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 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12674

Enhancing Security and Efficiency in Digital Crime Evidence Management through a Three-Tier Blockchain Architecture

Raghul K[1], Iraniyapandiyan M[2], Kumaran M[3]

Student, Department of CSE, Jaya Engineering College, Chennai, India[1]

Assistant Professor, Department of CSE, Jaya Engineering College, Chennai, India[2]

Professor, Department of CSE, Jaya Engineering College, Chennai, India[3]

Abstract: The current system for maintaining crime records and criminal data lacks comprehensive information on offences and perpetrators, making it less secure and susceptible to fraud. This study proposes the implementation of a blockchain-based system to safeguard data and improve security measures. By utilizing blockchain technology, crime investigators can access the database using their authentication credentials and view reports authored by police and witnesses. Investigators also possess the authority to update and modify data, expediting investigations and aiding in the identification of criminals. While previous research has focused on centralizing digital evidence management, this approach poses a risk of compromising confidential operational and investigative information if the central server is compromised. To mitigate this risk, a distributed system environment using blockchain technology is proposed for managing digital evidence and investigation data. However, the storage of massive volumes of data, such as evidence films, in a blockchain can adversely impact performance. Therefore, a three-tier blockchain architecture is proposed, consisting of hot and cold blockchains. The cold blockchain stores non-changing content and files, while the hot blockchain stores frequently changing information.

The study evaluates the system's performance in terms of digital crime evidence storage and query processing, highlighting the capabilities and benefits of the multi-level blockchain architecture. Implementing this three-tier blockchain architecture can significantly enhance the security and efficiency of digital crime evidence management, thereby improving the investigative process and aiding in the fight against crime.

Keywords: Crime Record, Blockchain, Security, Cryptography.

I. INTRODUCTION

Take into account a distributed network fabric with a ledger that records each transaction and is updated whenever a new one occurs. A copy of the ledger is carried by each component of the distributed network fabric, and the ledger is not under the jurisdiction of a single administrative entity. The problem is that once anything is entered into the ledger, it can never be removed. That brief explanation of blockchain technology was helpful. The first use of blockchain technology was highlighted in the main publication as being Bitcoin. This technology is currently maintained to protect Bitcoin transactions; several administrators take care of this digital record. Every system is a node in the bitcoin network, which records each transaction individually. The calculations and transaction computations are done independently by these nodes. All other nodes in the decentralised fabric network will receive the aforementioned transaction via a multi-hop broadcast. Combination is an important phase in a transaction.

A block is a valid transaction, and a blockchain network is composed of numerous valid blocks. In essence, a block cannot be connected to a blockchain until its authenticity has been established. A certain minimum number of consensuses must occur in the network before a block can be added. The block is often authorised using the proof of work, proof of stack, and byzantine fault tolerance consensus procedures. When a newly created block is connected to another block in a distributed fabric network, it assumes the identity of the other block with the extra nodes.

Every time a request is made to remove a verified block from the blockchain, it is computationally impossible to reorganise the network. Take into account the openness that would be created if the blockchain were built to enable police statements like First Investigation Reports (FIR). In this architecture, a node of the distributed fabric network that contains a copy of the blockchain is referred to as a zone. The technology creates a timestamped FIR and correlates it with the complaint each time a new complaint is submitted. A cryptographically generated hash key may be sent to the concerned

DOI: 10.17148/IJARCCE.2023.12674

complaint in order to verify the integrity of the block. In order to prove the authenticity of the block, we shall employ the consensus approach. The distributed fabric network's nodes will all receive broadcasts containing the valid block and the time stamp.

To register using a mobile device and submit a complaint, the user must have their personal AADHAAR number on hand. To effectively convey the complaint to the closest police station, the app has to know where the user is. Simple association with the hash key is all that is required to validate the block. Because a block will be securely connected to the blocks that came before as soon as it proves it is valid, invalidation is computationally challenging and too simple. More confirmations mean a block is more decentralised in terms of hash power.

II. SECURITY IN BLOCKCHAIN

One of the main features of the blockchain technology is the level of security it provides to the network. This method for data security uses cryptographically created blocks and a few algorithms, such as SHA-256 and hash trees. These algorithms only involve masking a person's identity, which will assist in the creation of a no-trust network. The user, who could be the complainant, suspect, witness, or officer, does not know the identity of the party engaged when a case is submitted; as a result, there is no need for manual involvement; the case will proceed without problem. The decentralisation of blockchain has a further advantage in that there wouldn't be a centralised authority to interfere. When a network has just one administrator, data erasure is trivial, resulting in a single point of failure. The solution we'll be talking about will be developed from open-source components, using Blockchain technology, and it will do away with all of these security concerns.

III. LITERATURE REVIEW

A blockchain-based strategy was created by Antra Gupta et al. (2019) to protect FIR systems. The recommended approach aims to provide a secure and irrevocable record of FIR complaints and related evidence. A smart contract on the blockchain is used to store the FIR report and any supporting documents in the system. When the FIR report is published on the blockchain, it cannot be altered or deleted and will only be seen to authorised individuals. The encryption keys would be kept on the blockchain, which would only allow authorised individuals to access the encrypted data.

The development of an online system for crime reporting and administration for the city of Riyadh by K. Tabassum et al. in 2018 with the provision of a centralised platform for both individuals and law enforcement organisations is intended to streamline the process of reporting and addressing crimes. To facilitate online crime reporting by the general public, a web-based application was employed in the system's development. The system ensures the security and correctness of the data using blockchain technology. By storing the criminal reports and supporting evidence on the blockchain, a tamper-proof record of the crime is produced.

In order to streamline the reporting and handling of crimes, a city of Riyadh online crime reporting and management system has been designed for both citizens and law enforcement agencies. In 2016 (Iyer A. et al.).

By enabling citizens to register FIRs online through a web-based application in 2017, Shivaganesh Pillai et al. hopes to increase citizen convenience and accessibility in the FIR registration and emergency reporting procedure. The software is linked to a server in the background that maintains a database with the FIR reports and related supporting documentation. The app also offers an SOS function that enables users to report emergencies and receive immediate assistance from law enforcement.

An electronic reporting system was created in 2019 by Sanjay Misra et al. for the Nigerian police to improve the effectiveness and efficiency of reporting and managing crime in Nigeria. This allows for public online reporting of crimes through a web-based application. The server maintains a database that houses the crime reports and related evidence. In order to create a tamper-proof record of the crime, the criminal reports and related evidence are saved on the blockchain. The system also contains a tool for law enforcement agencies to use while handling and looking into crimes. The service offers real-time updates on criminal conduct, together with information on the locations of law enforcement agencies and the status of the investigation.

In 2012, a mechanism for e-policing was created in Bangladesh to enhance e-government services. The suggested approach has helped to improve the effectiveness and efficiency of Bangladesh's law enforcement agencies, which will ultimately lead to a society that is safer and more secure. (Mollah Muhammad Islam et al., 2012)

DOI: 10.17148/IJARCCE.2023.12674

In order to improve the effectiveness, accountability, and responsiveness of governmental organisations in managing complaints, P. Kormpho et al. built a complaint management system in 2018. The network includes a dashboard that displays the number and type of complaints received, their status right now, and how quickly government entities responded to them. Additionally, the platform provides a feature for producing statistics and analytics on the complaints that have been received, which can help government organisations swiftly identify and fix issues.

A method for e-policing was created to improve the delivery of e-government services in poor countries. The proposed system aims to provide a quick and easy way to handle and report crimes. The researchers propose integrating mobile technology into the E-police system so that citizens can file crime reports using their mobile devices. Automatic communication with the nearest police station, GPS location tracking, and the collection of multimedia evidence are only a few of the features offered by the technology. In order to facilitate easy information exchange between police stations and convenient access, the researchers also advise using a single database to store and manage criminal records. et al., 2012; Muhammad Baqer Islam.

For national security agencies, a real-time criminal records management system was established. The intended plan is to provide a centralised platform for real-time crime record gathering, management, and storage, enabling quick response and action by security authorities. (Onuiri Ernest Oludele et al., 2015)

Create, Retrieve, Append, Burn, or CRAB (Create, Retrieve, Append, Burn), is a blockchain-based criminal record management system that was introduced by Tasnim et al. in 2018 to provide a decentralised, secure, and impenetrable platform for managing criminal records that can be accessed by authorised parties including law enforcement organisations, courts, and other relevant authorities. According to the research, blockchain technology should be used to store and manage criminal records. The answer uses a private blockchain to safeguard the confidentiality and privacy of the data. Additionally, it promotes the use of smart contracts to automate the management of criminal records, which can help to reduce errors and boost productivity. In the paper, it is highlighted the benefits of using blockchain technology to manage criminal records.

IV. PROPOSED METHODOLOGY

The following steps are often included in the technique for developing a Crime Record Management system using blockchain technology:

A. System requirements analysis: This entails knowing the needs and requirements of the parties participating in the FIR system. This would entail being aware of the data items that must be recorded, the various user roles and permissions, and the required security measures.

B. Design: The system architecture and database schema are designed in this step. Scalability, security, and usability should all be considered in the system design.

C. Creating smart contracts: A blockchain-based system's core component, smart contracts are created. In smart contracts, which are self-executing contracts, the specifics of the arrangement between the buyer and seller are explicitly written into lines of code. The smart contract code would need to be created in order to record the rules governing the FIR system and ensure that it functions as intended.

D. Integration: After being created, smart contracts must be incorporated into the blockchain network. This entails putting the smart contracts into use on the blockchain network and making sure they work as intended.

E. Testing: After the system has been integrated, it should be tested to make sure it performs as intended. This would involve testing for user experience, data correctness, and security flaws.

F. Deployment: The system can be set up in a live environment after testing. The system should be made scalable, secure, and simply accessible as part of the deployment process.

G. Maintenance: The system needs to be maintained after it is deployed to make sure it keeps working as planned. This would entail bringing the smart contracts up to date on a regular basis, keeping an eye out for security holes, and fixing any emerging system problems.

DOI: 10.17148/IJARCCE.2023.12674

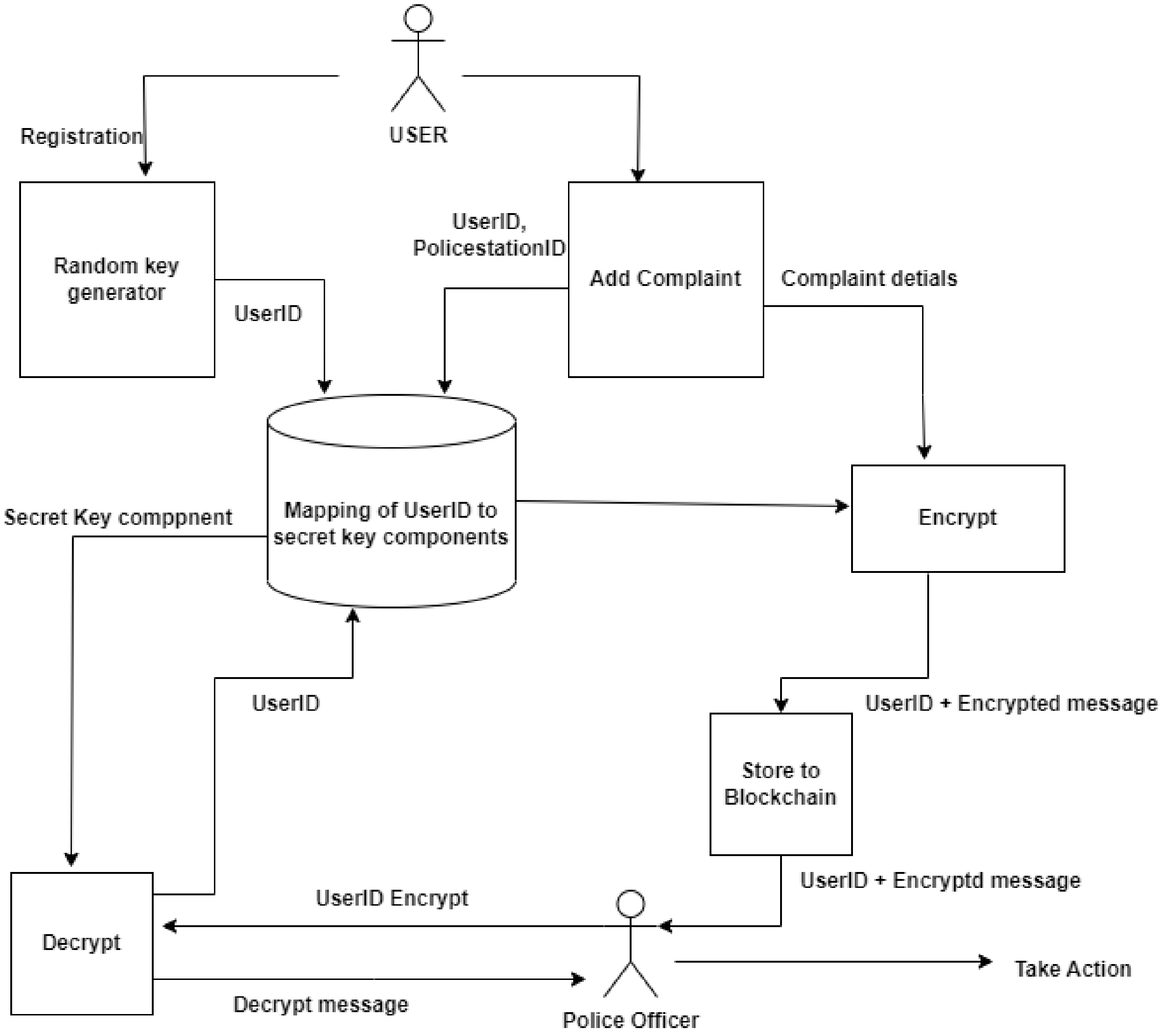

Fig 1: Crime Record management system using Blockchain technology

A. User files a grievance: The procedure is initiated when a user submits a grievance via an online form or application.

B. Complaint Verification: After a complaint is submitted, it is verified to make sure it is a legitimate complaint. This step is crucial to avoid the system becoming clogged with fake complaints. The verification procedure may entail verifying the user's identification, the incident's location and timing, and any supporting documentation.

C. Complaint registration: The complaint is registered on the blockchain network once it has been verified. This phase is adding a new block to the blockchain that contains the specifics of the complaint. A timestamp, a distinct ID, and other pertinent data are all present in the block. The integrity of the complaint record is ensured by the inability to change or remove a block once it has been put to the blockchain.

D. Complaint tracking: Through the system, the user can monitor the development of their complaint. They can see who is managing the complaint, when it was filed, and any updates or actions that have been taken. Between the public and the police agency, this openness helps foster confidence.

DOI: 10.17148/IJARCCE.2023.12674

E. Inquiry and response: The police department looks into the complaint and takes the necessary steps. This may entail accumulating further proof, speaking with witnesses, or making arrests. The police department adds the findings to the complaint record in the blockchain once the inquiry is over.

F. Complaint closure: Once a complaint has been handled, the system marks it as closed. The user is informed of the resolution, and a record of the complaint is stored on the blockchain for future use. To stop it from subsequently being used as evidence, the complaint may be designated as invalid or false.

Overall, the integration of blockchain technology into a police complaint management system guarantees that recordings of complaints are safe, open, and unchangeable. Additionally, it gives the police force an effective means of handling grievances and monitoring their resolution, which promotes greater responsibility and public confidence.

V. CONCLUSION

We recommend this technique in order to safeguard the FIR system. The system needs to be improved and simplified. To run the decentralised network we are building, trust is not necessary. A registered user may submit a complaint using any computer or mobile device with an internet connection. Considering that the blockchain will make the network more secure, irreversible, and decentralised, we may say that it will be a network free from corruption. The system's implementation and limitations will be covered in later articles.

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.