IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

JAVA BASED IMPLEMENTATION OF GOVERNMENT SCHEMES USING BLOCKCHAIN TECHNOLOGY

[1] Mayuri Fulwade, [2]Pallavi Kharat, [3]Dipti Shinde, [4]Prof. Mandalik S.Y.

[1,2,3,4]Computer Engineering Department,

[1,2,3,4]Jaihind College of Engineering, Pune, Savitribai Phule Pune University, Maharashtra, India

Abstract: Simple, convenient and effective interaction between the government and the citizen has become a common expectation in the modern information society. Electronic government solutions - based on automation of decision making processes on a nation-wide scale - are serving to meet these expectations, while generating efficiencies in government and social communications for each member of the society. Electronic government brings fundamental changes to the distributed governance system, and affects the entire range functions related to document management and processing. Belarus has made visible progress towards establishing an electronic government infrastructure and services. These achievements have been enabled primarily by accelerated development of information and communication technologies (ICTs). However, citizens' participation in e-governance in Belarus is still below the average for Eastern Europe, which is largely the result of limited penetration of interactive functions and online services available from the official web-sites of government bodies and institutions. the multiple technological solutions, varying in speed, and the degrees of reliability and data safety, several recent technological inovations stand out, based on radically new principles of compatibility and offering great promise for electronic government.

Index Terms **- blockchain technology, security, transparency, hash function, cryptography**

I. INTRODUCTION

An In essence, a blockchain is a transparent distributed data base that records de- tails on all transactions performed by the system's participants. In the context of electronic government, this means a technology that stores data on the results of all interactions between citizens and government agencies. Importantly, the data are interlinked, coded and stored by all members of the system, and are automatically updated to reflect the changes made. Users act as a collective notary that certifies the accuracy of the data in the system and guards against abuses and scheming attempts. Blockchain technology acts as a control on the egoistic motives that cause some people to engage in corrupt practices to the detriment of society and state sovereignty. It also creates a powerful incentive to abide by the rules that apply to all participants equally, thus creating a spirit of collective responsibility. Technically, blockchain is a technology that facilitates agreement among the participants on virtually any matter without the involvement of an intermediary; it thus creates a foundation for decentralised governance, promotes consensus-based social contracts and maintains a fair balance of interest beneficial to society. A registration system based on blockchain technology can enhance the safeguards normally offered by the traditional registries. The cost of transactions can be greatly reduced by eliminating the payment of state duties and intermediary fees, while the transactions themselves can become less time-consuming, and also more transparent and more secure. The development of Blockchain technology in e-government still needs discussion in different aspects; this technology offers a new method for delivering and managing public services, and there remains a need to establish standards, deploy solid management systems and ensure adequate security to make sure the services and platform are reliable, authoritative and supportive of long-term preservation. It has the potential to change Indian society in many aspects. Its

development still has both opportunities and risks, however. There is still a need for Blockchain companies and market administrators to actively collaborate with each other, implement Blockchain operations, and introduce innovative solutions. Therefore, the experience of the government could be the first step in the development of Blockchain-based public services. However, this will not be an easy goal to achieve

II. **Related work**

[1]"Comparison and Analysis of Governance Mechanisms Employed by Blockchain-Based Distributed Autonomous Organizations" by Stephen DiRose and Mo Mansouri, published in the 2018 13th Annual Conference on System of Systems Engineering (SoSE): This paper assesses governance mechanisms in blockchain projects, using the change in block size as an example. It describes, compares, and evaluates two key governance mechanisms, focusing on their effectiveness in reaching consensus and supporting the diverse needs of stakeholders. www.ijcrt.org © 20XX IJCRT | Volume X, Issue X Month Year | ISSN: 2320-2882 IJCRT1601009 International Journal of Creative Research Thoughts (IJCRT) www.ijcrt.org 26 [2]"A novel triple DES to enhance E-governance security" by Raja Sekhar Reddy and G. Murali, published in the 2017 International Conference on Energy, Communication, Data Analytics, and Soft Computing (ICECDS): This paper discusses the use of a novel triple DES algorithm to enhance security in E-Governance, particularly in the context of banking transactions, addressing the need for data encryption.

[3]"An approach to increase the awareness of e-governance initiatives based on cloud computing" by Sini Shibu and Archana Naik, published in the 2017 International Conference on Information, Communication, Instrumentation, and Control (ICICIC): This paper analyzes the cloud-based model of e-governance and proposes measures to raise awareness about government initiatives, particularly in the state of Madhya Pradesh, though it acknowledges the lack of focus on security parameters.

[4] "A framework for the monitoring and evaluation of e-governance projects in developing countries" by Sylvester Hatsu and Ernest Ketcha Ngassam, published in the 2016 IST-Africa Week Conference: This paper presents a framework for monitoring and evaluating e-Gov projects, concentrating on life cycle aspects but not emphasizing transparency concerns. "Implementation of e-governance: Only way to build a corruption-free Bangladesh" by S. A. Ahsan Rajon and Sk. Ali Zaman, published in the 2008 11th International Conference on Computer and Information Technology: This paper offers a comparative analysis of the current government structure in Bangladesh and the potential for implementing e-governance to combat corruption in various governance sectors. It highlights the adaptability of e-governance, particularly in the participation of mass citizens in decision-making processes and ensuring transparency in government sectors.

[5]"On SHEL model analysis and constitution — The research on the Chinese government's E-governance system based on the concept of good governance" by Liu Liu and Xiao-ming Liao, published in the Proceedings of the 2011 Cross Strait Quad-Regional Radio Science and Wireless Technology Conference: This paper introduces the SHEL model, encompassing Software, Hardware, Environment, and Liveware, as a basis for government e-governance in China. However, it also points out that the trust-based model could lead to potential corruption issues due to citizens' reliance on government authorities.

III. **Proposed algorithm**

A. SHA 256:

Hash Function SHA-256 (secure hash algorithm, FIPS 182-2) is a cryptographic hash function with a digest length of 256 bits.While the hash produced by SHA-256 is not truly unique (as there are a finite number of possible hash values and an infinite number of possible inputs), it is designed to be collision-resistant. Collision resistance means it should be extremely difficult to find two different inputs that produce the same hash value.

B. AES:

AES is used to encrypt the database. AES encryption involves key expansion, initialization of the state array, several rounds of state manipulation (each consisting of substitution, permutation, mixing, and key addition operations), and a final round that excludes the Mix Columns operation. The final state array represents the encrypted data, which is the ciphertext. The number of rounds depends on the key length (128, 192, or 256 bits). The described steps provide a high-level overview of the AES encryption process.

IV.MOTIVATION

In essence, a blockchain is a transparent distributed data base that records details on all transactions performed by the system's participants. In the context of electronic government, this means a technology that stores data on the results of all interactions between citizens and government agencies.

V.Objectives

1. To implement a java based web application.
2. To implement AES.
3.To implement visual cryptography.
4.To implement block chain.
5.To implement distributed database system using WLAN.

.

VI. METHODOLOGIES OF PROBLEM SOLVING

BCT Agricultural products are the foundation of the people's survival, and the qual- ity of agricultural products has always been the focus of attention of society and the government; the original agricultural product traceability system is too difficult to tamper with data due to the excessive concentration of data storage, it faces the challenge of fraudulent data tracing, and it is difficult for consumers to trust such traceability results. Moreover, the centralized storage method is not conducive to the centralized management of traceable data from many enterprises, and there will be problems of low traceability and difficulty in government supervision. The emergence of blockchain technology provides a new solution for data security problems of food traceability, its decentralization, anti-tampering and other characteristics and data encryption technology improve the difficulty of data fraud and ensure data security. If the blockchain is combined with the traceability of agricultural products, the safety of traceable data and the tampering of data can be guaranteed to the greatest extent, the producer's production behavior can be regulated, and consumers' confidence in food quality can be improved. This project mainly proposes a framework of agricultural product traceability system based on blockchain technology, it uses blockchain to store the traceability data of agricultural products safely, and proposes a traceability model of agricultural products, which can cover the entire industrial chain of agricultural products, and consumers can query the authentic source of traceability of agricultural products.

VII. SYSTEM ARCHITECTURE

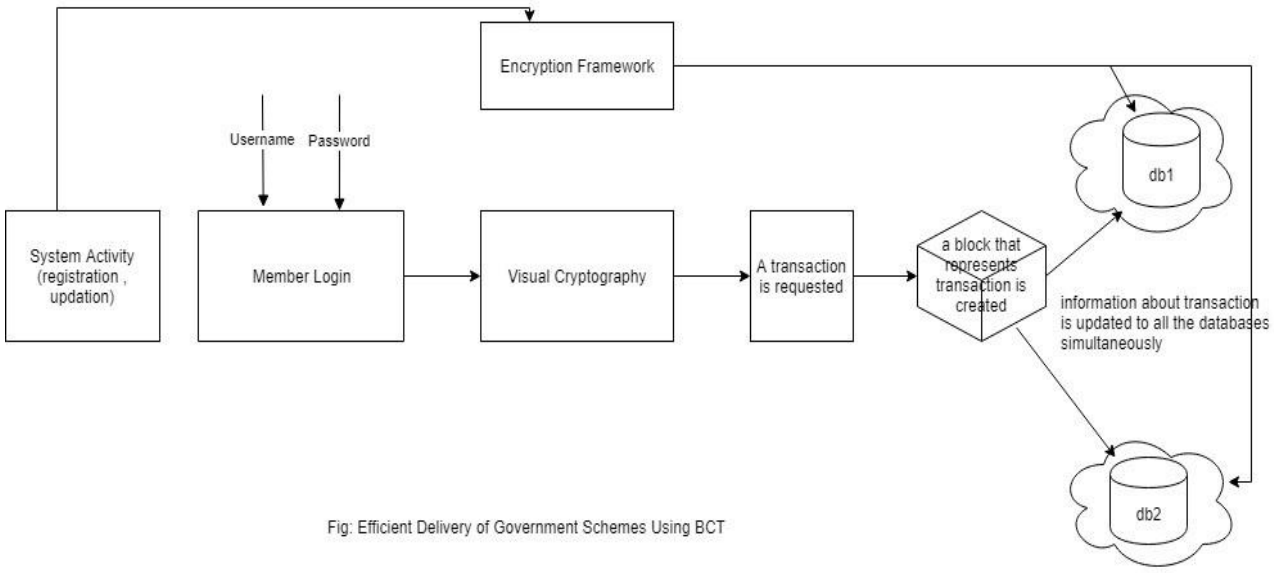

Fig: Efficient Delivery of Government Schemes Using BCT

Whenever any transaction will occur in the system, the record of that transaction is maintained in the form of hash value in a block. Each next block will get attached to the previous block and in this way a virtual block chain will occur. The hash value of a current block is generated using the data of a current block and the hash of the previous block. In this way if any of the block is tempered the Figure 1. System Architecture subsequent all the block's hash must be changed . Such multiple copies are maintained at different servers , which will

assure the data security and confidentiality. As everything is through application interface, it will maintain the transparency in the government schemes.

Visual cryptography is a cryptographic technique that involves splitting a secret image into multiple shares in such a way that knowledge of a subset of shares is required to visually reconstruct the original image. An authentication mechanism where a user needs to submit an image, and the system combines it with another image for successful login. This could be implemented using visual cryptography by generating shares of both the user-submitted image and a system-held image. The combined result, possibly through pixel-wise operations, forms the authentication key. Only when the user's input and the system-held image are correctly combined will the login be deemed successful, ensuring a visually authenticated access process.

Blockchain generation using SHA-256 involves creating a secure and tamper-resistant distributed ledger. In this process, each block in the blockchain contains a unique identifier known as a cryptographic hash, computed using the SHA-256 algorithm. When a new block is added to the chain, it includes a hash of the previous block, creating a continuous and irreversible chain of blocks. SHA-256 (Secure Hash Algorithm 256-bit) ensures the integrity of the blockchain by generating a fixed-size hash that is unique to the input data. Any alteration in the content of a block would require changing all subsequent blocks, making the blockchain resistant to tampering. The decentralized and consensus-driven nature of blockchain, coupled with SHA256's cryptographic strength, provides a robust foundation for securing data and transactions in various applications.

The Advanced Encryption Standard (AES) is a symmetric encryption algorithm widely adopted for its security and efficiency. It operates on fixed-size blocks of data and uses a symmetric key for both encryption and decryption. AES has three standard key sizes: 128, 192, and 256 bits. It employs a series of well-defined and standardized cryptographic transformations, including substitution permutation networks, providing a high level of confidentiality for sensitive information. AES is extensively used in various applications, ensuring secure data transmission and storage.

VIII. Mathematical Model

Let
S be Closed system defined as, S = Ip, Op, Ss, Su, Fi, A
To select the input from the system and perform various actions from the set
of actions A so that Su state can be attained.
S=Ip,Op,Ss,Su,Fi,A
Where,
IP1=Username, Password, image
Set of actions=A=F1,F2,F3,F4
Where
F1= Send Mail
F2= Merge Images
F3= Encrypt Database
F4= Generate Hash
S=Set of users
Ss=rest state, registration state, login state
Su- success state is successful analysis
Fi- failure state
Objects:
1) Input1: Ip1 = Username, Password
2) Input2 : Ip2= image from mail
1) Output1 : Op1 = Transaction Record
2) Output2 : Op2 = Encrypted Database
3) Output3 : Op3 = Hash Code

IX. RESULTS

OUTCOME

Transparent supply chain due to use of BCT, block chain of every transaction is maintained and can be tracked in future

SCREENSHOTS:

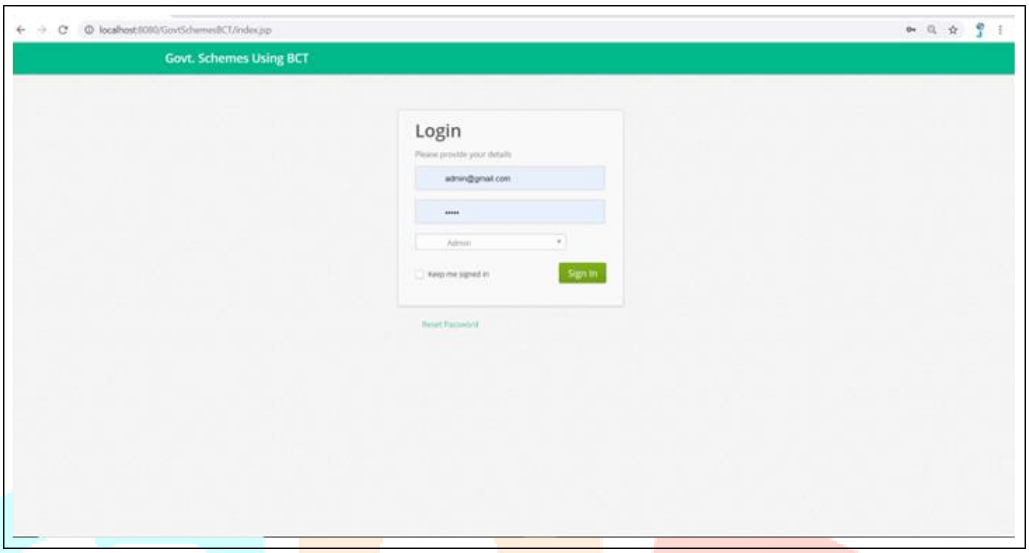

Figure 10.1: Login Page

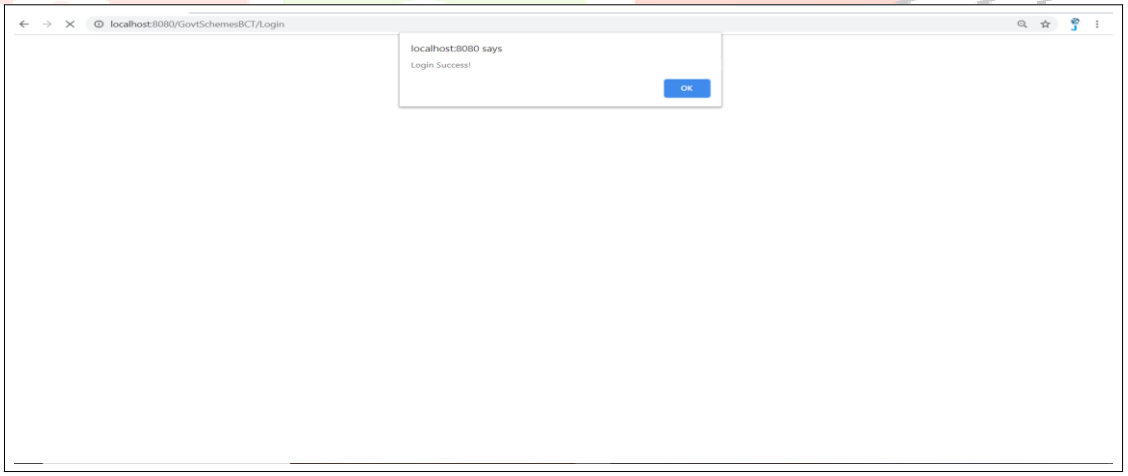

Figure 10.2: Admin(Central Gov) Login Success

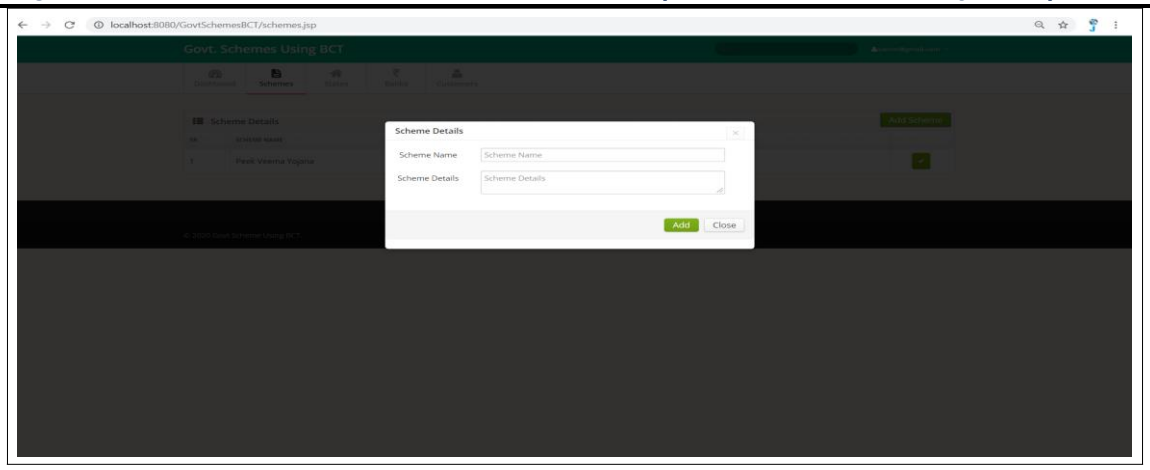

Figure 10.3: Add New Scheme

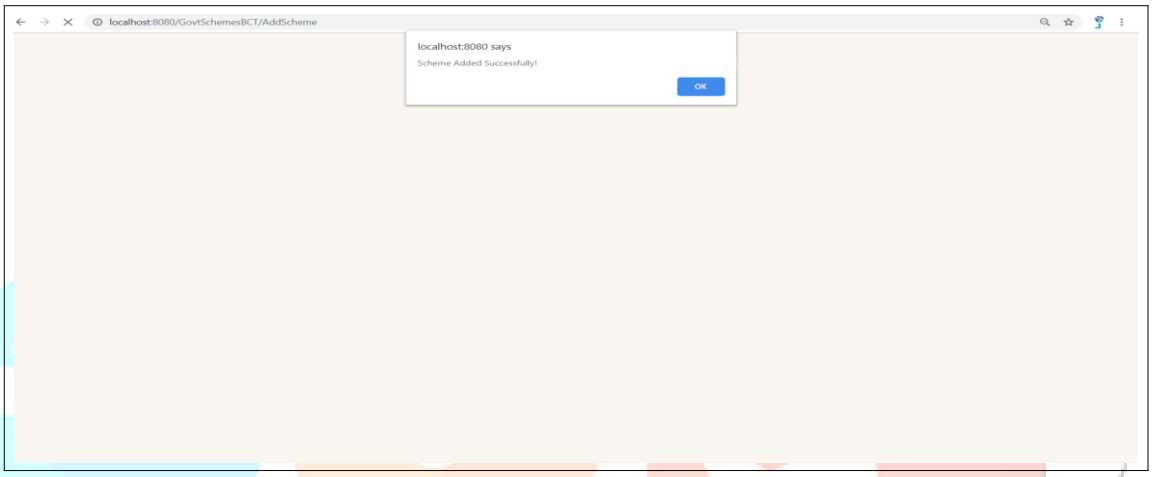

Figure 10.4: New Scheme Added Successfully

Figure 10.5: Share Uploaded Here

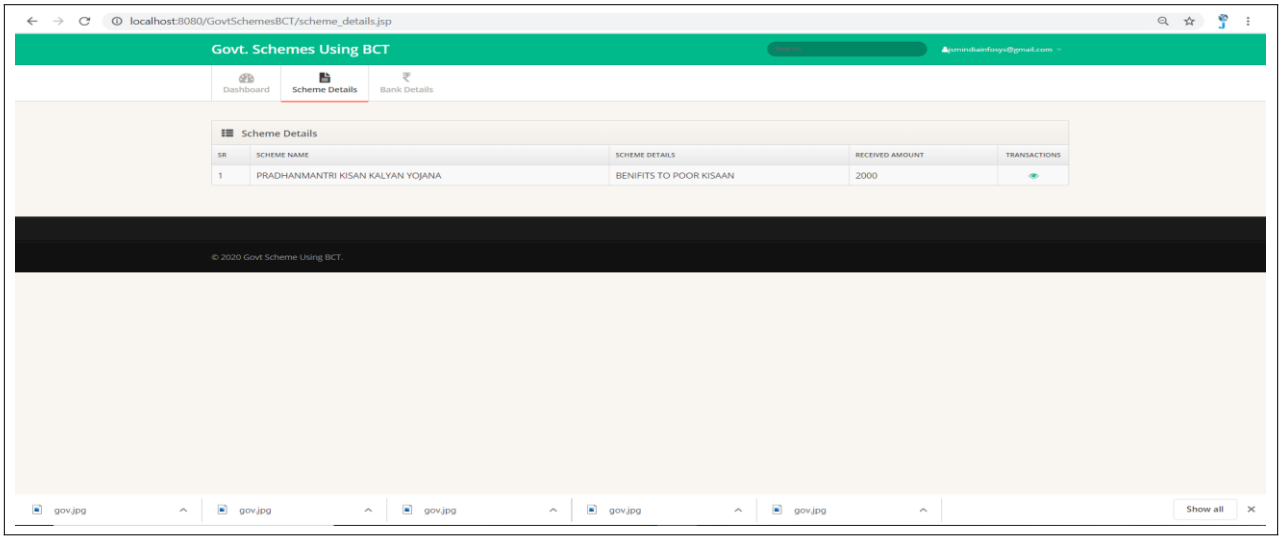

Figure 10.6: Scheme Details

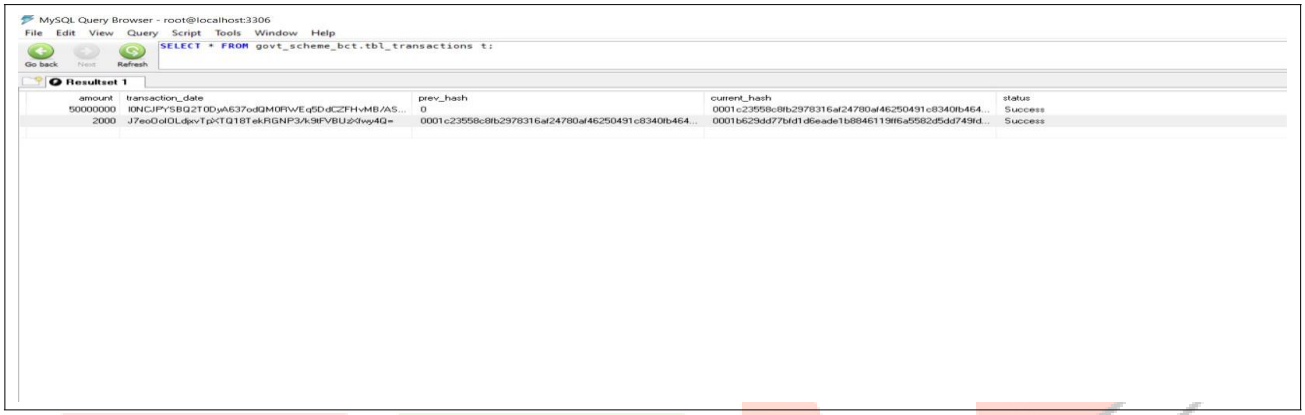

Figure 10.7: Block Chain Generated Mysql Database

X. CONCLUSION

Thus we are have implemented a prototype web based software application in Java for application of BCT in the efficient delivery of government schemes using BCT . We have implemented block chain features such as: 1. Decentralization 2. Visual Cryptography 3. Hash Algorithm 4. Encrypted Database. Thus it is possible to track government schemes and to deliver the schemes upto a commom man.

References

1. Yashita Goswami, Ankit Agrawal, Ashutosh Bhatia, " E-Governance: A Tendering Framework Using Blockchain With Active Participation of Citizens",
IEEE 2020 research paper
2. Aichih (Jasmine) Chang, Nesreen El-Rayes and Jim Shi, "Blockchain Technology for Supply Chain Management: A Comprehensive Review", MDPI
2022 research paper
3. Ioannis Lykidis , George Drosatos and Konstantinos Rantos,"The Use of Blockchain Technology in e-Government Services", MDPI 2021 research paper
4. Abhik Banerjee, Abhirup Deb, Sourav Mondal, Sounak Ghosh, "Decentralized Policy Feedback System for Privacy and Governance using Block chain and Sentiment Analysis for Smart City Applications", IEEE research paper
5. Jing Hua1, Xiujuan Wang, Mengzhen Kang1, Haoyu Wang1, Fei-Yue Wang,"Blockchain Based Provenance for Agricultural Products: A Distributed Plat- form with Duplicated and Shared Bookkeeping",2018
6. Raja Sekhar Reddy, G. Murali,"A novel triple DES to enhance E-governance security",2017

7. Sylvester Hatsu, Ernest Ketcha Ngassam," A framework for the monitoring and evaluation of e-governance projects in developing countries",2016
8. Liu Liu, Xiao-ming Liao," On SHEL model analysis and constitution — The research on Chinese government's E-governance system based on the concept of good governance",2011
9. Sini Shibu, Archana Naik," An approach to increase the awareness of e-governance initiatives based on cloud computing",2011
10. Stephen DiRose ,Mo Mansouri," Comparison and Analysis of Governance Mechanisms Employed by Blockchain- Based Distributed Autonomous Organizations",2018
11. L. Guo, C. Zhang, J. Sun, Y. Fang. "A privacy-preserving attribute based authentication System for Mobile Health Networks", IEEE Transactions on Mobile Computing, 2014.
12. A. Abbas, S. Khan, " A review on the state-of-the-art privacy preserving approaches in e-health clouds", IEEE Journal of Biomedical Health Informatics,2014.
13. J. Yang, J. Li, Y. Niu, " A hybrid solution for privacy preserving medi-cal data sharing in the cloud environment ", Future Generation Computer Systems,2015.
14. V. Goyal, O. Pandey, A. Sahai, B. Waters, " Attribute-based encryption for fine-grained access control of encrypted data ", Proc. 13thm ACM Conf. Computer and Comm. Security (CCS06), 2006.
15. R. Ostrovsky, A. Sahai, B.Waters, " Attribute-based encryption with non-monotonic access structures ", in: Proceedings of the 14th ACM Conference on Computer and Communications Security, ACM, 2007.
16. J. Han, W. Susilo, Y. Mu. " Improving privacy and security in decentralized cipher text-policy attribute-based encryption ", IEEE Transactions on Information Forensics and Security, 2015.
17. M. Li, S. Yu, Y. Zheng, K. Ren, W. Lou, " Scalable and secure sharing of personal health records in cloud computing using attribute based encryption", IEEE transactions on parallel and distributed systems, 2013.
18. M. Green, S. Hohenberger, B. Waters, " Outsourcing the decryption of ABE ciphertexts ", in Proc. USENIX Security Symp., San Francisco, CA, USA,2011.
19. J. Lai, R. H. Deng, C. Guan, J. Weng, "Attribute-based encryption with verifiable outsourced decryption ", IEEE Trans. Inf. Forensics Security, Aug.2013.
20. B. Qin, R. H. Deng, S. Liu, S. Ma, "Attribute-based encryption with efficient verifiable outsourced decryption ", IEEE Trans. Inf. Forensics Security, JULY.s2015.