iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VI **Month of publication:** June 2021

DOI: https://doi.org/10.22214/ijraset.2021.35473

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

Lightweight Authentication Protocol for NFC based Anti-Counterfeiting System in IoT Infrastructure

Dr. Rekha N[1], Greeshma P. S[2], Huda Matheen[3], Srividya Murthy[4], V. Deepthi[5]
[1]*Associate Professor, Department of Telecommunication, KSIT, Bengaluru, India*
[2, 3, 4, 5]*UG Student Department of Telecommunication, KSIT, Bengaluru, India*

Abstract: ***Counterfeit medications are known as the medications that were manufactured for the purpose of deceptively representing as authentic, effective and original in the market. Such medications cause severe health issues for patients. Counterfeited drugs have an inimical effect on the human health. The legal manufacturing companies also face threats to their revenue loss due to these counterfeited medicines. In this paper, we introduce a novel authentication protocol for anti-counterfeited drugs systems based on Internet of Things (IoT) to help checking the validity of drugs ''unit dosage''. Our protocol uses the near-field communication (NFC) as it is convenient for mobile environment. The protocol also offers reliable update phase for NFC. Furthermore, our scheme is complemented with performance evaluation along with the use of random oracle model for formal security analysis.***

Keywords: NFC, IoT system, Tomcat Server, Android, Eclipse Tool

I. INTRODUCTION

The broad majority of business extensively utilizes the innovative technology of Internet of Things which is persuading almost every facet of the world. However, the nature of public communication over the Internet makes the objects and devices of IoT vulnerable to numerous cyber-attacks. Moreover, various standard solutions of security developed for enterprise systems are not efficient and implementable to IoT devices. This becomes even more serious in the case of sensitive and critical systems such as anti-counterfeiting which is constructed by the use of IoT infrastructure. As a result, the critical systems of IoT based anti-counterfeiting face various protection and security challenges. Therefore, it is crucial to observe IoT specific security attacks and develop a reliable, scalable, and secure mechanisms of security.

CDs also called as fake drugs, counterfeit medicines or counterfeit pharmaceuticals are causing untold suffering to the populace especially in some African countries where it takes an alarming proportion from the total drugs in circulation. The harmful effect of CDs stretches from the people to businesses.

It has been reported that up to around 1 million innocent people can lose their lives around the globe every year, as a result of CDs related cases, and therefore it is one of the major global public health risk The global CDs trade is a multi-billion dollars industry which is steadily flourishing in Africa. In 2008, the United States Government estimated the global market value of the counterfeit industry to reach USD 500 billion with an increment rate of 1,700% during the past decade. The World Health Organization (WHO), estimated global sales of counterfeit medications to top USD 75 billion in 2010 alone, which is a 90% rise from 5 years before and could be more than 10% of all medicines sold worldwide.

In the third world countries, i.e., many African countries and part of Asia, the percentage in circulation is much higher and could be more than 30%. The risks for those involve in the dirty business in terms of either legal penalties or monetary loss are insignificant, and they generate huge profits through trafficking of counterfeit products regardless of possibilities for inflicting morbidity and mortality to mankind. The penalties labelled for pharmaceutical counterfeiters in most African countries did not match the magnitude of their crime.

Therefore, the profits driven by drug counterfeiting businesses in Africa are high enough to keep the business booming, on the other hand, the penalties labelled for it are too low to stop the crime from thriving, consequently yielding synergy for its rising prevalence. In addition, regulatory agencies for drug's quality, manufacture, importation, and sales in some of these countries are very weak. CDs continue to pose significant hazards to the public health, waste consumer's and governments income and reduce incentives that might otherwise be used to engage in research and development in the affected countries.

II. LITERATURE SURVEY

Counterfeit medicines are defined by World Health Organization (WHO) as those are fraudulently and deliberately unlabelled with identity [1]–[3]. Various products that are counterfeited, cause problems to various manufacturing companies such as automotive parts, jewellery, cosmetic, software food and beverage etc. Pharmaceutical products have serious threats from it. The counterfeit medicines do not offer any countermeasure to diseases, that is why the people, who use these medicines, suffer a lot. The legal manufacturing organizations are threatened by this problem because it causes loss in their revenue. Worldwide, the annual sale of counterfeit products is estimated as US$ 650 billion by the International Chamber of Commerce of Geneva [4]. WHO also estimated that the utilization of counterfeit products has caused almost 100,000 deaths in Africa in a year. According to the British ‘‘International Policy Network’, there were almost 700,000 death cases in a year due to utilization of tuberculosis and malarial medicines. Counterfeiting can happen with local as well as branded products. In some area of Latin America, Africa and Asia, the sale of counterfeited medicines are more than 30%, as noticed by WHO. It has been also reported that anti-malarial, steroids, hormones, anti-viral, anti-biotic and anti-cancer are general counterfeited medicines [1]–[3].

At the same instant, different organizations of various countries are trying to overcome the problem of counterfeited drugs. According to Xinhua News Agency of China, China is utilizing the technology in which each medicine package that is sealed with anti-counterfeit labels are traced and recognized. The border posts and airports in African countries use hand-held spectrometer, known as Tru-Scan, for the detection of counterfeit drugs with the help of their chemical composition analysis. Counterfeit drugs are also being detected by the simple and free-text message technologies. Companies such as Sproxil and mPedigree Network developed a system in which the labels on medicine packages with an encrypted code is used by the legal medicine manufacturing companies. The label on the drug package is scratched-off by the user who wants to buy that drug and send the code to the company’s system which checks the authenticity of medicine packet without any cost. After the verification of medicine packet, the system sends the response message to that user, whether the drug is fake or actual. Therefore, the drug package is known to authentic easily by the customer without any cost. But, the issue is that, this technique needs a lot involvement of user as it is not automated because users are required to remove the label and then to write the code and sending to the system [1]–[3].

Radio Frequency Identification (RFID) allows the identification of different items that use radio waves. A RFID reader usually communicates with RFID tags which have microchips containing the digital information [5]. To prevent counterfeiting, the anti-counterfeiting technology based on RFID has evolved as a powerful tool, because it has generally used anti-counterfeited approach (for example, chemical markers, finger-prints, shifting-inks, and colors). However, the automatic validation of authentic products are not used by these methods. The technology that enables different devices for communicating directly with each other without any use of central infrastructure networking (i.e. base station and access point) is known as Device-to-Device (D2D) communication [6]. Some common applications of D2D communications depend on Wi-Fi direct, blue-tooth and near field communication. NFC is a high frequency short-range wire-less communication technology, in which NFC enabled devices can communicate with each other up-to 10cm distance. The small amount of data is stored in microchips of NFC tags for transmitting to another NFC supported devices, like mobile devices. The technology of NFC is an enhanced version of the current RFID technology. Such technology provides facility to single device for containing both the interface of a reader and smart card. The data can easily be shared between NFC-based devices [7]–[9].

Recently, numerous authentication schemes have been developed for the networks of wireless sensor and ambient-assisted living system [10]–[17]. A new anonymous authentication scheme is presented by Yan et al. [18] in which trust levels and pseudonyms are authenticated in order to provide reliable social networking with secured privacy. Afterwards, various anti-counterfeiting techniques based on RFID have been proposed [5], [19]–[23]. But, the most existed anti-counterfeiting protocols based on RFID are insecure and having various flaws, like main-in-the middle, replay and reader impersonation threats. Some of them do not have sufficient capability for the mobile environment, also do not have adequate RFID changing phase with non user friendly environment. The anti-counterfeiting methods based on NFC are very helpful for mobility environment which have no requirement of card reader as customers just need a mobile device with enabled NFC to interpret the information saved in NFC-tag and transmits to the service provider. In our protocol, after every successful transaction or process of verification, the NFC tag record is updated in the repository. If there is a number of repositories between the user and the manufacturing company, then at every repository, the transaction of each NFC tag is required to be updated. These records are maintained at distributed database servers. These updated records can be observed by the respective database administration that where, when, and who updates the NFC tag. It also check whether a legal party updates the NFC tag or not.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

III.SYSTEM ARCHITECTURE AND DESCRIPTION

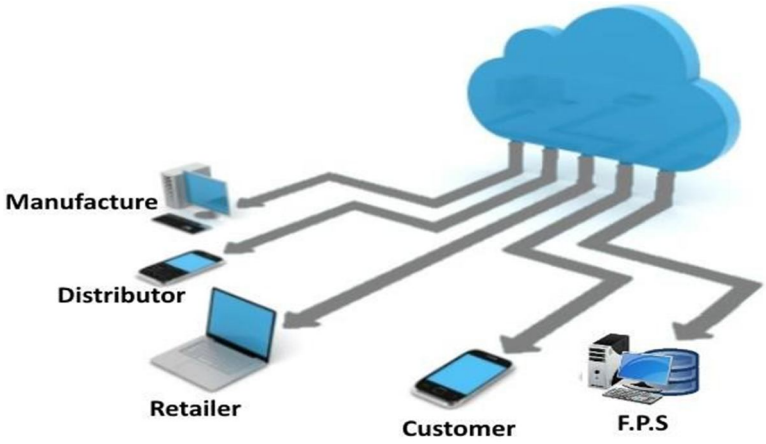


Figure 1. Generic architecture of the anti-counterfeiting system.

The interconnection of different objects and devices through the Internet is known as Internet of Things. The cloud and IoT based systems for anti-counterfeit are realised by developing a portal for anti-counterfeit. Such system design is shown in Fig. 1. The existence of the portal ensures to customers that the drug that they are about to purchase are legitimate and not injurious to health. The system is used by the manufacturers, retailers, distributors, and customers. The interaction and working of these users are elaborated as follows.

A. Administrator

The policies of the mechanism of anti-counterfeit is described by the administrator. The privileges are set by him to get access to the system. The system of code generation is maintained by the administrator and also the web services are provided to end users and clients by only him. The database of user's information and the data which helps to enable the authentication of product, is maintained by the administrator. The description of the product given by the manufacturer are also certified by the administrator so that fake drug products can easily be identified by the customers by scanning the purchased product. Moreover, the service or system updates can be offered by the administrator.

B. Manufacturer

The drug products are registered and the related details are entered in database by the web services. The system engenders a particular code for each drug product. Only corresponding manufacturer can access that unique code. That code is printed on related drug item in order to facilitate the authentication of each drug product using database that is maintained on the main server at the manufacturer end.

C. Ultimate Users

Retailers, customers and distributors are assumed as ultimate users and the role of these end users are elaborated as follows:

1) *Retailers and Distributors:* From manufacturers to customers, the process of drug tracking and delivering is the responsibility of retailers and distributors. The received product is authenticated by them and the tracking record of drug products are also updated by them on the database using APP or text message through an Internet browser or mobile device. If the tracking record is maintained at each level, then in the future, it can help to trace that at which level it is counterfeited.
2) *Consumer:* The originality of drug product using APP or text message can be checked by consumers with the help of computer or mobile. To verify the validity of the drug product by the anti-counterfeit system, the uncommon NFC tag is provided by customers. If the product is successfully authenticated then the condition of status in database is set as sold automatically, in order to prevent counterfeit. So, in this way, they can claim for the counterfeited product, if the status is already set to sold or authentication of product is not valid. Furthermore, the product feedback can be directly provided by the consumer to the manufacturer

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

IV. WORKING AND METHODOLOGY

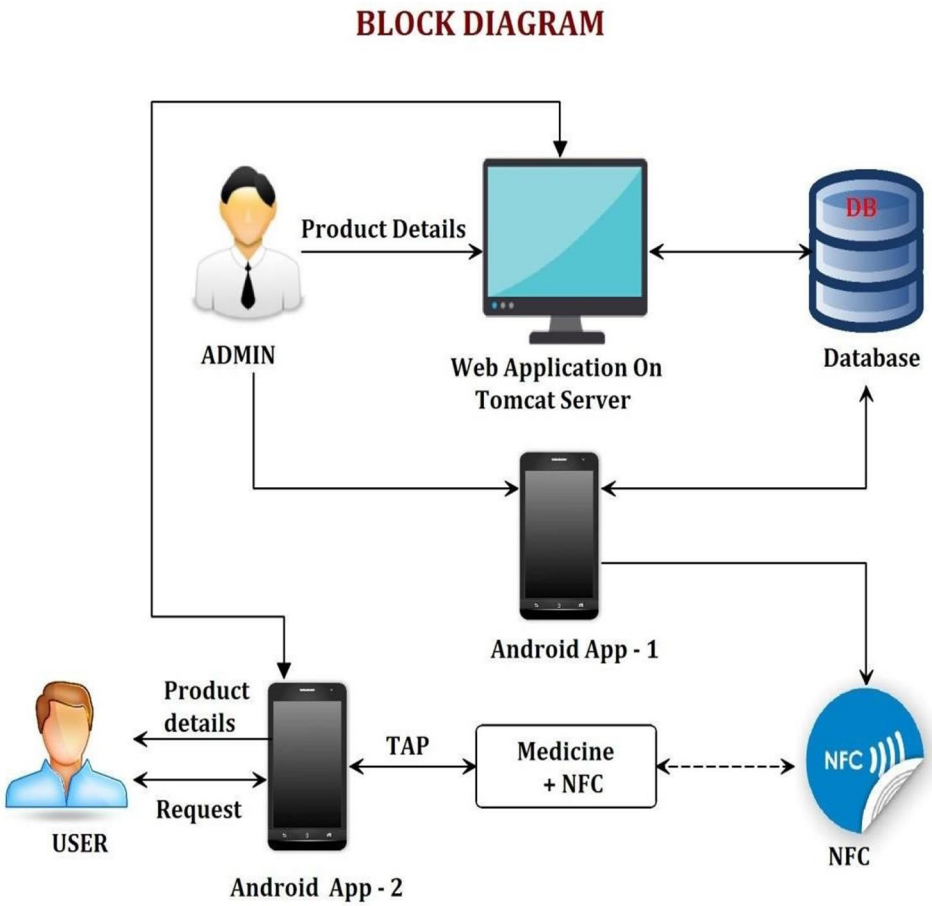


Figure2. Block Diagram of Proposed System

A new authentication protocol for the system of drug anti-counterfeiting in IoT environment is presented in this paper. Our protocol has the capability for the validation of online drug dosage forms with the help of mobile device. The counterfeiting of drug dosage forms are prevented by the proposed scheme. The protocol offers a secure and robust mechanism of mutual-authentication between the server and NFC tag attached to the form of drug dosage. In the proposed protocol, the NFC operated on mobile devices is used as an interface between the server and the NFC tag that helps in reading the stored information in NFC-tag and transmits this info to the server. Then, drug dosage forms are authenticated by the server and the response message is sent to the user of NFC enabled mobile device. At the end, the customer can easily take his decision after receiving the response from the server whether the drug is able to purchase or not.

A. The Working Of The System Of Anti-Counterfeit Is Described As Follows

Anti-counterfeit portal helps the end users such as distributors, retailers and consumers to check the authenticity of the drug packet through computer or mobile device. The status of the product with particular tag can be verified by the customers. If the product with particular tag is not already sold then the customer is intimated through message that the product is genuine. This successful verification proceed and the product purchase status is set to sold with that particular tag. However, if the sold status is already found set then customer is immediately intimated that the product you are going to purchase is fake or tempered. Instantly an alert message is also sent towards the manufacturer about this event. The authentication process is facilitated by a unique NFC tag which is placed on each product.

These properties help the customers to check whether the status of the product is set as sold in early or not. If the status is set earlier then obviously the drug product is counterfeited so in this way the system gives the warning to the manufacturer and the user. The information about the original product in the system must have to be maintained by manufacturer, so that the authentication is facilitated. Then the system engenders a unique NFC for each item. The specific database of concerned system is used to keep the product related information.

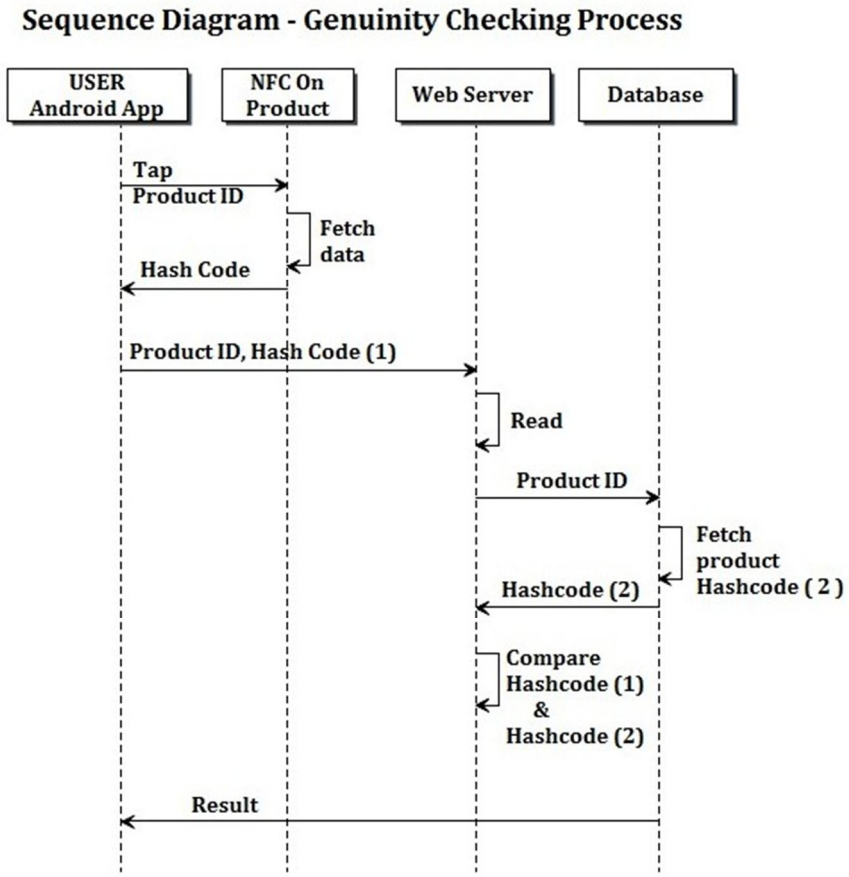


Figure 3. Genuinity Checking Process

B. Authentication Procedure Is Described As Follows

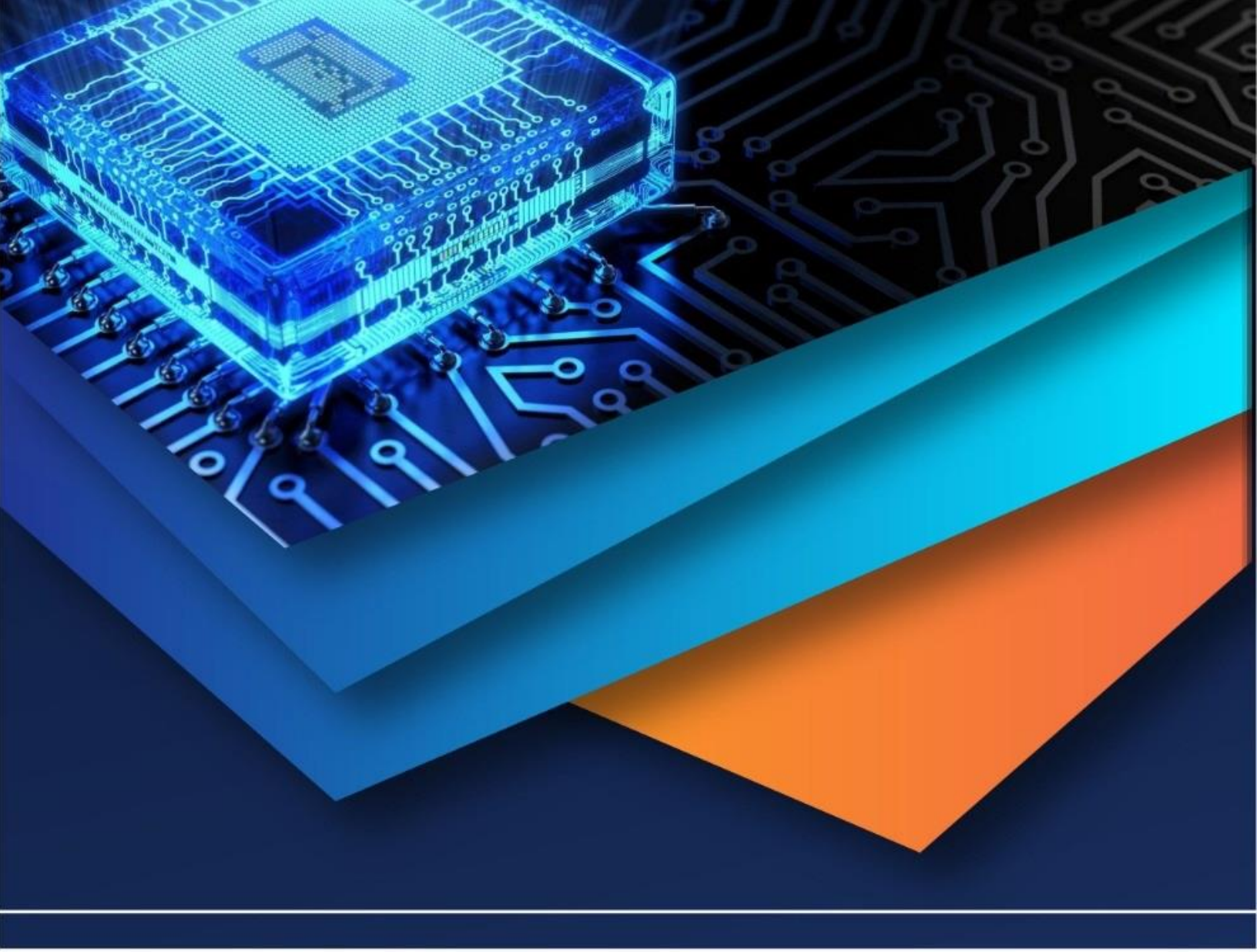
1) *Step 1:* When the anti-counterfeit system is accessed with the help of computer or mobile device by the end users then this procedure launches.
2) *Step 2:* The product NFC is provided by the end users. This NFC is decrypted by the system of anti-counterfeit.
3) *Step 3:* The information about expiry date and specific code of the product is recovered and authenticated after decrypting the NFC.
4) *Step 4:* The results can be recovered and viewed by the end users with the help of specific product code.
5) *Step 5:* At the last step of authentication method, the ultimate user is checked by the system, then the sold status of product is checked by the system if he is customer.
6) *Step 6:* The product item is set as sold status after authenticating the product successfully in order to identify the same product whether it is counterfeit or original.
7) *Step 7:* The product track record is updated by the system, if distributors and retailers are the end users. And in this case the sold status of product is not set by the system.

V. CONCLUSION

CDs are taking silent devastating toll of human beings every year and causing serious affliction, especially to the African nations. Drugs criminal organizations understand the high margins associated with counterfeit products, but among other reasons, lack of stringent laws and enforcement of the laws, corruption and minimal possibility of being prosecuted, serve as incentives for them to continue causing significant public health risks, by exposing millions of people to the danger of CDs. We introduced a novel authentication protocol for anti-counterfeited drugs systems based on Internet of Things. The scheme helps to check the validity of the drugs. It has been demonstrated that our proposed protocol is able to resist all the known attacks while preserving the novel approaches and functionalities. Furthermore, the security analysis shows that proposed protocol offers a better security and thus protect against most common attacks. The analysis of performance evaluation and formal security indicates that our protocol is also comparably better in term of computation cost and communication overhead.

REFERENCES

[1] W. Burns, ‘‘WHO launches taskforce to fifight counterfeit drugs,’’ in Bulletin of the World Health Organization, vol. 84. 2006, pp. 689–690.
[2] J. Sambira, ‘‘Counterfeit drugs raise Africa’s temperature,’’ Afr. Renewal, vol. 27, no. 1, pp. 5–7, May 2013. [3] Substandard, Spurious, Falsely Labelled, Falsifified and Counterfeit (SSFFC) Medical Products, WHO, Geneva, Switzerland, 2016.
[3] H. H. Cheung and S. H. Choi, ‘‘Implementation issues in RFID-based anti-counterfeiting systems,’’ Comput. Ind., vol. 62, no. 7, pp. 708–718, Sep. 2011.
[4] S. Choi and C. Poon, ‘‘An RFID-based Anti-counterfeiting System,’’ IAENG Int. J. Comput. Sci., vol. 35, no. 1, pp. 1–12, 2008.
[5] M. Wang and Z. Yan, ‘‘A survey on security in D2D communications,’’ Mobile Netw. Appl., vol. 22, no. 2, pp. 195–208, Apr. 2017.
[6] A. Bodhani, ‘‘New ways to pay,’’ Eng. Technol., vol. 8, no. 7, pp. 32–35, Aug. 2013.
[7] N. M. Smith and C. Cahill, ‘‘Continuous multi-factor authentication,’’ U.S. Patent 9 705 869, Jul. 11, 2017.
[8] Q. Z. Sheng, S. Zeadally, A. Mitrokotsa, and Z. Maamar, ‘‘RFID technology, systems, and applications,’’ J. Netw. Comput. Appl., vol. 34, no. 3, pp. 797–798, 2011.
[9] D. He and S. Zeadally, ‘‘Authentication protocol for an ambient assisted living system,’’ IEEE Commun. Mag., vol. 53, no. 1, pp. 71–77, Jan. 2015.
[10] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, ‘‘Anonymous authentication for wireless body area networks with provable security,’’ IEEE Syst. J., vol. 11, no. 4, pp. 2590–2601, Dec. 2017.
[11] D. He, N. Kumar, and N. Chilamkurti, ‘‘A secure temporal-credentialbased mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks,’’ Inf. Sci., vol. 321, pp. 263–277, Nov. 2015.
[12] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K.-R. Choo, ‘‘A three-factor anonymous authentication scheme for wireless sensor networks in Internet of Things environments,’’ J. Netw. Comput. Appl., vol. 103, pp. 194–204, Feb. 2018.
[13] F. Wu, L. Xu, S. Kumari, X. Li, J. Shen, K.-K.-R. Choo, M. Wazid, and A. K. Das, ‘‘An effifficient authentication and key agreement scheme for multigateway wireless sensor networks in IoT deployment,’’ J. Netw. Comput. Appl., vol. 89, pp. 72–85, Jul. 2017.
[14] J. Li, W. Zhang, V. Dabra, K.-K.-R. Choo, S. Kumari, and D. Hogrefe, ‘‘AEP-PPA: An anonymous, effifficient and provably-secure privacy preserving authentication protocol for mobile services in smart cities,’’ J. Netw. Comput. Appl., vol. 134, pp. 52–61, May 2019.
[15] S. Kumari, P. Chaudhary, C.-M. Chen, and M. K. Khan, ‘‘Questioning key compromise attack on Ostad-Sharif et al.’s authentication and session key generation scheme for healthcare applications,’’ IEEE Access, vol. 7, pp. 39717–39720, 2019.
[16] J. H. Kong, L.-M. Ang, and K. P. Seng, ‘‘A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments,’’ J. Netw. Comput. Appl., vol. 49, pp. 15–50, Mar. 2015. 76366
[17] Z. Yan, W. Feng, and P. Wang, ‘‘Anonymous authentication for trustworthy pervasive social networking,’’ IEEE Trans. Comput. Social Syst., vol. 2, no. 3, pp. 88–98, Sep. 2015.
[18] S. H. Choi, B. Yang, H. H. Cheung, and Y. X. Yang, ‘‘RFID tag data processing in manufacturing for track-and-trace anti-counterfeiting,’’ Comput. Ind., vol. 68, pp. 148–161, Apr. 2015.
[19] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede, ‘‘Public-key cryptography for RFID-tags,’’ in Proc. 5th Annu. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerComW), Mar. 2007, pp. 217–222.
[20] C.-L. Chen, Y.-Y. Chen, T.-F. Shih, and T.-M. Kuo, ‘‘An RFID authentication and anti-counterfeit transaction protocol,’’ in Proc. Int. Symp. Comput., Consum. Control, Jun. 2012, pp. 419–422.
[21] T. Ma, H. Zhang, J. Qian, S. Liu, X. Zhang, and X. Ma, ‘‘The design of brand cosmetics anti-counterfeiting system based on RFID technology,’’ in Proc. Int. Conf. Netw. Inf. Syst. Comput., Jan. 2015, pp. 184–189.
[22] T. Staake, F. Thiesse, and E. Fleisch, ‘‘Extending the EPC network: The potential of RFID in anti-counterfeiting,’’ in Proc. ACM Symp. Appl. Comput., 2005, pp. 1607–1612.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY