PREVENTION AND DETECTION OF FAKE CHEQUE SCAMS USING BLOCKCHAIN

Mrs.S.T. Santhanalakshmi[1], P. Srimanjari[2], K.B. Subrini[3], A.R. Swetha[4]

[1] Associate Professor, Department of Computer Science and Engineering, Panimalar Engineering College
[2] Department of Computer Science and Engineering, Panimalar Engineering College
[3] Department of Computer Science and Engineering, Panimalar Engineering College
[4] Department of Computer Science and Engineering, Panimalar Engineering College

***Abstract*—A fake cheque scam is one of the most common ways used to commit fraud against consumers. There is no existing method to authenticate checks and detect fake ones instantly. Instead, banks must wait for a period of more time and date to detect the scam. More precisely, our approach helps the bank to share information about provided and used cheques without exposing the bank's customer's data. Fake cheque scams come in many forms. They might look like business or personal cheques, cashier's cheques, money orders, or cheques delivered electronically. These scams work because fake cheques generally look just like genuine cheques, even to bank employees. They are published with the names and addresses of licit fiscal institutions. Banks are maintaining security services for money transaction for customer security purpose directly check with customer and requires their permission. If the response is received from the concerned customer only, the transaction will happen.**

Keywords—blockchain, cheque, security, authentication, fraud, bank.

I. Introduction

In our current society, cheques represent one of the dominant payment methods. The cheque is an order written by the depositor instructing the bank to pay a specific amount to a recipient from the depositor's bank account. Unfortunately, numerous malicious scammers exploit some flaws in the banking system to commit frauds. Indeed, frauds employing fake cheques are growing rapidly and cost billions of money. we focus on fake cheque scams. This fraud is achieved by getting people mainly through some email scam, establishing a relationship a business relationship most of the time sending them overpaid counterfeit paycheque and finally asking for the overpayment.

II. Literature Survey

Badis Hammi, Sherali Zeadally, Yves Christian Elloh Adja, Manlio Del Giudice, and Jamel Nebhen, 2021, "Blockchain-Based solution for Detecting and preventing Fake Cheque Scams" [1] - Published in IEEE Transaction on Engineering Management. This paper uses the methodology Digital Signature Algorithm. In this context, we propose a blockchain-based scheme to authenticate cheques and detect fake cheque scams. Our approach allows for the revocation of used cheques. The signature provides authenticity and ensures that the signature is verified and it requires a lot of time to authenticate the verification process.

Emart 77, Beirut, Lebanon, 2021, "The Role of Blockchain in Reducing the cost of financial transactions in the Retail industry" [2]- published in WCNC. This paper uses the methodology of consumer-packaged goods. The aim was to assess the role of blockchain in reducing the cost of financial transactions in the retail industry. Consumer packaged goods-and to some extent, services is arguably one of the most challenging industries to be successful in and is being a consumer limited resource that they are forced to accept.

Dilip Kumar Sharma, Sonal Garg, Priya Shrivastava, 2021, "Evaluation of tools and extension for fake news detection" [3]- published in IEEE International Conference on Innovation Practice in Technology Management (ICIPTM). This paper uses the methodology Bi-LSTM classifier. It is a sequence prediction model. It is a discriminative classifier model decision boundary between different classes and since Bi-LSTM has double LSTM cells so it is costly. It's not good for speech recognition.

Vikash Kumar Aggarwal, Nikhil Sharma, Ila Kaushik, Bharat Bhushan, Himanshu,2020, "Integration of blockchain and IoT(B-IoT): Architecture, solution, & Future Research Direction" [4] - published in 1st International Conference on computational Research and Data Analytics (ICCRDA). The methodology used is the Integration of Blockchain and IoT. This paper presents an introductory part of IoT enabled with blockchain, their key features, architecture layout, characteristic features of both the technologies, their futuristic solutions for different real-world problems, and different communicational models.

Jackie Jones, Damon McCoy, 2020, "The Cheque is in the mail: Monetization of Craigslist Buyer Scams" [5] - published in IEEE APWG Symposium. The methodology is a conservation classification strategy. This paper extends on previous works about fake payment scams targeting Craigslist. Compared to manual data entry automatic data entry greatly reduced error.

Abiola, Idowu, 2019, "An Assessment of Fraud and its Management in Nigeria Commercial Banks" [6]- published in IEEE paper European Journal of Social Science. The methodology used the is Pearson Product Moment Correlation Coefficient. The aim is to find practical means of minimizing the incidence of fraud in Nigerian banks. During this course of the investigation, efforts were made to identify various means employed in defrauding banks and at the same time determine the effects of the fraud on the banking services.

Sumeet Kumar,2018, "Simulating DDOS attacks on our us fibre-optics internet infrastructure" [7]

- published in the Proceedings of the 2017 Winter Simulation Conference. The methodology used is Cyber-attacks. In this research paper, we have designed a test-bed that mirrors the Internet infrastructure of the US and can simulate the internet traffic flow patterns for different attack targets. It is also used to estimate the degradation in the quality of service and the number of users impacted in two attack scenarios. A network simulation model is used to understand the internet business inflow pattern in a DDOS attack situation. Alerting data through remote access or damaging the system causes data loss.

Nazil Ismail Nawang,2017, “Combination anonymous offenders in the cyberspace: An overview of the legal approach in Malaysia” [8] - Published in the conference. These features are most common among internet users as they are empowered to publish online content anonymously or in the alternative to conceal their true identities behind fictitious names. It identifies the anonymous offender in the cyber world and the user must know the various laws that have been enacted to govern the publication of illegal content.

Haris Semic, Sasa Mrdovic, 2017, “IoT honeypot: A multi-component solution for handling manual and Mirai-based attacks” [9] - published in IEEE 25th Telecommunication forum TELFOR 2017. The methodology used in internet-of-things (IoT) devices. The honeypot operates with homemade and Mirai-grounded attacks. It is used to attain sufficient exposure to malicious traffic and security of collected data and the plank of security has left IoT devices vulnerable to various attacks that aim to take control of said bias and use them for various malicious purposes.

Bernie, S.Fabito, Angelique D.Lacasandile, Emeliza R.Yabut, 2017, “Leveraging crime reporting in Metro Manila using unsupervised crowd-sourced data: A case for the Report framework” [10] - published in International conference on control, electronics, renewable energy, and communication. This paper uses the methodology Ping ER Monitoring Agent. The aim is to provide a venue for victims of crimes to report their experiences without having to go directly to police stations. Those who have experienced the same offense in this area can link their reports with those previously reported offenses which refer to the same case. In this existing ping ER scripts which generate hourly, monthly and yearly reports can work seamlessly. This is because, in this framework, contents are addressed through hashes which is a widely used means of connecting data in a distributed network and the demerit is the downside of using an always-free tool is that it may be missing crucial features that you need, and with always-free tools, what you get is what you get.

Wendy Baker-Smemoe, Chair David Eddington Willian G.Eggington, 2015, “The language and Cross-culture Perceptions of Deception” [11] - published in Brigham young university. The methodology used is the Qualtrics survey block.

Research has shown that some verbal features can indicate a person is lying, this line of exploration has led to clashing results. very little exploration has been done to verify that these supposed linguistic features of deception are universal. Rather than creating two surveys, you could create two blocks of questions within one survey and randomly assign participants to one block or the other and the demerit is Qualtrics support could use some work. It can be difficult to help in the community.

III. EXISTING SYSTEM

A fake cheque scam has more disastrous consequences on the victims than many other attacks. In this context, we believe that the best solution to protect users is the detection of fake cheques well before they are cashed. The technique used is the Digital Signature Algorithm. It requires a lot of time for authentication. Verification of a given take a duration of greater than 48h.

IV. PROPOSED METHODOLOGY

To verify the authenticity of a given cheque, without exposing the bank's customer's personal data. To evaluate the performance of our proposed approach, we also deployed our cheque's authentication scheme based on the blockchain. The technique used is the SHA algorithm and AES algorithm. It requires less time for computation. Data transaction is the extra cozy manner to clients and charity through the bank. Bank asked the validated consumer and the client to give permission for the financial institution may be send the cash in charity.

V. PROJECT MODULES

There are five modules to this project. These modules explain how the actual process of detecting and preventing the fake cheque scam is carried out.

LOGIN

This is the first module in our project, here symbolizes a unit of work performed within a database management system (or similar system) against a database, and treated in a coherent and reliable way independent of other transactions. A transaction generally represents any change in the database user will transfer the amount to provider.

REQUEST

This module is used to help the user request for donation with the land longitude and user will update the report along with their opinion and they will be stored to the database.

DONATION

This module is used to help to the public to donate the amount with the land longitude and the public will update the report along with their opinion which will be stored the database.

RESPONSE

In this module, the bank will respond the data file fully analyzed data category-wise view bank will be responsible for your file stored in a database.

DONATION VIEW

In this module, the charity will view the donation and analyses the details stored for the file in the database.

VI. SYSTEM ARCHITECTURE

The system architect establishes the basic structure of the system, we can put a small part of data in the local machine and for the server in order to protect privacy. Also, based on computational intelligence, this algorithm can compute the distribution proportion stored in the cloud, fog, and local machine respectively. Through the theoretical safety analysis and experimental evaluation, the feasibility of our scheme has been validated, which is really a powerful supplement to the existing cloud storage scheme.

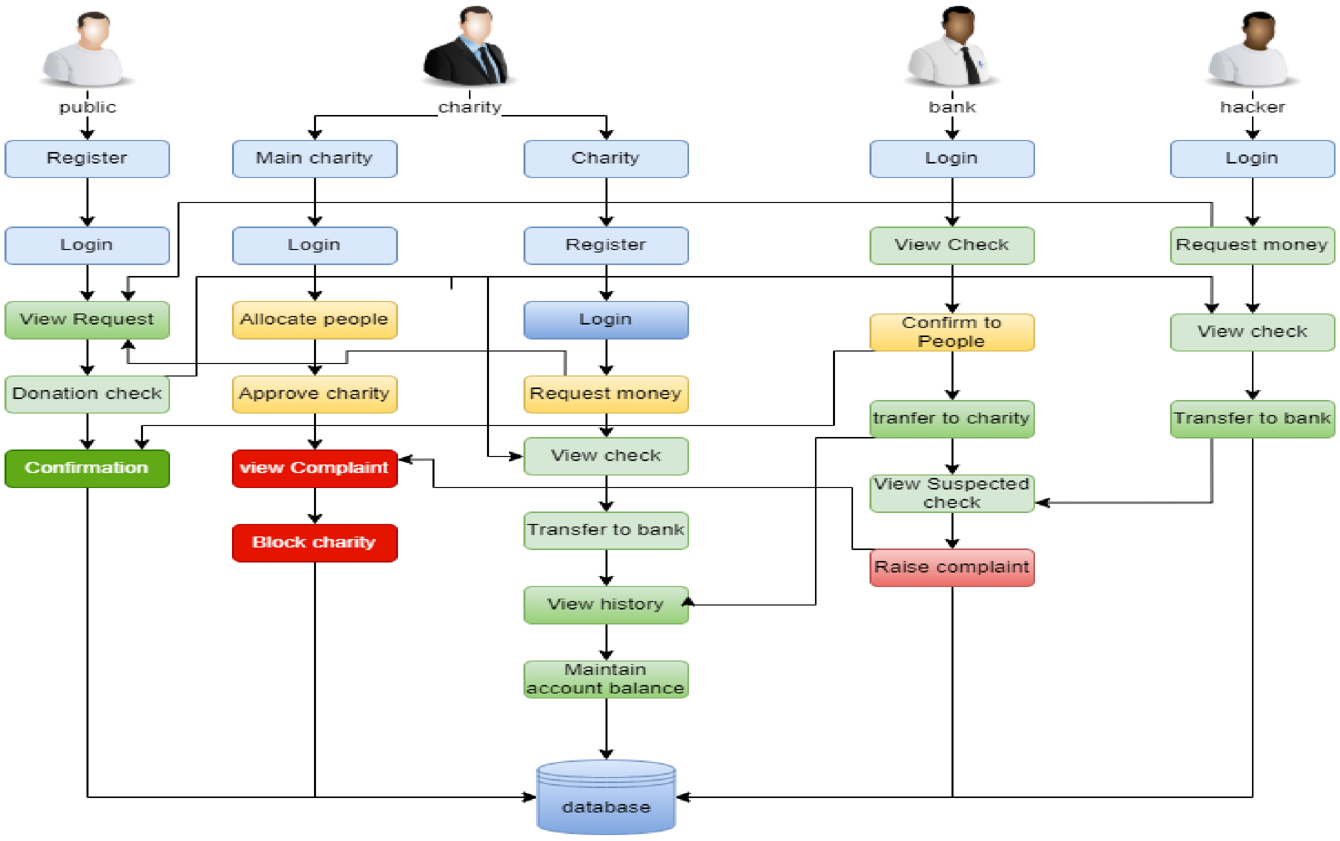


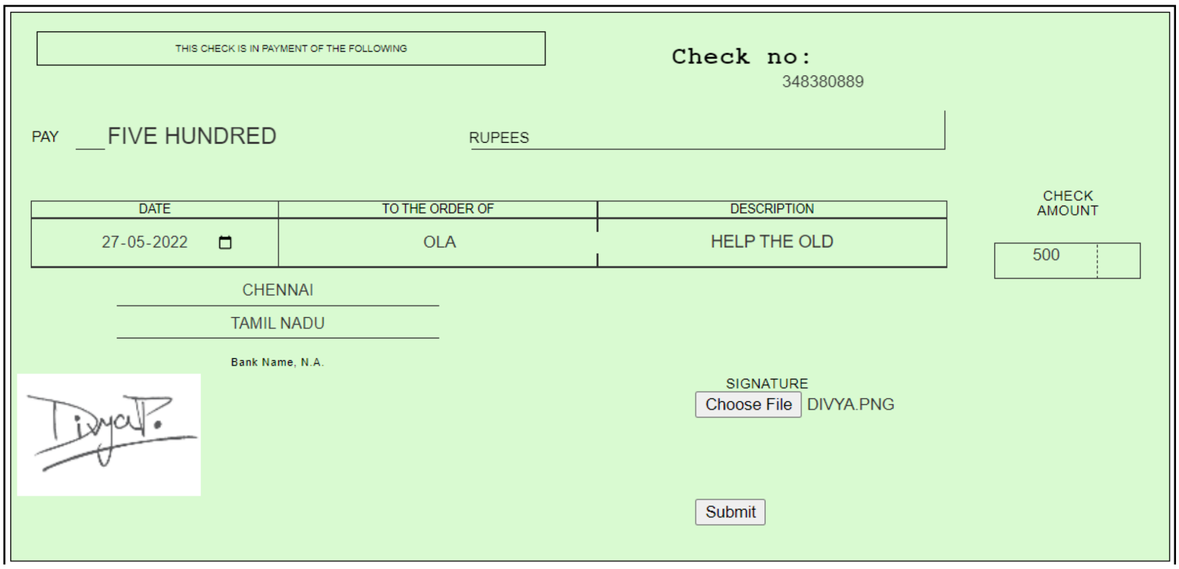
FIG 1 SYSTEM ARCHITECTURE DIAGRAM

VII. RESULT

The final step of the proposed system is to detect whether the cheque is fake or not. If the cheque is fake then the cheque number will be Encrypted. It can take for the bank to figure out that the cheque is fake. Use the information to recognize and them from this kind of action. The final output is verified by detecting the cheque is fake by the encryption process.

VIII. FUTURE ENHANCEMENTS

- Implementing the real-world database system.
- Improving the efficiency of protocols, in terms of the number of messages exchanged and in terms of their sizes, as well.
- Implement using two or more algorithms.



THIS CHECK IS IN PAYMENT OF THE FOLLOWING

Check no:
348380889

PAY FIVE HUNDRED RUPEES

DATE	TO THE ORDER OF	DESCRIPTION
27-05-2022	OLA	HELP THE OLD

CHECK AMOUNT 500

CHENNAI

TAMIL NADU

Bank Name, N.A.

SIGNATURE DIVYA.PNG

FIG 2. E-CHEQUE

IX. CONCLUSION

Banking scams involve attempts to access your account. Use the information to report, recognize and protect yourself from them. These scams work because of fake cheques that generally look just like real cheques, even to bank employees. They are frequently published with the names and addresses of legitimate financial institutions. They may even be actual cheques written on bank accounts that belong to identity theft victims. It can take for the bank to figure out that the cheque is fake.

X. REFERENCES

[1] Badis Hammi, Sherali Zeadally, Yves Christian Elloh Adja, Manlio Del Giudice, and Jamel Nebhen,

2021, “Blockchain-Based Solution for Detecting and preventing Fake Check Scams”.

[2] Emart 77, Beirut, Lebanon, 2021, “The Role of Blockchain in Reducing the Cost of Financial Transactions in the Retail Industry”.

[3] Dilip Kumar Sharma, Sonal Garg, Priya Shrivastava, 2021, “Evaluation of Tools and Extension for Fake News Detection”.

[4] Vikash Kumar Aggarwal, Nikhil Sharma, Ila Kaushik, Bharat Bhushan, Himanshu, 2020, “Integration of Blockchain and IoT (B-IoT): Architecture, Solution,& Future Research Direction”.

[5] Jackie Jones, Damon McCoy, 2020, “The Check is in the Mail: Monetization of Craigslist Buyer Scams”.

[6] Abiola, Idowu, 2019, “ An Assessment of Fraud and its Management in Nigeria Commercial Banks”.

[7] Sumeet Kumar, 2018, “ Simulating DDOS attacks on our us fiber-optics internet infrastructure”.

[8] Nazli Ismail Nawang, 2017, “Combating anonymous offenders in the cyberspace: An overview of the legal approach in Malaysia”.

[9] Haris Semic, Sasa Mrdovic, 2017, “IoT honeypot: A multi-component solution for handling manual and Mirai-based attacks”.

[10] Bernie S.Fabito, Angelique D.Lacasandile, Emeliza R.Yabut, 2017, “Leveraging crime reporting in Metro Manila using unsupervised crowd-sourced data: A case for the Report framework”.

[11] Wendy Baker-Smemoe, Chair David Eddington William G. Eggington, 2015, “The Language and Cross-Culture Perceptions of Deception”.

[12] S.Baker, 2018, “Don’t cash that cheque: BBB study shows how fake cheque scams bait consumers”, Tech Rep, Better Bus Bureau, Arlington Country, VA, USA.

[13] L. M. Rose, 2018, “Modernizing cheque fraud detection with machine learning”, PhD.D. dissertation, Dept. Financial Crime Compliance Manager, Utica College, Utica, NY, USA.

[14] Federal Trade Commission, 2018, “Consumer Sentinel network data book 2017”, Federal Trade Commission, Washington, DC, USA, Tech. Rep.

[15] C. Tressler, 2020, “ FTC: The bottom-line on fake cheque scams”, Federal Trade Commission, Washington, DC, USA, Tech. Rep.

[16] “2017 Internet crime report, “Federal Bureau of Investigation/Internet Crime Complaint Center, Washington, DC, USA, Tech. Rep,2018.

[17] K. Pak and D. Shadel, 2011, “AARP Foundation national fraud victim study”, AARP Foundation, Washington, DC, USA, Tech.Rep.

[18] C.-D. Chen and L.-T.Huang, 2011, “Online deception investigation: Content analysis and cross-culture comparison”, Int. J. Bus. Inf., vol. 6, no.1, pp.91-111.

[19] K. Christidis and M . Devetsikiotis, 2016, “Blockchains and smart contracts for the Internet of things”, IEEE Access, vol.4, pp.2292-2303.

[20] A.Reyna, C.Martin, J. Chen, E. Soler, and M. Diaz, 2018 “On blockchain and its integration with

IoT: Challenges and opportunities", Future Gener. Comput. Syst., vol.88, pp.173-190.

[21] M.T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, 2018, "Bubbles of trust: Adecentralized blockchain-based authentication system for IoT", Comput. Secure., vol. 78, pp. 126 - 142.

[22] R. M.Factora, 2014, "Financial and legal methods to protect individuals from financial exploitation in Aging and Money", Newyork, NY, USA: Springer, pp .109 - 122.

[23] C. W. Smith, 2001, "Defence to a payor bank's liability for kate returns", CCH Deposit Law Notes, vol. 2, no.6, p. 8.

[24] A. T. Riggs and P. M.Podrazik, 2014, "Financial exploitation of the elderly: Review of the epidemic - Its victims, national impact and legislative solutions", in Aging and Money. New York, NY, USA: Springer, 2014, pp.1 – 18.

[25] J. Jones and D. McCoy, 2014, "The cheque are in the mail: Monetization of Craigslist buyer scams", in Proc. APWGSymp. Electron. Crime Res., 2014, pp. 25 – 35.

[26] I.Abiola, 2009, "An assessment of fraud and its management in Nigeria commercial banks", Eur. J. Social Sci., vol.10, no.4, pp.628 – 640.

[27] J. A. Ojo, 2008, "Effects of bank frauds on banking operations in Nigeria", Int. J. Investment Finance, vol. 1, no. 1, p, 103.

[28]S. Chhabra, G. Gupta, M. Gupta, and G.Gupta, 2017, "Detecting fraudulent bank Cheques", in Proc. IFIP Int. Conf. Digit. Forensics, pp.245 – 266.

[29] R. Kumar and G. Gupta, 2016, " Forensic authentication of bank cheques", in Proc. IFIP Int. Conf. Digit. Forensics, pp. 311 – 322.