International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 25 Issue 7 – JUNE 2018.

# U-Prove Based Heuristic Optimization for Crowdsourced Authentication in E-Health network

A.Reka [#1] and B.Narmada [*2]

[#] *PG Scholar, Department of CSE, Dhirajlal Gandhi College of Technology, Salem*

[*] *Assistant Professor, Department of CSE, Dhirajlal Gandhi College of Technology, Salem*

***Abstract*— In eHealth networks has huge number of data records is to be available in big era. The patient's record is to be monitored and analyzed through the sensors. The patient's data records is to be collected it into the big data and provides the security then, we propose a U-prove based cybersecurity it carries a limited amount of information is to be stored under the authentication and verification process. It is a token based process is proposed for mobile device application to secure the patients data records in eHealth care environment. The authorized user developing a variety of authentication mechanisms like PIN, Password, Pattern etc.., to secure the information about patient's record.**

***Index Terms*— Big Data, Cybersecurity, eHealthcare, mobile applications, U-prove.**

## I. INTRODUCTION

A network is a cluster of two or more computer systems connected together. There are two types of computer networks. They are wired and wireless networks. The topology, protocol and architecture are the important characteristics of the networks. In wireless networks, the computers or any wireless devices are connected to form a network without wires. A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. Each system may also acts as nodes or as sensors. Here comes a sensor networks. When sensor devices form a network is called a sensor networks.

Wireless Sensor Network (WSN) are commonly distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, Pressure, vibration, etc. and to pass their data through the network to base station. Wireless Sensor Networks (WSN) consists of a large number of sensor nodes. The sensor nodes can be deployed either inside or very close to the sensed phenomenon. A sensor is the device which converts a physical phenomenon and also sound phenomenon to the electric signals e.g. heat, light, motion, vibration etc..,The more modern networks are bi-directional, also used for control the sensor activity.

The development of wireless sensor networks was motivated by some applications like military such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial procedural monitoring and control, structural health monitoring, and so on. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors. The topology of the WSNs can vary from a trouble-free network to an advanced multi-hop wireless mesh network.

In today's world, numerous challenges are faced regarding healthcare including the rise of chronic, non-communicable diseases, ever increasing healthcare costs, and aging societies. In order to cope with these challenges, Healthcare ecosystems have to evolve. The transition of the healthcare ecosystems from hospital centered, specialist focused approaches to distributed, patient centered care models are in full swing [2].This is strongly supported by the progressive deployment ofthe Internet of Things in healthcare and new strategies such ascyber-physical system based approaches under Industries 4.0 ormore precisely Health 4.0 [3, 4]. The flow of information willbe enhanced and facilitated by the 5th generation of mobilenetwork technology (5G) which will also enable device andnetwork virtualization and service aggregation [5].

Future health strategies such as Individualized Medicine / Precision Medicine are designed to enhance quality of experience, reduce dependencies and release efficiency reserves, especially in the context of the (self)-management of chronic,non-communicable disease [6]. However, at the same time, italso raises security and privacy concerns related to sensitivemedical information [7]. The more distributed the systemgrows, the higher the risks associated with the mobility of data and services.

Security and privacy are vital aspects of eHealth care systems and medical data records [8, 9]. In order to secure the patients' data in the more and more distributed eHealthcare environment, the development of strong and secure authentication mechanisms are inevitable for mobile devices. Mobile devices are the integral part of eHeathcare systems. Currently, most of the healthcare services are accessed through mobile devices (mHealth). To this end, various security measures have been taken by developing a variety of authentication mechanisms for mobile devices. However, most of them are knowledge-based mechanisms, for instance password, PIN, and secret patterns etc., which are vulnerable

to different security threats [10, 11]. Similarly, standard encryption technologies such as symmetric key encryption e.g.,advanced encryption standard (AES), and public key encryption e.g., Rivest, Shamir and Adleman (RSA), are not suitable for eHealth care environment [12, 13]. Therefore, there is a need for secure, efficient, and simple authentication mechanism for mobile devices, particularly in the eHealth care environment.

Recently, authentication technologies that incorporate attribute-based credentials have been developed for anonymous authentication [14-16]. U-prove [14] is one of such technologies, which has been developed by Credentica and taken over by Microsoft in 2008. Compared to other such technologies, U-prove is simple and efficient. U-prove has a claims-based architecture, which involves prover i.e., user, issuer and verifier. The issuer issues tokens to the user, which contain attribute based credentials. The token is similar to a public key infrastructure (PKI) certificate; however, with two main differences i.e., it provides intractability and minimal disclosure of the attributes.

Generally, U-Prove technology operates based on two main protocols: (1) issuance protocol, (2) presentation protocol or proving protocol. During the issuance protocol, the token is generated by combining the issuer's public key with the user's attributes. The issuer then signs the token for authentication with a blind signature mechanism. During the second protocol, i.e., the presentation protocol, the user presents the token to the verifier and disclose few numbers of attributes based on zero knowledge protocol in order to get access to the services. The verifier verifies the authenticity of the token from the issuer's signature. For further details regarding U-Prove technology, refer to [14].

## II. Related Work

There has been a great concern about massive volume of data for crowdsourced networks in academia and industry. One of the most obvious concern comes with how to process these data. In [8]_[10], we have proposed a data processing architecture for mobile eHealth network. WSNs are progressively becoming relevant for SHM applications, focusing on trustworthy collections of raw signals at relatively high synchronization [1], [3], [5], and [6]. Here, only discussing the sensor deployment view. Various best possible sensor deployment methods from engineering domains have been used for wired network systems. Some WSN devices are used and verified with an interest in knowing whether a wireless sensor device is best suitable for SHM [1]. These are also are not very alarmed with the effects of sensor faults, transmission faults, WSN separation, etc., on a deployed WSN on a structure. It may affect the performance of the sensor while monitoring the health status.

Zhang *et al.* designed a novel community-

centric framework to predict community activities [4]. The framework consists of community detection and community activity modeling. It extracts community activity patterns from big data collected physically and virtually. Kuang *et al.*proposed a unified tensor model [5]. This model can represent unstructured, semistructured, and structured data with a tensor model. In detail, each kind of data is represented by a subtensor, which is finally merged with a unified tensor. Also, a small but valuable core tensor is extracted using an incremental high order singular value decomposition.sw3

The monitoring health records has to be transmitted it into the patients credential process.The data is to be collected and stored under the authentication and verification process. Anonymous authentication of mobile devices is made in [12] by developing a secure authentication scheme. However, this scheme is based on elliptic curve scheme and pairings. Moreover, for the credentials non-transferability and security, the scheme uses the existing embedded mobile devices hardware security feature.Additionally, in this scheme, the issuer of credentials is the network operator. Similar scheme is developed in [13] for mobile devices accessing location-based services. Nevertheless, this scheme is comparatively more flexible and does not require mobile devices embedded hardware security feature for credential sharing prevention and security. On the other hand, while considering the anonymous attribute based authentication systems, Microsoft's U-Prove technology [14] is one of the most simple, efficient and widely used anonymous attribute based credentials (ABC) technologies in the public key infrastructure (PKI) domain. It is more powerful than the schemes in [12, 13] and has been adopted in various identity management systems, for instance, for anonymous credentials on electronic identity (eID) smart cards etc.

Moreover, in [28] a solution is developed for the secure mobile payment using nearfield communication (NFC) enabled mobile device and smart card with anonymous attribute based credentials technology like U-Prove. The NFC acts as a bridge between the secure credentials on smart card and the corresponding service providers. Similarly, in [29] the combined use of mobile phone and tamper resistant smart card, that could carry attribute based credentials such as U-Prove, is presented for online authentication. The mobile phone acts as a trusted card reader by scanning the credentials from the smart card via NFC and send them via secure channel to the verifier for the user authentication and authorization. The authors have studied U-Prove and involve trusted couple to supports personal attribute management and credential issuance that results in privacy-friendly and secure authentication. Furthermore, in [30] a healthcare architecture coupled with digital technology such as NFC and Bluetooth enabled android based mobile device and secure smart card capable of retainingthe secure credentials and EHR is proposed. The smart card could be in the form of external tag or it could be retained on the mobile device through card emulation or NFC P2P.

TheHealthcards and mobile devices are authenticated and authorized from a centralized hybrid cloud environment, which also provides the storage backup of EHR. Furthermore, for accessing the NFC tags, a weak MIFARE classic security algorithm Crypto 1 is used. However, the use of attribute-based

encryption is intended in their future work. On the other hand, the security authority in [31], which is a central point of contact in an open eHealth service platform from the project called data capture and auto identification reference (DACAR), incorporates the U-Prove technology for the

authentication and authorization of the users. In addition, Nastou et al. [32] in their discussion explain U-Prove by Microsoft that is based on cryptographic primitives and relies on difficulty of discrete logarithms. In [21], Hajny et al. state that the cryptographic ABC schemes have very few practical implementations till date and are mostly implemented on smart card. Furthermore, the existing solutions like in case of U Prove, the sessions are online unless several tokens are issued in advance. In this context the authors present a scheme specifically for physical access control applications that can work even in offline mode while avoiding collusion attacks in 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom) case of insecure hardware. The architecture of the given scheme includes entities that are issuer, revocation referee, user, and verifier.

The scheme is able to provide unlinkability, untraceable attribute verification, and anonymous. It utilizes two key cryptographic primitives, first one is the non interactive zero-knowledge proof of knowledge (PK) protocolsand other is based on the commitment schemes. The authors have conducted security analysis on the basis of the prior security proofs on RSA, OU, and DSA groups. Here, the main contribution of the authors is the implementation of common cryptographic primitives of ABCs, benchmarking on mobile devices and some of the outcomes.

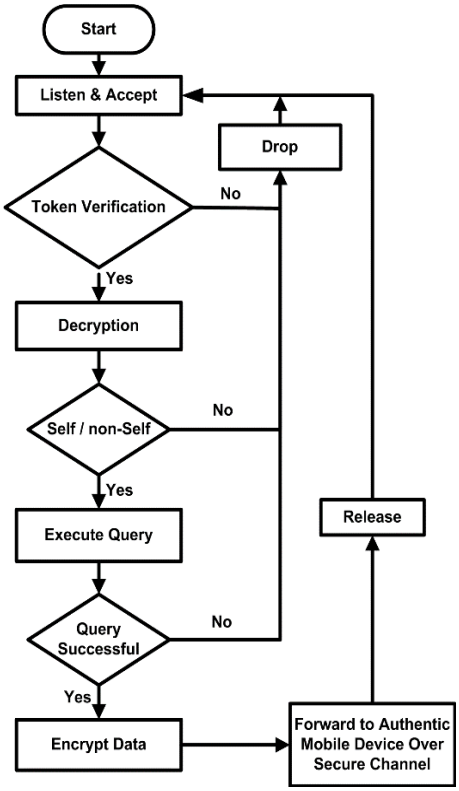


Fig 3.1 Process Flow at hospital server

## III. METHODOLOGY

On this paper, we present a at ease authentication framework for ehealthcare environment. in the proposed system, we include u-prove technology for authentication, privacy preserving information sharing, and comfy verbal exchange among hand-held devices. The framework of the proposed system is shown in discer the device involves servers that preserve the disbursed database of body of workers, patients, ehr, digital gadgets, and secure ehealth app as shown in discern moreover, so as to manage the cell gadgets authentication and verbal exchange protection, a u-provetechnology based totally server is carried out as proven in determine the server authenticates the cell gadgets with the aid of issuing them u prove tokens that include attribute primarily based credentials.

Such mobile-based tokens authorize the specialised fitness-caregiver to access the affected person's ehr from principal database in addition to directly from clinical devices implanted on the patient's frame. For a new tool to be registered in the device, the app is first downloaded via the person from the app server as given in discern. After the app is being mounted, the person registers himself in the database. Inside the 0.33 step, the cell device data of the registered person is accumulated by the app and is

securely transferred to the improved authentication and authorization server. The server receives the comfy massage, authenticate it and reply with the name of the game code on the registered cell range. This code is random this is regenerated through the server at every login and is makes use of as the general public key to talk and decrypt server packets. if the user presents the app with secret code, the app is then legal with the services for which the user is eligible. in this manner, the cozy app synchronizes and collects statistics by using fetching the hand-held tool facts consisting of, imei, mac, and sim card numbers, at the side of different attributes for example, patients ids, medical devices ids, issue fitness-caregiver ids and so on. u-show primarily based authentication & authorization method 2016 ieee 18th global conference on e-health networking, applications and offerings (healthcom) then this information is encrypted and forwarded it to the u-prove generation primarily based authentication server in reaction, on server aspect the u-show technology issuing protocol generates the tokens in step with the attributes that are obtained from the cellular gadgets as proven in step four of parent [2]. These attributes based totally tokens

are securely transferred to the authenticated mobile tool.

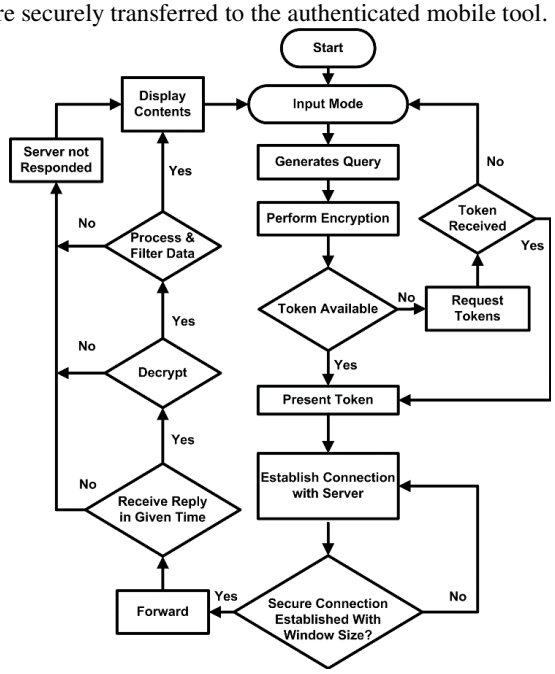


Fig 3.2 process flow at customer side

The authorized customers use such tokens to get right of entry to the information from crucial database by using verifying the concern gadgets using the presentation protocol as shown in step five and step 6, respectively, of parent 2. In addition, the legal person can also without delay get admission to the data from the ehealth kits/implanted devices by way of matching the token to the pre-registered policy primarily based attributes on such gadgets i.e., such devices work as a verifier in this scenario, as proven in step 7 and eight of discern 2. Hence, the hand held device with the medical doctor or nurse can perform direct conversation with the neighboring implanted gadgets or ehealth kits [37] based on assigned tokens. specifically, to those devices which might be pre-registered and are linked below patient's database whilst turning in to the legal nurse. these kits screen the specified physiological values consisting of ecg, glucose, bp etc., and ahead to the database server and/or to the legal hand held devices as a consequence. Furthermore, the server authorizes the services to the authenticated device based at the credentials. Moreover, the float chart of the entire method at server

facet is given in figure 3. the server first stays in concentrate and be given mode. While statistics is obtained, the server first verifies the token and then try and decrypt it primarily based on private key fig. three. procedure drift at server facet if decryption is a success the statistics packet is categorised as self, else in the case of non-self the server drops the newly receive data and goes again to listen and accept mode. Self statistics is then authenticated further based totally on tokens and according to the consumer stage, the privileges are given. The query is then executed based totally on the get entry to rights. The successfully accrued statistics is encrypted and forwarded to the authentic mobile device over a comfy channel. In case the question does not execute, the whole procedure is dropped and server is going returned into the concentrate and be given mode. Further, parent four offers the system at the patron side. In step one, because the person starts the software on his/her hand-held tool, it is going into an input mode. In keeping with the requirements of user, the app generates the question for the server and/or for the device, in case of direct device to system verbal exchange [37]. The entire section is then encrypted based at the random public key. In addition, the offline tokens are checked, if available the token is assigned to this encrypted segment. In any other case, the improved u-show based authentication and authorization server is asked for the tokens. Onwards, with a purpose to get right of entry to the services, these tokens are used to verify the concern gadgets by using the relevant database and different devices which will grant authorize access to the privileged users and to comfortable the relaxation of the communique. The tokens encompass the aforementioned attributes of every actor inside the ehealthcare state of affairs, a part of which can be disclosedthroughout the authorization and verificationsystem for getting access to the offerings.

## IV. Security Analysis

In this phase, we analyze the security of the proposedframework in phrases of the protocols used. We highlight the security factors of both the at ease communication initialization, the token issuance / presentation, and the records communique the usage of the endorse framework in the healthcare surroundings. even though the verifiers always accept simplest thesincere users primarily based on the proper credentials within the relaxed token but, which will keep away from any protection breach, a secure channel is wanted between the verifier and prover in addition to among the provider and prover [38].

Further, a relaxed connection is needed for the initial communication among the consumer and server when the utility is logging in. likewise, a comfy communique channel wishes to be maintained after gaining access to the statistics using u-prove token.In the proposed framework, this is achieved through the use of randomize public key infrastructure. Due to the fact the dynamic identification for specific classes' login is relaxed [39, 40] and similarly, the generation of random keys insure secure network cease to stop communications [41]. Moreover, it's far supplied in [19] that due to the cozy nature of the personal key in the u-show technology, using u-show token mitigates assault which include eaves dropping or replay. correspondingly, u-prove presents unlinkability and privateness due to the fact the issuer makes use of blind signature to sign the token and the prover makes use of zero-understanding protocol when provides the token [19, 42].

Consequently, normal assaults such as

phishing, jamming, relay, and physical attacks the use of a sidechannel, phone robbery or loss, malware on phones, and maximum of the cyberattacks on ehealthcare utility primarily based cell device are tackled with the aid of the proposed safety mechanism. That is because of random public key based comfy tunneling with the tokens presentation based totally mobile tool authentication. The attacker does no longer avail the credentials because of dynamicity and cannot

generate evidence.

Moreover, there are and more devices / factors worried to authenticate. In case of loss without consumer info and greater than that with out protection code a public key from server, the relaxed ehealth app on cell device will now not login to set up relaxed channel with server for conversation. On the other hand, maximum of the prevailing authentication methods are knowledge-based totally, as an example password, pin, and mystery patterns and so forth., which might be prone to one of a kind security threats [10, 11]. Further, trendy encryption technology which include symmetric key encryption e.g., advanced encryption widespread (aes), and public key encryption e.g., rivest, shamir and adleman (rsa), aren't appropriate for ehealthcare surroundings [12, 13]. Conversely, schemes for Hippocratic records exchange based on honest non-repudiation (fnr) techniques which includes [43], and other such mechanisms are not feasible for mobile gadgets in ehealth networks. Consequently, the proposed framework is cozy and appropriate for ehealthcaresurroundings.

## V. CONCLUSION

In this paper, the enhanced U-Prove technology based security framework is proposed to authenticate and authorize a mobile device in both modes, whether offline or online. Firstly, we have to be collect the data's from sensor and transfer/make it into the document or report. It has to be analysed through the server side When the server does not respond the device works in offline mode to acquire real time data directly from the implanted devices and/or eHealth kit. We have to be proceed some process flow diagram to extract the information. Last but not the least; we present the security analysis that shows the strength of the proposed security mechanism.

## REFERENCES

[1] M. Z. A. Bhuiyan, G. Wang, and J. Cao, "Sensor placement with multiple objectives for structural health monitoring in WSNs," in IEEE 9th Int. Conf. High Perform. Comput. commun. (HPCC), 2012, pp. 699–706.

[2] M. Z. A. Bhuiyan, J. Cao, G. Wang, and X. Liu, "Energy-efficient and fault-tolerant structural health monitoring in wireless sensor networks," in Proc. IEEE 31st Symp. Reliable Distrib. Syst. (SRDS), 2012, pp. 301–310.

[3] C. Buragohain, D. Agrawal, and S. Suri, "Power Aware Routing for Sensor Database," Proc. IEEE INFOCOM, 2005.

[4] P. Cheng, C. N. Chuah, and X. Liu, "Energy-aware node placement in wireless sensor network," in Proc. Global Telecommunication. Conf.(GLOBECOM), 2004, pp. 3210–3214.

[5] Heo G, Wang ML, Satpathi D. "Optimal transducer placement for health monitoring of long span bridge". Soil Dynamics and earthquake Engineering 1997; 16:495–502.

[6] D. C. Kammer, "Sensor placement for on-orbit modal identification and correlation of large space structures," J. Guid. Control. Dyn., vol. 14, no. 2, pp. 251–259, 1991.

[7] S. Kim, S. Pakzad, D. Culler, J. Demmel, G. Fenves, S. Glaser, and M. Turon, "Health monitoring of civil infrastructures using wireless sensor networks," in Proc. 6th Int. Symp. Inform. Process. Sensor Networks (IPSN), 2007, pp. 254–263.

[8] G. Hackmann, F. Sun, N. Castaneda, C. Lu, and S. Dyke, "A holistic approach to decentralized structural damage localization using wireless sensor networks," Comput. Commun., vol. 36, no.

[9] C. Humer and J. Finkle, Your medical record is worth more to hackersthan your credit card. ed. Re uters, 2014, avilable at: http://www.reuters.com/article/us-cybersecurity-hospitalsidUSKCN0HJ21I20140924.

[10] S. A. Fricker, C. Thümmler, and A. Gavras (Editors), Requirements Engineering for Digital Health: Springer, 2015.

[11] O. Vermesan and P. Friess, Building the Hyper-connected Society: River Publishers, 2015.

[12] M. Hermann, T. Pentek, and B. Otto, Design principles for Industrie 4.0 scenarios: A literature review. fakultät Maschinenbau, Audi Stiftungs lehrstuhl Supply Net Order Management. Dortmund:Technische Universität Dortmund, p.15, 2015, avialable at: http://www.leorobotics.nl/sites/leorobotics.nl/files/bestanden/2015%20-%20Hermann%20Pentek%20%26%20Otto%20-%20Design%20Principles%20for%20Industrie%204%20Scenarios.pdf.

[13] European 5G PPP Association (2015), White Paper on eHealth Vertical Sector, avialable at: https://5g-ppp.eu/wp content/uploads/2016/02/5GPPP-White-Paper-on-eHealth-Vertical-Sector.pdf.

[14] F. S. Collins and H. Varmus, "A new initiative on precision medicine, "New England Journal of Medicine, vol. 372, pp. 793 – 795, 2015.

[15] B. M. Silva, J. J. Rodrigues, I. de la Torre Díez, M. López-Coronado, and K. Saleem, "Mobile health: a review of current state in 2015,"Journal of biomedical informatics, vol. 56, pp. 265 – 272, 2015.

[16] S. Avancha, A. Baxi, and D. Kotz, "Privacy in mobile technology for personal healthcare," ACM Computing Surveys (CSUR), vol. 45, p. 3, 2012.

[17] A. Gawanmeh, H. Al-Hamadi, M. Al-Qutayri, S.- K. Chin, and K. Saleem, "Reliability analysis of healthcare information systems: State of the art and future directions," in 17th IEEE International Conference onE-health Networking, Application & Services (HealthCom), Oct. 2015,pp. 68 – 74.