IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Impact Factor: 6.252

Volume 2, Issue 3, May 2022

Prevention Based On Blockchain

Subbulakshmi B[1], Nikila E[2], Vimal Raj S[3], Rajasekaran T[4]

Students, Department of Computer Science and Engineering[1,2,3]
Assistant Professor, Department of Computer Science and Engineering[4]
SRM Valliammai Engineering College, Chengalpattu, India

Abstract: *Introduced new paradigms and is increasingly contributing to the enhancement of banking quarter products. The purpose of this article is to examine a few of the most important and well-known enabled banking zone offers, as well as their current benefits and challenges. The fake cheque scam is one of the most prevalent methods of defrauding people. There is currently no method for rapidly authenticating cheque and detecting bogus ones. Instead, banks must wait for a longer length of time to uncover the fraud. More specifically, our solution enables banks to communicate information about provided and used cheque while protecting the personal information of bank clients. Fake cheque can take many different shapes. They could appear to be commercial or personal cheque.*

Keywords: Authentication, Blockchain, Fake cheque

I. Introduction

Cheque are one of the most common payment methods in today's culture. A check is an order written by a depositor instructing the bank to pay a certain sum from the depositor's bank account to a designated recipient. Unfortunately, many nasty scammers take advantage of banking system weaknesses to conduct fraud. Frauds using forged cheque are on the rise, costing billions of dollars. We concentrate on cheque fraud. This fraud is carried out by first obtaining people through an email scam, then creating a business relationship with them, usually by giving them an overpaid counterfeit pay cheque, and lastly demanding the over payment. Due of the issue of internet fraud, many charities and financial institutions have begun to notify consumers when potentially fraudulent transactions occur.

II. Literature Review

Using unsupervised crowd-sourced data to improve crime reporting in Metro Manila: A case for the iReport framework. [1]Emeliza R. Yabut, Bernie S. Fabito, Angelique D. Lacasandile. Crimes are activities that cause harm to a person or a group of people. It disturbs the peace, instils fear, and obstructs many people's daily routines. Unfortunately, data show that a considerable number of crimes in the Philippines are not reported to the appropriate authorities. If adequate action is not taken, this threat will continue to exist and terrorise the community. This project proposes the creation of a mobile application that uses unsupervised crowdsourcing data to collect indexed crime reports in Metro Manila. Its goal is to create a safe space for crime victims to share their stories.

[2] Summet Kumar, Kathleen M Carley.Liberia's Internet access was attempted to be brought down by a DDoS attack. The attacks reportedly devoured over 500 Gbps of bandwidth on the Africa Coast to Europe (ACE) fibre lines, which connect Europe and Africa to the Internet. The event demonstrates the Internet infrastructure's vulnerability. We need a simulation testbed that can mimic the Internet's complexity while also allowing us to quickly test attacks and get insight into real-world attack situations. Using a simulation, we attempt to identify such vulnerable points in this study. Our original work on 'Simulating DDoS Attacks on the US Fiber-Optics Internet Infrastructure,' which was accepted as a full paper at the Winter Simulation Conference, is summarised in this paper. This paper presents a honeypot solution for detecting and reporting telnet attacks on Internet of Things (IoT) devices. Manual and Mirai-based attacks are used to operate the honeypot. In order to achieve sufficient exposure to hostile traffic and data security, a multi-component design is used. The honeypot's configuration and extra files are described. Mirai is used to test Honeypot, and the results are discussed. The conclusion and directions for further work are then provided.

DOI: 10.48175/568

III. PROPOSED SYSTEM

The block diagram for the proposed system is shown in Fig 1. To authenticate the authenticity of a cheque without disclosing the personal information of the banks' customers. We used our check's authentication system based on the blockchain to test the performance of our suggested solution. It requires less computation time. Clients and charities benefit from more convenient data transactions. When a bank asks a validated customer for permission, the financial institution may send money to charity.

Before paying a cheque, each bank (Cashing-Bank) must verify that the cheque came from a reputable source (another bank). This can be done if each bank communicates information about the cheque it has issued. In other words, when a bank gives a customer a chequebook, it discloses information on the customer as well as the checks. However, no bank will share such information with other banks, owing to the following factors: (1) User privacy: because the users have dealt with this bank rather than another.

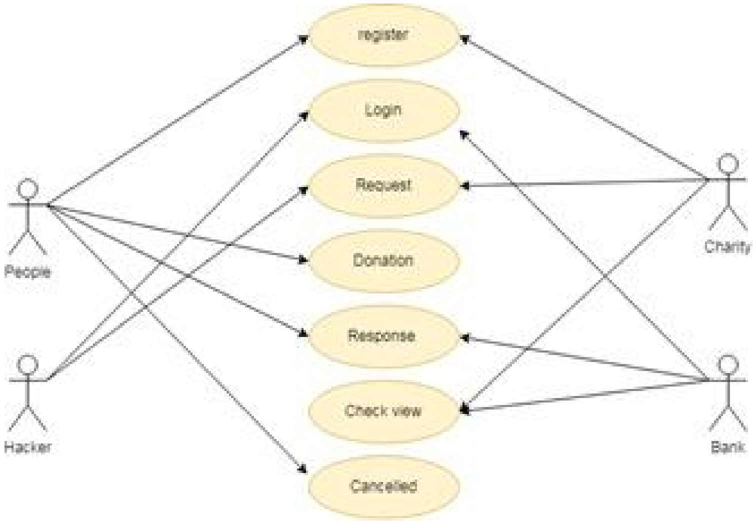


Figure 1: Use case diagram of proposed system

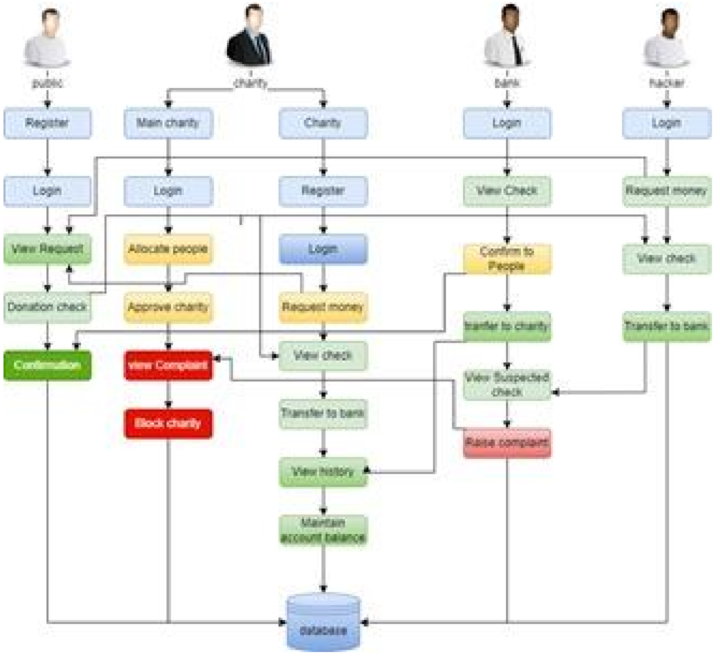


Figure 2: Block diagram for proposed system

DOI: 10.48175/568

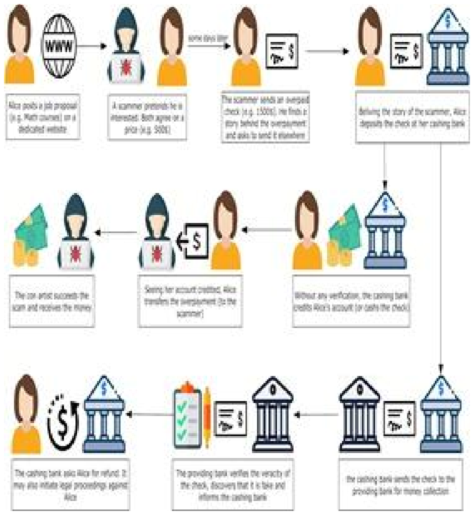

WWW
Alice posts a job proposal (e.g. Math courses) on a dedicated website
A scammer pretends he is interested. Both agree on a price (e.g. 500$)
some days later
The scammer sends an overpaid check (e.g. 1500$). He finds a story behind the overpayment and asks to send it elsewhere
Believing the story of the scammer, Alice deposits the check at her cashing bank
Without any verification, the cashing bank credits Alice's account (or cashs the check)
Seeing her account credited, Alice transfers the overpayment (to the scammer)
The con artist succeeds the scam and receives the money
the cashing bank sends the check to the providing bank for money collection
The providing bank verifies the veracity of the check, discovers that it is fake and informs the cashing bank
The cashing bank asks Alice for refund. It may also initiate legal proceedings against Alice

Figure 3: System Architecture of cheque Scam

Figure 1: The Display unit of the proposed system

IV. Methodology

When a deposited check is cashed, it must be marked as "no longer valid" because it has been utilised. In the same vein, if a bank wants to revoke a check or a chequebook for whatever reason, such as check theft, the associated check must be marked as "no longer valid" because it has been revoked.

The use of checks for payment is fully random, in contrast to chequebook logic, where all checks have consecutive numbers and are supplied at the same time. Some clients will use their checks on a regular basis, while others will go through a chequebook over months or years. As a result, it is necessary to keep track of each used check separately in order to avoid it being lost.

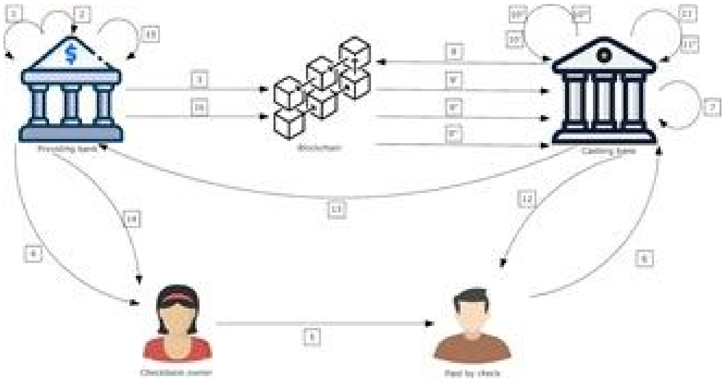


Figure 2: The Mechanism of the Bank Transfer

DOI: 10.48175/568

V. HASH FIELD

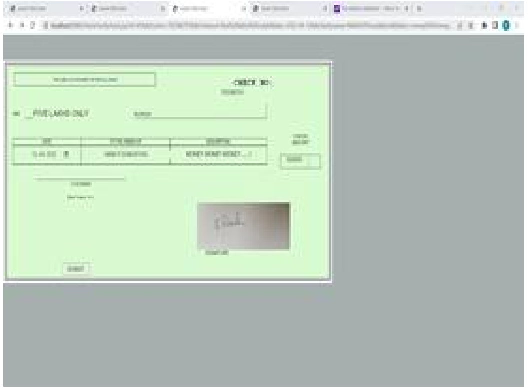
The hash field contains a hash computed on the following fields

- **Lagrange polynomial:** the computed polynomial.
- **Full Name:** the customer's full name.
- **Providing-Bank:** the bank that provided the check book.
- **Account number: the customer's account number.**

Table 1: Hash Field of Software

FIELD	SIZE(BYTES)
Hash(Check number||Full name||Providing-Bank||Account number)	32
Signature(Check number||Full Address||Providing-Bank||Routing number||Account number)	64

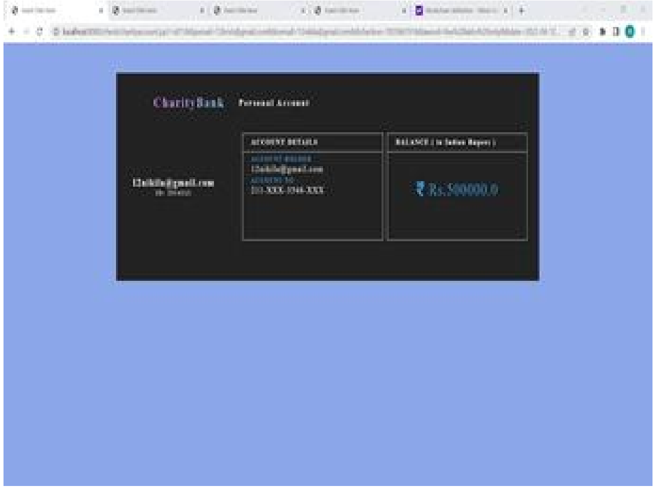
VI. RESULTS AND DISCUSSION



CHECK NO:

FIVE LAKHS ONLY

Figure 3: Output of proposed system



CharityBank Personal Account

12nikhilu@gmail.com

ACCOUNT DETAILS	BALANCE (in Indian Rupee)
ACCOUNT HOLDER 12nikhilu@gmail.com ACCOUNT NO 211-XXX-3546-XXX	₹ Rs.500000.0

Figure 4: Output of the system

VII. CONCLUSION

Scammers attempt to gain access to your bank account. Use this knowledge to spot them, report them, and defend yourself. These schemes operate because fraudulent checks, even to bank staff, resemble real checks. The names and addresses of reputable financial institutions are frequently printed on them. They could even be legitimate checks written on identity theft victims' bank accounts. It can take a long time for a bank to realise the check is a forgery.

ACKNOWLEDGMENT

We thank the anonymous reviewers for their valuable comments which helped us improve the content, organization, and presentation of this paper.

REFERENCES

[1]. Steven Baker. Don't Cash That Check: BBB Study Shows How Fake Check Scams Bait Consumers. Technical report, Better Business Bureau (BBB), September, 2020.

[2]. Lydia M Rose. Modernizing Check Fraud Detection with Machine Learning. PhD thesis, Utica College, 2021.

[3]. Federal Trade Commission. Consumer sentinel network data book 2017. Technical report..

[4]. Colleen Tressler. FTC: The bottom-line on fake checks scams. Technical report, Federal Trade Commission (FTC), February 10, 2020.

[5]. Federal Bureau of Investigation/Internet Crime Complaint Center. internet crime report. Technical report.

[6]. Karla Pak and Doug Shadel. Aarp foundation national fraud victim study. Washinton, DC.

[7]. Chun-Der Chen and Li-Ting Huang. Online deception investigation: Content analysis and cross-cultural comparison. International Journal of Business and Information.

[8]. Konstantinos Christidis and Michael Devetsikiotis. Blockchains and smart contracts for the internet of things. IEEE Access, 4:2292–2303,

[9]. Ana Reyna, Cristian Martín, Jaime Chen, Enrique Soler, and Manuel Díaz. On blockchain and its integration with iot. challenges and opportunities. Future Generation Computer.

[10]. Mohamed Tahar Hammi, Badis Hammi, Patrick Bellot, and Ahmed Serhrouchni. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. Computers & Security, 78:126–142, 2018.

[11]. Ronan M Factora. Financial and legal methods to protect individuals from financial exploitation. In Aging and Money, pages 109–122. Springer.

[12]. Craig W. Smith. Defense to a payor bank's liability for late returns CCH Deposit Law Notes,2(6):8, 2021.

[13]. Ann T Riggs and Paula M Podrazik. Financial exploitation of the elderly: review of the epidemic—its victims, national impact, and [13]legislative solutions. In Aging and Money, pages 1–18. Springer.

[14]. Jackie Jones and Damon McCoy. The check is in the mail: Monetization of craigslist buyer scams. In APWG Symposium on Electronic Crime Research (eCrime), pages 25–35.

[15]. Idowu Abiola. An assessment of fraud and its management in nigeria commercial banks. European journal of social sciences, 10(4):628–640.

[16]. JA Ojo. Effect of bank frauds on banking operations in nigeria.

[17]. International Journal of Investment and Finance, 1(1):103.

[18]. Saheb Chhabra, Garima Gupta, Monika Gupta, and Gaurav Gupta. Detecting fraudulent bank checks. In IFIP International Conference on Digital Forensics, pages 245–266. Springer.

[19]. Rajesh Kumar and Gaurav Gupta. Forensic authentication of bank checks. In IFIP International Conference on Digital Forensics, pages 311–322. Springer, 2020.

[20]. Romanoff E Smagala. Coded checks and in methods of coding. US Patent 3,829,133.

DOI: 10.48175/568