IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.047 ⁜ Vol. 10, Issue 7, July 2022

DOI: 10.17148/IJIREEICE.2022.10712

ATTRIBUTABILITY OF SPURIOUS MEDICINE SUPPLY CHAIN THROUGH BLOCKCHAIN

Vismaya S M[1], Chandan M N[2]

PG Student, Dept of MCA, P.E.S College of Engineering Mandya, Karnataka, India[1]

Assistant professor, Dept of MCA, P.E.S College of Engineering Mandya, Karnataka, India[2]

Abstract: Healthcare supply chains are complex networks that span organizational and geographic boundaries and act as the structural foundation for a variety of services that are necessary for daily life. Due to the inherent complexity of such systems, it is possible to introduce impurities like false data, a lack of transparency, and a shoddy data provenance. The creation of spurious pharmaceuticals, which not only has a significant detrimental effect on people's health but also costs the healthcare industry a lot of money, is one effect of these limits within the present supply chains. The need for a robust, end-to-end track and trace system for pharmaceutical supply chains has thus been highlighted by a recent study. To assure product safety and eliminate fakes, the pharmaceutical supply chain needs a comprehensive product recall procedure. Healthcare supply chains encounter difficulties with concerns relating to data privacy, openness, and authenticity because the majority of track and trace systems now in use are centralized. In this study, we suggest a block chain-based strategy for effective product tracing in the healthcare supply chain that makes use of smart contracts and decentralized off-chain storage. To ascertain how successfully the system can enhance attributability inside pharmaceutical supply chains, we test and confirm it before providing a cost and security analysis.

Keywords: Healthcare Supply Chains, Track and Trace System, Pharmaceutical Supply Chain, Attributability Pharmaceutical Supply.

I.INTRODUCTION

Since many small businesses give processing power and storage space to cloud storage, Block Chain is the most modern and practical way to access it. Each block consists of the crypto currency, hashes, timestamps, and transaction information from the preceding block. Block Chain is developing collection of blocks of papers that are encrypted linked. Block Chain cloud storage systems divide user data into manageable portions. After that, distribute a second security layer across the network. This is made feasible by utilizing elements of the Block Chain including hashing, private and public encryption, and transaction data (ledgers). Another benefit is that the node does not keep an excessive amount of data because it just saves what is required. Every important piece of information is kept secure since just a fraction of the data is made available to the users. Data redundancy and load balancing calculations are used to provide quick response and high availability. We provide a Block Chain-based method for tracing the supply chain of medicines that displays in-depth information about the application that is simple to comprehend with algorithms. To assess the system's efficiency in boosting supply-chain tracing, we used testing and validation together with cost and security analysis. Block chain technology aids in ensuring a rigorous transaction and tracing each and every step of the supply transaction when it comes to preventing fake medicine from entering the supply chain.

II.LITERATURE SURVEY

The International Medical Products Anti-Counterfeiting Taskforce (IMPACT) strives to put an end to the deadly drug trade that, according to statistics, takes the lives of tens of thousands of people each year. "We need to help people become more aware of the growing market in counterfeit medicines and the public health risks associated with this illegal practice" remarked Dr. Howard Zucker, assistant director-general for the WHO department cluster for health technology and pharmaceuticals. Retailers, pharmacists, and hospital staff will be urged by the taskforce to inform the authorities of any concerns they may have regarding the validity of a drug or vaccine. The taskforce will support nations as they work to simultaneously battle corruption in the departments of their police forces and customs authorities responsible for upholding laws against drug counterfeiting. Drug manufacturers will be exhorted to make it more difficult to replicate their goods [1]. The substantial threat that drug fraud poses to society is caused by it. The people's health is negatively impacted by the use of fake medications, and causes the manufacturers of reputable medicines to lose money

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.047 ⁜ Vol. 10, Issue 7, July 2022

DOI: 10.17148/IJIREEICE.2022.10712

organizations. There have been numerous anti-counterfeiting. Methods have been suggested. The bulk of current systems, however, are unsafe and open to various assaults like replay and man-in-the-middle attacks. Although more recent technologies, including mobile technology and RFID, have been employed for tracking and tracing high-quality medications, traditional technologies like barcode scanning and RFID are still commonly used. to defend against these many assaults and bogus medications. We have recommended secure QR code technologies that can only be accessed by the selected company that has regulatory authority over medical supply companies [2].

III.PROBLEM DEFINITION

Spurious drugs lead to cause problems in human health and even tend to death impacts. Spurious drugs distribution is reaching the 3rd party distribution where that effect in the treatment of the public health system in hospitals. They can also lead to loss of public confidence not only medicine but also in public health.

IV.PROPOSED SYSTEM

In proposed work medicines need to take patents approve from FDA and sends to manufacture medicine transaction, distributor transaction and medical shop(Pharmacy) transaction details secured using SHA-256 algorithm and block chain concepts. Medicine supply chain trace completely to avoid spurious drug and maintain transparent in medicine transaction. Manufacture company get medicine patent approval from FDA for manufacturing medicine. Medicine ingredients details encrypted using AES Rijndael algorithm for security process. FDA department further get medicine details decrypt data using AES Rijndael algorithm and verify medicine ingredients details and approve or reject medicine patent.

A. System Architecture

Significant actors in this architecture will be included by the application manager or administrator, It is an important tracking system where data is secured in each and every stage of supply method before medications are permitted to sell the medicine has to take approve from the FDA medicines need to take patents approve from FDA and sends to manufacture medicine transaction, distributor transaction and medical shop (Pharmacy) transaction details secured using SHA-256 algorithm and block chain concepts. Medicine supply chain trace completely to avoid spurious drug and maintain transparent in medicine transaction. Manufacture Company gets medicine patent approval from FDA for manufacturing medicine. Medicine ingredients details encrypted using AES Rijndael algorithm for security process. FDA department further get medicine details decrypt data using AES Rijndael algorithm and verify medicine ingredients details and approve or reject medicine patent. Once the medicine manufacture based on Primary or secondary order the medicines is supplied and finally reaches to the patients or users. This system helps to track and trace the medicine in each level with the help of block chain technology where there is no involvement of man in middle attack is possible and if any tamper occurred it is easily recovered in this system and sales quantity details also tracked and medicines stock details will be tracked with high security and safety measures.

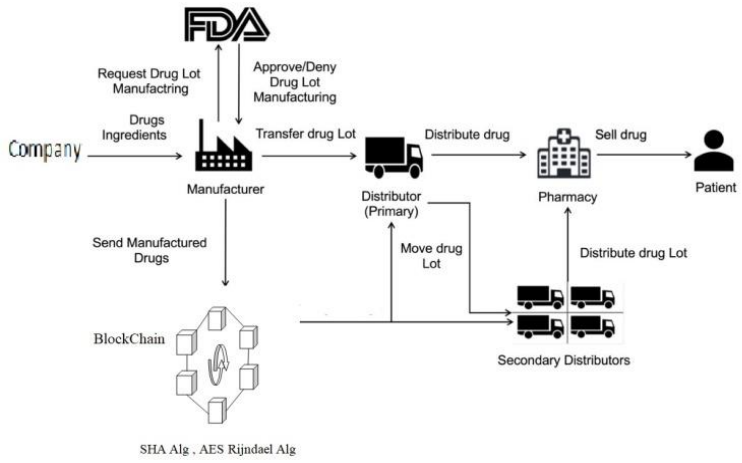

Figure 1: System Architecture

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.047 ⁜ Vol. 10, Issue 7, July 2022

DOI: 10.17148/IJIREEICE.2022.10712

V.IMPLEMENTATION

The application will be updated with all the medicine supply chain transaction level is produced this supply system transaction is secured and saved in this application whereas the system uses hash format. The SHA-256 technique is used to protect the transaction, and the hash is subsequently passed to several different entities for security, including the AES Rijndael encryption algorithm. Before a 128-bit key is generated, the AES Rijndael encryption technique will go through ten rounds. This key will be kept on file by the AWS S3 services for safety and security reasons.

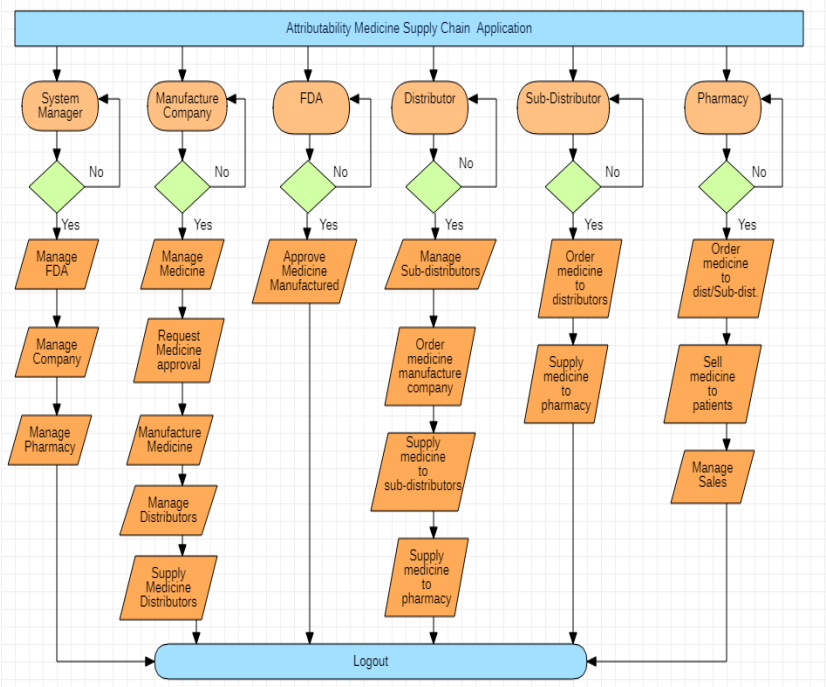

Figure 2: Workflow diagram

A. AES Rijndael Algorithm

The symmetric key cryptography method AES was released by MST. Rijndael came up with the algorithm. The Rijndael encryption algorithm is another name for it. AES serves as DES's substitute. AES employs the block cypher technique. The normal text and encrypted text sizes must coincide. An input key's size is equal to that of plain text.

AES allows three alternative key lengths of 128, 256, and 192 bits in addition to data lengths of 128, 192, and 25 bits. AES uses many rounds of processing when working with different key bits, such as when performing encryption 10 times with a 128-bit key. The 192-bit key completes 12 rounds of encryption. Data is encrypted using a 256-hit key for 14 cycles.

AES Rijndael Algorithm steps:

Figure 3 depicts the AES algorithm steps.

1. SubBytes: It is byte-by-byte substitution during the forward process. The corresponding substitution step used during decryption is called InvSubBytes. This step consists of using a 16 × 16 lookup table to find a replacement byte for a given byte in the input state array. The entries in the lookup table are created by using the notions of multiplicative inverses in GF(28) and bit scrambling to destroy the bit-level correlations inside each byte.

2. ShiftRows: It is for shifting the rows of the state array during the forward process. The corresponding transformation during decryption is denoted InvShiftRows for Inverse Shift-Row Transformation. The goal of this transformation is to scramble the byte order inside each 128-bit block..

3. Mix Columns: It is for mixing up of the bytes in each column separately during the forward process. The corresponding transformation during decryption is denoted InvMixColumns. The goal is here is to further scramble up the 128-bit input block. The shift-rows step along with the mix-column step causes each bit of the ciphertext to depend on every bit of the plaintext after 10 rounds of processing.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.047 ⁜ Vol. 10, Issue 7, July 2022

DOI: 10.17148/IJIREEICE.2022.10712

4. Add round key: The 16 bytes of the matrix, which are now thought of as 128 bits, are XORed with the 128 bits of the round key. If this is the last round, the output is the cipher text.

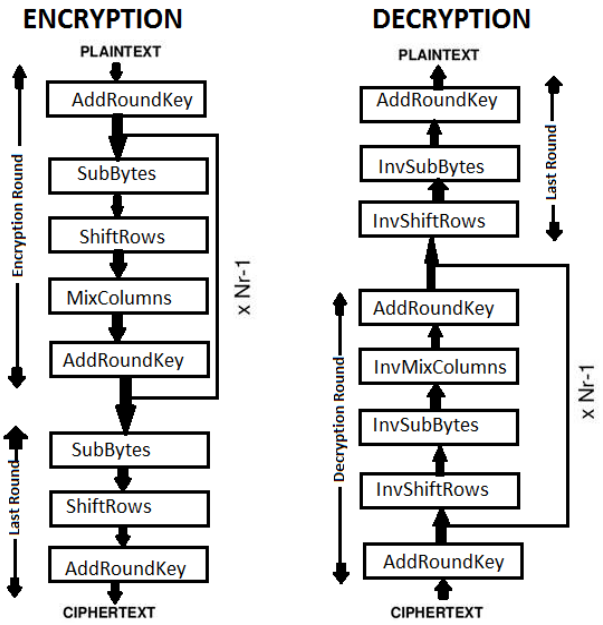

Figure 3: AES encryption and decryption

B. SHA-256 Algorithm

A group of hash functions used in cryptography is known as the Secure Hash Algorithms (SHA). The SHA-256 algorithm constructs a 256-bit (32-byte), substantially unique hash. Hash is a so-called one-way function. This qualifies it for use with challenge hash authentication, anti-tampering, and digital signatures in blockchain.

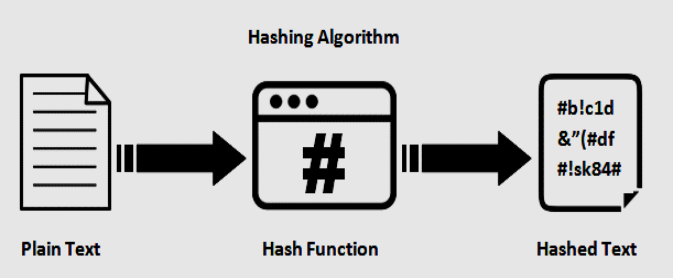

Figure 4: Hashing Algorithm

Working of SHA-256

- Arbitrary length message string 'M'.
- Convert it to binary.
- Pre-processing Stage:
  a) Padding a message M
  b) Parsing the Message M
  c) Setting initial hash values H_0……H_7
- Hash Computation
  a) Establish the message schedule.
  b) Initialize the variables a, b, c, d, e, f, g, and h.
- Determine the intermediate hash values.
- Add the hash values for H0, H1, H2, H3, H4, H5, H6, and H7.
- 256-bits Message digest.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.047 ⁜ Vol. 10, Issue 7, July 2022

DOI: 10.17148/IJIREEICE.2022.10712

- M + P + 64 = n x 512 i.e., M = original message length P = padded bits.
- The bits we append to the message should begin with a "1" and continue with a "0" until we are 64 bits less than a multiple of 512.

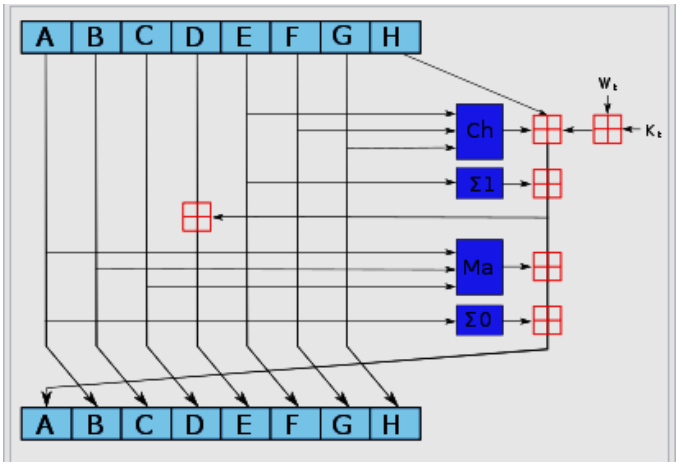

Figure 5: SHA-256 Algorithm

CONCLUSION

The suggested system's drug attributability throughout pharmaceutical supply chains emphasizes its importance, particularly for safeguarding against fake medications. In order to track and trace medications and create tamper-proof logs In order to improve the pharmaceutical supply chain, we developed and tested a BlockChain-based solution. We are securing them with the help of using algorithms like SHA-256 and AES Rijndael algorithm which is used to encrypt and decrypt the hash key value and then store in the form of QR code in AWS S3 services and fetch the approved or secured details to achieve end to end transparency. The application becomes safer and secure as in result we are using the Block Chain technology.

REFERENCES

[1] W. Burns, “WHO launches taskforce to fight counterfeit drugs,” Bull. World Health Organ, vol. 84, no. 9, pp. 689–690, 2006.

[2] Kavita Kumari , Kavita Saini. “CFDD (CounterFeit Drug Detection) using Blockchain in the Pharmaceutical Industry.” Volume 08, Issue 12 (December 2019),ISSN: 2278-0181

[3] Randir Kumar, Rakesh Tripati. ”Traceability of counterfeit medicine supply chain through BlockChain.” In information of IT, NIT, 2019 11th International Conference on Communication Systems & Networks (COMSNETS)

[4] H. Kwame Adjei, “Counterfeit Drugs: The Relentless War in Africa,” Pharm. Pharmacol. Int. J., vol. 2, no. 2, pp. 45–47, 2015.

[5] World Health Organization, “Substandard, spurious, falsely labeled, falsified and counterfeit (SSFFC) medical products,” Who, no. January, pp. 2–5, 2016.

[6] H. H. Cheung and S. H. Choi, “Implementation issues in RFID-based anti-counterfeiting systems,” Compute. Ind., vol. 62, no. 7, pp. 708–718, 2011.

[7] Y. Li, T. Marier-Bienvenue, A. Perron-Brault, X. Wang, and G. Pare, ´ “BlockChain Technology in Business Organizations: A Scoping Review,” no. January, 2018.

[8] Paik, Michael, Ashlesh Sharma, Arthur Meacham, Giulio Quarta, Philip Smith, John Trahanas, Brian Levine, Mary Ann Hopkins, Barbara Rapchak, and Lakshminarayanan Subramanian. ”The case for Smart Track.” In Information and Communication Technologies and Development (ICTD), 2009 International Conference on, pp. 458-467. IEEE, 2009.

[9] V. Ramani, T.Kumar, A. Bracken, M. Liyanage, and M. Ylianttila,“Secure and ef_cient data accessibility in blockchain based healthcare systems," in Proc. GLOBECOM, Dec. 2018, pp. 206_212.

[10] N. Ri_, E. Rachkidi, N. Agoulmine, and N. C. Taher, “Towards using blockchain technology for eHealth data access management," in Proc. IEEE 4th Int. Conf. Adv. Biomed. Eng., Oct. 2017, pp. 1_4.