A SURVEY FOR SECURE AUTHENTICATION SCHEME FOR ML BASED ANTI-COUNTERFEITING SYSTEM

Kandra Preethi[1], Annal Priyadarshini.D[2], C.E. Akshaya Shalini[3], Ms.RamyaDevi K[4]
[4]*M.E, Assistant Professor,* [1,2,3]*Dept. of Computer Science and Engineering, S.A. Engineering College, Chennai 600-077, India*

Abstract: *Counterfeit meds are known as the prescriptions that were made for the reason of misleadingly addressing as genuine, successful and unique on the lookout. Such prescriptions cause extreme health issues for patients. Counterfeited drugs inimically affect the human health. The legitimate producing organizations additionally face dangers to their income misfortune because of these counterfeited meds. In this paper, we present a novel authentication protocol for anti-counterfeited drugs systems dependent on machine learning to help checking the legitimacy of medications "unit dosage". Our protocol utilizes machine learning as it is helpful for portable climate. Besides, our plan is supplemented with execution assessment alongside the utilization of random oracle model for formal security analysis. Results show that proposed convention opposes the greater part of regular related defects practically in equivalent registering cost with more added security highlights.*

I. INTRODUCTION

Counterfeit products are fakes or unauthorized replicas of the real product. Counterfeit products are often produced with the intent to take advantage of the superior value of the imitated product. The word *counterfeit* frequently describes both the forgeries of currency and documents, as well as the imitations of items such as clothing, handbags, shoes, pharmaceuticals, automobile parts, unapproved aircraft parts (which have caused many accidents), watches, electronics (both parts and finished products), software, works of art, toys, and movies. Counterfeit medicines are defined by world health organization (who) as those are fraudulently and purposely unlabeled with personality. Different items that are counterfeited cause issues to different assembling organizations, for example: car parts, gems, jewelry, software, food and drink and so on, drug items have genuine dangers from it. The counterfeit medicines don't offer any countermeasure to sicknesses that is the reason the individuals, who use these medicines, endure a ton. The lawful assembling organizations are undermined by this issue since it causes misfortune in their income. We aim to overcome this issue with our proposal.

II. CURRENT ANTI-COUNTERFEITING SCHEME:

a. Alphanumeric Token: A unique identity is designated to each item which is tagged on its packing. Each layer of packing has different

length of code. The code consisting of both letters and numbers and often other symbols (such as punctuation marks and mathematical symbols). The unique IDs of product are maintained by utilizing secure database. Web application facilitates the ultimate users (retailers, distributors or consumer) in order to check the originality of drug.

b. ***Collision Resistance:*** A decentralized ledger could be used for creating a self-executing contract, otherwise called a smart contract. They are a digital form of contract, stored in the form of codes in execute only when a certain criterion is met. It executes without any influence of a middle-man, in a conflict freeway. Smart contracts can be implemented to further secure the supply chain and make it more efficient. Notifying the receiver that the medicines are not being handled properly and may be contaminated. Similarly, smart contracts can be used to initiate payment to the sender as soon as the consignment reaches the consignee. A fake drug gets into the supply chain as its appearance is imitated as much close as possible to the original one.

c. ***Medical Chain Data Storage in Retailer:*** Each participant will share their public key, hash value of previous transaction, encrypted private key by manufacturer. The private key consist the details of medicine which is manufactured by pharmaceuticals agency. The transaction of medical chain here is secure and tempered-proof. Illegitimate participant can't get access to the block of transaction due to public key verification of participant (recipient) and digital signature verification of sender. This structure provides the non-repudiation verification using the sender cryptographic signature.

d. ***Drug Development and Trial Phase:*** Manufacturer generates an encrypted private key for the details and attaches the transaction to the Retailer shop. If any participants want details of drugs, then public key must be shared by that participant to the manufacturer. Manufacturer will encrypt the private key and will send back to the participant. Private Key
will be decrypted by the valid participant by their public key. The illegitimate user cannot access the patients, only legitimate can access the patients using public key.

e. ***Third-party Verifier Verification Phase:*** Third-party verifiers such as hospitals, pharmacies, patients, patient's family members, inspection agencies, etc. can download the certificate, signature, and then the third-party verifier verifies if the verification fails, the expiry date of the drug is tampered with by the drug distributor. If the signature between the drug manufacturer and the material supplier data are verified, and the third-party verifier can confirm that the drug is legal.

I. ADVANTAGES

The unique IDs of the products are maintained by utilizing secure database. It is an automated process using distributed secure database.

Proposed protocol offers a better security and thus protect against most common attacks.

III. LITERATURE SURVEY

1. *Public Awareness and Identification of Counterfeit Drugs*: IEEE, 2016, Ronald J. Prineas.
   The illegal trade in counterfeit drugs is a major setback to the fight against many diseases. Information on public awareness and ability to identify counterfeit drugs is scanty. Awareness to the public will not able to check the validity of drugs.

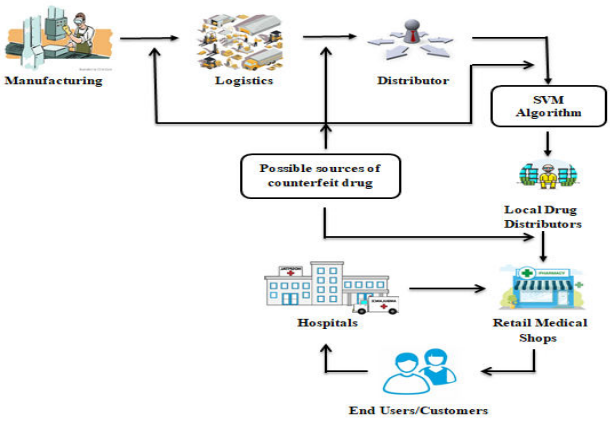
2. *Secure Authentication Scheme For Medicine Anti-counterfeiting System In IoT Environment:* Research Gate, 2010, Akosh Kumar Das. The new authentication scheme for medicine anticounterfeiting system in the Internet of Things environment, which is used for checking the authenticity of pharmaceutical products. The scheme utilizes the near field communication (NFC) and is suitable for mobile environment, also provides efficient NFC update phase.

3. *The Menace of Fake Drugs: Consequences, Causes and Possible Solutions*:IEEE, 2017, A. Chika. The business of fake drugs is a illegal crime that is increasing annually worldwide. The paper is aimed at examining the problem of drug counterfeiting business with emphasis on the causes and possible solutions.

4. *Research on dual anti duplication and anti-counterfeiting technology of QR code based on metamerism characteristics*: IEEE, 2019, Chen Fang. Ordinary QR code does not have the function of anti-duplication, and it is easy to be copied and counterfeited. In order to overcome this loophole, an anti-counterfeiting method using CMYK color printing mechanism characteristics embedded with pseudo-random noise is adopted to generate a QR code with dual anti duplication and anti-counterfeiting.

5. *Anti-counterfeiting using phosphor PUF*: IEEE, 2016, Dan jiang. An anti-counterfeiting system normally encodes a digital identifier in a physical identifier in essence. The physical identifier is cloneable or reusable the counterfeit products could easily cheat the anti-counterfeiting system.

IV. ARCHITECTURE DIAGRAM:



V. CONCLUSION

We presented a novel validation convention for anti-counterfeited drugs frameworks dependent on Internet of Things. The conspire assists with checking the legitimacy of the medications. It has been exhibited that our proposed convention can oppose all the known assaults while protecting the novel methodologies and functionalities. Besides, the security investigation shows that proposed convention offers a superior security and along these lines ensure against most basic assaults. The investigation of execution assessment and formal security demonstrates that our convention is additionally equivalently better in term of calculation cost and correspondence overhead.

.

VI. REFERENCES

1. T. Bhatia and A. K. Verma, "Cryptanalysis and improvement of certificate less proxy signcryption scheme for e-prescription system in mobile cloud computing", Ann. Telecommun., vol. 72, no. 9, pp. 563-576, Oct. 2017.

2. L. Li, S. Zhou, K.-K.-R. Choo, X. Li and D. He, "An efficient and provably-secure certificate less proxy-signcryption scheme for electronic prescription system", Secure. Commun. Netw., vol. 2018, pp. 1-11, Aug. 2018.

3. Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption)", Proc. Annu. Int. Cryptol. Conf., pp. 165-179, 1997.

4. M. Mambo, K. Usuda and E. Okamoto, "Proxy signatures for delegating signing operation", Proc. 3rd ACM Conf. Comput. Commun. Secur. (CCS), pp. 48-57, 1996.

5. C. Gamage, J. Leiwo and Y. Zheng, "An efficient scheme for secure message transmission using proxy-signcryption", Proc. 22nd Australas. Comput. Sci. Conf., pp. 420-431, 1999.

6. C. Zhou, G. Gao, Z. Cui and Z. Zhao, "Certificate-based generalized ring signcryption scheme", Int. J. Found. Comput. Sci., vol. 29, no. 6, pp. 1063-1088, Sep. 2018.

7. A. Karati, C.-I. Fan and R.-H. Hsu, "Provably secure and generalized signcryption with public verifiability for secure data transmission between resource-constrained IoT devices", IEEE Internet Things J., vol. 6, no. 6, pp. 10431-10440, Dec. 2019.

8. I. Ullah, A. Alomari, N. U. Amin, M. A. Khan and H. Khattak, "An energy efficient and formally secured certificate-based signcryption for wireless body area networks with the Internet of Things", Electronics, vol. 8, no. 10, pp. 1171, Oct. 2019.

9. A. Braeken, "Pairing free certificate based signcryption schemes using ECQV implicit certificates", KSII Trans. Internet Inf. Syst., vol. 13, no. 3, pp. 1546-1565, 2019.

10. I. Ullah, N. Amin, J. Khan, M. Rehan, M. Naeem, H. Khattak, et al., "A novel provable secured signcryption scheme PSSS: A hyper-elliptic curve-based approach", Mathematics, vol. 7, no. 8, pp. 686, Jul. 2019.

11. C. Zhou, "An improved lightweight certificateless generalized signcryption scheme for mobile-health system", Int. J. Distrib. Sensor Netw., vol. 15, no. 1, pp. 1-16, Jan. 2019.

12. I. Ullah, N. U. Amin, M. Zareei, A. Zeb, H. Khattak, A. Khan, et al., "A lightweight and provable secured certificateless signcryption approach for crowdsourced IIoT applications", Symmetry, vol. 11, no. 11, pp. 1386, Nov. 2019.