e-ISSN: 2582-5208

International Research Journal of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Volume:05/Issue:02/February-2023 Impact Factor- 6.752 www.irjmets.com

SURVEY ON SECURE FIR SYSTEM USING BLOCKCHAIN

Sarosh Sheikh*1, Niranjan Sid*2, Abhishek Popale*3, Prajwal Sute*4,
Prof. Poonam Kadam*5

*1,2,3,4,5Dr. D.Y. Patil College Of Engineering And Innovation, Pune, India.

ABSTRACT

Technology has been applied to every conceivable task, whether directly or indirectly. Industry, agriculture, criminal justice, governmental workstations, and other fields all make use of technology. It is more crucial than ever to take appropriate action against the offender to make sure that the victim obtains justice in light of the increase in crime rates. Unfortunately, it doesn't always work out like this. The e-FIR data is initially kept locally in a police station's central database, which is later shared with the head office (HQ) of police stations; nevertheless, because the police station has local control over the e-FIR database, it is simple to modify the e-FIR data; It is possible to generate a mechanism to prevent this. The main problems with the conventional method are e-FIR data trustworthiness, fake registration, and non-registration. Because corruption, inefficiency, and a lack of transparency are the root causes of these issues, creating a system like this would give the populace access to one that is devoid of corruption. An effort was made to protect the integrity of e-FIR data and stop fake registration by using blockchain.

I. INTRODUCTION

Information and communication technologies (ICT) are fundamental to the concept of smart cities. ICT invest in human social life to improve citizens' quality of life by promoting economic development, sustainable good governance, wise resource management, and efficient mobility, all while ensuring citizens' security and privacy. In a city where smart cars, smart schools, smart hospitals, smart utilities, and so forth are all connected to the Internet to exchange massive amounts of data on a daily basis, there should be a smart and secure framework for managing Electronic First Information Report (e-FIR) data in a police station. It's more crucial than ever to maintain accurate records and distribute information due to the increase in document size. Likewise, across boundaries to safeguard national security If you have trustworthy and time-stamped records, the process will be simpler to finish. In order to safeguard national security, it is crucial to understand the intricacies of the classification of offences. 1.) Cognizable offences – This refers to offences that may be recognised within borders. If you have trustworthy and time-stamped records, the process will be simpler to finish. Understanding the specifics of the classification of offences is crucial. 1.) Cognizable crimes are significant felonies that police can seize without a warrant. Crimes include murder, robbery, the death of a Dowary, kidnapping, and more. 2.) Non-cognizable offences are less serious ones that the police cannot be held accountable for without a warrant. Forgery, cheating, and assault are only a few instances. A lawsuit may be filed for any type of offence, however a FIR is only for crimes that are legally punishable. One of the most sensitive categories of public information is criminal records. Integrating criminal records into a blockchain can safeguard the rigidity and dependability of documents, which frequently aids in keeping data safe from intruders. This study suggests a blockchain-based approach for managing criminal records that helps to protect and maintain data integrity.

II. LITERATURE REVIEW

A Blockchain Proxy for Lightweight IoT Devices by Gero Dittmann, Jens Jelitto.

A new platform called blockchains enables companies to automate business processes like asset lifecycle management and supply-chain management (SCM). The internet of things (IoT) can offer essential inputs for these procedures, such as GPS coordinates or sensor readings for temperature, humidity, pressure, mechanical shock (impact), and vibrations, as well as details on the status of shipments and weather information. An SCM system built on a blockchain, for instance, can be used to perform cold-chain monitoring by having a temperature sensor in a shipping container send periodic reports of its measurements.

Design of Cross-border Network Crime Detection System Based on PSE and Big Data Analysis by Xingchen Yu.

To speed up the detection of cybercrime worldwide, a novel cross-border cybercrime detection system is developed by combining the PSE theory with the idea of big data analysis. The U-boot network development board and the OpenStack criminal information detecting component are coupled in the TFTP server to establish the hardware running environment of the cross-border network crime detection system. By analysing the characteristics of detection information, calculating the cross-border network detection domain, and directional planning of network crime information, the cross-border network crime detection system based on PSE and big data analysis is designed with the basis for hardware implementation.

Real Time Crime Detection Using Deep Learning Algorithm by P.Sivakumar; Jayabalaguru. V; Ramsugumar. R; Kalaisriram. S

Because the crime rate and the number of criminals are increasing daily, major worries regarding security issues are being raised. The goal of police authorities is to prevent and identify crime before it occurs. Recent technologies, in particular CCTV, are often employed in both public and private settings to minimise crime, but they need to be monitored by humans. Managing numerous screens at once is difficult for a human. It results in several errors. Our Real-Time Crime Detection Technique was put up as a potential remedy for these problems. It keeps track of real-time recordings and alerts the neighborhood's cybercrime administrator when a crime occurs along with its present position.

Time, Place, and Modus Operandi: A Simple Apriori Algorithm Experiment for Crime Pattern Detection by Peng Chen, Justin Kurland.

Given the fast-paced nature of contemporary police work, the development and use of advanced data mining techniques for crime research can play a critical role in preventing future harm and assisting in crime prevention. This article aims to address the problem of identifying likely repeated offending tendencies by utilising factors from police-recorded crime data that have previously gone underutilised. A crime data processing method that extracts the three variables time, setting, and modus operandi from police-recorded crime event data is suggested in order to achieve this. Each crime-event feature is modelled using the Apriori algorithm, which is frequently used for frequent item set mining and association rule learning from large datasets.

Crime Pattern Detection Using Data Mining

by Shyam Varan Nath

Data mining can be used to model problems with criminal detection. In addition to being a social irritant, crimes cost our society heavily. Any study that expedites the criminal investigation process will be successful. 10% of offenders are responsible for 50% of offences. Here, we look at how a data mining technique called clustering can be used to speed up the criminal investigation process by identifying crime patterns. We will look at k-means clustering with a few modifications to help identify crime patterns.

Network Crime Information Retrieval Framework based on Facial Image Recognition by Yijun Cai, Dian Li, Yuyue Wang.

Based on facial image recognition, this study develops a framework for network-based criminal information retrieval. Due to the expertise and professionalism of criminal techniques, the range of criminal strategies, and the high level of crime concealment, detecting cybercrime is significantly more challenging than detecting traditional instances. Due to this, it is exceedingly challenging to examine the case, which lowers the likelihood of detection.

The face analytic model is used to create an efficient criminal data modelling system. The regular term of the ideal coding coefficient matrix is introduced to represent the coefficients of samples for similar types that are as similar as possible.

III. EXISTING SYSTEM

The online system varies from state to state. Every state adheres to a specific pattern. It is not available in certain states, while in others, it can only be done in circumstances that are cognizable. An e-FIR can only be used to report cognisable offences like murder, rape, dowry death, kidnapping, etc. The police are permitted to conduct an arrest in these circumstances without a court warrant. For non-cognizable offences like assault, cheating, harassment, and so on, only a report may be submitted online. The police will upgrade it to a FIR once they have the Magistrate's approval. . In some states, you can submit your FIR or complaint online. Currently, criminal records are kept in a single node, and internet file transfers are risky. Transactions can have data altered since the Internet protocol is so easily cracked. In the present systems, data can be accessed by third parties, but in blockchain, data cannot be changed. We can safely file a FIR if someone tries to change data because the transaction is recorded in the blockchain and is easily traceable because the hash value changes. In the current system, non-registration, false registration, and the veracity of e-FIR data are the main causes for concern. Corruption, inefficiency, a lack of openness, and a lackadaisical attitude toward the situation are the root causes of these problems. e-FIR data is initially kept locally in a police station's central database before being shared with the station's headquarters (HQ). The e-FIR data could be easily changed because the e-FIR database is handled locally. Because of this, employing blockchain can help us better address security issues and assure data integrity. Blockchain is a fraud-resistant, distributed ledger that can record all transactions in a Peer-to-Peer (P2P) network. A computerised system for tracking crime, documenting its history, and preserving data is currently lacking. reported on the police station's computer systems, and it might be altered under any conditions.

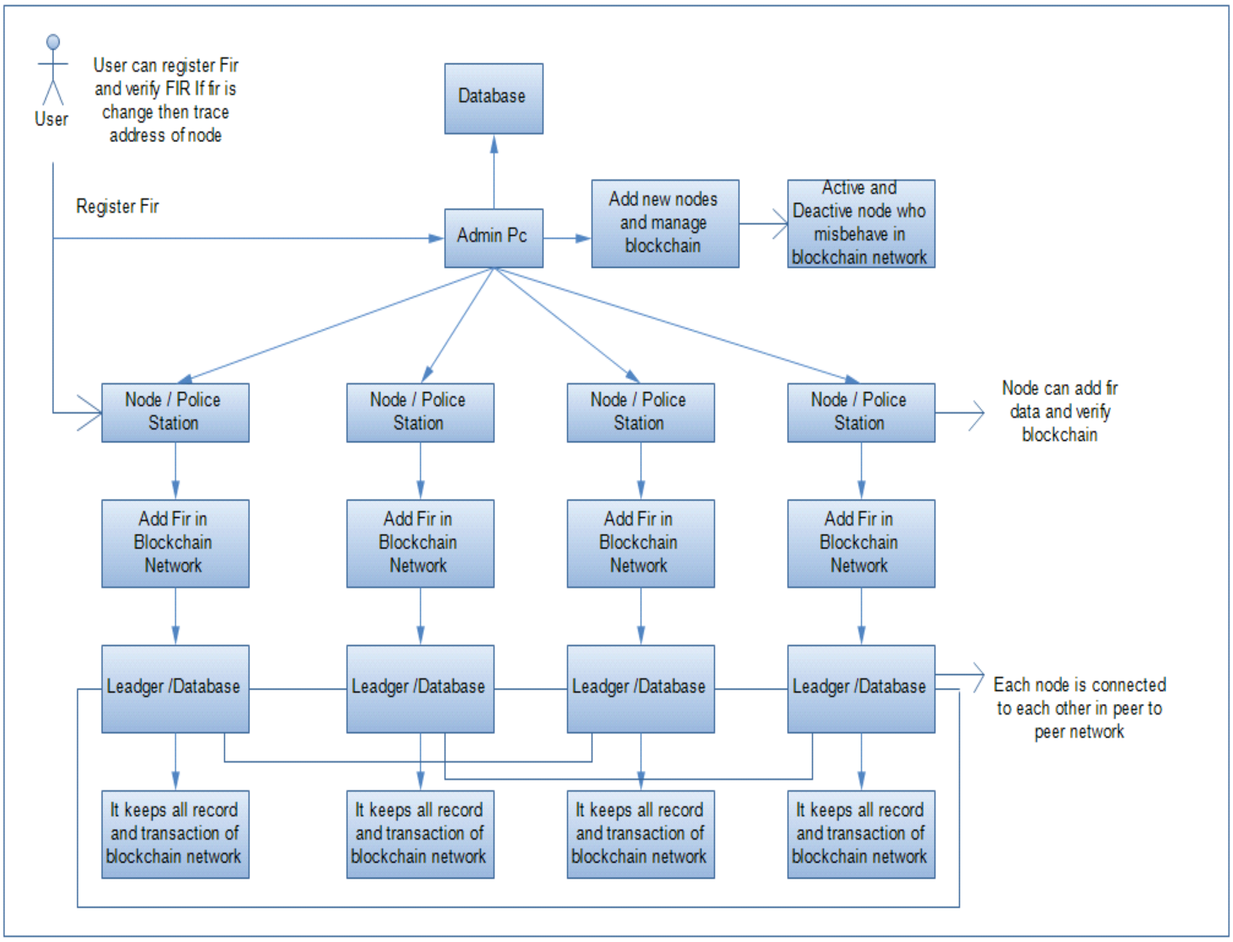
User
User can register Fir and verify FIR If fir is change then trace address of node
Database
Register Fir
Admin Pc
Add new nodes and manage blockchain
Active and Deactive node who misbehave in blockchain network
Node / Police Station
Node / Police Station
Node / Police Station
Node / Police Station
Node can add fir data and verify blockchain
Add Fir in Blockchain Network
Add Fir in Blockchain Network
Add Fir in Blockchain Network
Add Fir in Blockchain Network
Leadger /Database
Leadger /Database
Leadger /Database
Leadger /Database
Each node is connected to each other in peer to peer network
It keeps all record and transaction of blockchain network
It keeps all record and transaction of blockchain network
It keeps all record and transaction of blockchain network
It keeps all record and transaction of blockchain network

Figure 1. System Architecture

IV. ABOUT BLOCKCHAIN TECHNOLOGY USED

Blockchain technology is motivated by the requirement for decentralization, which is achieved by distributing computing workloads across all nodes in the blockchain network. Decentralization solves several problems that traditional systems have, such as the single point of failure. Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.

V. ALGORITHMS

SHA 256

- A hash, which is a fixed size for any size of source text, is not "encryption" because it cannot be reversed to reveal the original text. This enables comparison of "hashed" versions of texts instead of decrypting the text to retrieve the original version when it is appropriate to do so. Hash tables, integrity checks, challenge handshake authentication, digital signatures, etc. are a few examples of such uses.
- A client can send a password's hash over the internet for server validation without running the risk of the original password being intercepted thanks to challenge handshake authentication (also known as challenge hash authentication).
- Anti-tampering measures include linking a message's hash to the original so that the recipient can re-hash the message and compare it to the one provided. The message remains unchanged if they match; this can also be used to verify that there was no data loss during transmission.
- Although the process of creating a digital signature for a document is more complicated, you can sign a document's hash by encrypting it with your private key. By decrypting the signature with your public key to recover the original hash once more, anyone may then verify that you authenticated the text by comparing it to their own hash of the text.
- It should be noted that since hash functions are made to be quick to compute, they are vulnerable to brute-force attacks and should not be used to store encrypted passphrases. Key derivation algorithms like bcrypt and scrypt are more suitable for password storage because they are slow to compute.

VI. CONCLUSION

To improve the underdeveloped area of record administration in police stations using blockchain technology in order to prevent data manipulation and fraudulent report submission. Based on the results, a consensus-based strategy for utilising blockchain to guarantee the secrecy of offence data stored in police station databases has been presented. Users won't need to go to a police station to file a FIR; they can do so from anywhere, at any time. People have access to all government information and can engage with the government directly. People can also examine the status report for their case. They will have direct access to higher-ups, which will improve relations between the people and the police as well as between the government and its constituents. Blockchain is a technology that combines hash chains, consensus mechanisms, and cryptographic algorithms to offer services like consensus. Irreversibility traceability is required for online data. In this project, we are attempting to use a blockchain network to secure data in police departments based on these programmers. Because criminal histories and records are sensitive documents and sharing them online poses a risk, we are attempting to use the blockchain to protect data on a distributed network.

VII. REFERENCES

[1] Irie K, Scott A, Hasegawa N. Investigation of the detection ability of an intrinsic fluorescence-based bioaerosol detection system for heat-stressed bacteria.[J]. Ecological Economics, 2017, 131(2):499-509.

[2] J. Flatley, C. Kershaw, K. Smith, R. Chaplin, and D. Moon, "Crime in england and wales 2009/10, London: Home Office, 2010.

[3] 3 Kadhe, S., Garcia, B., Heidarzadeh, A., El Rouayheb, S. and Sprintson, A., 2019. Private informat ion retrieval with side informat ion. IEEE Transactions on Information Theory, 66(4), pp.2032-2043.

[4] Guo, J., Fan, Y., Pang, L., Yang, L., Ai, Q., Zamani, H., Wu, C., Croft, W.B. and Cheng, X., 2019. A deep look into neural ranking models for informat ion ret rieval. Informat ion Processing & Management, p.102067.

[5] Hsinchun Chen, Wingyan Chung, Yi Qin, Michael Chau, Jennifer Jie Xu, Gang Wang, Rong Zheng, Homa Atabakhsh, "Crime Data Mining: An Overview and Case Studies", AI Lab, University of Arizona, proceedings National Conference on Digital Government Research, 2003. available at: http://ai.bpa.arizona.edu/

[6] Hsinchun Chen, Wingyan Chung, Yi Qin, Michael Chau, Jennifer Jie Xu, Gang Wang, Rong Zheng, Homa Atabakhsh, "Crime Data Mining: A General Framework and Some Examples", IEEE Computer Society April 2004.

[7] Y. Lin, T. Chen and L. Yu, "Using Machine Learning to Assist Crime Prevention", 2017 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI), pp. 1029-1030, 2018.

[8] C. Chauhan and S. Sehgal, "A review: crime analysis using data mining techniques and algorithms", 2017 International Conference on Computing Communication and Automation (ICCCA), pp. 21-25, 2017.

[9] S. Kadhe, B. Garcia, A. Heidarzadeh, S. El Rouayheb and A. Sprintson, "Private information retrieval with side information", IEEE Transactions on Information Theory, vol. 66, no. 4, pp. 2032-2043, 2019.