A Secured And Tamper Free Authentication And Verification Of Transactions Over The Network In Cash Logistics Industry

Lebbaeus Denis, Dr.T.Krishnakumar, Dr.M.Karthikeyan, Dr.S.Sasipriya

Abstract: Technology framework for secured and tamper free authentication mechanism of identity and verification of transactions over the network in cash logistics industry using IOT to avoid identity thefts and cash robberies during the storage, transportation, handling and dispensing of cash. This paper presents a comprehensive and a fundamentally new way to transact business. The whole process flow of the cash logistics with the security based authentication factors of and methods to control cyber security threats over the cash logistics network. Here in this paper I have utilized cryptographic security, decentralized agreement, and a mutual open record (with its appropriately controlled and permissioned perceive ability), Blockchain advancements which can significantly change the manner in which it sort out the monetary, social, political, and logical exercises.

Index Terms: Minimum 7 keywords are mandatory, Keywords should closely reflect the topic and should optimally characterize the paper. Use about four key words or phrases in alphabetical order, separated by commas.

1. INTRODUCTION

THE adoption of IoT-based advances opens up new open doors in different parts of our everyday lives, for example, home mechanization, smart transportation, and manufacturing. With the development of installed figuring equipment and system innovation, the coordination of these two advances makes enormous scale self-ruling IoT frameworks appear. Progressively reasonable arrangements should be proposed, and a few specialists began to present new ideal models by utilizing a decentralized innovation for the IoT gadget access control, that is Blockchain. From a calculated level, Blockchain is a sort of verified, dispersed database involved by various friends that can follow, confirm, and execute exchanges and store data from a huge assortment of substances.

2 EXISTING SYSTEM

Photo Identity

Physical security and data security, get to control is the specific confinement of access to a spot or other asset. The demonstration of getting to may mean expending, entering, or utilizing. Consent to get to an asset said to be approval is a system of business procedures, arrangements and advancements that encourages the administration.In this unique circumstance, get to is the capacity of an individual client to play out a particular errand in real money coordinations which is attained through the Photo list available with the concerned Client while permitting a Cash Collection Executive for performing Cash Pickup /Cash Delivery or if any. This Photo list will be sent by the agent handling the CE's with the concerned head signature via mail. So by this as evident and to confirm that the no fraud lent activity is done this photo list operation is utilized.

- *Lebbaeus Denis, Research Scholar, Bharath Institute of Higher Education and Research (BIHER), Chennai, India. Chief Technology Officer, Radiant Cash Management Services Pvt. Ltd. Email: lebbaeusdenis@gmail.com.*
- *Dr.T.KrishnaKumar,Professor, Department of Computer Science and Engineering, Bharath Institute of Higher Education and Research (BIHER), Chennai, Email: drkk@bharathuniv.ac.in*
- *Dr.M.Karthikeyan, Professor and Principal, Department of Computer Science and Engineering,Tamilnadu College Of Engineering, Coimbatore*
- *Dr.S.Sasipriya, Professor, Department of Computer Science and Engineering, Sri Krishna College of Engineering and Technology, Coimbatore. E-mail: sasipriyakarthi@yahoo.com*

Dynamic Photo Identity

In the realm of ID, there are heaps of choices. Furthermore, the arrangement that works best for individual organizations and associations is commonly founded on what their particular distinguishing proof needs are. Dynamic models of procedures are required for some associations in different viewpoints, running from control building to the regular sciences, coordination and financial aspects. Every now and again, such exact models can't be inferred utilizing hypothetical contemplations alone. Dynamic Photo Identity is System Barcode / QR based Auth which will send a control no like CIBIL. This unique control No assigned for dedicated CE transferred through QR / Barcode carries the necessary info regarding the Cash Executive in order to verify that the exact CE has come to provide service.

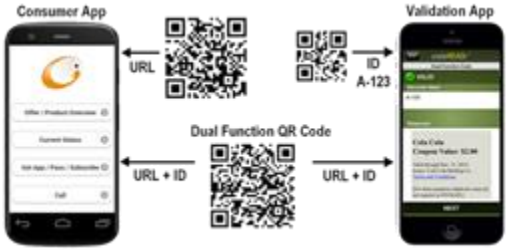

***Figure 1**: Identity*

Transactional operation

Blockchain innovation is an ongoing leap forward of secure registering without incorporated expert in an open arranged framework. From information the board viewpoint, a Blockchain is a circulated database, which logs an advancing rundown of exchange records by arranging them into a progressive chain of squares. From security point of view, the square chain is made and kept up utilizing a shared overlay organize and verified through smart and decentralized usage of cryptography with swarm registering. The QR Code confirmation instrument is a verification ability that allows an enlisted gadget to filter a QR Code to validate the client. It gives a totally option in contrast to-secret phrase technique for confirming a client. There are a few instances of well known applications which utilize this methodology. For instance, to

login into a web session with Whatsapp, you should sign in on your telephone and afterward examine a QR code in the web interface. The existing system based on QR code transaction is explained and the incorporation of Blockchain for tamper free and verification of transactions to overcome threats is explained.

3 PROPOSED SYSTEM

APPROACH 1: Bank Owned Utility App

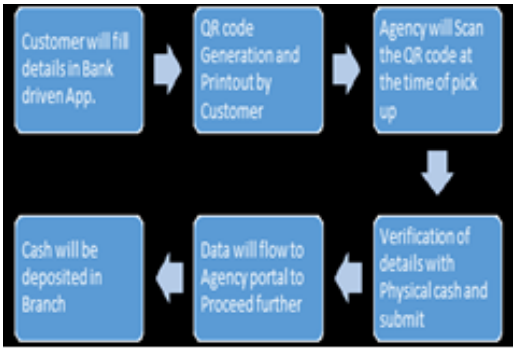

Figure 2: *Proposed Block Diagram*

WORKING PROCESS:

Initially customer will have the “BANK OWNED UTILITY APP” which is provided by the bank in which the details of the particular transaction will be updated by the customer itself. After updating all those details, the app will generate a QR code which will be taken as printed version by the customer and the same will be pushed to the Agency handheld device. At the time of pick up / Delivery, CE has to scan the QR code of the Pickup/ Delivery location in his mobile or handheld device. Once it is done, the data will be extracted from QR code and will be populated in the versatile application possessed by our CE. After getting the necessary particulars in our mobile app, CE will verify the details including physical cash and will update the “SEAL NUMBER, REMARKS BY CE and REASON” in the mobile app. Later those data will be available in the database and will be preceding it further and ends up in cash deposition. For Transactional correctness QR, Point ID, Multiple point codes, Transactions Entry submit, along with Lat & Long. Retail Point will get a QR in his mobile or Barcode in his system by web application these transactions will be displayed if it is correct click yes and this will generate a QR code to be scanned by CE , this unique no is the cash receipt no and No bills / invoice needs to be given for this pickup. The server upon auth confirmation will send an email with unique receipt no assigned with the transaction with client code wise pickup amount.

APPROACH 2: Point wise QR code and Barcode on deposit slip.

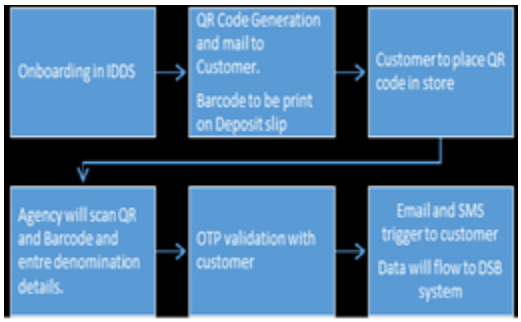

Figure 3: *Working Progress*

WORKING PROCESS:

Initially QR Code will be generated using Stop ID on the time of enrolling a customer by the client and the same has to be shared to the customer in the form of Email as PDF attachment. In the mean time, bank has to generate Barcode for each Deposition and same has to be printed in Deposit slip. After getting Email with QR code and necessary details, customer has to place the printed version of QR code in their store. At the time of pick up / Delivery, CE has to scan the QR code which will include “Stop ID, Customer Code, Hierarchy Code, Sub Customer Code, and Division Code “of the pickup / Delivery location in his Mobile or Handheld device. Once it is done, the data will be extracted from QR code and will be populated in the versatile application possessed by our CE. After getting the necessary particulars within the mobile app, CE will verify the details including physical cash and will update the “TOTAL AMOUNT, DENOMINATION DETAILS, SEAL NUMBER, REMARKS BY CE and REASON” in the mobile app. Later customer gets OTP where customer has to validate the details which are updated by CE in their mobile app and enter the OTP to finish the validation and transaction will be pushed to agency portal. At the end customer will get confirmation SMS and Email, data will flow to the DSB database and finally ends up in cash deposition. At the time of cash deposition CE has to scan the Barcode no of the Deposition slip (OTP Is optional). Bank, 0n enrolling a client and stop ID would generate QR code (Vendor mobile capture friendly) that would be shared in the form of email PDF attachment. QR code shall be generated at the time of new client induction or modification of existing client. The customer will be taking a printout and will make it available QR code at the pickup location. The Printout would contain the name of the client and effective data in normal readable form for identification. Tamper obstruction of Blockchain implies that any exchange data put away in the Blockchain can't be altered during and after the procedure of square age. There are two potential ways that the exchange data might be altered: (1) Miners may endeavor to mess with the data of got exchange; (2) Adversary may endeavor to mess with the data put away on the Blockchain. For the main sort of altering, an excavator may endeavor to change the payee address of the exchange to himself. Be that as it may, such endeavor can't be succeeded, since every exchange is compacted by a safe Hash work, for example, SHA-256, at that point marked by the payer utilizing a safe mark calculation, for example, ECDSA lastly, the exchange is sent to the whole system for confirmation and endorsement through mining. For the second sort of altering, an enemy will bomb its endeavors to change

any chronicled information put away on the Blockchain. This is a direct result of the two security systems utilized in the dispersed stockpiling of Blockchain, the hash pointer and Cryptographic method.

HCI NO HIDDEN CODE IDENTIFICATION:

A payment system manifests itself in a way that it less prone to thefts, misuse and robbery for renders, without HCI No is still discovered simple for the programmer to hack the exchange subtleties, HCI codes which keeps up security while playing out the exchanges, It is difficult to recognize the exchange subtleties, Unless these security highlights are looked upon. The concealed codes will be known to the customer and clients who execute, which keeps up the protection and security.

SEAL TAG NO:

Seals have been intended for explicit security applications like fixing of significant or classified reports, money dealing with or key administration. Seal tag or security packs are used in moving money or interior bank correspondence. Security envelopes, security names and tapes are likewise being used to maintain bank security in its day by day tasks. Especially for the uses of money/assets in-travel (CVIT), seal labels are assuming a fundamental job. Seal labels, in this manner taking care of issues to anticipate altering in different areas, for example, Post Offices, Customs, Airlines, Catering, Transport of resources, Banks, and each sort of transport.

4 WEB APPLICATION - FACTORS OF AUTHORIZATION

4.1 User Id & Password

Essential authentication is a HTTP standard confirmation technique intended to permit a Web program or another Web customer to give credentials - as a user ID and password - when making a solicitation to a server framework. Basic Authentication is upheld by most of Web customers and is the authentication mechanism that can be executed with the least additional effort. Basic - user give their user IDs and passwords by entering them in a browser spring up. The client credentials are shipped in the HTTP header as a base-64 encoded string. Digest - advanced form of basic authentication. For this verification system, the client credentials are hashed utilizing a message condensation and sent over the system in hashed position. Form - users utilize a pre-arranged Web page to enter their authentication credentials. The validation data is then moved to the server in the URL as URL parameters.

Security Considerations

The various techniques for Web-based access validation with a user ID and password empower to utilize a straight forward confirmation system that is generally upheld by Web programs. The HTTP techniques for validation with a user ID and password, be that as it may, give insignificant insurance to the confirmation accreditations during their transport and depend on the presumption that the association between the Web customer and the server can be trusted. Accordingly, for expanded security of the entrance to SAP Net Weaver frameworks, you need to utilize transport layer security components in mix with the HTTP strategies for verifying users with a user ID and password. An extra security thought is that when utilizing just HTTP strategies for confirmation with a user ID and password, the server framework isn't validated. This can expose the client's accreditations to specific attacks, for instance phishing assaults, and along these lines bargain the general security of your frameworks. The web application gets the message which contains the client Token. The token can be utilized for the API calls made in the web application as it currently will convey the client's character.

4.2 Captcha code

CAPTCHA represents entirely Automated Public Turning Tests to differentiate Humans and Computers. Captcha requests that we demonstrate that somebody is a human and not a Robot. Since all we need is to check a case and it will make sense of, on the off chance that you are a human or robot. Web security has turned out to be essential, as the act of web is embryonic these days. To shield organize from malware and to improve web security, investigates has been accomplished for quite a while. The most serious issue is phishing attacks just as access of web benefits by unlawful users. CAPTCHA-based methodologies are successful against phishing assaults. A CAPTCHA is a program that verifies locales against bots by making and assessing tests that human can pass yet current PC ventures can't.

4.3 Security Images

Once logged in to the web application after several stages of verification in password and CAPTCHA the application allows updating the next level of authentication which is Security Image auth. Clients can arrangement and pick any or a mix of alternatives dependent on their needs, while applications can arrangement strategies to authorize the degree of security, which gives most extreme adaptability and boundless conceivable outcomes to stay away from alter. For picture-password logins, the number of choices would be several tiers of strength less than that of even a six-character password.

4.4 OTP Email / Mob

With the expansion in digital security threats, it has turned out to be increasingly more important to overhaul the security benchmarks of your web applications. These days, great deals of online web applications are requesting that clients include an additional layer of security for their record. They do it by empowering 2-factor verification. There are different strategies for actualizing 2-factor verification, and TOTP (the Time-based One-Time Password calculation) validation is one of them. SMS-based/Email Based - OTP: In this methodology, each time the client signs in, they get a text to their enrolled phone number, which contains a One Time Password.

4.5 USB Device which can be connected with Mob/ System (Yubikey)

The new web validation standard, WebAuthn, that recently declared by W3C, is quickly picking up appropriation by driving stages and administrations. WebAuthn is an advancement of the FIDO U2F standard, initiated by Yubico and Google, and effectively sent since 2014 by a large number of users with YubiKey security keys. In this new validation scene, an outer security key, for example, the YubiKey assumes the significant job of a foundation of trust. As clients move between various stages and registering devices, having this compact base of trust is basic for empowering quick bootstrapping on new

gadgets and for recouping when gadgets are lost, taken or supplanted. In the case if a telephone or PC is lost, taken or supplanted, the YubiKey can be utilized as a simple technique to restore trust with online records and re-register the inside authenticator on another gadget. With an outer base of trust like the YubiKey, where the client's certification can't be messed with, it enables a high level of trust to be moved from gadget to gadget and build up every one of them as a confided in substance, in this way ensuring the record. RBAC – "Software in which we can set our pattern of Auth" It is a way to deal with confining framework access to approved clients. It is alluded to as job based security. Inside an association, jobs are made for different employment capacities. The authorizations to play out specific activities are alloted to explicit jobs. Individuals or staff (or other framework clients) are alloted specific jobs, and through those job assignments obtain the PC authorizations to perform specific PC framework capacities. Since clients are not alloted authorizations legitimately, yet just get them through their job (or jobs), the executives of individual client rights turns into a matter of basically doling out suitable jobs to the client's record; this disentangles basic tasks, for example, including a client, or changing a client's area of expertise.

5 CONCLUSION

Because of the need, hardware/software security structures and compelled assets, IoT gadgets are defenseless against various security attacks. This paper examines potential security and protection challenges in haze empowered IoT framework. The fundamental objective of this work is to give knowledge on verifying enormous information created by fog enabled IoT applications. We began with various IoT applications that produce gigantic measure of information pursued by fog enabled engineering, haze empowered IoT applications security pre-requisites and fog enabled security challenges.

REFERENCES

[1] X. Zha, et al. "Blockchain for IoT: The tradeoff between consistency and capacity", Chin. J. Internet of Things 1 (1) (2017)
[2] S. Huckle, et al. "Internet of things, blockchain and shared economy applications,", 2016.
[3] Dorri, et al. "BlockChain: A Distributed Solution to Automotive Security and Privacy," IEEE Commun. 2017
[4] J. Wang, et al. "A Blockchain Based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications," IEEE 2018
[5] M. S. Ali, et al. "Iot data privacy via blockchains and ipfs," in 7th International Conference for the Internet of Things, 2017.
[6] F. Lombardi et al., "A blockchain-based infrastructure for reliable and cost-effective iot- aided smart grids," 2018
[7] Erik Hofmann, et al. "Supply chain finance and blockchain technology: the case of reverse securitization". Springer, 2017.
[8] G. Hileman & M. Rauchs, "Global Blockchain Benchmarking Study. Cambridge", United Kingdom: Cambridge Centre of Alternative Finance, 2017.
[9] M. Conoscenti, A et al. "Blockchain for the Internet of Things: A Systematic Literature Review," in IEEE/ACS 2016,
[10] Li, J.; Greenwood, et al. "Blockchain in the built environment: Analysing current applications and developing an emergent framework".
[11] Liao, et al.. "Design of a blockchain-based lottery system for smart cities applications". In Proceedings of the 2017
[12] Dinh, et al.: "A framework for analyzing private blockchain". In Proceedings of the 2017
[13] Yu, et al.. "Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things". IEEE Wirel. Commun. 2018,
[14] Zhao, et al. "Blockchain based Privacy-Preserving Software Updates with Proof-of-Delivery for Internet of Things".
[15] Gervais, A et al. "On the security and performance of proof of work blockchains". 2016.