

DETECTING AND PREVENTING CHECK SCAM IN BANKING SYSTEM USING BLOCKCHAIN

A. Vidhya (vidhyaraj1988@gmail.com)

S. Rajalakshmi (rajalakshmiraji651@gmail.com)

R. Sruthi (rshruti451@gmail.com)

Department of Computer Science and Engineering,

Jeppiaar Engineering College, Chennai, India

Abstract - Check scam is one of the major issue faced by most of the people. In most cases fake check may look similar to the real check, even the bank employees may think it is a real one. Generally, the bank will take a period of time, in order to detect the scam. In our country there are many charity centers for different set of people and they require help from the people who are really willing to donate. But even if some of the public willing to help, they where not donating because of trust issue. In the proposed system, the public can donate money through check using a web application though which the public can transfer the money in a secured way. Here SHA algorithm and blockchain is used to make secured transaction and AES algorithm is used to identify the check scam.

Key Words: Blockchain, SHA algorithm, AES algorithm

1.INTRODUCTION

Blockchain is a decentralized distributed ledger system that make digital asset's records transparent. It is a revolutionary technology that gains a lot of attention because of its ability to eliminate risks and frauds on a large scale. In today's world, there are many people who still craves for basic needs such as food, clothing and shelter. Some of the people who live above the poverty line cannot help directly to needy people. So we can use charity as a platform to help the people. But some people hesitate to help charity because fake things are rising up very clear than the original. So with the help of blockchain technology and cryptographic algorithms such as SHA and AES algorithms, the transactions will be secured in a way that no one can trace the transaction. In existing system, cheque scams are detected using blockchain technologies like namecoin and hyperledger and using cryptographic algorithms such as Digital Signature Standard (DSS) and Secure Hash Algorithm (SHA). In proposed system, charity website is developed using Html, CSS and JS and the data entries are stored in Mysql database and the transactions are secured using Secure Hash Algorithm (SHA) and Advanced Encryption Standard (AES) algorithm is used to detect the scam.

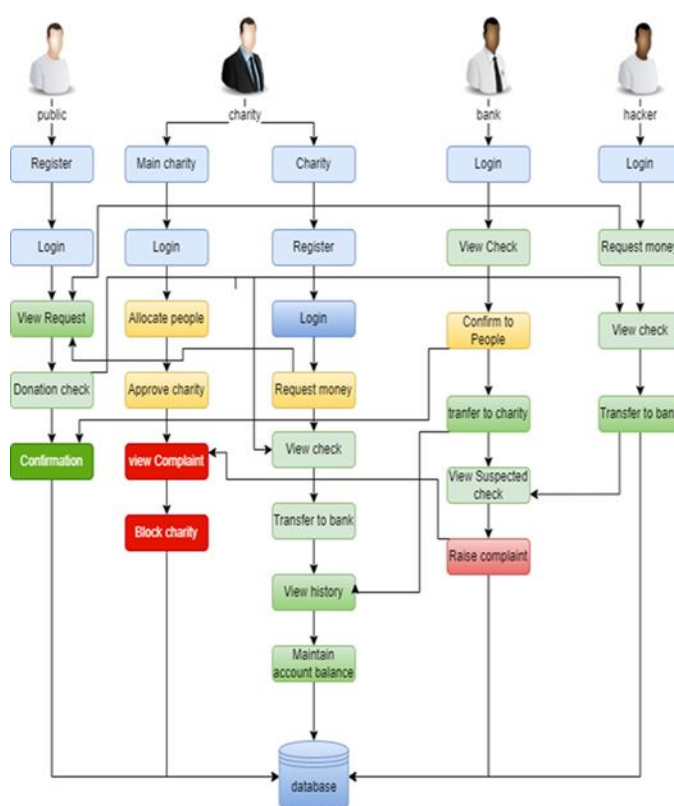


Fig- 1: Architecture diagram

2. LITERATURE SURVEY

2.1. Block chain technology for protecting the banking transaction without using tokens:

Here centralized database is used by the banking system which makes the attacker easy to get access to data and this makes the system insecure. The disadvantage of this centralized system can be mitigated by reforming it with blockchain technology instead of tokens. For storing and accessing data across a database, blockchain employs a decentralized architecture. This reduces attacks on database hack. Transactions done through blockchain technology are verified by each block in the chain, making them more secure and allowing the banking system to operate more quickly.

2.2. Expeditious banking using Blockchain Technology:

The current financial infrastructure is heavily centralized, making it subject to load defaults and frauds such as the PNB, Videocon, and Kingfisher scams, among others.. Block chain technology has been used by banks all around the world, and it is the technology of the future for regulation and fraud prevention. They're employing block chain technology to decentralize banking and eliminate all forms of authoritarian surveillance. The model includes block chain encapsulated in the process of NEFT (National Electronic Fund Transfer) using IFSC (Indian Financial System Code) incorporating the protocols set down by RBI for secure and decentralized fund transfer. The blocks will consist of the process computed in java micro services. Consensus algorithms is used to connect the ledgers within themselves.

2.3. Blockchain Technology based Electoral Franchise:

Many applications, such as smart cities, online banking, and others, have relied heavily on technology in recent years. In democratic countries, the voting system is proving to be an essential model for choosing the best leader. Despite the hype, the existing voting system requires more integrity and privacy in order to preserve sensitive data. This can be accomplished by leveraging numerous cutting-edge technological ways available in today's digital environment. As a result, the proposed work has integrated blockchain technology into the existing voting system to increase the voting system's security features. The immutable and distributive nature of this technology helps to limit attacks and threats on the voting mechanism. They have used Dagger Hash algorithm and ETH/TRX crypto coins to develop a BCT based voting system.

3. PROPOSED SYSTEM

In recent days there are many charity centers for different set of people and they require help from the people who are really willing to donate. But even if some of the public are ready to help, they were not donating because of trust issue they have on those charity whether the donated amount were really utilized by the people who are in need. In the proposed system, the public can donate money through checks using a web application were only the authorized charity will be permitted by the main charity.

Whenever the charity deposits the check, the bank will verify with the public whether they donated or not. If any fake charity tries to deposit the check, then the bank will verify whether the charity is authorized or fake one with the help of AES algorithm. Then the main charity will block the suspected charity. This will be helpful to reduce the check spams and also the donated amount will be reaching the desired people who are in need of help.

4. IMPLEMENTATION

Here there are five major roles such as public, main charity, charity, bank and the hacker. Charity is a trustable one which helps needy people and at the same time, the hacker will login and act fake like a trustworthy charity with same charity name. Main charity will allocate the people and approve all the individual charity. Public will login into the charity and the public will view the request of money requested by both charity and the hacker(fake charity). After viewing the money request, the public will donate the cheque. At the same time both charity and hacker will view the cheque. Both charity and hacker take the cheque to the bank. Bank will login and view the cheque donated by public and they will verify the cheque by contacting the owner of the cheque and if the public confirm the cheque, then the money will be transferred to the charity. Then the charity will view the history that who are the people donated to them.

All the transaction details and the information records are stored in Mysql database. If incase the public is not ready to confirm the cheque or the bank identify the fake check, then it is considered as suspected check and the bank will raise the complaint and the main charity will view the complaint and blocks the charity and the original charity has to change the username and password immediately because the hacker came with the charity name which is an existed trustable charity. Even though digitalized world helps us in a lot of ways. But, one of the major attacks involved in this digitalized world is money scams. So with the help of this project, major money attack is avoided.

5. RESULT AND DISCUSSION

Check spam is the major problem faced by most of the people. Here we have implemented the check spam detection in a charity management system. In recent days there are many charity which was organized by authorized main charity where whoever willing can donate money in order to help others. But most of us will refuse to donate because of trust issue that the money that we donate will reach the desired person or not. The proposed system will be helpful for the charity who are in need of help as well as the people who are willing to donate.

Here we proposed a web application where people can transfer the money in a secured way. SHA algorithm is used to generate the hash value were unique code will be generated for each transaction, whereas the first hash value will be given to the second person and the second value will be given to the third person as chain process. In this way the transaction will be secured using blockchain whenever the bank transfer the amount to charity. AES algorithm is used in case any fake charity try to transfer the check the check number will get encrypted and the bank will raise complaint to the main charity and the charity will be deactivated.

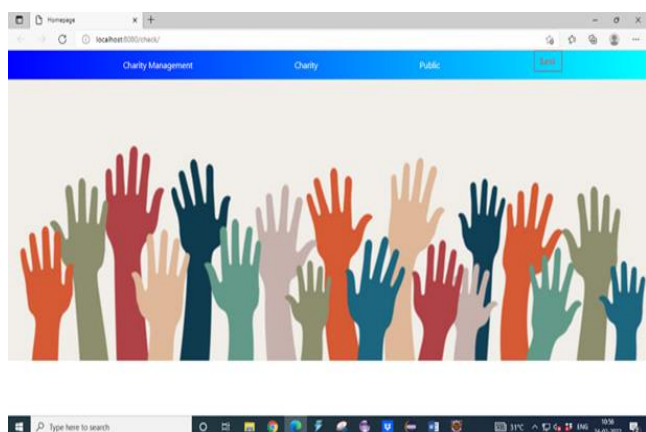


Fig-2: Homepage

The Fig.2 is the homepage of the implementation, here there is separate page for charity management, charity, public and bank.

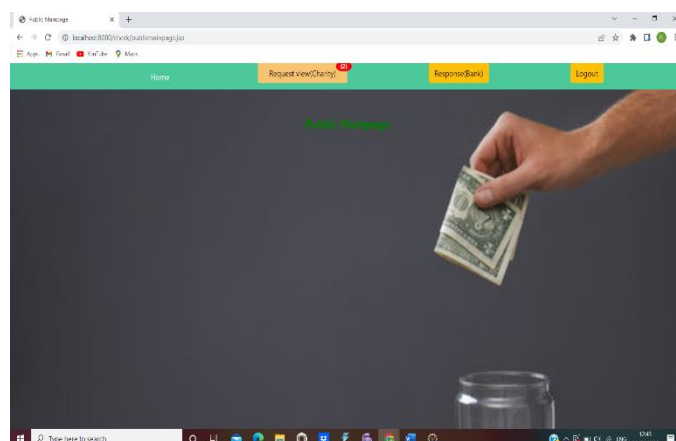


Fig- 5: Public Main Page

The Fig.5 is the public main page, here the public can view the request from charity and can give response to the bank, whether they have donated or not.

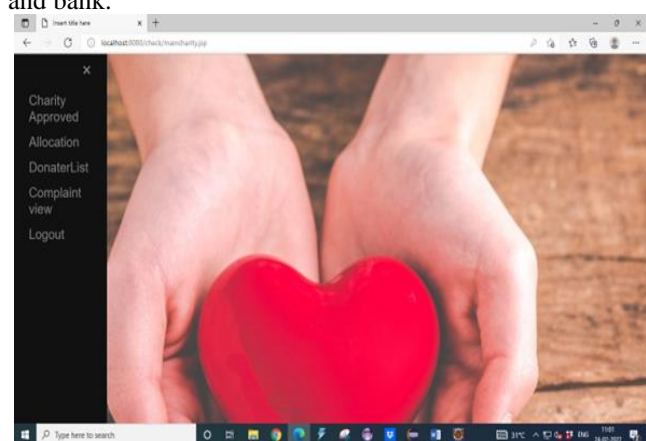


Fig- 3: Charity Management

The Fig.3 is the main page of charity management, where they will give approval for the sub charity and can view donator list and complaint.



Fig- 4: Charity Main Page

The Fig.4 is the main page of the charity, they can give request to the public and the donation received from the public and can check the account balance.

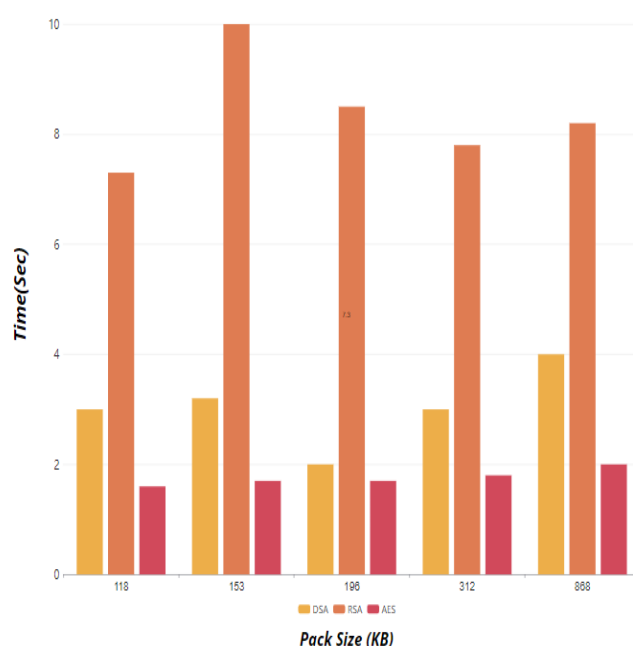


Fig-6: Encryption decryption time of AES algorithm

TABLE- I: Comparison of algorithm

SL. No	Pack Size (KB)	DES Time(s)	RSA Time(s)	AES Time(s)
1.	118	3.0	7.3	1.6
2.	153	3.2	10	1.7
3.	196	2.0	8.5	1.7
4.	312	3.0	7.8	1.8
5.	868	4.0	8.2	2.0

The AES algorithm takes least encryption and decryption time when compared to DES and RSA. It is more secure than the other two algorithm.

6.CONCLUSION AND FUTURE WORK

In this paper we have implemented cryptographic algorithm and blockchain in a charity management system in order to make the transaction secure and to identify the fake check scam, which will be highly helpful for the charity and the people who are willing to donate and to develop trust for the people, that the money that they donate will reach the desired charity in need. In future we can enhance by using real time database and can develop this as a web hosting site which will be accessible for everyone on the internet.

REFERENCES

- [1] S. Baker, "Don't cash that check: BBB study shows how fake check scams bait consumers," Tech. Rep., Better Bus. Bureau, Arlington County, VA, USA, Sep. 2018.
- [2] Banerjee, Mandrita, Junghee Lee, and Kim-Kwang Raymond Choo. "A blockchain future for internet of things security: A position paper." *Digital Communications and Networks* 4.3 (2018): 149-160
- [3] *Federal Trade Commission*, "Consumer sentinel network data book 2017," Federal Trade Commission, Washington, DC, USA, Tech. Rep., Mar. 2018.
- [4] N. Kabra, P. Bhattacharya, S. Tanwar, and S. Tyagi, "MudraChain: Blockchain-based framework for automated cheque clearance in financial institutions," *Futur. Gener. Comput. Syst.*, vol. 102, pp. 574–587, 2020.
- [5] Supriya Thakur Aras, Vrushali Kulkarni, Blockchain and Its Applications – A Detailed Survey I , *International Journal of Computer Applications* (0975 – 8887) Volume 180 – No.3, December 2017
- [6] Neetu Settia, "Cryptanalysis of Modern Cryptographic Algorithms", *IJCST* Vol. 1, Issue 2, December 2010
- [7] .S. Goyat 2012, "Genetic Key Generation For Public Key Encryption Cryptography", (*IJSCE*) ISSN: 2231-2307, Volume 2nd, issue-3rd, July 2012
- [8] Li Mingfei. Simulation of Multi-source Network Data Privacy Protection Based on Private Block Chain. *Computer Simulation*, vol. 36, no.8, pp. 266-270, 2019.
- [9] Zuhar Musliyana, "Security enhancement of advanced encryption standard (AES) using time-based dynamic key generation", *ARPN Journal of Engineering and Applied Sciences*, Vol. 10, No. 18, October 2015.
- [10] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for IoT," *Comput. Secur.*, vol. 78, pp. 126–142, 2018.
- [11] Hammi, Mohamed Tahar, et al. "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT." *Computers & Security* 78 (2018): 126-142.
- [12] M. A. El-Wahed, S. Mesbah, and A. Shoukry, "Efficiency and security of some image encryption algorithms," in *Proceedings of the world congress on engineering*, vol. 1. London, 2008, pp. 2–4.

