IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

To Secure Crime Data Alert and User Alert System using Blockchain

Bhagyashri Sable[1], Prajakta Throat[2], Komal Hire[3], Pushpak Bhole[4], Mayur Kale[5], Mr. Rahul Dhokane Sir[6]
Students, Department of Information Technology[1,2,3,4,5]
Guide, Department of Information Technology[6]
Sir Visvesvaraya Institute of Technology, Nashik, Maharashtra, India

Abstract: *In the current scenario, the demand for computerization and data security has been increasing to combat with the increasing rate of crimes in the society. In the existing solution for prison management system there exist substantive data symmetry among prisons. Thus, during access of any prisoner detail, system may provide inappropriate details. Our objective is to implement a novel approach that stores the prisoner's credentials and efficiently verifies the prisoner's credentials via the blockchain technology. Our proposed solution is implements in the Hyperledger framework and the experimental result shows that our proposed solution is beneficial for the existing and upcoming investigation department.*

Keywords: Prisoner's Credentials, data security, block chain. Criminal records, Cryptography.

I. INTRODUCTION

The current Criminality Record Checker (CRC) needs steady gathering of the considerable number of detainment facilities. The current jail system is not effective with incorporated method for putting away the information. To forestall altering of detainee's information we use to store data in blocks which is most significant blockchain innovation in CRC. The blockchain innovation lays a decent asphalt for the usage of CRC with the assistance of its highlights like immutability, transparency, and distributed method for storing the prisoner's records. The existing framework possess centralized storage and always needs the backups for the prisoner's data stored in the central sever. The major consideration for the administration is to safeguard the prisoner's information from unauthorized access and efficiently retrieval for the prisoner's data [1,2]. Managing and using this information can end up being lumbering, in any event, for cutting edge governments. The government agencies such as law enforcement agencies have separate databases, which makes a hindrance in the ease of information stream among various government organizations.

The presence of different databases additionally expands the expense of security and consequently, the likelihood of unlawful changes are expanding bit by bit. With this increasing number ofrecords, it becomes essential to keep record in the data sharing framework which is workable in the worldwide.

In the law enforcement government agency, it is necessary to convey the prisoner record nationally and internationally without compromising the security. In order to satisfy such demand, it is essential to have precise and tiny records such that prisoners record get globally available and without bypassing the security policy. Recently, we have reviewed the new technology named as block chain where an individual cannot control the whole chain system. In the CRC, we propose to use such technology for preventing the danger of information altering is lessening. Additionally, the characteristic of the blockchain implies that it is incredibly hard to crack and furthermore the danger of data being interfered with is significantly diminished contrasted with current frameworks that utilization customary computerized databases. One of the points of our framework is to guarantee that evidence data isn't altered during accessing of the prisoner's record in the court. The prisoner's record are stored in the cloud and their logs and provenance are placed in the blockchain [3-10].

In the centralized database (DBS), it is possible that system get attacked by the hackers, which may cause serious harm for the legitimacy of the information. The security of the framework heavily depends upon the DBS framework. The SQL injection attacks have gotten increasingly basic as of late. SQL injection is an exceptionally dangerous attack wherein hackers attempt to access the data stored in a DBS. The decentralized nature of blockchain ensures that characteristic issues of the system, similar to hardware and programming glitches, does not effects on an integrity of the information. Since the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

information has different duplicates placed on every site of the system. An Information in the blockchain is undisputable, suggesting that all progressions are transparently visible in the whole system.

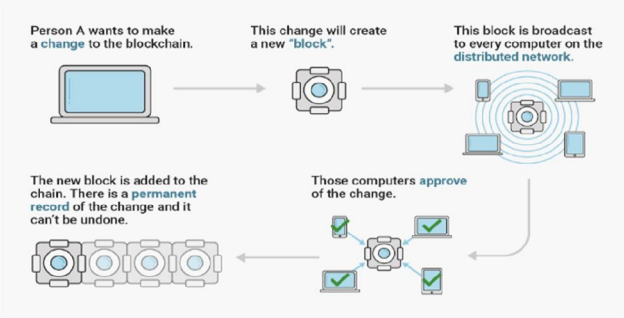

Figure 1: Insertion of a new block in blockchain.

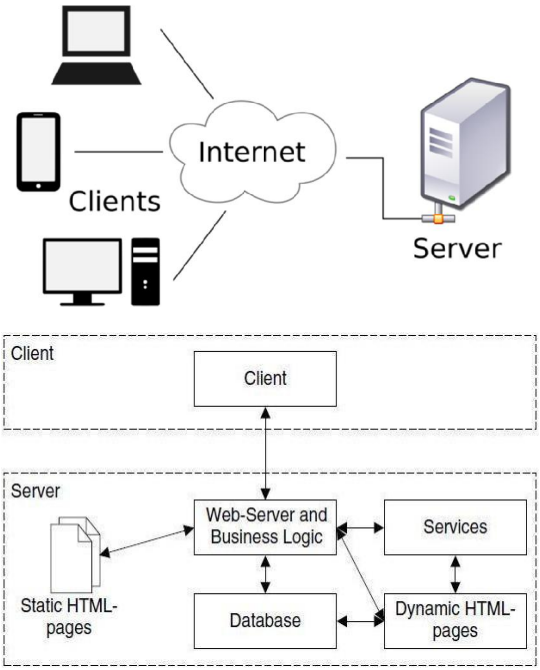

Figure 2: Prototype of client-server architecture in Criminality record checker.

The updation conducted on the data is checked by numerous sites, and consequently misrepresented information would not be able to discover its route in the blockchain. Any endeavor to threaten the frameworkshould remember synchronous attacks on minimum 51% ofsites of a blockchain to affect a single block. Our framework utilizes a distributed management for data. The clients of our framework are pre-enlisted. The sender must primarily sign into the framework. At this point they digitally sign the data. Our framework verifies the digital signature to authenticate that the data is valid or not. The authenticated data is the encrypted suing encryption algorithm. The encryption algorithm uses the randomly generated key to conduct the process for encryption. The metadata is forwarded on the blockchain. The location for the authenticated data in the blockchain is accessed via the system. The system at this point stores basic searching parameters, passport number, similar to case number, name of accused and national identification number in a nearby DBS.

II. Literature Survey

The Blockchain technology was first proposed by Satoshi Nakamoto in 2008, it is a public transaction ledger of the cryptocurrency bitcoin. It is a chain of blocks where each block contains information like hash value of previous bock and time-stamp. From the above method integrity and security of the block is ensured and we can identify the invalid block. The

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

first application of this technology was Bitcoin, which allows cash transaction using internet. The author gave a resolution to the problem of double spending. The system uses the method of timestamp by hashing the block into continuous chain based of proof of work mechanism. The introduction of the DAPP and smart contract comes was mentioned in this paper. We have blocks in the Ethereum blockchain, these blocks are linked together and each block we have list of transaction similar to bitcoin. Inside these transactions we do have timestamp and other parameters which we can programme on it. Ethereum blockchain gets stored in every miner's computer which is called a node, it uses the proof of work algorithm to verify the network. The block contains the smart contract which has the code snippet that runs in each block, when the code computation is successfully executed in each miner's computer. It is sent to whole network so that the other miners can agree. The successful verification of the block will be added to the chain. The author did a thorough study about the IPFS. According to the author they want to make the web completely distributed by running it top of the peer to peer networks, it will work similarly how bit-torrent works. In the current scenario when we want to download the content from the web, we have to provide the exact location which we call a URL. Present-day, the model which is followed to download the content is centralize i.e. it is govern by a particular organization – this is called location- based addressing, but if the server is down then we will not get the content. There is a chance that there must be someone who will have the copy of that content in their device which we were searching yet we won't be able to get that. To solve this issue IPFS works from location-based addressing to content-based addressing. All the files in the internet will have a unique figure print. When we want to download the file, we have to compare the hash value and the content will be available. In IPFS there are different types of file that we can store, an object is created in which files are stored, and these objects can only store up to 256kb of data. So, to store a file like a video n-1 number of objects are created and in n object all the n-1 objects are linked in a sequential manner. This can be used as a file system. The biggest disadvantage of this system is to keep the file available. So, to avoid this we can incentivize people to keep the file available or we can proactively make the file distributed so that the file is available – this defines the system of Filecoin. This paper describes about the software that can be used to create blockchain based solution for businesses. Hyperledger is an open source platform, in 2015 people from different industry came together to make blockchain more accessible to the world. In this platform the member who are linked to the transaction will only be notified, this create privacy and confidentiality of the transaction. Hyperledger fabric came up with the concept of permissioned blockchain technology. In this paper the author talks about decentralized crowd based platform that will identify the scams in internet and it will also provide notification to the other people about the scams in the internet, due to the growth of the cryptocurrency the scams have also increased like phishing website, fake projects and various scam scheme have grown these days. It works with the help of any browser. When a person will do any transaction through the internet there will be a flag which will appear in the browser which will say whether the website is safe or not if these notification does not appear then that person can provide them a report about the website and the crypto police give them a reward. The report will be verified by the officers of crypto police. The main task of crypto police is to report fraud in the cryptocurrency market. In this paper, the author discusses about the importance of blockchain in the medical field. The sensitive data in the medical field is getting manipulated this enfeeble the integrity of data.

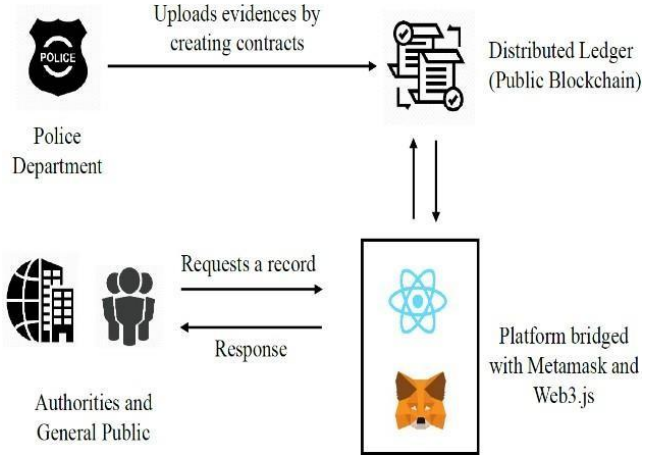

Figure 3: Working Model of Criminality record checker.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

IV. Security In Blockchain

In our blockchain we used RSA Asymmetric cryptography to provide security in the system. Basically, RSA Asymmetric cryptography contains a keypairs of two parts:

1. Public key, and
2. Private key.

The public key is shared among everyone where anyone can view the public details of the account in the network. It is strongly tied with the password (private key) for security purposes. Although the keys are strongly tied with each other but it is not possible to extract the private key using public key or vice versa. Additionally, it is also not feasible to validate any operation on the account with using only the public key.

A private key is similar to a password and is linked with a certain public key. Private key is not publicly available to everyone and is not shared with anyone in order to provide security to an account. It is kept secret and known only to the receiver. The private key is used to provide authenticity actions on the accounts. Unlike with 'normal accounts', to access and know the account details, or to take any important action, one must use the private key at the receiver end which is known to receiver only so that security can be provided to an account using RSA algorithm.

In the graphic below one can see how public keyand private key pairs work in practice, when sender is sending a message to receiver end securely. Initially sender encrypts the message with the public key of the receiver and then sends encrypted message to the receiver safely, on the other end when this encrypted message reaches to the receiver then the receiver receives this message and decrypts it using the private key of the sender which is known to receiver only. In this way the security is provided to the message using RSA Asymmetric cryptography.

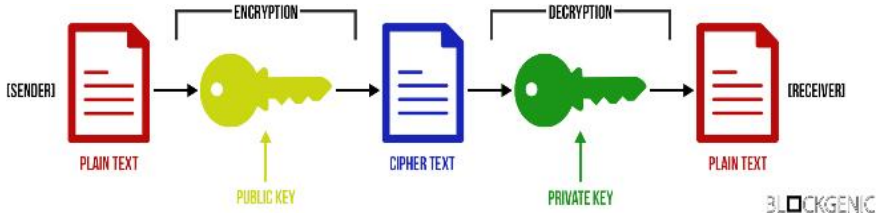

Figure 4: Security in Blockchain.

V. Methodology

In this system we have used decentralized and distributed network in order to store prisoner's data in form of blocks. The blocks are interconnected with each other and are creating the a chain of prisoner records. In this system our objective is to implement both hyperledger fabric as well as Ethereum network because we are providing our system not only for private use but also for public use. In hyperledger fabric network the data is kept in private mode, whereas in ethereum the data is kept for public use.It is expected that the hyperledger exchange and recover the data as per agreement. It must also permit the utilization for plugin modules such that various organizations advance the use for smart contract. In our proposed system the blockchain is only used for security purpose we have created different levels of trusted contacts and only if the higher authority allows the data to get storedin blocks then only it will be in blockchain database.

There are 2 higher authorities which will provide green signal to data which needs to be stored in blocks, once the data gets stored it cannot be manipulated. The blocks will contain all the necessary details of prisoner.

- **Blocks:** It represent a block of transaction, which has been broadcast in the whole system. Whenever any new block of new transaction is authenticated by the system, block is added in the trailer end of the blockchain. This sequence of blocks is always increasing, or ledger of transaction that the system has authenticated. The primary block in a blockchain is named as the Genesis block. This primary block holds the zero hash value for previous block because genesis block doesn't have any previous block. The next block will have the hash value of the previous block and this chain continues.
- **Blockchain:** When blocks are connected with previous hash values and starts forming a chain then we declare it as a blockchain.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

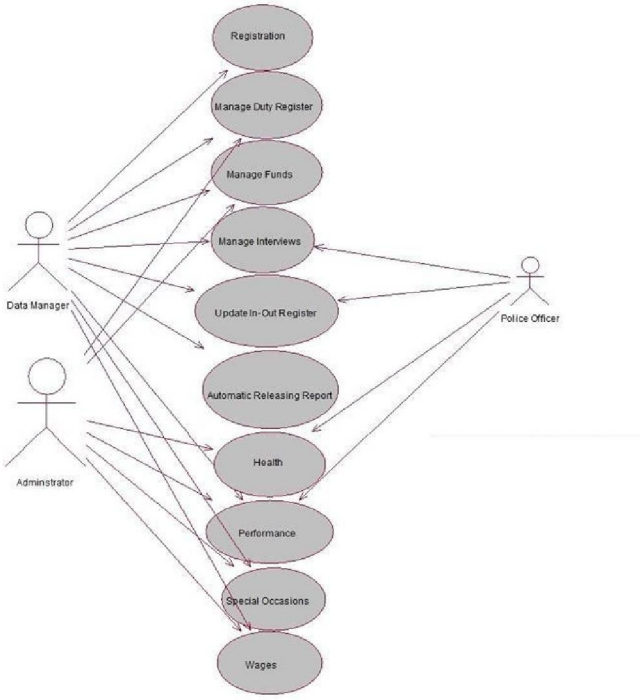

Figure 5: Use Case Diagram

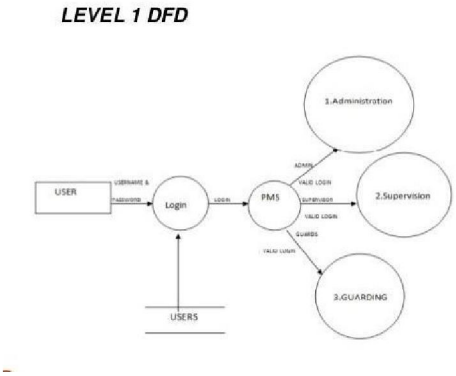

Figure 6: Data flow diagram

VI. PROPOSED ALGORITHM

The algorithm for processing our proposed work is as follows.

5.1 RSA Key Pair Generator

```
package blockchain; import java.io.File;
import java.io.FileOutputStream;
import java.io.IOException;
import java.security.*;
import java.util.Base64;
public class RSAKeyPairGenerator {
        private PrivateKey privateKey;
        private PublicKey publicKey;
        public RSAKeyPairGenerator() throws NoSuchAlgorithmException {
```

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

```
                KeyPairGenerator keyGen = KeyPairGenerator.getInstance("RSA");
                keyGen.initialize(1024);
                KeyPair pair = keyGen.generateKeyPair();
                this.privateKey = pair.getPrivate();
                this.publicKey = pair.getPublic();
        }
        public void writeToFile(String path, byte[] key) throws IOException {
                File f = new File(path);
                f.getParentFile().mkdirs();
                FileOutputStream fos = new FileOutputStream(f);
                fos.write(key);
                fos.flush();
                fos.close();
        }
        public PrivateKey getPrivateKey() {
                return privateKey;
        }
        public PublicKey getPublicKey() {
                return publicKey;
        }
```

5.2 RSA Util Algorithm

```
package blockchain;
import java.security.*;
import java.security.spec.InvalidKeySpecException;
import java.security.spec.X509EncodedKeySpec;
import java.util.Base64;
public class RSAUtil {
        public static PublicKey getPublicKey(String base64PublicKey){
                PublicKey publicKey = null; try{
                        X509EncodedKeySpec keySpec =
                        new X509EncodedKeySpec(Base64.getDecoder().decode(base6 4PublicKey.getBytes()));
                        KeyFactory keyFactory = KeyFactory.getInstance("RSA");
                        publicKey = keyFactory.generatePublic(keySpec);
                        return publicKey;
                } catch (NoSuchAlgorithmException e) {
                        e.printStackTrace();
                } catch (InvalidKeySpecException e) {
                        e.printStackTrace();
                }
        return publicKey;
        }
}
```

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

VI. EXPERIMENTAL OUTPUT

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

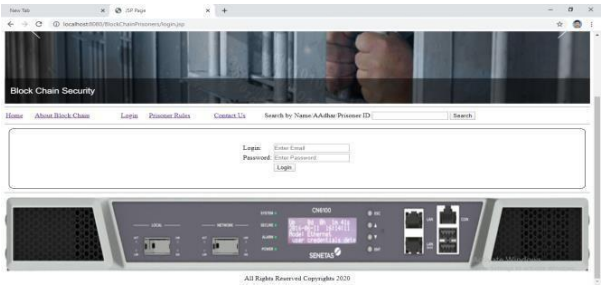

Figure 7: Login Form

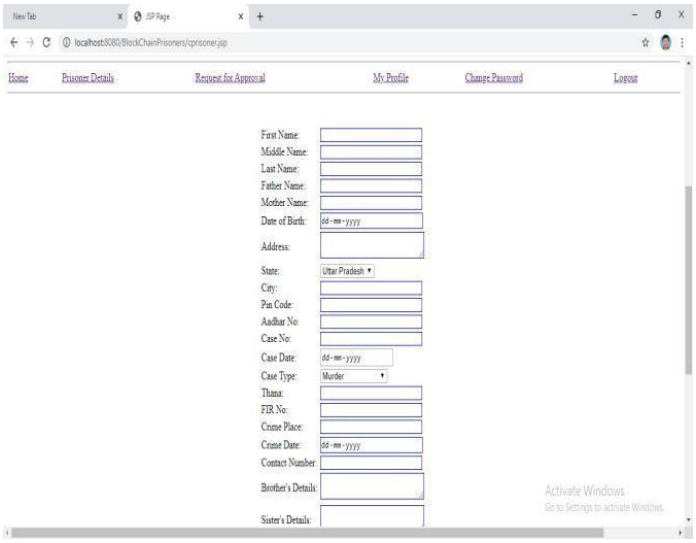

Figure 8: Prisoner's Entry Form

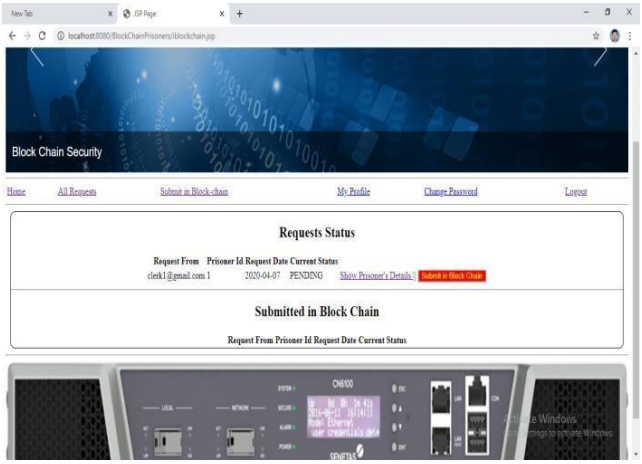

Figure 9: Prisoner's Record Request Form

VII. CONCLUSION

Nowadays, computers and mobile phones are used by most of the population of the world and with the help of internet one can look around it. As a result, Criminality record checker needs to be advanced and reliable. This application will present an advanced, reliable, cheap and efficient online criminality record checker with an attractive and intelligible web

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

GUI, thereby it reduces the work of entering the data manually. It is a software which helps the authority to work easily with the criminals and related crimes. The reason behind creating this sort of system described in the paper is to present an idea of implementation of blockchain in criminality record checker.

REFERENCES

[1]. Sourav Bhowmick, "Criminal Report Management System", Department of Computer Science and Engineering, ADMAS Institute of Technology, 2013.

[2]. Mohammad Shahnawaz, "Crime Reporting and Crime Updates", 3rd International Conference on System Modeling in Research Trends (SMART) College of Computer Science and Information Technology (CCSIT), Teerthanker Mahaveer University, Moradabad, 2014.

[3]. Alston, E. (2019). Constitutions and Blockchains: Competitive Governance of Fundamental Rule Sets. Working paper 2019.003. Center for Growth and Opportunity, Utah State University, Logan, UT.

[4]. Atzori, M. (2015). Blockchain Technology and Decentralized Governance: Is the State Still Necessary?

[5]. Atzori, M. (2017). Blockchain Governance and the Role of Trust Service Providers: The TrustedChain® Network. Available online at: https://trustedchain.it/wp-content/uploads/2017/11/ATZORI_-

[6]. TrustedChainWhite-Paper.pdf

[7]. Baars, D. (2016). Towards Self-sovereign Identity Using Blockchain Technology (Master's thesis). University of Twente, Enschede, Netherlands.

[8]. Bandyopadhyay, P. (2018). The origin of blockchain–from cypherpunks to Satoshi to IBM medium. Availableonlineat: https://medium.com/datadriveninvestor/cypherpunks-to- satoshi- to-ibm-819ebcfdd674

[9]. 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