International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

SECURE AUTHENTICATION SCHEME FOR MEDICINE ANTI-COUNTERFEITING SYSTEM IN IOT ENVIRONMENT

K.Kiruthika[1], M.Afiyafirdhouse[2], S.Kavitha[3]

[1]Asst.Prof, [2,3]UG Scholar, Department of Computer Science,
Panimalar Engineering College, India.

Abstract - *Pharmaceutical is one of the medications taken by everybody in the world when they are contaminated by a few ailments. A portion of the business corporates for getting high benefit offer the lapsed medication which is exceptionally unsafe to the patients who admission it, in some cases it might even take them until the very end. Along these lines, for falsifying this issue we propose this arrangement which depends on the Internet of things (IoT). The manufacturer fabricates the prescription and updates the record which can be seen by any of the clients who utilizes this interface. After the execution of this strategy, patients would intake medicines with complete trust. We utilize the Near Field Communication (NFC) for making this thought into a restorative transformation. This plan is secured by a few conventions which can shield the huge corporates and other undesirable access. This strategy is extremely successful contrasted with the current framework. Presently the lapsed meds will be disposed of from the restorative business.*

Key Words*: *NFC tag, counterfeit expired medicines, IoT for medical enhancement, secure medicines.

1.INTRODUCTION

Each human in this world makes due with the assistance of the vitality from the sustenance and water. A sound nourishment drives mankind to a solid life. There are a few kinds of eating methodologies accessible in light of the supplements accessible on the sustenance. At any rate, a solid individual needs the greater part of the supplements which can be given just by the adjusted eating regimen. On the off chance that any of the supplement content in our body decreases which may prompt a portion of the maladies. Likewise, these days because of the awful condition our body gets influenced by a few infections. For getting rid of these ailments we allow the medicines which can be the cure for those.

Those meds have an expiry date which is the lifetime of the pharmaceutical. After the expiry of the pharmaceutical, it might produce dangerous results. As the prescriptions are produced using the blend of chemicals it might have complex substance properties which are extremely hard to get it. Some of the time because of this dangerous impact, it might cause the human life. Along these lines, the pharmaceuticals ought to be demolished after the expiry date.

A solution achieves the patient on a long adventure. The begin put is the manufacturing industry, where the pharmaceuticals are made. Next, the prescriptions make a long voyage to a few sub-merchants and after that, it, at last, achieves the medicinal shop. From that point, the patients can take them and utilize it for curing their sicknesses.

A portion of the corporates is getting an incredible misfortune in the transfer of the lapsed prescription. They couldn't care less about the human esteem and they change the date of expiry rather than disposal.

The government is making a few guidelines and making the strict assessment for precluding the offers of the terminated drugs to spare the human life. Despite the fact that, a portion of the officers in control are getting the bribe and permitting to offer the pharmaceuticals.

By utilizing our proposal individuals can utilize the prescriptions which are not terminated with no dread. They can even check the expiry date which can't be changed by any people who assume part in the middle of the chain. The equipment can be reused by eradicating the expiry date (only by trusted authorities) and nourishing new information to them. Along these lines, this empowers the reusability of the equipment which is making the framework more viable than the past states.

2.RELATED WORK

2.1 RFID Based Product Tracking [1]

In this paper, the creator proposes by giving the RFID to the item and follow the item. The customer confirmation should be possible with this technique. By this strategy, the client can confirm the item before getting them. In our framework, we utilize NFC labels which are more proficient than this framework.

2.2 Location Based RFID Verification [2]

In this paper, the item is followed towards the entire lifecycle. The area administrations of the client are taken for the check of the item. The check is done in light of the RFID which is set on the item. The client points of interest are exceptionally secured in our framework than this framework.

2.3. Unclonable RFID Tags [3]

The talk on this paper is focused on the RFID based confirmation of the item. This paper likewise gives another framework to RFID which can't be cloned. Our framework additionally gives another technique by which the code can't be cloned.

2.4. Public Key Security in RFID Verification [4]

The security highlights are refreshed than the current framework. The restricted confirmation is done on this strategy. In any case, this strategy does not give security from the replay assaults and RFID cloning. Our technique can give preferable security over this framework.

2.5 Data Synchronization [5]

The paper gives new techniques to give a proficient framework to confirmation of the item. This framework likewise gives the answer for the information synchronization. The antilust item can likewise be discovered utilizing their technique. Our framework likewise gives a superior synchronization of items.

2.6 RFID Clone Resistant System [6]

This paper gives a decent framework which can make RFID which can't be cloned. Our framework likewise furnishes a tag with mystery codes which can't be cloned.

3. PROPOSED ALGORITHM

- The Diffie - Hellman Algorithm is configured to use devices communicate to each other using the Internet.
- This Algorithm checks for the authentication of the server by exchanging the shared secret key.
- The Key Exchange is done by the Information server, Authentication server and Database server by the help of the Diffie-Hellman Algorithm.
- The usage of key exchange process is security, to verify whether the three servers are authorized server or authorized server

4. PROBLEM DEFINITION

The offers of lapsed prescriptions for cash is the fundamental reason. In the chain, the terminated pharmaceuticals will be returned back to the highest point of the chain. The chain is shown in Fig 1. This prompts the wastage of cash contributed to manufacturing meds and furthermore the vehicle charges for their fare is additionally high. For this issue, they eradicate and republish the expiry date of the medications and dispatches them to the market. They couldn't care less about the general population's lives who take those prescriptions.

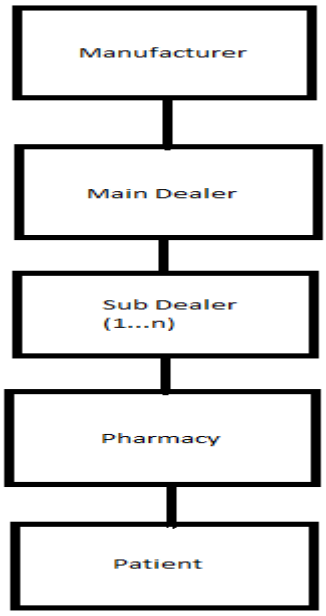

Fig – 1: Chain of medicine transport

5. EXISTING SYSTEM

In the current framework, the creator suggests that the client can check the expiry of the meds by checking the encoded codes. The codes are fixed or imprinted on the drug which can be seen when scratching the region where the code is printed. In the wake of getting that scrambled arbitrary content, they can forward those to the producer who made those meds. At that point, he will answer the client about the solution he purchased and the expiry date of the prescription.

5.1 Disadvantages of the Existing System

• The maker may resell the solutions which are expired.

• The maker is the special case who knows the unscrambling key for that encoded content.

• The client needs to aimlessly trust the maker subtle elements.

• It needs the direct link to the client with the producer.

• Any insidiousness expected individual can duplicate those codes to make copy prescriptions under that maker name which can't be discovered utilizing this framework.

6. IMPLEMENTATION

We proposed another strategy for stopping the reuse of the lapsed prescriptions. We have a few stages of making this issue to an end. The critical techniques utilized here are Near Field Communication (NFC) to get insight about the prescription expiry date. What's more, it likewise gives the

client the detail of the pharmaceutical their use and the measurements. In view of their classification, the client can take the dose. Additionally, it has a portion of the essential notes about the solution like do's and don'ts about the pharmaceutical.

This technique begins with the maker and closures with the client. The technique is made into progress with the assistance of the NFC tag with the codes. Each hub in the chain can make their record by enlisting to the application made particularly for the cell phone. Amid the enrolment procedure, the client can pick their part in the chain. The client might be the patient who purchases the medication for usage or the therapeutic businessperson who purchases the drugs for providing to the patients. The client can check and confirm the dates about the prescription and the insights about the solution which are put away in the NFC tag.

Presently there is another player in this framework a trusted individual who screens the framework from the maker side. He is in charge of the making of the codes and points of interest in the NFC tag. For the reuse of the label that individual just has the authority to revise the codes in the tag. Thus, the producer related loopholes can be fixed.

Presently the maker, sub-merchants, therapeutic businesspeople, and the customers can introduce the application for following points of interest of the solutions. Presently every one of the hubs of the chain is secured, so the patients can get just the great medications. This should be possible by enrolling their profile on the cell phone application. The registration screen is shown in Fig 2. At whatever point they require those subtle elements they can utilize this NFC tag to get the insights about the prescription.

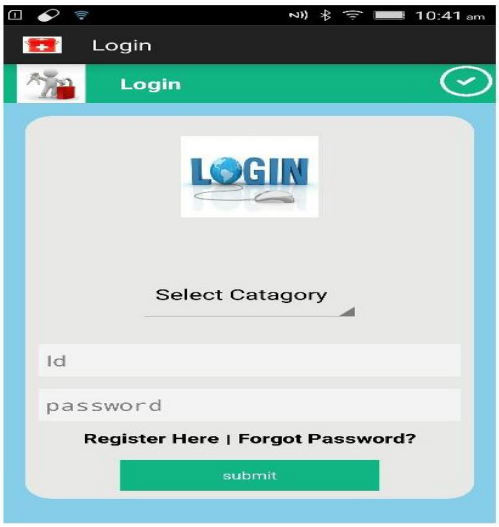

Fig - 2: Registration screen for clients

This aggregate framework depends on the Internet of things (IoT) by which the solution can give the precise and unique insights about the pharmaceutical.

We additionally utilize three servers for keeping up our security. The servers utilized are authentication server, database server, information server. These servers are utilized for the client verification which is the imperative piece of our security. The association is set up just when the security key is sent for verification. On the off chance that the client neglects to verify then the association with the server is impossible.

The NFC label refreshing must be done with a specific end goal to make the points of interest implanted in the tag. It is finished by the verified individual who is on the producer side. The points of interest refreshed in label just can be perused by the client at another end.

6.1 Internet of Things

Web of things alludes to giving the energy of correspondence to this present reality things over the web to make colossal applications. In this proposition, we utilize the web of things which makes the medications to speak with the client. The system association is built up between the client and the NFC label which is joined to the solution.

Amid another stage, the NFC tag is made to shape a system with the trusted individual who has the expert to change the subtle elements in the NFC tag.

6.2 Near Field Communication Tag

The equipment utilized as a part of this proposition is Near Field Communication tag. This is a little label which contains some encrypted code which must be decrypted by the application. So just the first codes can be utilized. It makes the correspondence with cell phone gadgets having a Near Field Communication gadget.

6.3 Advantages of the Proposed System

- Expired meds are totally expelled from the chain
- The client does not have to rely upon any individual in the framework for the getting insights about the solutions
- Duplicate solutions can't be made as the code can't be seen by the client.

7. SECURITY PROTOCOLS AND VERIFICATION

The framework utilizes a portion of the security protocols for making this framework a powerful. The protocols utilized are the Real or Random model (ROR) [7] and furthermore with extra security with session key (SK) security. This area additionally examinations the quality of our framework with a portion of the casual assaults. It likewise demonstrates the security of the framework which is confirmed by AVISPA tool.

7.1. Real or Random Model (ROR)

In this model, the security key is traded safely utilizing cryptography. The key is sent regularly with some arbitrary models and if any of the intrusions happen the gate crasher can't get the right key. Just the recipient can get the right key. This execution makes our framework more compelling in the security concern.

7.2. Session Key (SK) Security

The session key has arbitrarily produced a key which makes our framework more viable in the correspondence framework. The security is made to the following level by the execution of the session key. This key is additionally called a master key as it is utilized to encrypt and decrypt the information. This framework additionally makes the proposal all the more safely transmit the information.

7.3 Replay Attack

This assault should be possible by getting the subtle elements which are in any form (encoded). The assailant will resend this information for the check and for getting access in the session. For the check, he sends the information which is followed by the client and he retransmits similar information to pick up the entrance to the record. This assault can't be performed in our strategy as we utilize the session key strategies which changes the key after some particular session gets over.

7.4 Man in the Middle Attack

In this assault, the aggressor gets in the middle of the two transmitting clients. He at that point peruses every one of the parcels send between them without demonstrating any affirmation. Along these lines, the client may not know and send the information to the system. This sort of assaults is pointless in our framework as the transmitting information are the conclusion to end scrambled so the aggressor can't read the information without the key despite the fact that he gets the parcels. Along these lines, this assault is additionally anticipated in our framework.

7.5 Assurance Against Tag Cloning

A portion of the assailants may endeavor to clone the tag for making the phony meds and discharge them in the market. On the off chance that they cloned the label then the client may not get the right insights about the medications. In this way, our strategy has an extra security highlight in which it keeps the aggressor from making the clones of the tag by keeping the codes secure and it can't be perused by any of the clients. Just the trusted credential has the entire access to the code in the tag.

7.6 Client Impersonation Attack

In the client impersonation attack, the aggressor mimics and carry on like a client to pick up the entrance of the client. This assault can't be performed by the aggressor in our framework. In the event that an aggressor attempted to do the client pantomime assault, the timestamp gets invalid and the framework finds the assailant.

7.7 Server Impersonation Attack

The assailant makes the phony character of the server and tries to get to the next server will be server impersonation assault. In this assault, the assailant can't get the entrance to the system. Our framework is secured by the session key which is just known to the server of the system.

7.8. Mutual Authentication

Our framework additionally has another security highlight in which both server and customer will validate each other. This sort of confirmation is called mutual authentication. This security highlight can take out the aggressor who mimics to assemble access to the system.

8. AVISPA Tool Verification

Automated Validation of Internet Security Protocols and Applications is a broadly utilized device which is utilized for the check of security in any applications. By this apparatus, the programmed confirmation of the security is done and the outcome demonstrates the provisos in the security of the framework by which the aggressor may pick up the entrance to the framework.

9. IMPLEMENTATION

The execution part is done in a few phases. The cell phone application establishment at that point took after by the NFC label refresh. Adding NFC tag to the right pharmaceutical box is additionally one of the vital procedures in this stage. In the event that the individual wrongly labels the crate then the client may get confounded about the pharmaceuticals. Presently the underlying stages get cleared.

Fig – 3 : Ready for Scanning NFC tag

The cell phone application is introduced on each client's gadget. Presently they can make their profile and sign into the framework. Presently the gadget is prepared to scan the NFC tag. The scanning phase is shown in fig 3.

The label refreshing is finished by the trusted individual who is on the manufacturing side.The update process of dosage details is shown in Fig 4. He refreshes the NFC tag and afterward appends the tag to the right meds. Presently the refreshing procedure gets finished. Next, the solutions are transported to the particular spots.

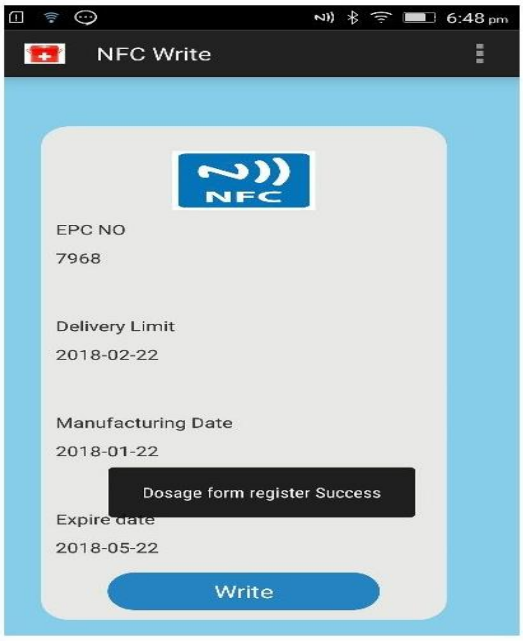

Fig – 4 : Successful dosage form update

Here the labeled medications are gotten by the sub-merchants. Now, the sub-merchants can read the pharmaceutical details with the assistance of the NFC tag.

After the fulfilment of the chain, the patients get the meds. They additionally can check the details of the drugs and expiry date of the prescription by utilizing the tag.

10. CONCLUSION

In this manner, by giving the framework the terminated medicines can be totally dispensed from the market. This technique is turned out to be secure by the AVISPA tool which is a computerized instrument for finding the security protocols. The therapeutic stores have just the unexpired medications. In the event that they give lapsed medications then the client can discover it by utilizing our strategy. Moreover, the client likewise can get the points of interest of the meds and their dosage by utilizing this technique. The security of this framework is additionally high so the shrewd aim people are not ready to carry out any wrongdoing on this framework.

REFERENCES:

[1] S. H. Choi and C. H. Poon, "An RFID-based anti-counterfeiting system,"IAENG Int. J. Comput. Sci., vol. 35, no. 1, pp. 1–12, 2008.

[2] J. Kim, D. Choi, I. Kim, and H. Kim, "Product authentication serviceof consumer's mobile RFID device," in Proc. 10th IEEE Int. Symp.Consum. Electron. (ISCE), St. Petersburg, FL, USA, 2006, pp. 1–6.

[3] A. B. Jeng, L.-C. Chang, and T.-E. Wei, "Survey and remedy of the technologies used for RFID tags against counterfeiting," in Proc. Int.Conf. Mach. Learn. Cybern., Baoding, China, 2009, pp. 2975–2981.

[4] 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, Taichung, Taiwan, 2012, pp. 419–422.

[5] S. H. Choi, B. Yang, H. H. Cheung, and Y. X. Yang, "Data management of RFID-based track-and-trace anti-counterfeiting in apparel supply chain," in Proc. 8th Int. Conf. Internet Technol. Secured Trans.,London, U.K., 2013, pp. 265–269.

[6] P. Tuyls and L. Batina, "RFID-tags for anti-counterfeiting," in Topics in Cryptology—CT-RSA. San Jose, CA, USA: Springer, 2006, pp. 115–131.

[7] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in Proc. 8th Int.Workshop Theory Pract. Public Key Cryptography (PKC), vol. 3386.Les Diablerets, Switzerland, 2005, pp. 65–84.