International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 06 | June 2021 www.irjet.net p-ISSN: 2395-0072

Blockchain based Digital Forensics Investigation Framework

Prof. Renuka B S [1], Kusuma S[2]

[1]*Associate Professor, Dept. Of Electronics & Communication, JSS Science and Technology University, Mysuru, Karnataka, India.*
[2]*PG student, Dept. Of Electronics and Engineering, JSS Science and Technology University, Mysuru, Karnataka, India.*

Abstract - Nowadays the tampering of the digital forensic data is happening everywhere so that to maintain the integrity and provenance of the precious digital forensic data from the malicious activities, we adapted a method of hashing the forensic data using the SHA-256 algorithm and encrypt the data using AES Rijndael algorithm. And store this encrypted data using Blockchain technology. Visual Studio is used to implement the windows application for forensic data i.e. client and server application. Server application design with AES Rijndael algorithm for encrypt the forensic data and blockchain technology used to store the encrypted data in blocks. The TCP remoting concept is used to communicate between the client and the server application. ADO.Net is used to communicate between the windows application and MySQL database.

Key Words: AES Rijndael, SHA-256, Blockchain, TCP remoting, ADO.Net.

1.INTRODUCTION

The main problem in forensic evidence (digital or not) is to maintain its integrity. Based on the investigation evidence it links the particular person to the criminal activities. If the data got tampered with or altered by someone it helps the crime person to escape from the legal punishment and sometimes person who is not involved in a criminal activity got punished. To avoid this illegal activity we have to maintain the integrity of the investigation evidence till it reaches the final stage i.e. from investigation to producing the evidence to the court.

For demonstration purposes, we are taking one of the crime activities i.e. Murder. To investigate the case need to collect the forensic reports from the forensic staff and doctor's report from the doctor based on evidence from died person i.e. blood spatter, fingerprint, drug details. After this, we are making these investigation data to be protected by hashing the crime ID, Police ID, Log date using the SHA-256 algorithm. From this hashing we get a 64 Character length hash value, after getting the hash value first two characters are converts to ASCII to get the private key. The private key is used to encrypt the forensic and doctor's report using the AES Rijndael algorithm. Finally, we push the data to the blockchain to store the data as a decentralized method. Blockchain technology is the one used to recover the data when data got tampered with by someone.

2. BACKGROUND STUDY

A. Blockchain.

The blockchain is a technology used to record the details in chain of the blocks. Every block in blockchain points to the hash value of the previous block. The first block in the blockchain called genesis [1], which contains only the hash value of the next block. If the data got tamper in the blockchain, it can be recovered due to decentralized nature of the blockchain. Bitcoin is the cryptocurrency it uses blockchain technology to make the transaction transparent [1].

B. CRAB- Blockchain Based Criminal Record Management System.

CRAB architecture [2] gives a detail about the how the data exchanges between sender and receiver with storing of the data in the SQL database with blockchain technology. It as an information about sender login to the functional unit (FU) with password and ID, then it sends the criminal identification data (CID) to the FU. FU sends verified criminal data with CID to the SQL database. Transaction details from FU is stored to the blockchain and block number where meta data is stored is return to the functional unit. FU sent CID, block id and encryption key to local server, and send the request to local server for data. Server processed the request and send the data, as well Request the database with CID. Then data storage sends the encrypted data to the FU. Functional unit update the CID, block id and encryption key to local server. At last decrypted data is send to the receiver.

C. Chain-of-custody

Chain-of-custody is a documentation of the record. It contains all the necessary steps that investigator must follow to study the crime investigation [3]. There is no proof that data is not getting tampered so to avoid the tampering and maintain purity and integrity of the evidence, we are using Chain of custody with blockchain.

3. METHODOLOGY

In this section we introducing our architecture. As in figure 1, There are five modules in investigating the forensic case as follows.

1.Application manager.

2.Police.
3.Forensic Staff.
4.Doctor.
5.Higher Officer.

Application manager: The application manager can able to add the Area, Police station, Forensic staff, Doctor, and Higher officer.

Police: Police can investigate the crime based on the report generated by forensic staff and doctor.

Forensic Staff: Forensic staff collect the data from a crime scene (i.e. Blood spatter, Fingerprint) and generate the Forensic report.

Doctor: The doctor generates the doctor's report by examining the body and post-mortem.
The Forensic and doctor's report is encrypted and store in the blockchain to avoid altering the original data.

Higher officer: Higher officer can able to log in to view the forensic and doctor's report. And also have the authority to recover the data when tampering of the data happens in the blockchain. Based on the reports and few data collected in crime place are used for investigation of the case and also this investigation log is store in blockchain to avoid the alteration of the data.

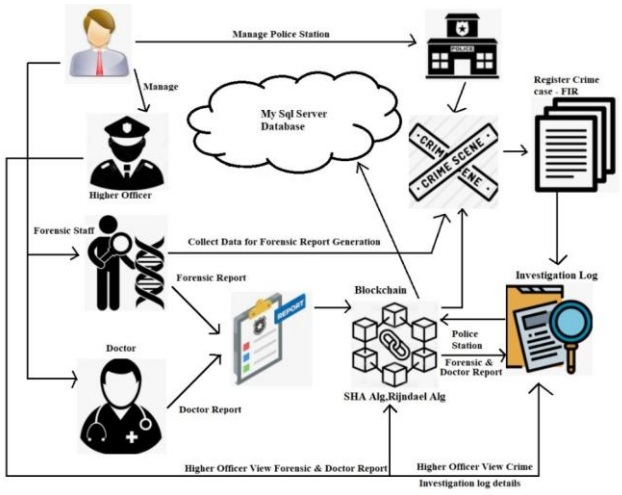

Figure 1:Proposed sysytem for digital forensic framework using blockchain technology.

4. PROPOSED WORK

Server Application:

Server application process the request sent by the client application. Both server and the client applications are communicate using TCP remoting. Figure 2, shows the design of the server application, it has three buttons start server, stop the server and exit the server. Before start's the server its status is 'IDLE', after the server start's status is changed to 'RUNNING' and once we click on stop server it shows status as 'STOP'.

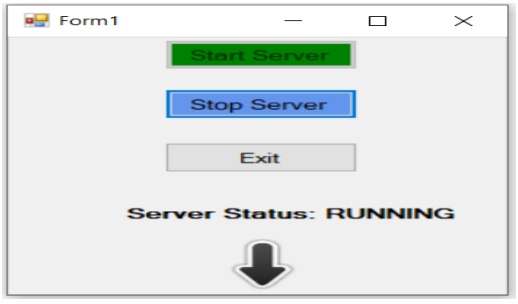

Figure 2: Server Application with "Running" Status.

Client Application:

The client application sent the request to the server using the IP address and port number of the server.

Server application process the request by using the DLL (Dynamic Link Library) references. The login page of the client application is shown in Figure 3. It has Five user types i.e. Application manager, Police, Forensic Staff, Doctor, and Higher officer.

Login to the client application using one of the user types, user Id, Password, and server IP details. User Id and password are set in MySQL table before given as login.

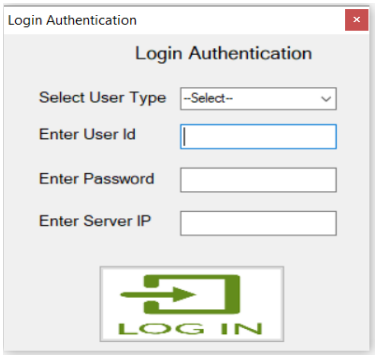

Figure 3: Login Authentication page for Client application.

Client application has five modules those are explained as follows:

Module 1: Login as an application manager.

After successful login as an application manager. He can add areas where the crime occurred, police station for each area, add higher officer based on the roles such as DGP, ADGP, IGP, SP, DSP, SI, ASI, forensic staffs, and doctors as shown in figure 4. For security purposes, the application manager has only permission to add the details to the application not to view or edit the investigation details. After adding the details by the application manager, the mail is sent to the respective person using SMTP protocol which includes ID and

password for e.g. Police Station ID:283518 & Password:4470, and these details also updated in the MySQL database.

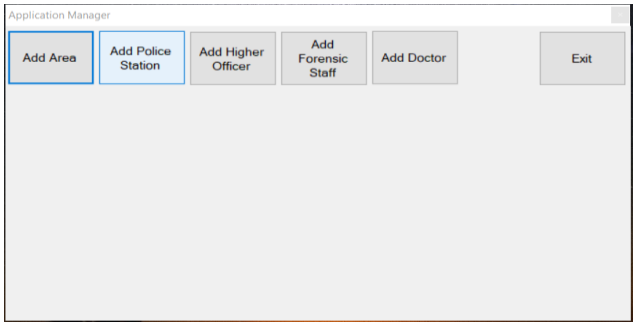

Figure 4: Application manager page to add area, police station, higher officer, forensic staff, and doctor.

Module II: Login as Police.

After successful login as police using user ID and password which was randomly generated in module I with IP address of the server. As in figure 5, police can add the crime data i.e. Crime name, crime place, and description. he can add crime logs based on the forensic and medical reports accessed by him in the blockchain. After the investigation by police, he can add the crime log to the database and store it in the blockchain. For security reasons, police can only view the medical and forensic report and recover if the report got tampered.

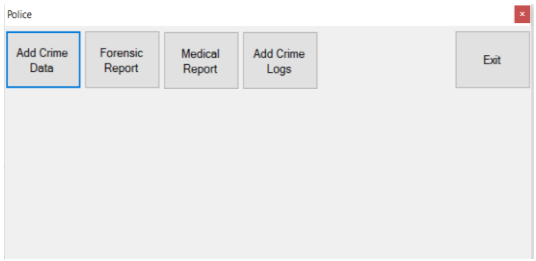

Figure 5: Page to add crime data, crime logs and fetch the forensic and doctor's report.

Module III: Login as Forensic Staff.

Once the login as forensic staff success with using user id and password of particular forensic staff that is randomly generated from module I. After successfully login it navigates to the page forensic as shown in figure 6, where forensic staff click on add forensic data, then forensic staff select the police station and crime. After selecting these details, staff can add a description of the case based on the collected information from the crime scene i.e. blood sample, fingerprint. Based on this information forensic staff can generate the report by saying some description.

Figure 6:Forensic staff navigation page to add forensic data and generate the forensic report.

For security concerns, the forensic report is encrypted using the AES Rijndael algorithm and stored as blockchain in MySQL database as in figure 7. This same data also stored in the temporary database to recover the data in the original database if the data got tampered in the original database as the figure 7. The forensic staff is not able to edit or view the details in the blockchain once he added the details in blockchain. In the blockchain as in figure 7, it has blocks namely,SlNo(serialnumber),PSId(Policestationid),crid(crime id),FSId(forensicid),LogDate,FSHV(forensic staff hash value) and FS Report. In blockchain data added from the second row and its hash value is stored in the generic block(Starting row).

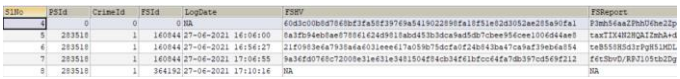

Figure 7: Storing the data in the blockchain.

Module IV: Login as Doctor.

After successful login as a doctor with using doctor id and password generated in module I. The doctor can generate a medical report based on the dead body investigation. This scenario is shown in figure 8.

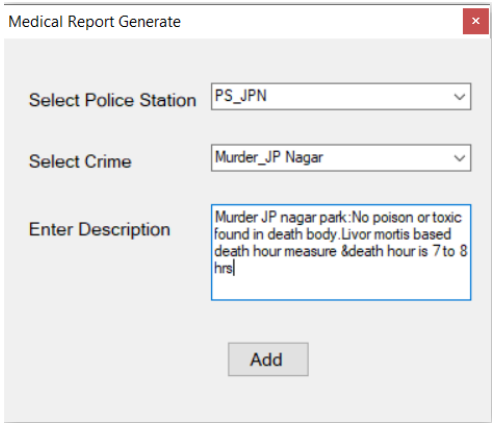

Figure 8: Doctor report generated based on the dead body investigation by the doctor.

For the security concern, the medical report is encrypted and stored as blockchain in MySQL database. This scenario is the same as forensic reports generate and stored in the blockchain in the MySQL database.

Module V: Login as a Higher officer.

After successful login as a higher officer with user id and password that generated in module I. As in figure 9, the higher officer can able to view the forensic report, medical report, and crime logs. When the higher officer started to view the reports or crime log, the mail is triggered with an access key and sent to higher officer mail and also logged in MySQL database. Using the correct access key higher officer can able to view the report content that is shown in figure 10. If the access key is wrong it gives an error saying as access key validation fail.

Figure 9: Navigation page for a higher officer to view forensic, doctor reports, and crime logs.

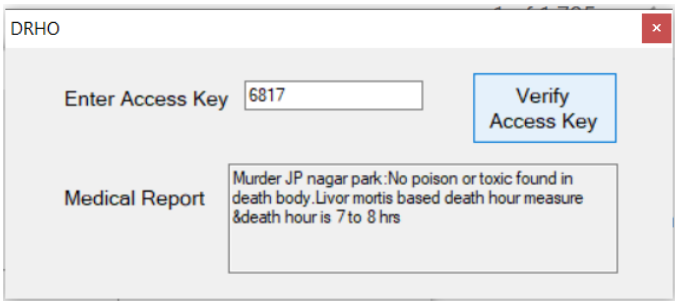

Figure 10: Doctor report view by a Higher officer.

Tampering Application:

Tampering application is the one which we are using as tamper the doctor and forensic report as the third party. Figure 11, shows the navigation page for tamper of the forensic report, doctor report, and crime logs.

Figure 11: Tamper application to tamper forensic, medical, and crime logs.

5. RESULT

For more security purposes we were given authority to the higher officer to view and recover the collected doctor report, forensic report, and crime log. And police can view and recover only doctor reports and forensic reports and based on this data police can generate the crime log. Figure 12, shows the tampered forensic report. For tampered data, it shows as tamper image with red in color and recover button is enabled and view button is disabled.

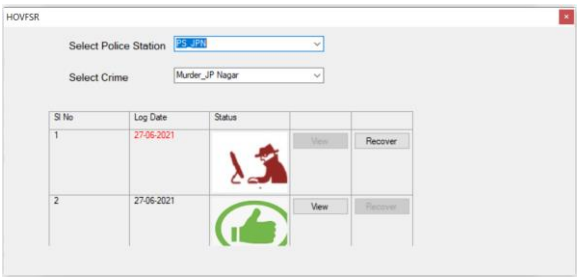

Figure 12: Tampered and non-tampered data view page.

Once the police or higher officer click on the recover button then data got recovered and the image becomes a successful image and its color turns to green and the view button is enabled with disabled of the recover button. Recovered data is shown in figure 13.

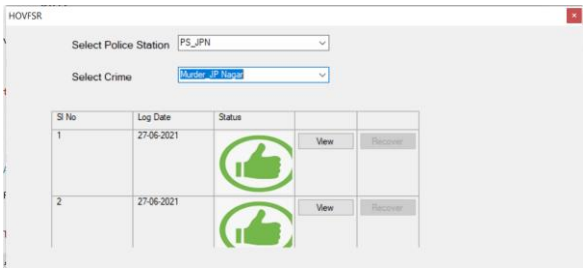

Figure 13: Page with Recovered data.

6. CONCLUSIONS

In our proposed work we have designed an application to store the forensic data as blockchain in MySQL database to secure the forensic evidence that was collected from forensic staff, doctor and police investigation. Third-party can able to tampered the application but it can be recovered from the temporary database. In this way, we have implemented a project to protect forensic data.

REFERENCES

[1] "Blockchain: Challenges and Applications". Pinyaphat Tasatanattakool, Chian Techapanupreeda, IEEE 2018.
[2] Abdullah Al Omar, Shahriar Rahman, Report on the criminal record management system. conference paper 2018 December, research gate.
[3] Dr.S. Harihara Gopalan and S. Akila Suba . Forensic-chain: Blockchain-based digital forensics chain of custody. Digital Investigation, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-2S11, September 2019.

BIOGRAPHIES

Prof. Renuka B S.
Associate Professor, Dept. Of E&C,
JSSSTU, Mysuru.

Kusuma S
M.Tech, Networking and Internet engineering,
Dept. of E&C, JSSSTU, Mysuru.