*International Journal of Advance Research, Ideas and Innovations in Technology*

INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

IJARIIT

ISSN: 2454-132X

Impact Factor: 6.078

(Volume 7, Issue 3 - V7I3-1545)

Available online at: https://www.ijariit.com

# Blockchain based data privacy preservation for financial sector

*Prathiba K. C.*
prathibakc.sse19@rvce.edu.in
*RV College of Engineering, Bengaluru, Karnataka*

*S. G. Raghavendra Prasad*
raghavendrap@rvce.edu.in
*RV College of Engineering, Bengaluru, Karnataka*

## ABSTRACT

***Whenever people want to store information over the internet in cloud storage, security is the primary thing that comes to mind. There are more chances that anyone will leak such data if we store a data as it is or transfer a data as it is over the internet. In request to decrease the demand of monetary item data update among multi organizations, oversee multi-dimensional and broadened monetary information encryption, improve the traceback capacity, we propose a blockchain-based financial area.***

***Keywords***— *Cloud storage, Data Encryption, blockchain, monetary multidimensional*

## 1. INTRODUCTION

Blockchain has discovered its way into major media features on a close regular schedule, somehow eighteen months prior, it was a word utilized by a generally modest number of individuals to portray the shared conveyed record innovation. As the establishment of monetary organizations, financial items assume a significant part in gathering client needs and offering monetary administrations. Not quite the same as customary items, product data item that experiences multi-dimensional activities, multi significant support and long haul supervise. A sequential of superior arrangements has been advanced for monetary item the board. For instance, electronic structure has been chosen for some convoluted money items the executives. Nonetheless, very of few methods are able to address the issues of an inexorably necessity for monetary items the board.

To accomplish multi-client information sharing, proposed property-based encryption. With the quick improvement of account Sectors, appropriated capacity stages have gotten broad consideration through an organization of various stockpiling gadgets. With the expanding prominence of these capacity stages, circulated stages that store information have become an objective of digital assaults. To reduce the danger of statistics leakage, proposed on blockchain.

Cryptographic forms of money, for example, Bitcoin and 250 comparative alt-coins, epitomize at their center a convention a component for a conveyed organization of computational hubs to intermittently concur on a bunch of new exchanges. Planning a protected blockchain convention depends on an open test in security, that of planning an exceptionally adaptable arrangement convention open to control by byzantine or subjectively hubs.

Exchange rates straightly accessible for mining the more power of organization, higher the product exchange blocks chose per unit time. Productive in its organization messages and emails enemies of up to absolute force. In fact, consistently segments or parallelizes the mining network for more modest panels, every one of which measures a disjoint arrangement of transactions. While sharing is normal in non-byzantine settings, the primary contender for a protected sharing convention with the presence of byzantine foes.

## 2. RELATED WORK

### 2.1. Standards for financial services

There are currently several standards in development for specifying vehicle Insurance for finance, including HIPAA, Open, the fitness degree 7 (HL7) financial product file structure and continuity of care report. HIPAA affords security measures and privateness protection mechanisms to shield finance records data. HIPAA has defined personal identifiable facts including Vehicle number, Vehicle ID, credit score card range, motive force's license quantity, domestic address, smartphone number, fixed deposit. Described the necessities that ought to be taken into consideration for privateness in data. To preserve monetary data non-public in a cloud surroundings, they defined how the Finance system need to keep in mind the subsequent of services.

### 2.2. Privacy-Preserving approaches for finance

Several survey papers have reviewed privateness-retaining coverage-based get entry to manipulate. The information in the record can identify with energy exchanging, land and an assortment of different areas. There are different Big Data examination enhancements originating from this reality. For example, misrepresentation anticipation, as the blockchain innovation permits the monetary establishments check each exchange constant. In this manner said, rather than investigating the records of the misrepresentation that all around occurred, the banks can recognize hazardous or deceitful exchanges on the fly and forestall the extortion completely. This paper contains privacy-maintenance strategies in pressure HQ Clouds as cryptographic techniques and non-cryptographic methods. Cryptographic methods are used for encryption schemes which include feature- based totally encryption (ABE) to shield fitness information in Finance HQ Cloud.

## 3. PROBLEM STATEMENT

Whenever people want to store information over the internet in cloud storage, security is the primary thing that comes to mind. There are more chances that anyone will leak data if we store a data as it is or transfer a data as it is over the internet.Industry structures for the sharing of information that is beneficial to the enterprise as a whole. In this case, a majority of gamers in industry need to come collectively and agree on this type of platform could look. Utilizing the block chain to make sure safety for the financial services. IoT empowers objects to share and control information between objects since things are associated with the Internet. It is conceivable to submit malignant assaults, for example, information altering, or protection encroachment, while sharing information on articles over the Internet.

## 4. SYSTEM DESIGN

System Architecture layout-identifies the general hypermedia shape for the WebApp. Architecture design of specialist, not under any condition like PC programming languages that are run locally on the functioning structure (OS) of the contraption. Applications are made for user through a web application with a working association affiliation. User("client") for communicating using Android app. Admin for controlling user activities.

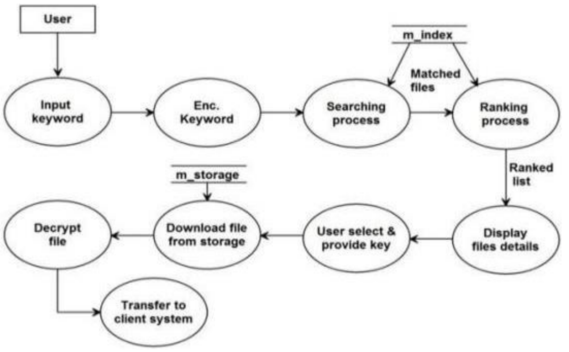


**Fig.1 System Design of blockchain encryption**

The monetary funds which uses financial services deals of monetary or cash related administrations by substances (associations, sole merchants and organizations) that are occupied with monetary administrations related exercises like loaning, speculation the executives, protection, businesses, installments and asset move administrations. The monetary industry is classified based on the plan of action of the organizations present in the business, and most firms offer different administrations. Incomes incorporate expenses, premium installments, commissions or exchange charges. The monetary market is fragmented into loaning and installments; protection (suppliers, and re-safety net providers); speculations; and unfamiliar trade administrations.

Blockchain being used as the accompanying huge thing after the creation of the web. One zone where these are likely going to have a huge impact is the money related region. The blockchain, as a kind of appropriated record advancement (DLT), can change grounded financial foundations and bring lower costs, speedier execution of trades, improved straightforwardness, auditability of undertakings, and various favorable circumstances. Cryptographic types of cash hold the assurance of another nearby automated asset class without a central position. Blockchain will lessen the enormous duplication of data that makes postponements, clashes and disarray in numerous parts of monetary services. For services, when an organization of banks partakes in advance, having one shared record implies they don't all have to monitor it freely. Global installments and corporate stock records are different models where there are tremendous shortcomings because of copy record-keeping and mediators. "End clients won't see the adjustments in the profound pipes of monetary administrations, yet it will permit new specialist organizations to arise and new items to be advertised".

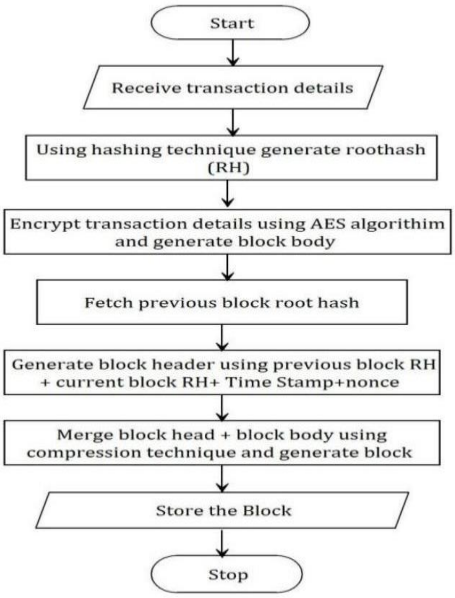

Start
Receive transaction details
Using hashing technique generate roothash (RH)
Encrypt transaction details using AES algorithim and generate block body
Fetch previous block root hash
Generate block header using previous block RH + current block RH+ Time Stamp+nonce
Merge block head + block body using compression technique and generate block
Store the Block
Stop

**Fig. 2 Blockchain creation process**

## 5. IMPLEMENTATION

The framework ought to be an electronic application that must be created utilizing progressed Java innovation with the Tomcat web worker and MySQL data set.

1.Framework should have 2 entertainers: Admin and User.

2.The administrator is the superuser and he is additionally called confided in power (TA).

3.Admin can enlist an information client.

4.Data clients can ready to login into their landing page with an approved secret phrase.

5.Data clients give the vehicle protection records, Once Data user login he can transfer records into the blockchain worker.

6.Data clients ready to download records from Block Chain Server.

The MVC arrangement shows that an application includes data model, introduction data, and control data. The model necessitates that are separated into various items. MVC is a more unmistakable proportion of a construction plan, yet not for an outright application. MVC all things considered identifies with the UI/association layer of application. You're truly going to require a business thinking layer, possibly some layer and data access layer.

It is implemented using following steps in creation process:
Step 1: Receive transaction details.
Step 2: Using hashing formula for generating root-hash.
Step 3: Encrypt transaction details using AES algorithm and generate the block.
Step 4: Fetch previous block root hash.

Step 5: Generate block header using previous block root hash.
Step 6: Merge both blocks using compression techniques.
Step 7: Store the block.

### 5.1 JAVA and J2EE

It allows software developers to "write once, run Anywhere"(WORA), because of this compiled Java code can run on any systems manually. Packages are typically compiled to bytecode that could run on any Java digital system (JVM) no matter of pc requirements. Maximum well-known programming languages in use, especially for python-web server programs, are mentioned nine million developers. Java was the first superior by means of the use of Java Enterprise Edition (Java EE), previously, presently Jakarta EE, is a tough and rapid (i.e. Not based totally on modern-day Java eleven at the same time as can also paintings with later it or later than Java eight) with specs for company abilities together with allotted computing and internet offerings.

### 5.2 Eclipse

Is integrated development of environment (IDE) used in pc programming, and is the broadly used JEE IDE. It incorporates a workspace and an extensible plug-in tool for customizing the surroundings. Eclipse is good for a beginner also its free, has a ton of features and its straight-up java features and lots of free IDEs for java. Most of the people like eclipse of any other resources. Since it is possible to set up text pad so we can compile and run inside it for simple problems. This open source IDE has long been one of the most reliable and oft-used IDEs.

### 5.3 Tomcat

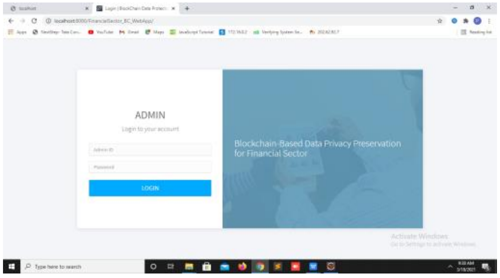
The Apache Tomcat, software is a open source implementation of the "Java" Servlet specifications. Tomcat project is intended to be collaboration of the best of breed developers from around the world. It refactors the creation of WebSocket end point, decoder and encoder instances to be more IOC friendly.

### 5.4 Android

Android App is a software program designed to run on an Android device or emulator. The time period also refers to an APK record which stands for Android bundle. Android apps can be written in Java, and C++ and are run inner Virtual Machine. The API just stores the request in a block. The queue has 2 channels, which might be for the user and the admin. The requests can either enroll a person, question facts from the blockchain network, or invoke or perform a transaction. The execution people use the Hyperledger Fabric Node.js SDK to carry out the requests.

## 6. RESULTS AND ANALYSIS

End result is the very last result of actions or events expressed qualitatively or quantitatively. Performance assessment is an operational evaluation, is a hard and fast of fundamental quantitative dating amongst the overall performance quantities.

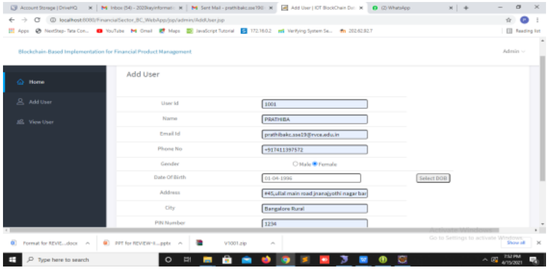

localhost:8080/FinancialSector_BC_WebApp/

ADMIN
Login to your account

Admin ID
Password
LOGIN

Blockchain-Based Data Privacy Preservation for Financial Sector

Fig. 3 Admin Login

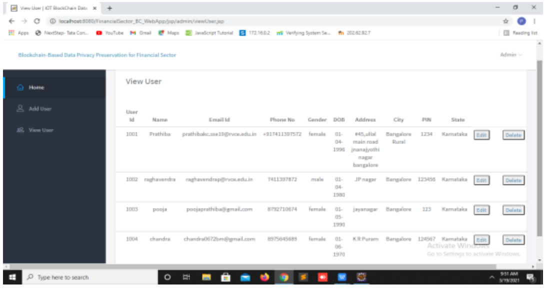

localhost:8080/FinancialSector_BC_WebApp/jsp/admin/AddUser.jsp

Blockchain-Based Implementation for Financial Product Management

Add User

User Id: 1001
Name: PRATHIBA
Email Id: prathibakc.sse19@rvce.edu.in
Phone No: +917411397572
Gender: ○ Male ● Female
Date Of Birth: 01-04-1996 Select DOB
Address: #45,ullal main road jnanajyothi nagar bar
City: Bangalore Rural
PIN Number: 1234

Fig. 4 User Details

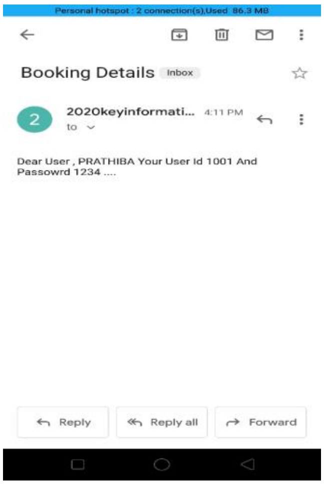

localhost:8080/FinancialSector_BC_WebApp/jsp/admin/viewUser.jsp

Blockchain-Based Data Privacy Preservation for Financial Sector

View User

| User Id | Name | Email Id | Phone No | Gender | DOB | Address | City | PIN | State | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1001 | Prathiba | prathibakc.sse19@rvce.edu.in | +917411397572 | female | 01-04-1996 | #45,ullal main road jnanajyothi nagar bangalore | Bangalore Rural | 1234 | Karnataka | Edit | Delete |
| 1002 | raghavendra | raghavendrap@rvce.edu.in | 7411397872 | male | 01-04-1980 | JP nagar | Bangalore | 123456 | Karnataka | Edit | Delete |
| 1003 | pooja | poojaprathiba@gmail.com | 8792710674 | female | 01-05-1990 | jayanagar | Bangalore | 123 | Karnataka | Edit | Delete |
| 1004 | chandra | chandra0672bm@gmail.com | 8975645689 | female | 01-06-1970 | K R Puram | Bangalore | 124567 | Karnataka | Edit | Delete |

Fig. 5 Adding User Details


Personal hotspot : 2 connection(s),Used 86.3 MB

Booking Details Inbox

2020keyinformati... 4:11 PM
to

Dear User , PRATHIBA Your User Id 1001 And Passowrd 1234 ....

Fig. 6 User Booking Details

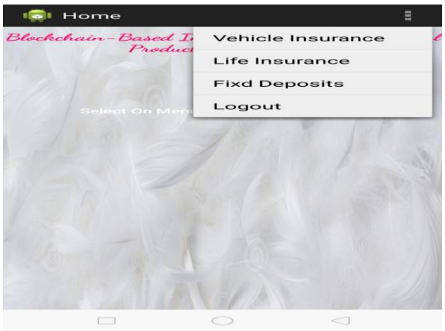
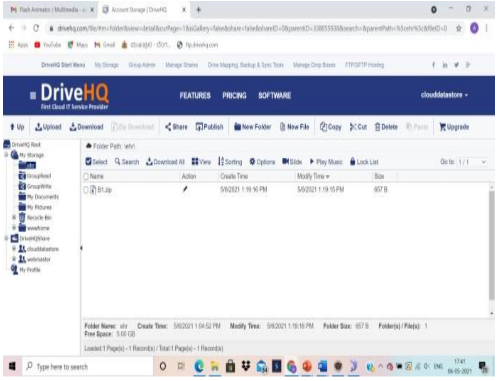


Fig. 7 Android App



Folder Path: \ehr

| Name | Action | Create Time | Modify Time | Size |
|---|---|---|---|---|
| B1.zip | | 5/6/2021 1:19:16 PM | 5/6/2021 1:19:15 PM | 657 B |

Folder Name: ehr Create Time: 5/6/2021 1:04:52 PM Modify Time: 5/6/2021 1:19:16 PM Folder Size: 657 B Folder(s) / File(s): 1
Free Space: 5.00 GB
Loaded 1 Page(s) - 1 Record(s) / Total 1 Page(s) - 1 Record(s)

Fig. 8 Cloud Storage

## 7. CONCLUSION

Centralized financial data is monetarily effective and may make esteem, both monetary and political, for those gatherings who approve, construct, work and regulate the frameworks that utilization it. Frequently, the interests of such gatherings are not lined up with the populaces they serve. To acknowledge secure transaction search over encoded information against clients and cloud specialist. Monetary area depend on the inability to meet the necessities for advancement by proficient market members. Not with standing simply mechanical issues like absence of quality, adaptability, performance.

Based on Hyperleger, pattern a financial sector as the advantages of monetary product inquiries, upkeep and traceability amongst multi-financial institutions. Automation of the complete device improves the efficacy of Financial Sector. It offers a pleasant graphical person interface which proves to be better when compared to the prevailing machine.

## 8. REFERENCES

[1] Han junhua, Zhou and Wang Hongchang, "Hazard of coordination of innovation and account in the period of enormous information and mechanical oversight of square chain [J]", Scientific the board research, vol. 37, no. 1, pp. 92-95, 2019.

[2] G. I. J. Kingsley and W. J Jakubowski, “System and strategies for exchanging complex monetary items”, US, 2019.

[3] A. Gervais, G. O. Karame, K. W¨ust, V. Glykantzis, H. Ritzdorf, and S. Capkun, “On the security and performance of proof of work blockchains,” in Proceedings of ACM SIGSAC Conference on Computer and Communications Security (CCS’16), pp. 3–16, New York, NY, USA, 2018.

[4] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “The blockchain model of cryptography and privacy-preserving smart contracts,” in 2016 IEEE Symposium on Security and Privacy, May 2019.

[5] W. T. Tsai, R. Blower, Y. Zhu, and L. Yu, “A system view of financial blockchains,” in IEEE Symposium on Service-Oriented System Engineering (SOSE’16), pp. 450–457, Mar. 2016.

[6] J. Linnenbringer, W. Hedish, J. Ryan, M. J. Watkins and M Majikes,” Method and System for creating”. Electornics structures for Purchasing FINANCIAL PRODUCTS, 2018.

[7] Swan M. Blockchain: Blueprint for a new economy. O'Reilly Media Inc., 2015.

[8] A. Kosba, A. Miller, E. Shi, Z. K. Wen, and C. Papamanthou, Hawk: “The blockchain model of cryptography and privacy-preserving smart”,2017.

[9] Nakamoto S. Bitcoin “A peer-to-peer electronic cash system”. https://bitcoin.org/bitcoin.pdf,(2018). K. Elissa, “Title of paper if known,” unpublished.

[10] Gramoli, V. (2017). from “Blockchain consensus back to Byzantine consensus”. Future Generation Computer Systems,2019.