IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁒ Impact Factor 8.102 ⁒ Vol. 12, Issue 3, March 2023

DOI: 10.17148/IJARCCE.2023.12373

FIR SYSTEM USING BLOCK CHAIN TECHNOLOGY

Bharath Kumar V[1], Dr. Mir Aadil[2]

Student, MCA, Jain Deemed to be University, Bangalore, India[1]

Assistant Professor, School of CS & IT, Jain Deemed to be University, Bangalore, India[2]

Abstract: In police stations, there are records of crimes. Crime Records are unable to locate crimes and the offenders who committed them. To maintain the crime and criminal data under the current system, a FIR is used. It has less security and makes fraud simple to do. Each time, a manual update has been made to the record. This system's primary goal is to secure data utilising block chain technology. Using their authentication credentials, Crime Investigators can view the data form database. The reports, which are prepared by witnesses and police officers, are accessible to the investigator (writer).

Investigators have the authority to edit data (i.e., update, remove, and so on), and this data aids investigators in speeding up their investigations and identifying offenders more quickly. Previous research has focused on the centralized handling of digital evidence, however if a centralized system server is breached, sensitive operational and investigation data may be exposed. As a result, there is a need to manage digital evidence and investigative information in a distributed system setting using block chain technology. Performance is reduced when massive amounts of data, such evidential films, are kept in a block chain because more data must be processed only once before being generated. As a result, we suggest three-tier block chain architecture, with hot and cold block chains for digital evidence. Information that changes regularly is stored on the hot block chain, whereas material that does not change, such as files, is saved in the cold blockchain. To assess the system, we compared the storage and inquiry processing performance of digital crime evidence across the multi-level block chain system's capacities.

Keywords: FIR, Blockchain, Security, Cryptography.

I. INTRODUCTION

Consider a distributed network fabric with a ledger that keeps track of every transaction and updates whenever a new one happens. Each member of the distributed network fabric carries a portrait of the ledger, and there is no single administrative body that controls the ledger. The issue is that once anything is added to the ledger, it cannot be taken out. That was a succinct description of blockchain technology. In the main publication, Bitcoin was mentioned as the first application of blockchain technology. To protect Bitcoin transactions, this technology is currently kept up to date; numerous administrators look after this digital record. In the bitcoin network, which keeps track of individual transactions, every system is a node. These nodes independently carry out the calculations and compute the transactions. The aforementioned transaction will be disseminated to all other nodes in the decentralised fabric network using a multi-hop broadcast. A transaction's combination is a crucial step.

A block is a legitimate transaction, and a blockchain network is made up of many legitimate blocks. In essence, we have to show the legitimacy of a block before we can attach it to a blockchain. The network requires a specific minimum number of consensuses before a block can be added. Proof of work, proof of stack, and byzantine fault tolerance consensus procedures are typically used to authorise the block. When the freshly produced block is linked with the other block in the distributed fabric network, it impersonates the other block with the additional nodes.

It is computationally unfeasible to reconfigure the network each time a request is made to remove a validated block from the blockchain. Consider the transparency that would result from the blockchain being designed to support police statements, such as First Investigation Reports (FIR). A distributed fabric network node that has a copy of the blockchain is referred to as a zone in this architecture. The technology generates a timestamped FIR each time a fresh complaint is submitted and associates it with the complaint. To authenticate the block's integrity, a cryptographically produced hash key may be supplied to the concerned complaint. We will use the consensus method to show that the block is genuine. The valid block and the time stamp will be broadcast to every node in the distributed fabric network.

DOI: 10.17148/IJARCCE.2023.12373

The user must have their personal AADHAAR number available in order to register using a mobile device and file a complaint. The location is necessary for the app to efficiently transfer the complaint to the closest police station. To validate the block, just association with the hash key is necessary. Invalidation is computationally difficult and too simple since as soon as a block shows that it is valid, it will be securely connected to the blocks that came before. As a block receives more confirmations, the hash power becomes more decentralised.

II. SECURITY IN BLOCKCHAIN

The degree of security that the blockchain technology offers to the network is one of its key characteristics. A few algorithms, including SHA-256 and hash trees, are utilised in this technique to safeguard data using cryptographically constructed blocks. These algorithms simply involve disguising a person's identity, which will aid in the development of a no-trust network. When a case is submitted, the user—who may be the complainant, suspect, witness, or officer—does not know the identity of the person involved, therefore there is no need for manual involvement; the case will progress without issue. As there would be no centralised authority to meddle, the decentralisation of blockchain offers an additional benefit. Data deletion in a network is simple when there is only one administrator, creating a single point of failure. We will be creating the system we are going to discuss from the open-source market, which will rely on the Blockchain technology, and it will eliminate all of these security risks.

III.LITERATURE REVIEW

A blockchain-based approach was developed by Antra Gupta et al. (2019) to safeguard FIR systems. The suggested solution is made to offer a safe and unchangeable record of FIR complaints and associated evidence. The FIR report and supporting documentation are stored in the system utilizing a smart contract on the blockchain. Only authorized people will be able to see the FIR report and supporting documentation, and once the report has been published on the blockchain, it cannot be changed or removed. Only authorized users would be able to access the encrypted material because the encryption keys would be stored on the blockchain.

For the city of Riyadh, K. Tabassum et al. has developed an online system for crime reporting and administration in 2018, with the provision of a consolidated platform for both individuals and law enforcement organizations, is intended to simplify the process of reporting and handling crimes. A web-based application was used in the system's construction to enable online crime reporting by the public. Blockchain technology is used by the system to guarantee the data's security and accuracy. The criminal reports and associated evidence are stored on the blockchain, creating a tamper-proof record of the crime.

An online crime reporting and management system has developed for both individuals and law enforcement organizations for the city of Riyadh, it is intended to simplify the process of reporting and handling crimes. (Iyer A. et.al., 2016)

In 2017, to register FIRs and use an SOS (emergency) system online, Shivaganesh Pillai. et.al. aims to improve citizen convenience and accessibility in the FIR registration and emergency reporting process by allowing citizens to register FIRs online through a web-based application. The program is connected to a backend server that stores the FIR reports and associated evidence in a database. Also, the platform has an SOS feature that enables citizens to report situations and get prompt assistance from law enforcement.

In 2019 Sanjay Misra. et.al., developed an electronic reporting system for the police in Nigeria to make Nigeria's reporting and administration of crime more effective and efficient. Which uses a web-based application that enables online crime reporting from the public. The server stores the crime reports and associated evidence in a database. The criminal reports and associated evidence are stored on the blockchain, creating a tamper-proof record of the crime. A tool that helps law enforcement organizations handle and investigate crimes is also included in the system. The service includes in-the-moment updates on crime activity, including details on the locations of law enforcement agencies and the state of the investigation.

An e-police system to improve the e-government services in Bangladesh was developed in 2012. The suggested method has been contributing to increase the effectiveness and efficiency of Bangladesh's law enforcement organizations, which would ultimately result in a society that is safer and more secure. (Mollah Muhammad Islam. et.al., 2012)

Complaint management system that can effectively handle and manage citizen complaints is implemented by P. Kormpho et.al. in 2018, to increase the complaint-handling efficiency, accountability, and responsiveness of governmental organizations. The network comprises a dashboard that shows the quantity and nature of complaints received, their current state, and how quickly government agencies responded to them. The platform also has a tool for creating reports and analytics on the complaints that have been received, which can assist government organizations in quickly identifying and resolving problems.

An E-police system was developed to enhance the provision of e-government services in underdeveloped nations. The suggested system intends to offer a quick and clear method for managing and reporting crimes. The academics suggest incorporating mobile technology into the E-police system so that people can report crimes using their mobile phones. The technology has functions including automatic communication to the closest police station, GPS location monitoring, and multimedia evidence collection. The researchers additionally recommend using a central database to store and manage criminal records, allowing for simple information sharing between police stations and convenient access. (Muhammad Baqer Islam. et.al., 2012)

A real-time criminal records management system introduced for national security agencies. The designed scheme seeks to offer a centralized platform for real-time crime record collection, management, and storage, enabling swift response and action by security agencies. (Onuiri Ernest Oludele. et.al, 2015)

A blockchain-based criminal record management system dubbed CRAB (Create, Retrieve, Append, Burn) is introduced by Tasnim et al. in 2018 to offer a decentralized, secure, and impenetrable platform for managing criminal records that can be accessed by authorized parties including law enforcement organizations, courts, and other pertinent authorities. The findings argue storing and managing criminal records using blockchain technology. The solution makes use of a private blockchain to protect the data's security and privacy. It additionally advocates automating the management of criminal records using smart contracts, which can assist to lower errors and increase efficiency. The advantages of utilizing blockchain technology for handling criminal records are highlighted in the report.

IV. PROPOSED METHODOLOGY

The methodology for implementing a FIR system using blockchain technology typically involves the following steps:

A. System requirements analysis: This involves understanding the requirements and needs of the stakeholders involved in the FIR system. This would include understanding the data elements to be captured, the different user roles and permissions, and the necessary security measures.

B. Design: This involves designing the system architecture and database schema. The design should ensure that the system is scalable, secure, and easily accessible.

C. The creation of smart contracts: Smart contracts are the foundational element of a blockchain-based system. The details of the agreement between the buyer and seller are directly encoded into lines of code in smart contracts, which are self-executing contracts. To record the regulations regulating the FIR system and guarantee that it operates as planned, the smart contract code would need to be built.

D. Integration: Once the smart contracts have been developed, they need to be integrated into the blockchain network. This involves deploying the smart contracts onto the blockchain network and ensuring that they function as intended.

E. Testing: Once the system is integrated, it should be tested to ensure that it functions as intended. This would include testing for security vulnerabilities, data accuracy, and user experience.

F. Deployment: After testing, the system can be deployed to production. The deployment process should ensure that the system is easily accessible, scalable, and secure.

G. Maintenance: Once the system is deployed, it needs to be maintained to ensure that it continues to function as intended. This would include regular updates to the smart contracts, monitoring for security vulnerabilities, and addressing any system issues that arise.

DOI: 10.17148/IJARCCE.2023.12373

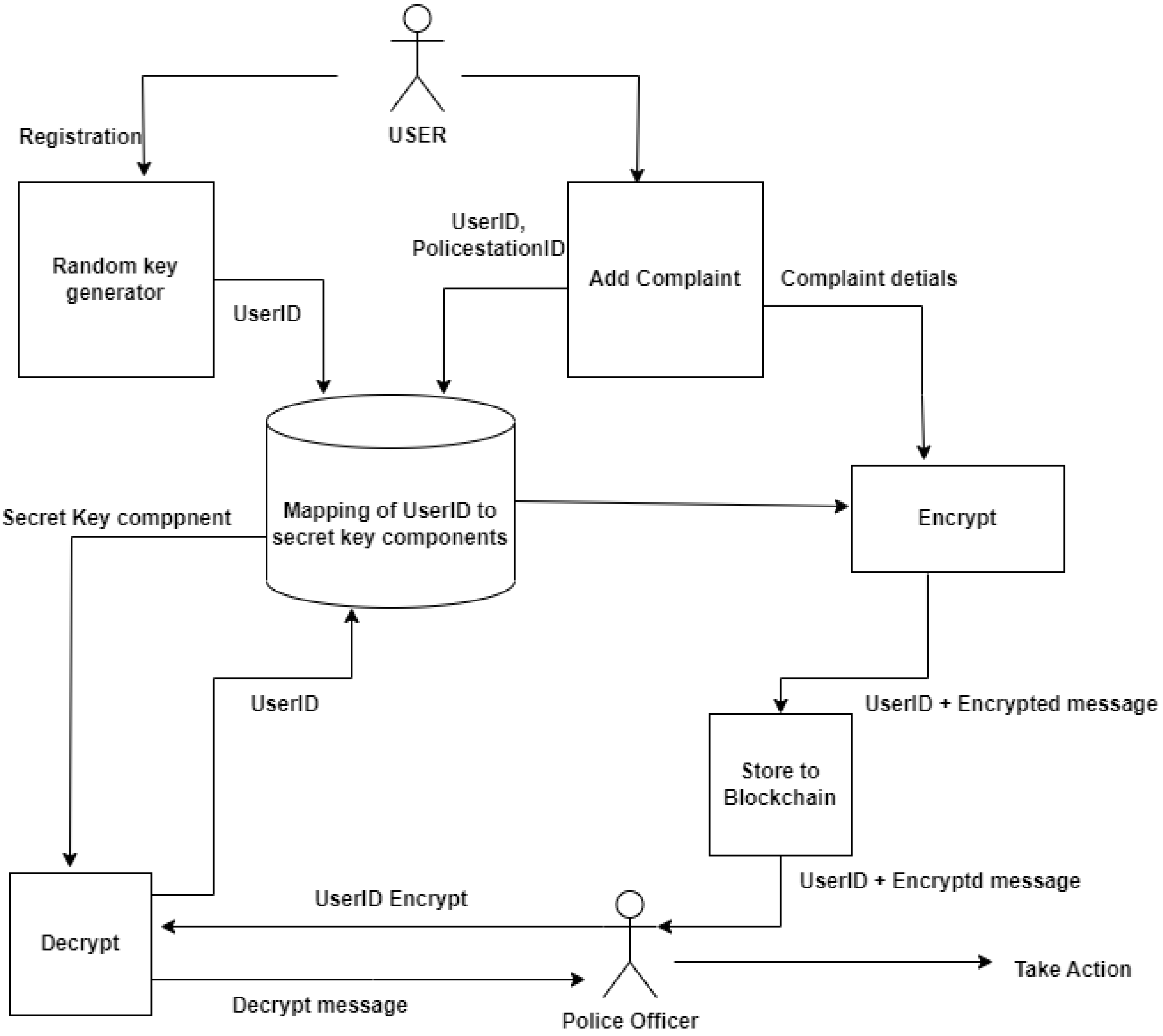

Fig 1: FIR system using Blockchain technology

A. User submits a complaint: The process starts when a user submits a complaint through an online form or application.

B. Complaint Verification: Once the complaint is submitted, it goes through a verification process to ensure that it is a genuine complaint. This step is essential to prevent false complaints from clogging up the system. The verification process can include checking the user's identity, verifying the location and time of the incident, and examining any supporting evidence.

C. Complaint registration: After the complaint is verified, it is registered in the blockchain network. This step involves creating a new block in the blockchain with the details of the complaint. The block contains a unique ID, timestamp, and other relevant information. Once the block is added to the blockchain, it cannot be altered or deleted, ensuring the integrity of the complaint record.

D. Complaint tracking: The user can track the progress of their complaint through the system. They can see when the complaint was registered, who is handling it, and any updates or actions taken on it. This transparency helps build trust between the police department and the public.

E. Investigation and resolution: The police department investigates the complaint and takes appropriate action. This can involve gathering more evidence, interviewing witnesses, or making arrests. Once the investigation is complete, the police department updates the complaint record in the blockchain with the outcome.

DOI: 10.17148/IJARCCE.2023.12373

F. Complaint closure: After the complaint is resolved, it is marked as closed in the system. The user is notified of the outcome, and the complaint record remains in the blockchain for future reference. If the complaint was false or invalid, it can be marked as such to prevent it from being used as evidence in the future.

Overall, the use of blockchain technology in a police complaint management system ensures that complaint records are secure, transparent, and tamper-proof. It also provides an efficient way for the police department to manage complaints and track their progress, leading to better accountability and public trust.

V. CONCLUSION

This system is what we're suggesting in order to protect the FIR system. Our goal is to simplify and improve the system. No trust is required to operate the decentralized network we are creating. Any device with an internet connection can be used by a registered user to submit a complaint. We may state that the network will be a corruption-free network since the blockchain will make it more secure, unchangeable, and decentralized. Future papers will explore the system's limitations and implementation.

REFERENCES

[1] Gupta, Antra and D. V´ılchez Jose. “A Method to Secure FIR System using Blockchain.”. International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-1, May 2019.

[2] K. Tabassum, H. Shaiba, S. Shamrani and S. Otaibi,” e-Cops: An Online Crime Reporting and Management System for Riyadh City,” 2018 1stInternational Conference on Computer Applications Information Security (ICCAIS), Riyadh, 2018, pp. 1-8, doi: 10.1109/CAIS.2018.8441987.

[3] Iyer A, Kathale P, Gathoo S and Surpam N 2016 E-Police System-FIR Registration and Tracking through Android Application International Research Journal of Engineering and Technology 3(2) 1176-1179.

[4] P. A. K. S. Y. K. S. , Shivaganesh Pillai, “Online Fir Registration and Sos System”, int. jour. eng. com. sci, vol. 5, no. 4, Dec. 2017.

[5] Sanjay misra, Rytis Maskeliunas, Robertas Damaševičius 2019, Design and Implementation of an E-Policing System to Report Crimes in Nigeria. 10.1007/978-981-13-6351-1 21

[6] Mollah, Muhammad Islam, Sikder Aman Ullah, Engr. Mohammad. (2012). Proposed e-police system for enhancement of e-government services of Bangladesh. 881-886. 10.1109/ICIEV.2012.6317444.

[7] P. Kormpho, P. Liawsomboon, N. Phongoen and S. Pongpaichet,” Smart Complaint Management System,” 2018 Seventh ICT International Student Project Conference (ICT-ISPC), Nakhonpathom, 2018, pp. 1-6, doi:10.1109/ICT-ISPC.2018.85239.

[8] Mollah, Muhammad Baqer Islam, Kazi Islam, Sikder. (2012). E-Police System for Improved E-Government Services of Developing Countries. Canadian Conference on Electrical and Computer Engineering.10.1109/CCECE.2012.6335057.

[9] Onuiri, Ernest Oludele, Awodele A, Olaore O, Sowunmi A., Ugo-Ezeaba. (2015). A REAL-TIME CRIME RECORDS MANAGEMENTSYSTEM FOR NATIONAL SECURITY AGENCIES. European Journal of Computer Science and Information Technology.

[10] Tasnim, Maisha Omar, Abdullah Rahman, Shahriar Bhuiyan, Md. (2018). CRAB: Blockchain Based Criminal Record Management System.294-303. 10.1007/978-3-030-05345-1 25.