International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 06 | June - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Fake Check Scam Detection and Prevention using Blockchain based SHA-Algorithm

Mr. G. Rajasekaran[1], Abbas Hasan[2], Joshi P[3], Pushpa Tiwari[4]

[1]*Associate Professor, Dept of CSE, Dhaanish Ahmed College of Engineering, Chennai.*

[2,3,4]*Final year student, Dept of CSE, Dhaanish Ahmed College of Engineering, Chennai.*

---*****---

ABSTRACT - Counterfeit check stunt is maybe the most striking attack used to submit threatening against customers. Presently, there is no current answer for affirm checks and see counterfeit ones immediately. Considering everything, banks should hold it together so that a time of additional time and date might be able to see the trick. Fundamentally more unequivocally, our framework helps the keeps cash with sharing data about gave checks and utilized ones, without revealing the banks' clients' own exceptional information. Counterfeit truly breaks down come in many plans. They may seem like business or individual checks, right hand's checks, cash orders, or a check passed on electronically. These tricks work since counterfeit checks for the most part look an immense heap of like authentic checks, even to bank prepared experts. They are reliably printed with the names and addresses of solid cash related foundations. Banks are remaining mindful of thriving relationship for cash exchange to client security reason obviously check with client and requires their consent. It what's more sensible real trust their have Register login and embraced by rule branch and extraordinary objective required boat off client and expecting client need to help surprising with causing they can help by give check to fabulous objective which passed to bank and amount to is exchange to exceptional practical and the bits of information concerning fair obvious inside and out exchange will pass on off supervisor branch and remained mindful of by fundamental branch. Expecting reaction got from concern client just, exchange will be occurred.

Key words : **Block chain based check stunt, Fake really take a gander at stunt, securable remuneration cash**

I. INTRODUCTION

Information isolating between banks going preceding paying a check, each bank (Cashing-Bank) ought to guarantee that the check was truly given by a confided in ace in customer. This testament would be conceivable expecting bank share data about its gave checks. Considering everything, when a bank gives a checkbook to a client, it shares the data about the client and about the gave checks. Bank will share such data, fundamentally for client security since the clients have drawn in with this bank and not with another and for business question: persevering through that clients' data are open, nothing gets any bank a long way from reaching these individuals and offering them its affiliations.

II. EXISTING SYSTEM:

Thought:

Counterfeit check stunt has more horrendous outcomes on the misfortunes than different assaults. In this specific situation, we accept that the most fitting reaction for secure clients is the disclosure of fake checks quite a while before they are exchanged.

Technique: Progressed Signature Algorithm.

Damage: It requires bundle of time for computation.

III. PROPOSED SYSTEM:

Thought:

To authenticate the realness of a given check, without uncovering the banks' customers' own special data. To evaluate the introduction of our proposed approach, we in like manner gave our check's attestation plot subject to the square chain.

Technique: SHA Algorithm, AES Algorithm

Advantage: It requires less time than Digital Signature estimation.

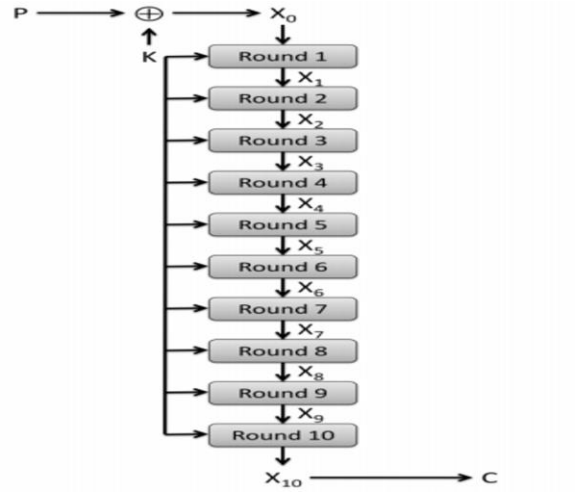
IV. SYSTEM IMPLEMENTATION

ALGORITHM USED:

The AES appraisal (in any case called the Rijndael estimation) is an even square code computation that takes plain text in squares of 128 pieces and converts them to encode text using keys of 128, 192, and 256 pieces. Since the AES appraisal is seen as secure, it is in the general standard.

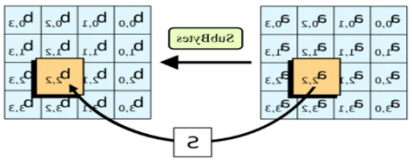
How does AES function?

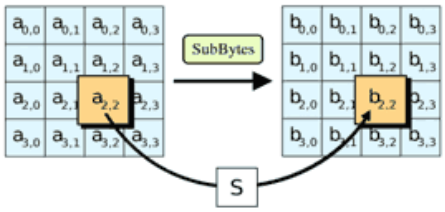
The AES appraisal uses a substitution stage, or SP relationship, with various rounds to pass on figure text. How much changes depends on the key size being used. A 128-digit key size works with ten changes, a 192-piece key size orchestrates 12 rounds, and a 256-cycle key size has 14 rounds. These rounds requires a round key, but since only one key is inputted into the evaluation, this essential ought to be associated with get keys for each round, including cycle 0.



Substitution of the bytes

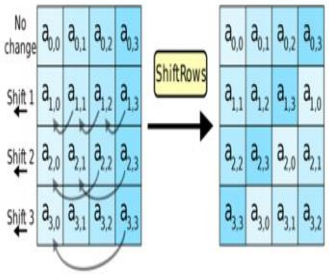
In the basic turn of events, the bytes of the square text are subbed reliant upon rules worked with by predefined S-boxes (short or substitution boxes).

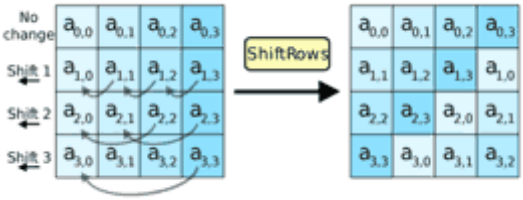




2. Shifting the rows

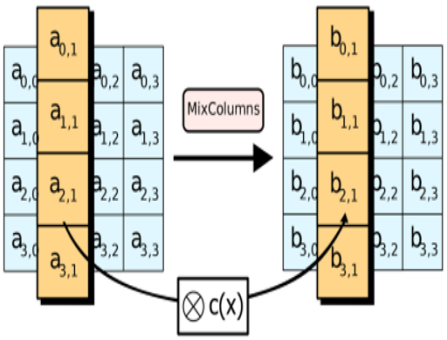
Next comes the change step. In this development, all lines with the exception of the first are moved by one, as displayed under.

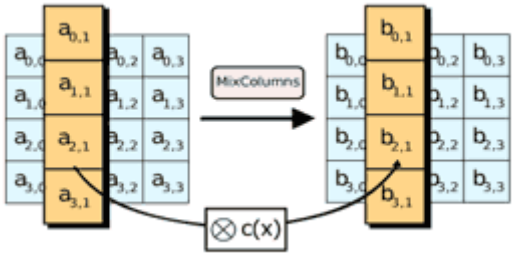




3. Mixing the columns

In the third step, the Hill figure is utilized to scramble up the message more by blending the square's regions.

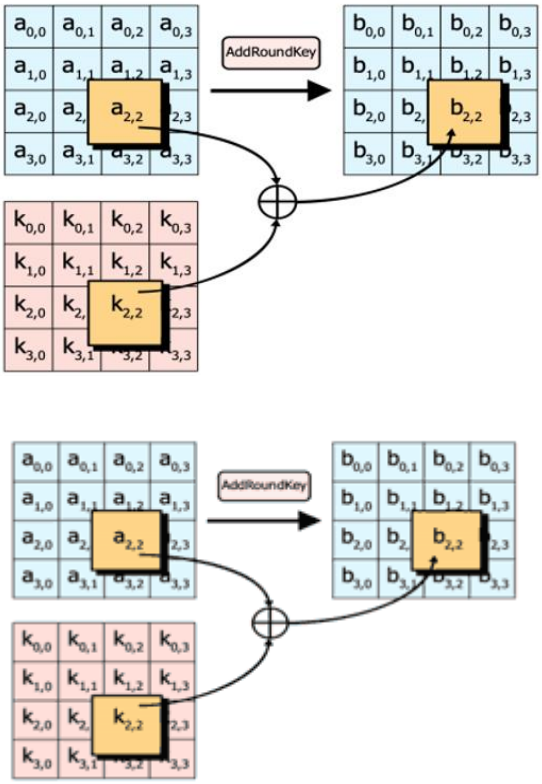




4. Adding the round key : In the last turn of events, the message is XO Red with

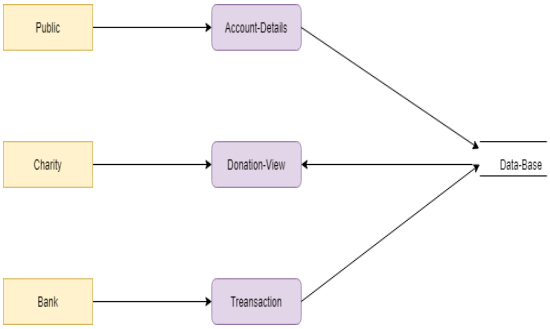
At the point when done endlessly, these strategies guarantee that the last code text is secure.the person round

key.



DATAFLOW DIAGRAM

A data stream diagram (DFD) is a graphical depiction of the "stream" of data through an information structure. It changes from the flowchart as it shows the data stream rather than the control stream of the program. A data stream diagram can in like manner be used for the portrayal of data dealing with. The DFD is planned to show how a structure is disengaged into more unassuming portions and to include the movement of data between those parts.



SHA ALGORITHM

In the field of cryptography and crypt analytics, the SHA-1 algorithm is a crypt-formatted hash function that is used to take a smaller input and produces a string that is 160 bits, also known as 20-byte hash value long. The hash value therefore generated, is known as a message digest which is typically rendered and produced as a hexadecimal number which is specifically 40 digits long.

Characteristics

- The cryptographic hash functions are utilized and used to keep and store the secured form of data by providing three different kinds of characteristics such as pre-image resistance, which is also known as the first level of image resistance, the second level of pre-image resistance and collision resistance.
- The cornerstone lies in the fact that the pre-image crypt resistance technique makes it hard and more time consuming for the hacker or the attacker to find the original intended message by providing the respective hash value.
- The security, therefore, is provided by the nature of a one way that has a function that is mostly the key component of the SHA algorithm. The pre-image resistance is important to clear off brute force attacks from a set of huge and powerful machines.

- Similarly, the second resistance technique is applied where the attacker has to go through a hard time decoding the next error message even when the first level of the message has been decrypted. The last and most difficult to crack is the collision resistance, making it extremely hard for the attacker to find two completely different messages which hash to the same hash value.
- Therefore, the ratio to the number of inputs and the outputs should be similar in fashion to comply with the pigeonhole principle. The collision resistance implies that finding two different sets of inputs that hash to the same hash is extremely difficult and therefore marks its safety.

Uses of SHA Algorithm:

These SHA algorithms are widely used in security protocols and applications, including the ones such as TLS, PGP, SSL, IPsec, and S/MIME. These also find their place in all the majority of cryptanalytic techniques and coding standards which is mainly aimed to see the functioning and working of majorly all governmental as well as private organizations and institutions. Major giants today such as Google, Microsoft, or Mozilla have started to recommend the use of SHA-3 and stop the usage of the SHA-1 algorithm.

THE JAVA FRAMEWORK

Java is a programming language at first made by James Gosling at Sun Microsystems and passed on in 1995 as a point of convergence of Sun Microsystems' Java stage. The language translates a huge load of its sentence structure from C and C++ at any rate has a less risky article model and less low-level work environments. Java applications are usually joined to byte code that can run on any Java Virtual Machine (JVM) paying minimal admonition to PC organizing, "make once, run any spot". Java improvement's adaptability, adequacy, stage flexibility, and security gain it the ideal ground for network signing up. From PCs to data centres, game control neighbourhood genuine supercomputers, telephones to the Internet, Java is out of control!

Objectives of java

- To see spots of Java, considering everything, in our customary presence, research java.com.
- Java has been attempted, refined, extended, and showed by a real region. With its adaptability, comfort, and portability, Java has become vital for engineers by engaging them to:
- Make activities to run inside a Web program and Web affiliations
- Enable server-side applications for online gatherings, stores, studies, HTML structures making due, and that is only the start.

To be an Object-Oriented language, any language ought to follow basically the four ascribes.

1. Inheritance: It is the most by and large saw system for making the new classes and using the lead of the current classes by extending them just to reuse the current code and adding choice a component relying on the circumstance

2. Embodiment: It is the strategy for joining the information and giving the reflection.

3. Polymorphism: Polymorphism is the procedure for giving the unmistakable help by the cut-off focuses having an overall name subject to the signs of the approach.

4. Dynamic confining: It is the technique for giving the best steadiness to a program about the specific kind at runtime.

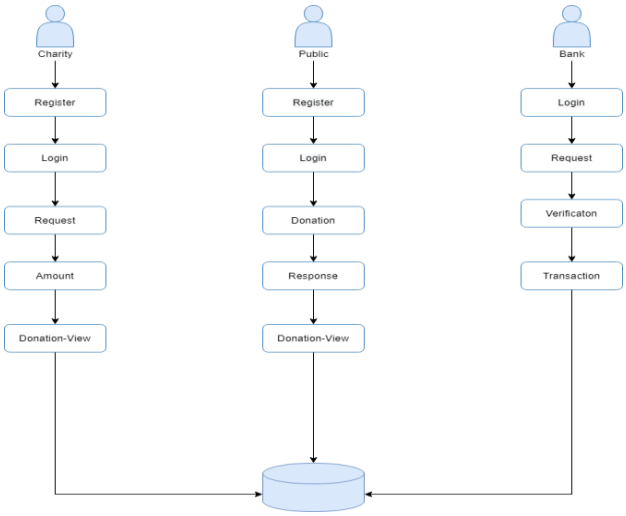


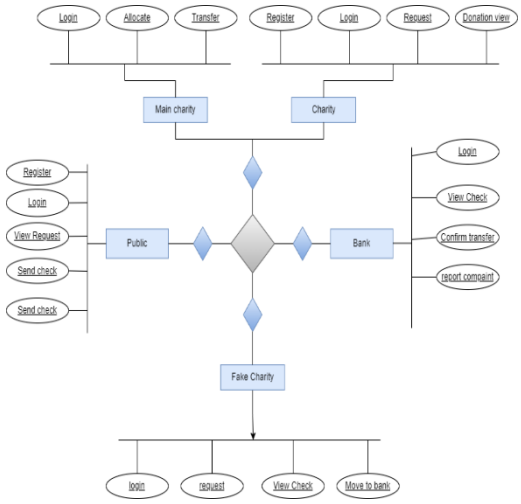
Fig. 1. System Architecture

V. MODULES

The system module is categorized into four sub-modules namely,

- ✓ Module 1: Charity Management
  - ➢ Charity Management Login
  - ➢ Charity Donation View
  - ➢ Bank Response View
  - ➢ View Charity Request
  - ➢ Response
- ✓ Module 2: Charity Operation
  - ➢ Charity Register
  - ➢ Charity Login
  - ➢ Charity Request
- ✓ Module 3: Public Donation
  - ➢ Public Register
  - ➢ Public Login
  - ➢ Charity Request View
- ✓ Module 4: Bank Money Operation
  - ➢ View Account Balance
  - ➢ Response (Bank)

VI. WORK FLOW



VII. CONCLUSION

Banking stunts harden attempts to get to your record. Utilize this data to see, report, and safeguard yourself from them. These tricks work since counterfeit really looks at by and large look a great deal of like authentic checks, even to bank prepared experts. They are reliably printed with the names and addresses of ensured cash related establishments. They might even be real checks got on cash related harmonies that have a spot with rebate pressure disasters. It can take for a bank to sort out that the check is a phony.

VIII. FUTURE ENHANCEMENT

1. Executing a genuine data base system.
2. Improving the capacity of shows, the degree that number of messages exchanged and to the degree their sizes, too.
3. Implement using two are more appraisals.

REFERENCES

[1] Badis Hammi, "Blockchain-Based Solution for Detecting and Preventing Fake Check Scams," Le Kremlin-Bicetre, France, UK, June, 2021.

[2] C. Tressler, "FTC: The bottom-line on fake checks scams," Federal Trade Commission, Washington, DC, USA, Tech. Rep., Feb. 2020.

[3] 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.

[4] L. M. Rose, "Modernizing check fraud detection with machine learning," Ph.D. dissertation, Dept. Financial

Crime Compliance Manage., Utica College, Utica, NY, USA, 2018.

[5] *Federal Trade Commission*, "Consumer sentinel network data book 2017," FederalTrade Commission,Washington, DC, USA,Tech. Rep., Mar. 2018.

[6] "2017 Internet crime report," Federal Bureau of Investigation/Internet Crime Complaint Center, Washington, DC, USA, Tech. Rep., 2018.

[7] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT: Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, 2018.

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

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

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

[11] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things, *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[12] A. T. Riggs and P. M. Podrazik, "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.

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

[14] R. M. Factora, "Financial and legal methods to protect individuals from financial exploitation," in *Aging and Money*. New York, NY, USA: Springer,

2014, pp. 109–122.

[15] K. Pak and D. Shadel, "AARP Foundation national fraud victim study," AARP Foundation, Washinton, DC, USA, Tech. Rep., 2011.

[16] C.-D. Chen and L.-T. Huang, "Online deception investigation: Content analysis and cross-cultural comparison," *Int. J. Bus. Inf.*, vol. 6, no. 1, pp. 91–111, 2011.

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

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

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