert System for New User to Find Safe Area using Blockchain

Prof A.B.GHANDAT
Dept of Computer Engineering,
JSPM'S Jayawantrao Sawant College Of Engineering,Pune,India

Shubham S Matole,
Dept of Computer Engineering,
JSPM'S Jayawantrao Sawant College Of Engineering,Pune,India

Kedar R Patil
Dept of Computer Engineering
JSPM'S Jayawantrao Sawant College of Engineering ,Pune ,India

Tushar D Waghmare
Dept of Computer Engineering
JSPM'S Jayawantrao Sawant College Of Engineering, Pune ,India

Pranav M Manglekar,
Dept of Computer Engineering,
JSPM'S Jayawantrao Sawant College of Engineering, Pune ,India.

Abstract:- The digital world has become an integral part of our daily lives, and with this increasing reliance comes a growing threat of cybercrime. Hackers and cybercriminals can exploit the open nature of the internet to access sensitive information, steal money, and disrupt operations. To combat this issue, organizations and individuals must implement advanced layers of security to protect their data and financial information. One key aspect of this security is data encryption, which uses mathematical algorithms to scramble data, making it unreadable to unauthorized parties.

Cryptology is the science of encryption and plays a vital role in protecting data from cybercrime. It provides various layers of security such as data security, organizational security, and identity management, to ensure that only authorized personnel can access sensitive information. Different encryption methods such as RSA, Elliptic Curve, DES, and AES are commonly used, but each has its own unique set of strengths and weaknesses.

Recently, a new approach to prevent cybercrime is proposed, which is based on blockchain technology. Blockchain is a distributed ledger technology that allows data to be stored in a decentralized and secure way. This makes it difficult for hackers to tamper with the data, and ensures the integrity of the information. By using blockchain-based cryptography methods, we can add an extra layer of security to the data, making it even more difficult for cybercriminals to access sensitive information.

I. INTRODUCTION

The web has given culprits an entirely unexpected technique for exploiting organizations and individuals for their own special advantage. Cybercrime can be portrayed as violations performed through a PC and the web.

What makes cybercrime difficult to indict is that web advancement grants people to execute bad behaviors from wherever in the world. The developer who exhausted your monetary equilibrium could be your close by neighbor or someone going against the norm side of the world.

Presently a day's clients don't have thought regarding wrongdoing in new region human wellbeing is most significant variable in world. Additionally, the wrongdoing information access by programmers or assailants by hacking action so we will construct framework which give security to the two information and human by utilizing blockchain shrewd contact. Cybercrime is considered as PC correspondence get practices which are either un legal or correspondence Get practises that are either illegal or rejected by clear-cut gatherings and that are also controllable done across the entire association medium. Correspondence get practices which are either un legal or considered denied by unambiguous get-togethers and which can be controlled over furthermore, got done with complete association medium. Cybercrimes imply criminal clatter in which the association or PC is a principal piece of the wrongdoing to take over responsibility for contraption or association. Individual and associations One of the most important challenges in the current technological world is security. Obtaining personal information and government data is extremely difficult due to cybercrime. Currently, network security professionals are using a variety of strategies and tactics to try and stop sophisticated criminals. Cybercrime is on the climb in Africa after the high-level medium covered universally.

The large quantity of detention facilities necessitates regular social events for Criminality Record Checker (CRC). The current prison system cannot manage the data effectively with a combined approach. The most important blockchain development in CRC is the usage of blocks to store information in order to prevent tampering with prisoner data. With the help of its attributes like changelessness, simplicity,

and distributed method for storing the prisoners' records, the blockchain development creates a suitable foundation for the usage of CRC. The detainees' records. The current system has concentrated capacity and generally needs the reinforcements for the detainee's information put away in the focal cut off. The significant thought for the organization is to shield the detainee's data from unapproved access and effectively recovery for the detainee's information [1,2].

Overseeing and utilizing this data can turn out to be stumbling, regardless, for state-of-the-art legislatures. The public authority offices, Police departments, for instance, have separate data sets, which complicates the flow of data across various government agencies. The availability of numerous data sets also raises the expense of security, increasing the likelihood of illegal alterations. With the quantity of records increasing, it is important to keep track of the data so that it may be shared in a structure that is functional overall.

In the policing organization, it is crucial to disseminate the detainee record widely and internationally without jeopardizing security. It is essential to have precise and minute records so that inmates can meet such interest.

Records become available on a global scale without getting beyond security measures. Recently, we looked at the square chain innovation, which gives no one person any influence over the chain. We suggest using this innovation in the CRC to prevent the risk of data altering is decreasing. Additionally, compared to present structures that use typical automated data sets, the blockchain's attribute says that it is incredibly tough to break and that the chance of information being slowed down is significantly reduced. One of the hallmarks of our system is the prevention of proof data modification during access to the detainee's record in court. The detainee's record, together with their logs, are stored in the cloud. The detainee's record is put away in the cloud and their logs and provenance are set in the blockchain [3-10].

II. RELATED WORK

The Blockchain idea, which is a public trade record of the virtual currency bitcoin, was initially put forth by Satoshi Nakamoto in 2008. Each square in the chain of squares carries information such as a hash value of a previous block and a time stamp. We can identify the invalid square using the aforesaid technique, which also guarantees the square's honesty and security. This technology was primarily used for Bitcoin, which allows for online currency exchange. The problem of double spending was given a purpose by the creator.

The framework uses a timestamping method that involves hashing each block into a non-stop chain depending on the verification of each job component. This study referred to the DAPP and savvy contract presentations. Blocks exist in Ethereum. Blockchain is a system of interconnected squares where each square contains a list of exchanges like bitcoin. These exchanges contain timestamps and various boundaries that we can configure. Each excavator PC, which is referred to as a hub, is installed with the Ethereum blockchain, which it uses. the proof of work calculations to evaluate the structure. When the code computation is carried out in each digger PC, the square has the intelligent contract that has the program scrap that runs in every square. To allow different diggers to accept, it is shipped off to the complete corporation. The chain will be extended by the square's actual check. The author wrote a thorough report on the IPFS. By hosting the web on top of shared organizations, as suggested by the author, they can completely spread it; this will act similarly to how bit-deluge does. Currently, in order to download something from the internet, we must provide a specific location, or URL. The method used nowadays to download content is known as area-based tending to and includes elements like having the content administered by a certain organization. However, if the server is down, we will not be able to access the content. Most likely, someone will have a replica of the material in their device for which we were searching, but we will not have the choice to purchase it. IPFS uses both area-based addressing and content-based management to solve this problem. Every single document on the internet will have an impressive figure print. The hash value must be examined whenever we need to download a document for the content to be available.

Different types of records can be stored in IPFS. An article is created in which records are stored, and these items can add up to 256 kilobytes of data. In this manner, n-1 articles are created in order to store a document, such as a movie, and in an object, all n-1 articles are sequentially connected. This can be used as a framework for documents. The document's accessibility is this framework's biggest flaw. As a result, in order to prevent this, we can encourage people to maintain the document accessible or we can deliberately disseminate the document with the intention that it is accessible; this describes the organization of File Currency. This paper describes a product that may be used to create blockchain-based solutions for businesses. A group of people from diverse industries gathered in 2015 to create Hyperledger, an open-source platform, in order to increase the accessibility of blockchain. The parties involved in the exchange may be informed at this point, ensuring the security and confidentiality of the transaction. The concept of permissioned blockchain innovation was developed by Hyperledger texture. The author of this paper discusses a decentralized swarm-based platform that will identify web tricks and alert others to those tricks. As digital currencies have grown in popularity, so too have web tricks, such as phishing sites, fake businesses, and other trick conspiracies that have emerged recently. It functions with the aid of any program. When a person conducts an online transaction, a banner indicating whether the site is secure or not will appear in the application. If this notice does not appear, the

person can report the site to the crypto police, who will then give them a reward. The crypto police officials will verify the report. The main goal of the crypto police is to expose extortion in the market for digital currencies. The author of this essay evaluates the value of blockchain technology in the realm of medicine. This crippling control over sensitive information inside the medical area reducing the honesty of information

III. PROPOSED METHOD

A. Introduction:

Access to accurate and secure criminal records for a specific area is crucial for individuals and families looking to move to a new location. This information can provide insight into the overall safety and security of an area, allowing individuals to make informed decisions about where to live and raise their families. Factors such as crime rate, types of crimes, and the safety of a neighborhood are essential to consider when deciding to move to a new area. However, providing this information is not without its challenges. Traditional methods of collecting and distributing criminal records are often prone to errors and inconsistencies, and the sensitive nature of the information makes it a target for hackers and other cybercriminals. Additionally, many jurisdictions have different reporting standards and protocols for criminal records, making it difficult to access and compare data across different areas.

The use of blockchain technology offers a solution to these challenges by providing a secure and tamper-proof method for storing and distributing criminal records. Blockchain technology is a decentralized system that allows for the secure and transparent storage and transfer of digital information. Using complex algorithms and cryptography, it creates a tamper-proof digital ledger that can be used for a variety of applications, such as financial transactions and supply chain management. By utilizing blockchain technology, the criminal records can be stored on a public ledger that is accessible to authorized users, while at the same time ensuring the confidentiality of the information. Additionally, the use of blockchain technology enables the creation of a standardized format for criminal records that can be easily accessed and compared across different jurisdictions. through the integration of objects, products,and operators and providing context awareness with the helpof the Internet.

B. Security In Blockchain:

The Advanced Encryption Standard (AES) algorithm is a widely used symmetric key encryption algorithm that is designed to provide a high level of security for sensitive information. It is a block cipher that encrypts data in fixed-size blocks (128 bits) and uses a fixed-size key (128, 192, or 256 bits) for both encryption and decryption.

The AES algorithm works by dividing the plaintext message into 128-bit blocks and then applying a series of mathematical operations, such as substitution, permutation, and mixing of round keys, on each block. These operations are controlled by a key schedule algorithm that generates a unique set of round keys for each 128-bit block. The key schedule algorithm uses the key provided by the user to generate a unique set of round keys for each block of the plaintext message.

The AES algorithm uses a combination of substitution and permutation operations to encrypt the data. Substitution operations involve replacing one value with another, while permutation operations involve rearranging the order of the bits. These operations are controlled by the round keys generated by the key schedule algorithm.

After the encryption process, the original plaintext message is transformed into an unreadable ciphertext. To decrypt the ciphertext, the same key and mathematical operations are used in reverse order. The key schedule algorithm is used to generate the round keys in the reverse order, and the same substitution and permutation operations are applied in reverse order. This process allows the receiver to obtain the original plaintext message.

The AES algorithm is considered to be very secure and efficient in encrypting large amounts of data. It has been analyzed extensively by experts in the field of cryptography and is widely accepted as a secure encryption algorithm. However, just like any other symmetric key algorithm, it requires a secure way to distribute the key. If a malicious actor obtains the key, they would be able to decrypt the ciphertext and access the original message. Therefore, it is important to use a secure key distribution method such as a key exchange protocol to securely exchange the key between the sender and the receiver.

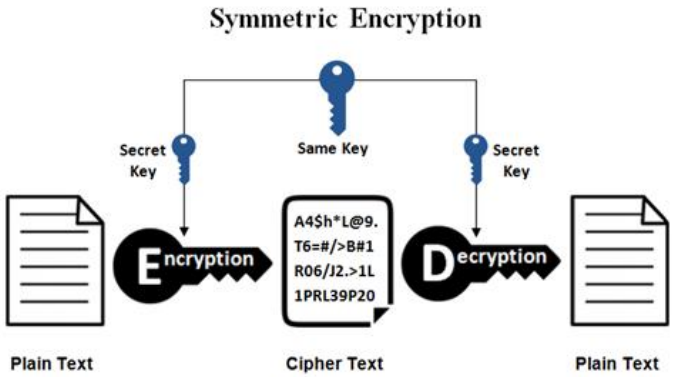

Fig 1: security in blockchain

C. Methodology:

In our proposed area crime rate alert system, we are utilizing a decentralized and distributed network based on blockchain technology to store criminal's data in the form of blocks. This allows for a secure and tamper-proof way of storing sensitive information related to criminals, as well as

enables easy access and sharing of this information among authorized parties.

The blocks in the blockchain are interconnected, creating a chain of records for each criminal. This allows for a clear and transparent view of the criminal's history and current status, which can aid in making informed decisions regarding the criminals.

To provide both private and public access to the system, we are implementing both the Hyperledger Fabric and Ethereum network. The Hyperledger Fabric network is a permissioned blockchain, meaning that access to the network is restricted to certain authorized parties. This makes it suitable for private usage where only authorized parties need to access the criminal's data. On the other hand, Ethereum network is a public blockchain, where the data is accessible to anyone. This makes it suitable for public usage where the data can be accessed by anyone who is interested.

The Hyperledger Fabric network is also designed to exchange and recover data as per agreements. This means that authorized parties can share and access the data in a controlled and secure manner. Additionally, it allows for the use of plugin modules for organizations to advance the usage of smart contracts.

In our blockchain-based area crime rate alert system, we are utilizing the security features of blockchain technology to ensure the integrity and reliability of the data. We have implemented a multi-layered system of trusted contacts, where different levels of authorities can verify and approve the data before it is stored in a block. Once the data is stored in a block, it cannot be altered or tampered with, providing a tamper-proof record of the criminal's information. This includes details such as personal information, criminal history, current status, and any other relevant information that is necessary for identifying and tracking the criminal.

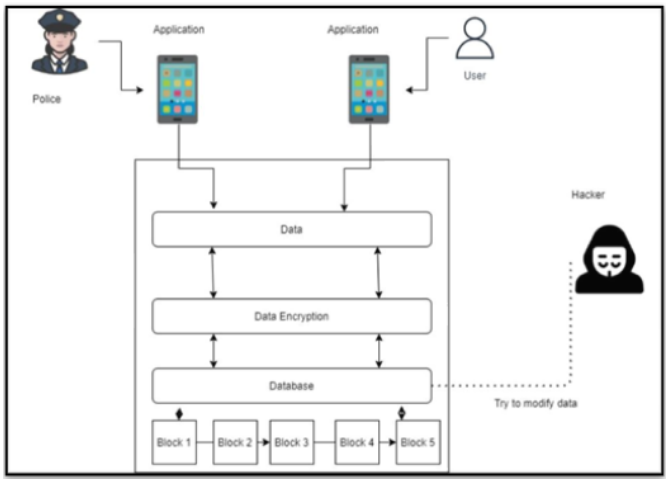

Fig 2 :System Design

Fig 3: Registration screen 1

D. Implementation:

- Police administrator: An individual who transfer wrongdoing report of region to the server
- Client: An individual who can check wrongdoing report of region transfers by police
- Hacker: An individual who attempt to change information of region wrongdoing report in data set

➢ *Experimental-Output:*

After implementing the project, the generated output is given below.

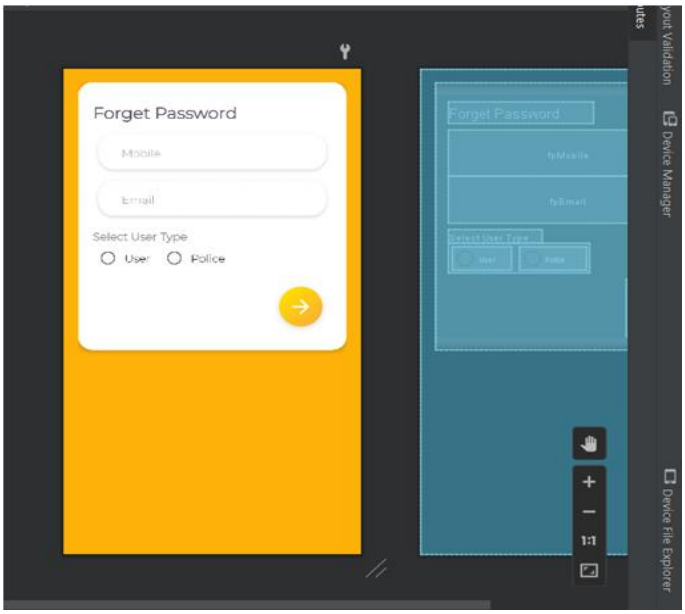

Fig 4:forgot password screen

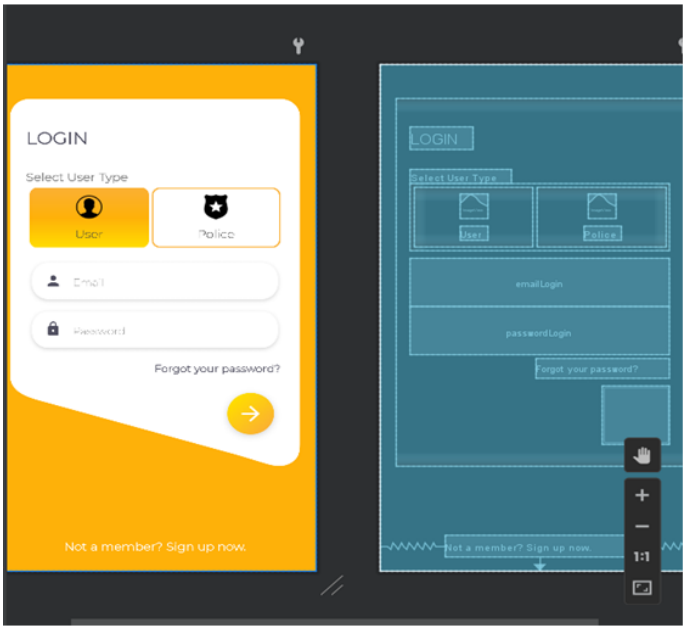

Fig5 : login Screen

IV. CONCLUSION

In today's digital age, the majority of the population uses computers and mobile phones to access the internet. As a result, there is a need for an advanced and reliable online criminal record checker. Our proposed system aims to provide just that, with an efficient, cost-effective, and user-friendly web interface. This will help reduce the need for manual data entry and make it easier for users to check criminal records and identify safer areas with lower crime rates.

REFERENCES

[1]. "Information, information all over", The Economist, 25 February 2010, accessible at http://www.economist.com/hub/15557443 (Downladed on April 30, 2012).
[2]. Bertino, "Enormous Data - Opportunities and Challenges", Panel Position Paper, Proceedings of the 37th Annual IEEE Computer Software and Applications Conference, COMPSAC 2013, Kyoto, Japan, July 22-26, 2013.
[3]. J. Manyika, M. Chui, J. Bughin, R. Dobbs, P. Bisson, and A. Marrs. Problematic innovations: Advances that will change life, business, and the worldwide economy. http://www.mckinsey.com/experiences/business innovation/disruptive_technologies, May 2013.
[4]. Bertino, S. Nepal, R. Ranjan, "Building Sensor-Based Big Data Cyberinfrastructures", IEEE Cloud Computing 2(5): 64-69 (2015).
[5]. Atzori, M. (2017). Blockchain Governance and the Role of Trust Service Providers: The TrustedChainÂ® Network. Available online at: https://trustedchain.it/wp-content/uploads/2017/11/ATZORI_-TrustedChainWhite-Paper.pdf
[6]. Baars, D. (2016). Towards Self-sovereign Identity Using Blockchain Technology (Master's thesis). University of Twente, Enschede, Netherlands.
[7]. Bandyopadhyay, P. (2018). The origin of blockchain from cypherpunks to Satoshi to IBM medium.
[8]. Higgins, S. (2014). Factom outlines record-keeping network that utilises bitcoin's blockchain. Coindesk. Available online at: https://www.coindesk.com/factom-white-paper-outlines- record-keeping-layer-bitcoin
[9]. Cheng, S., Duab, M., Domeyer, A., Lnudqvis, M.: Using blockchain to improve data management in the public sector. https://www.mckinsey.com/business-functions/digital- mckinsey/our-insights/using-blockchain-to-improve-data- management-in-the-public-sector
[10]. Open Trading Network: UK police – blockchain solutions on the horizon. https://medium.com/@otncoin/uk-police-blockchain-solutions-on-the-horizon- 60e3e1932ef3
[11]. Anh, D.T.T., Zhang, M., Ooi, B.C., Chen, G.: Untangling blockchain: a data processing view of blockchain systems. IEEE Trans. Knowl. Data Eng. 30(7), 13661385 (2018).