ANONYMS AUTHENTICATION SCHEME FOR MEDICINE ANTICOUNTERFEITING SYSTEM IN IOT ENVIRONMENT USING NFC

[1] S.Sapna , [2] V.Janani, [3] T.Mahalakshmi, [4] N.Surya

[1] *Stundent, Department of cse, panimalar institute of technology,Sapna.S, chennai, tamil nadu*

[2]*Stundent, Department of cse, panimalar institute of technology,Janani.V, chennai, tamil nadu*

[3]*Stundent, Department of cse, panimalar institute of technology,Mahalakshmi.T, chennai, tamil nadu*

[4]*Assistant Professor, Department of cse, panimalar institute of technology, Surya.N, chennai, tamil nadu*

ABSTRACT

Authentication and privacy protection are important security mechanisms for keeping things safe in the Internet of Things environments. In particular, an anonymous authentication scheme is a privacy preserving authentication technique which provides both authentication and privacy preservation. An authentication scheme with anonymity in mobility networks was proposed recently. However, it was proven that it failed to provide anonymity against passive adversaries and malicious users and security against known session key attacks and side channel attacks. We propose an anonymous authentication scheme for intercommunication between the things in the Internet of Things environments. The proposed scheme provides not only anonymity and security, but also untraceability for the thing. Moreover, we only use low cost functions, such as hash functions and exclusive-OR operations in consideration of limited computing power of the thing.

Keywords – *Internet of Things, Authentication scheme, Radio frequency identification(RFID), Public key Cryptosystem(PKC)*

1. INTRODUCTION

Counterfeit medicine as "one which is deliberately and fraudulently mislabeled with respect to identity and/or source".Counterfeiting of various products creates problem to different manufacturing industries such as food and beverage, automotive parts, software, cosmetic, jewelery, etc. It causes serious threat to pharmaceuticals products. People, who purchase and use counterfeit medicines, suffer a lot because these medicines do not provide any relief to their diseases. The concern issue threatens the public health and also causes revenue losses to the legitimate manufacturing organizations.According to WHO data, there are about 100 000 deaths happened in a year in Africa due to use of counterfeit drugs.The British "International Policy Network" estimated that 700 000 deaths in a year are happened due to the use of counterfeit malaria and tuberculosis drugs. Counterfeiting can be happened with branded as well as generic products. WHO further noticed that more than 30% of medicines on sale are counterfeited in some part of Africa, Asia and Latin America. After authentication of drug package, the system responses with a text message accordingly whether it is fake/actual. Thus, a consumer can easily come to know the authenticity of the drug package very easily and without any cost. However, the drawback with this technique is that

it is not fully automated as the consumer first needs to scratch off the label, and then to type the code and send to the system, which requires a lot of users involvement . The radio frequency identification (RFID) permits identification of unique items which use radio waves. An RFID reader typically communicates with RFID tags that contain digital information in microchips [5]. RFID-based anti-counterfeiting technology has emerged as an effective tool to prevent counterfeiting, because it complements the commonly used anticounterfeiting methods (for example, colors, shifting inks,fingerprints and chemical markers) . These methods, however, do not use the automatic verification of product authenticity. Device-to-device (D2D) communications is a type of technology which enables devices to communicate directly with each other without the involvement of fixed networking infrastructures (for example, access point and base station) .

2. PROBLEM DEFINITION

The drawback with this technique is that it is not fully automated as the consumer first needs to scratch off the label, and then to type the code and send to the system, which requires a lot of users involvement.

3. EXISTING SYSTEM

In our existing system the manufacturing organizations use label on the drug packages with an encrypted code. When a customer/consumer wants to buy that drug, he/she scratches off the label on the drug package and text the code to the system of company which authenticates the drug package without any charge. After authentication of drug package, the system responses with a text message accordingly whether it is fake/actual. Thus, a consumer can easily come to know the authenticity of the drug package very easily and without any cost.

4. PROPOSED WORK

The proposed scheme is also capable to prevent the counterfeiting of medicine dosage forms. It further provides secure mutual authentication between the NFC tag placed on a dosage form and the server. In the proposed scheme a NFC enabled mobile device acts as an interface between the NFC tag and the server,which reads the information, stored in the NFC tag and sends the information to the server. The server verifies the authenticity of the dosage forms and sends response to the NFC enabled mobile device user. On the basis of the response received from the server, the customer (patient) can take his/her decision whether to purchase that medicine or not.

5. WORKING PRINCIPLE

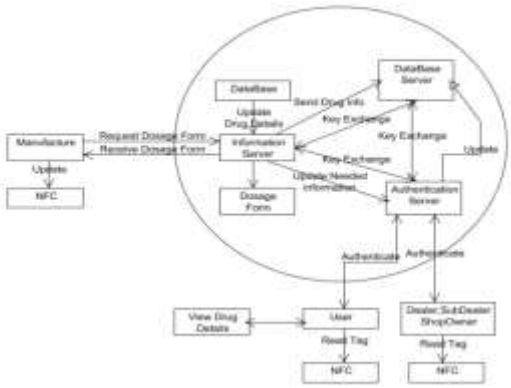

Fig- **1 Architecture diagram**

The system architecture of medicine anticounterfeiting in IoT environment. As we know in IoT every physical objects such as servers, MUs have an IP address for Internet connectivity, all these devices communicate to each other using the Internet. In the given architecture, we have three different types of servers: 1) information server *(*IS*i)*; 2) authentication server *(*AS*j)*; and 3) database server *(*DS*k)*. Apart from that we have MU at the manufacturer site and a customer who wants to buy the medicine's dosage forms. Both user at the manufacturer site and customer can communicate with the servers. Note that all users have near field (NFC) enabled mobile device and all servers are able to communicate with each other. Initially, each manufacturer at the manufacturer site registers the details of dosage forms (package) to the information server using their NFC enabled mobile device. After the successful registration *(*IS*i)* sends this information to AS*j* and DS*k*. This considered architecture is different from the existing architecture [5]. In this architecture AS*j* has the complete information which is required to check the authenticity of the dosage forms. Therefore we are not using any pedigree server which is available in the current architectures [5]. During the authentication process some screened records are generated at AS*j* which are then sent to DS*k* for storage. These records will be then used for the future authentication. The steps involved in dosage forms anti-counterfeiting process are given in Section I-B The roles of various servers are described below.

5.1 Information Server (ISi)

The initial registration of each dosage form is done at IS*i*. In addition, IS*i* sends the registration information of dosage forms to AS*j* and DS*k*.

5.2 Authentication Server (ASj*)*

It is used for the authentication of the dosage form. It authenticates the dosage form on the basis of the information provided by the IS*i*. It also sends the authentication response (whether fake or real) to the customer/patient and also to the DS*k*.

5.3 Database Server (DSk)

It stores the information provided by the IS*i* and AS*j*. The screened records generated during the authentication process are stored in DS*k*. In the proposed scheme, an NFC tag is updated after each successful authentication process. This server maintains these records. If there are *n* number of sites between the manufacturing organization and a customer (consumer), the NFC tag needs to be updated at these sites. These information are also stored at this server. By seeing these records, the authority (i.e., database administrator) can observe who, when and where the NFC tag was updated, and it will be useful in cross checking whether the NFC tag is updated by a legal intermediate party. It is not desirable to maintain all these records at the AS*j*, because we want to dedicate authentication process solely on the AS*j*. Due to this reason, the role of DS*k* is sential.

5.4 Implementation Site

The proposed medicine anticounterfeiting system in IoT environment is efficient and has more usability as it suits the mobile environment. As far as implementation is concerned the pharmaceutical companies can also implement this type of anti-counterfeiting system in their information technology department. But this act will not be fully trusted by the customers/patients. So, it would be betterif a trusted third party, say digital anti-counterfeiting party, can implement this type of system.

5.5 Usability of the Proposed System

Our scheme is secure as well as user friendly. A customer (patient) just needs the NFC enabled mobile device with the Internet connectivity to check authenticity of medicine package. So, the user can perform anti-counterfeiting process anywhere, anytime in any part of the world.

6. STEPS FOR ANTI COUNTERFEITING PROCESS

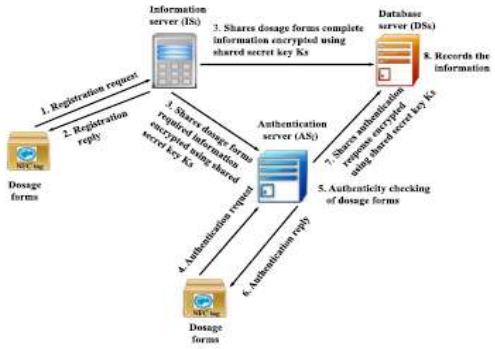

Fig -2Anti counterfeiting process

steps involved in dosage forms anti-counterfeiting process and also discussed below. 1) In the first step the user at the manufacturer site registers the medicine's dosage forms to the *(*IS*i)*. IS*i* then computes some information which is required for the authentication process and sends this to the NFC tag of the dosage forms for storage. Steps involved in dosage forms anti-counterfeiting process. Structure of EPC. The IS*i* shares the dosage forms complete information with the *(*DS*k)* and the limited information which is only used for the authentication to the *(*AS*j)*.To check the authenticity of the dosage forms the customer/patient sends authentication request to AS*j*, then AS*j* checks the authenticity of the dosage forms and response to the patient accordingly. AS*j* also shares authentication response with DS*k*. DS*k* stores all screened records which can be used in the future authentications/transactions process. Each medicine package has an NFC tag, which contains various information related to the product. It consists of an electronic product code *(*EPC*)* [19]. An EPC is a universal identifier that provides unique identity of some physical object and it can be easily stored in NFC tag [20]. Two identical products can be distinguished by the EPC. EPC contains several information such as product's manufacturing date, its origin, batch number, etc. The basic format of the EPC is given in It contains the following fields: 1) header; 2) EPC manager number; 3) object class *(*OC*)*; and 4) serial number *(*SN*)*. The header field identifies the length, type and version of EPC. The EPC manager number maintains the subsequent partitions. The SN field is a unique SN for each EPC. The lengths of header, EPC manager number, OC, and SN are 8, 28, 24, and 36 bits, respectively. Thus, the total length of EPC is 96 bits.

7. EXPERIMENTAL RESULTS

7.1 Login, Registration

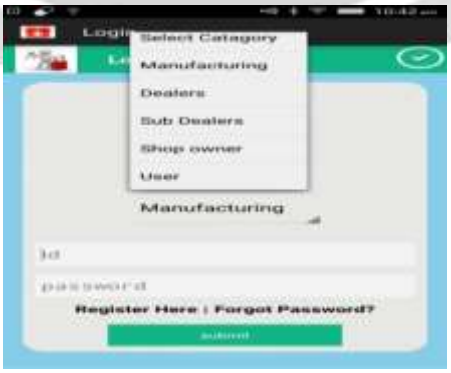

Fig -3 Login, Registration

7.2 Manufacturing register

Fig-4 Manufacturing register

7.3 Manufacturing Login

Fig -5 Manufacturing Login

7.4 Dealer register

Fig -6 Dealer register

7.5 Dealer login

Fig -7 Dealer login

7.6 Sub dealer login

Fig -8 Sub dealer login

7.7 Sub dealer register

Fig -9 Sub dealer register

7.8 User registration

Fig -10 User registration

7.9 User login

Fig -11 User login

8. CONCLUSION

Anonyms Authentication Scheme for Medicine Anticounterfeiting System in IoT Environment using NFC medicine's dosage forms. The proposed scheme is shown to be secure against various known attacks. Furthermore, the formal security verification using the powerful and broadly used AVIPSA tool shows that the proposed scheme is secure. Our scheme is comparable in terms of computation and communication costs, and also provides additional functionality features as compared to other existing schemes. In addition, we have implemented the proposed scheme using the widely accepted NS2 simulator and the simulation results demonstrate the practicability of the scheme. Overall, better tradeoff among security, additional functionality features and efficiency shows that the proposed scheme is appropriate for the anti-counterfeiting of medicine's dosage forms.

9. ACKNOWLEDGEMENT

We express our sincere thankfulness to our Project Guide **Mrs.N.Surya** for her successful guidance to our project. Without the help it would be a tough job for us to accomplish this task. We thank our guide for her consistent guidance, encouragement and motivation throughout our period of work. We also thank our Head of the Department (CSE) **Dr.V.Subedha** for providing us all the necessary facilities.

REFERENCE

[1] Mohammad Wazid (S'17) received the M.Tech. degree in computer network engineering from Graphic Era University, Dehradun, India. He is currently pursuing the Ph.D. degree with the International Institute of Information Technology, Hyderabad, Hyderabad, India. His current research interests include security, remote user authentication, Internet of Things, and cloud computing. He has published over 40 papers in international journals and conferences in the aboveb areas. Mr. Wazid was a recipient of the University Gold Medal and the Young Scientist Award by UCOST, Department of Science and Technology, Government of Uttarakhand, India.

[2] Ashok Kumar Das (M'17) received the Ph.D. degree in computer science and engineering, M.Tech. degree in computer science and data processing, and M.Sc. degree in mathematics from IIT Kharagpur, Kharagpur, India. He is currently an Assistant Professor with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, Hyderabad, India. His current research interests include cryptography, wireless sensor network security, security in vehicular ad hoc networks, smart grid, Internet of Things (IoT) and cloud computing, and remote user authentication. He has authored over 130 papers in international journals and conferences in the above areas. Dr. Das was a recipient of the Institute Silver Medal from IIT Kharagpur. He is in the Editorial Board of the *KSII Transactions on Internet and Information Systems* and the *International Journal of Internet Technology and Secured Transactions* (Inderscience), and a Guest Editor for the

Computers and Electrical Engineering (Elsevier) for the special issue on big data and IoT in e-healthcare, and has served as a Program Committee Member in several
international conferences.

[3] Muhammad Khurram Khan (M'07–SM'12) is currently a Full Professor with the Center of Excellence in Information Assurance, King Saud University, Saudi Arabia. He has edited seven books and proceedings published by Springer-Verlag and the IEEE. He has published over 300 papers in international journals and conferences and he is an inventor of several U.S./PCT patents. His current research interests include cybersecurity, biometrics, multimedia security, and digital authentication. Dr. Khan is a Fellow of the IET, U.K., the BCS, U.K., the FTRA, Korea, and a member of the IEEE Technical Committee on Security and Privacy and the IEEE Cybersecurity Community. He is the Editor-in-Chief of a well-reputed journal *Telecommunication Systems*. He is also on the Editorial Board of several international journals, including the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, *Journal of Network and Computer Applications*, *IEEE Communications Magazine*, IEEE ACCESS, IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, *IEEE Consumer Electronics Magazine*, *PLoS ONE*, *Security & Communication Networks*, *Electronics Commerce Research*, and *IET Wireless Sensor Systems*.

[4] Abdulatif Al-Dhawailie Al-Ghaiheb received the Ph.D. degree in clinical pharmacy (pharmacokinetic/dynamic) and M.Sc. degree in pharmacy from the Queen's University of Belfast, Belfast, U.K. He is currently a Full Professor of Clinical Pharmacy with the College of Pharmacy, King Saud University, Riyadh, Saudi Arabia. His current research interests include information security and cloud computing. **Neeraj Kumar** (M'16) received the Ph.D. degree in computer science and engineering from Shri Mata Vaishno Devi University, Katra, India, in 2009. He was a Post-Doctoral Research Fellow with Coventry University, Coventry, U.K. He is currently an Associate Professor with the Department of Computer Science and Engineering, Thapar University, Patiala, India. He has authored over 160 technical research papers published in leading journals and conferences. Some of his research findings are published in top cited journals, such as the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, the IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, the IEEE NETWORK, the IEEE COMMUNICATIONS, the IEEE WIRELESS COMMUNICATIONS, the IEEE INTERNET OF THINGS JOURNAL, and the IEEE SYSTEMS JOURNAL. He has guided several Ph.D. and M.E./M.Tech. research scholars.
Athanasios V. Vasilakos (SM'11) is currently a Professor with the Luleå University of Technology, Luleå, Sweden. He has published over 500 technical research papers in leading journals and conferences in his areas of research. Dr. Vasilakos served or is serving as an Editor for several technical journals, such as the IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, the IEEE TRANSACTIONS ON CLOUD COMPUTING, the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, the IEEE TRANSACTIONS ON CYBERNETICS, the IEEE TRANSACTIONS ON NANOBIOSCIENCE, the IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE, the IEEE TRANSACTIONS ON CLOUD COMPUTING, the *IEEE Communication Magazine*, *ACM Transactions on Autonomous and Adaptive Systems*, the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, and *ACM Transactions on Autonomous and Adaptive Systems*. He is also the General Chair of the European Alli