Secure Fuzzy Extractor based remote user validation scheme for Wearable devices

J. Gowthami,
Dept. of Computer Science and Engineering,
Kongu Engineering college,
Erode, India.

Dr. N. Shanthi,
Dept. of Computer Science and Engineering,
Kongu Engineering college,
Erode, India.

***Abstract*— With the rapid development of the Internet of Things (IoT), wearable technology is gaining a significant importance in the recent era. Major applications of wearable technology are fitness trackers, healthcare, smart shoes, sleeping cycles, wearable computers, smart watches etc. These intelligent devices function in conjunction with mobile terminals to provide ease of access and data analysis of sensitive information, generated from the wearable devices. The data from these devices are private data of users and authentication plays a major role in securing these data against the illegal access.**

This paper presents a Fuzzy extractor adopted authentication scheme for legitimate access of information from the wearable devices. This scheme promotes session key generation and mutual authentication. Further, the security can be enhanced with the use of Fuzzy Extractor for session key agreement. The mechanism proposed is validated with the use of most used AVISPA (Automated Validation of Internet Security Protocols and Applications) tool and the result obtained assures that it is strong against various security attacks. Also, the functionality feature analysis confesses the efficiency of the proposed scheme. Thus the remote user authentication method proposed can be concluded as more suitable for resource-constrained wearable devices.

Keywords*— *Internet of Things, AVISPA, Wearable devices, Fuzzy Extractor, Chebyshev chaotic map

I. INTRODUCTION

The phrases "**wearable technology**", "**wearable devices**", and "**wearables**" denote the electronic gadgets or computers that are integrated into items like clothing and accessories which can easily be worn on the body. These wearable gadgets work similar to mobile phones and laptop computers. Also, these wearable devices can outperform the hand-held devices altogether [2]. The wearables are a part of the Internet of Things (IoT) technology. Some examples of the wearable devices include variety of computerized wristwatches such as the Apple iWatch, fitness tracking devices, Smart glass such as the revolutionary Google Glass, jewellery, headgear, belts, arm-wear, wrist-wear etc [1].

Wearable technology is making significant changes in day to day life of human beings. With an increase in development, wearable devices are being utilized and used by wide range of users, by connecting them to the Internet and accessing through several smart devices like smartphones and tablets. Fig. 1 gives the statistic information of the number of connected wearable devices worldwide from 2016 to 2021[3].

A. Authentication Network model

The network model for authentication of wearable devices is given in Fig.2, which is adapted from [4]. In the given model, the user is assumed to wear several devices like smart glasses, smart shoes, smart watches etc. These devices are connected to the Internet and the data gathered from these devices can be transmitted to smart devices like Tablets, Smartphones etc. Initially, the various users and different wearable devices and cloud server must register themselves with the trusted Registration Authority (*RA*). After their successful registration, the information such as identity, password and secret keys are stored in these devices. In the authentication model given in Fig. 2, a person wears several wearable devices, such as a smartglass (eyes), smartwatch (wrist), movement tracking device (thigh) etc. The primary task of these devices is to capture the physical details of the user such as heart rate, amount of calories burnt, distance covered etc and sent the covered data to his/her tablets/mobile phones. Also, these data are made available to a cloud server for further mining of data, analysis and decision making.

This authentication can be categorized into two [4, 5] as follows,

- *MODEL 1 – Local Authentication*

  This authentication would enable the authentication between the smart devices and the wearables. It is required if users need to access the data of the wearable devices from his/her smartphone or tablet etc.

- *MODEL 2- Global Authentication*

  This would enable the authentication of the smart devices, external data user and the cloud server where the data from the wearable devices is stored. This is needed in a case like medical care. If a remote user needs to consult a doctor, the personal information of the user from the wearable devices must be provided to the doctor for consultation and remote monitoring. Hence this authentication would permit the physician to access the personal details of patients for their treatment.

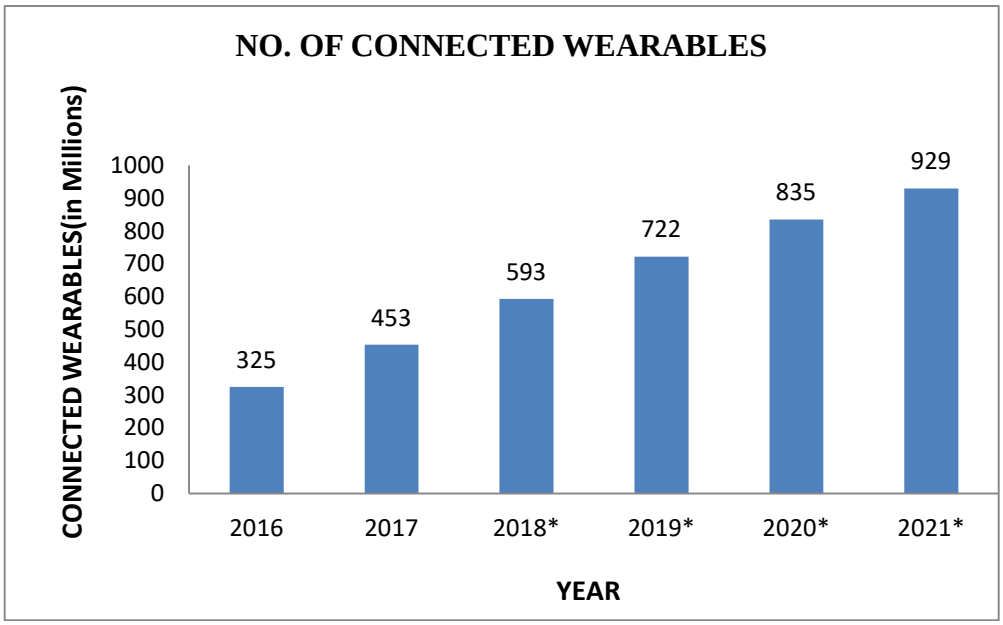

Fig.1. Number of connected wearable devices worldwide from 2016 to 2021 (in millions)[3]

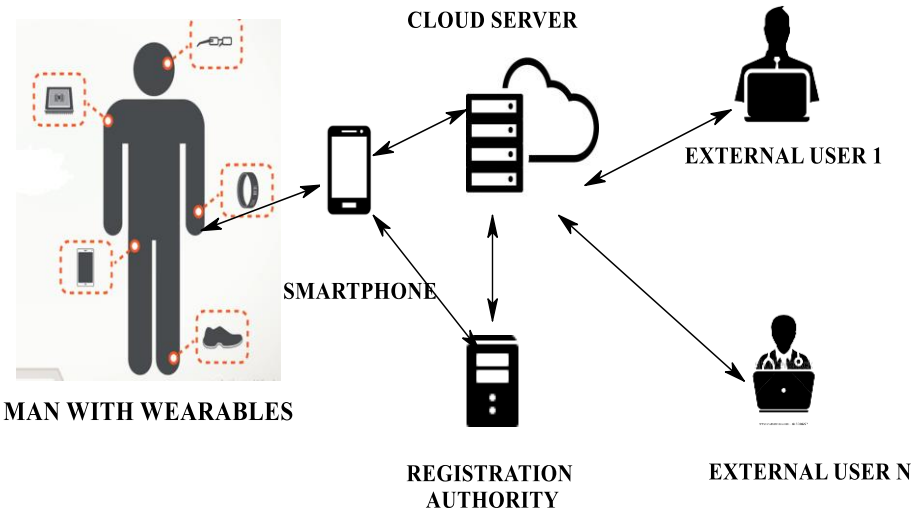

Fig.2.Authentication model of proposed user authentication scheme [4]

II. THREAT MODEL

The commonly used Dolev-Yao [6] threat model is adopted for our scheme. According to this, the wearable device and the endpoint terminals are not trusted and they are assumed to communicate over an insecure channel.

Also, the popular CK-adversary model [7], [8] is considered, which is for modeling the key-exchange protocol security. In this model, an attacker *A* can sent/receive the messages and can alter some information including the session keys, private keys, and session state. Therefore, an authenticated key-exchange protocol can lose some part of secret information (e.g., session ephemeral secrets, session key, and long-term private keys), which have a great impact in the security of communication [9].

This paper contains the following sections. Section 2 gives the threat model assumed for the given scheme. Various works that are related to the wearable authentication is given in section 3. Section 4 provides the necessaries of the proposed methodology. The proposed authentication scheme is given in section 5. Implementation of the mechanism with the implementation results and the performance analysis of the proposed scheme are given in section 6. Finally, Section 7 concludes this paper.

III. RELATED WORKS

The major research works done in the field of wearable device authentication have been discussed in this section.

Liu et al [4] introduced two protocols for the purpose of secure access to the information in the wearable. The First

scheme utilized Bluetooth as an important component of the communication channel between the users and the wearable. The Second scheme had the QR code as a visual out-of-band (OOB) channel for secure transmission of messages. It is referred as two-path challenge-response authentication scheme and it can be used in certain circumstances where only limited pairing is needed between the users and the wearable.

Sun et al[10] put forward a token based wearable authentication system particularly used for transient authentication. It is based on Diffie–Hellman public key exchange protocol. It uses modular exponentiation operations and asymmetric encryption/decryption and one-way hash function for mutual authentication and session key establishment between a wearable device and mobile device.

Liu et al [5] introduced an authentication mechanism particularly used for deployment of cloud assisted wearable devices. It supports both local and global verification. Long et. al [11] developed an authentication scheme particularly for wearable devices in the medical field. They made it using the popular standards of AES and SHA. It provides two-way authentication between the wearable device and the remote server. They confessed that it provides security against various network threats. They also tested and validated the protocol on a microcontroller and server communicating over the local network.

A new authentication mechanism especially used for Assisted Living (AAL) system was proposed by He and Zeadally[12].It was based on elliptic curve cryptography and particularly used for monitoring the health of elderly people. This had three levels of communication: Intra-BAN, Inter-BAN, and Beyond-BAN. A tree-based yoking-proof scheme was given by Chien et al. [13], in which the tags are arranged with a tree-like structure and the tags here can be identified with the paths updated.

Diez et al. [14] gave a self-authenticable point-to-point authentication mechanism for wearable devices. It would make a secure mutual authentication between a wearable device and mobile terminals. Amin et al.[16] proposed an anonymity preserving mutual authentication protocol for wearable health monitoring systems(WHMSs) and it provides an efficient login, robust mutual authentication, and user-friendly password change. However Jiang et al.[17] showed that it suffers from several flaws such as stolen mobile device attack, desynchronization attack, and sensor key exposure. To overcome these issues Jiang et al. [17] introduced an authentication protocol for(WHMSs) based on quadratic residues.

A secure obfuscated PIN authentication protocol (SEPIA) for automatic teller machine (ATM) had been suggested by Khan et al. [15]. In this, a Google Glass or a smart device is used to scan a QR code on the terminal screen and to provide a designation of the cloud server to acquire a secret PIN for secure authentication. This SEPIA protects the user against the shoulder-surfers and partial observation attacks along with the typical relay, replay, and man-in-the-middle (MITM) attacks.

Challa et al. [18] reviewed some of the recent protocols for the authentication of Implantable Medical Devices (IMDs). They gave a broad classification of existing authentication protocols of IMDs into four approaches namely- proximity-based, proxy-based, biometrics-based, and hybrid approach. Also, they gave a detailed analysis of communication and computation overheads and functionality features of several schemes and addressed the issues to be resolved in the near future.

Arshad and Rasoolzadegan [19] gave an authentication scheme particularly applied for Global Mobility Network (GLOMONET). This scheme applies Elliptic curve cryptography to overthrown the security weakness of the other schemes. It uses BAN logic and ProVerif tool to establish its security strengths.

Karuppiah M and Saravanan R[20] gave a user authentication scheme especially for roaming service in GLOMONET. Later Li et al.[21] analyzed their scheme and suggested that it suffers from problems like perfect forward secrecy and session key update, and the session key would be revealed by home agent. Also, it faces clock synchronization problem and efficiency problem. To overcome its shortcomings, ECC based authentication scheme for roaming service of GLOMONET in smart city was proposed by Li et al.[21].

Wu et al.[22] proposed a new authentication scheme for wearable devices. It is lightweight and it works with help of cloud server and satisfies mutual authentication and anonymity. This scheme is verified by Proverif tool and informal security analysis ensures that it satisfies all the security requirements. Though several schemes exist for authenticating the lightweight environment of IoT, they lack some functionalities and suffer from security attacks. To overcome these, a new authentication scheme for wearable devices has been proposed in the following section.

IV. MATHEMATICAL PRELIMINARIES

In this section, some mathematical preliminaries such as Collision-resistant one-way hash function, Chebyshev chaotic map, Fuzzy extractor which are used in the proposed scheme are explained.

A. Collision-resistant one-way hash function

A collision-resistant one-way hash function h: A → B, where A ={0,1}* and B ={ 0,1}^{n}, is a deterministic algorithm that takes an input as an arbitrary length binary string x ∈ A and produces an output y ∈ B, a binary string of fixed-length, n. Let $\mathrm{Adv}_{\mathrm{A}}^{\mathrm{HASH}}(t_1)$ denote an attacker A's advantage in finding a collision. Then, we have

$$Adv_A^{HASH}(t_1) = Pr\,[(x, x') \in_R A: x = x', and\ h(x) = h(x')] \quad (1)$$

where in (1), Pr[E]denotes the probability of a random event E, and (x, x′) $\in_R$ A denotes the pair (x, x′) is selected randomly by A. In this case, the adversary A is also allowed to be probabilistic and the probability of the advantage is computed over the random choices made by the adversary A with the execution time t_1. The hash function h (·) is then called collision-resistant, if $\mathrm{Adv}_{\mathrm{A}}^{\mathrm{HASH}}(t_1) \leq \epsilon_1$, for any sufficiently small $\epsilon_1 > 0$[23-26].

B. Fuzzy extractor

A fuzzy extractor (27-29) has the ability to extract a uniformly random string *b* and a public information *par* from the biometric template *f* with the error tolerance *t*. In the reproduction process, the fuzzy extractor recovers the original biometric data *b* for a noisy biometric *f′* using *par* and *t*. Suppose that $M=\{0,1\}^m$ be a finite *m* dimensional metric space of biometric data points, $d : M \times M \rightarrow Z^+$ a distance function, which is used to calculate the distance between two points based on the metric chosen, *l* the number of bits of the output string b_i and *t* the error tolerance, where Z^+ is the set of all positive integers.

The fuzzy extractor (*M*, *l*, *t*) is defined by the following two algorithms:

- **Gen:** This is a probabilistic algorithm that takes a biometric information $f_i \in M$ as input and outputs a key data $b_i \in \{0, 1\}$ and a public reproduction parameter par_i. In other words, Gen $(f_i) = \{b_i, par_i\}$.
- **Rep:** This is a deterministic algorithm that takes a noisy biometric information $f_i' \in M$ and a public parameter par_i related to f_i, and then it reproduces the biometric key data b_i. In other words, Rep $(f_i', par_i)=b_i$ provided that the condition $d(f_i, f_i') \leq t$ holds.

A basic tool needed in the development of fuzzy extractor is the secure sketch[40]. It allows the precise reconstruction of a noisy input. On input B a procedure outputs a sketch c. Then, given c and a value B′ close to B, it is possible to recover B. The sketch is secure in the sense that it does not reveal much information about B even if c is known. Thus, it is possible to store c.

In the same way, secure sketch can de explained as a pair of efficient randomized procedures: Sketch (Sket) and Recover (Rec). The sketching procedure, Sket, starts with the sketch, B, as input and returns a string $c \in \{0,1\}*$. The recovery procedure Rec takes an element B′ and $c \in \{0,1\}*$ and returns the corre-sponding value B. The correctness is again depending on the distance between B and B′.

V. PROPOSED SCHEME

The scheme proposed for wearable device authentication consists of the following three phases and Table 1 gives the explanation for the notations for the terms used in the proposed protocol.

[1] Registration Phase
[2] Login Phase
[3] Authentication Phase
[4] Biometric and Password update Phase

A) Registration Phase

This phase includes two registrations. This phase is essential for all the users and the wearable devices before starting the communication session. This is mainly to enhance the security of the established communication session.

The two registrations of the Registration phase are,

- User Registration
- Wearable Device Registration

TABLE I NOTATIONS

Notations	Description
U	User
RA	Registration Authority
WD	Servers
$\oplus$	XOR operation
K_{UR}, K_{WR}, K_R	Secret keys
SK	Shared session key
RI_i	Hashed Identity
UM_i, UN_i	User calculated parameter
RP_i	Hashed password
$h(.)$	One way hashing
$Gen(),Rep()$	Fuzzy Extractor functions
R_i, R_j	Random Nonce
T_i	Current timestamp
ΔT	Maximum transmission delay
$\|\|$	Concatenation Operator
UID_i	U_i's Identity
PWD_i	password
BM_i	personal biometrics

1) User Registration Phase

In this phase, the user U will register with the Registration Authority, RA. Any number of U can register with the RA. Fig.3 gives the brief steps involved in registration between the U_i with the RA.

STEP 1: U gives his/her Identity, Password and Biometrics ID_i, PW_i, B_i respectively as input in to the Smart device. The key is generated from the input Biometrics with the Fuzzy extractor function Gen $(B_i) = (\sigma_i, \tau_i)$. The hashed forms of Identity, password are calculated from $HID_i=h(UID_i||h_i)\oplus a_i$, $HPD_i=h(PW_i||h_i)\oplus a_i$ respectively. The calculated values are sent as registration parameters to RA.

STEP 2: The operations $RP_i=h(R_i||PW_i)$, $RI_i=h(R_i||ID_i)$ are performed to generate the hashed key for the inputs. Then $< RP_i, RI_i, \sigma_i >$ are sent as request for registration to the RA.

STEP 3: RA after receiving the request parameters, calculate $A_i=h(RI_i||K_R)$, $B_i=h(RP_i||K_{RU})$, $C_i=h(\sigma_i||K_{RU})$, $D_i=A_i\oplus B_i$, $E_i=A_i\oplus C_i$.

STEP 4: RA will then sent $<\sigma_i, D_i, E_i, A_i, K_{RU}>$ back to U as a result of successful registration. The received parameters are then stored in the U's smartphone or tablet.

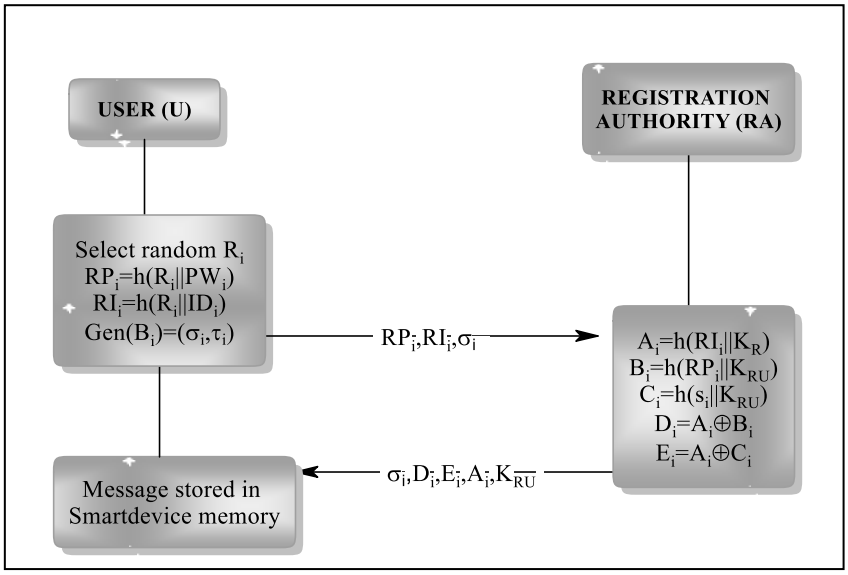

Fig.3. User Registration Phase

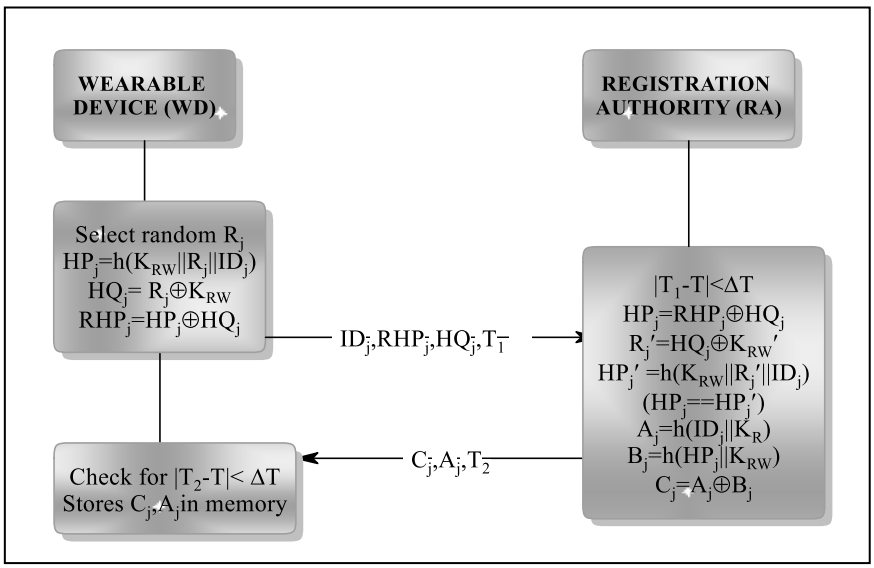

Fig.4. Wearable Device Registration Phase

B) Wearable Device Registration Phase

In this, any of the wearable devices WD_j can register with the RA. Fig.4 gives the overview of registration steps involved between the WD with the RA.

STEP1: WD registers with RA using an identity ID_j and random nonce R_j. The key K_{RW} is the key involved in this registration process. The following operations $HP_j=h(K_{RW}||R_j||ID_j)$, $HQ_j= R_j\oplus K_{RW}$ $RHP_j=HP_j\oplus HQ_j$ are performed. The values $< ID_j, RHP_j, HQ_j, T_1>$ are sent as registration parameters to RA.

STEP 2: RA will then check for the validation of timestamp using $|T_1-T|<\Delta T$. If the condition is valid then the values $HP_j=RHP_j\oplus HQ_j$, $R_j'=HQ_j\oplus K_{RW}'$, $HP_j'=h(K_{RW}||R_j'||ID_j)$,$(HP_j==HP_j')$, $A_j=h(ID_j||K_R)$, $B_j=h(HP_j||K_{RW})$, $C_j=A_j\oplus B_j$ are calculated.

STEP 3: WD will then check for the validation of timestamp using $|T_2-T|<\Delta T$. The values $< C_j, A_j, T_2>$ are sent to the WD from RA and are stored in their memory.

C) Login Phase

In the login phase, the user U can login to get the data of the desired wearable device .The login request parameters are sent to RA for verification. Fig.5 gives the overview of registration steps involved between the WD with the RA.

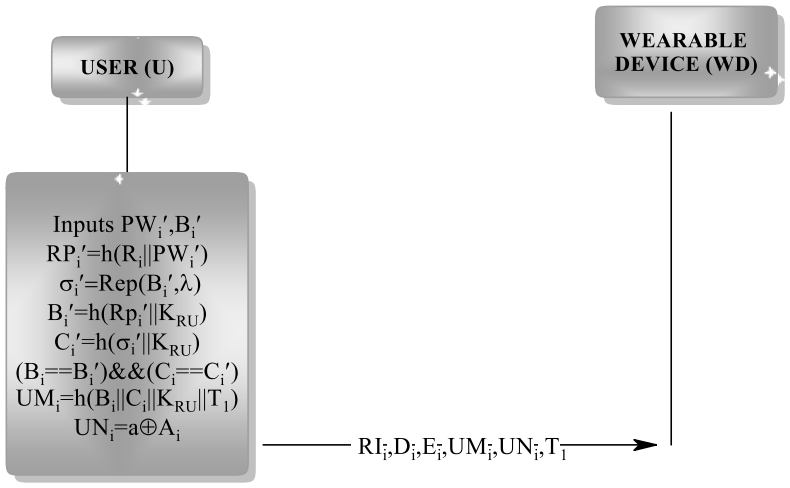

Fig.5. Login Phase

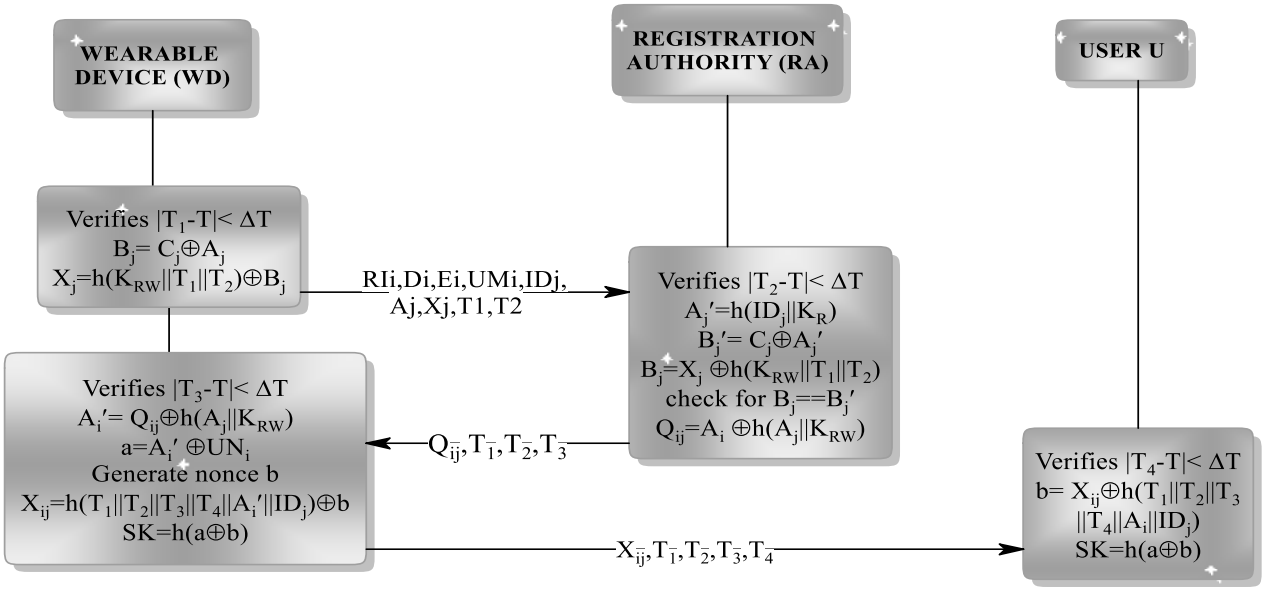

Fig.6. Authentication Phase

STEP 1: *U* inputs ID_i', PW_i', B_i' in his/her smartphone/ tablet. The following operations are performed. $RP_i'=h(R_i||PW_i')$, $s_i'=Rep(B_i',l)$, $B_i'=h(Rp_i'||K_{RU})$, $C_i'=h(s_i'||K_{RU})$.

STEP 2: The user is verified with validation of the condition- $(B_i==B_i')\&\&$ $(C_i==C_i')$. Then the values UM_i , UN_i are calculated by $UM_i=h(B_i||C_i||K_{RU}||T_1)$,$UN_i=a\oplus A_i$. After that < RI_i, D_i, E_i, UM_i, UN_i, T_1> are sent to RA as login request parameters.

D) Authentication Phase

After the successful validation of U_i, RA would forward the request parameters to WD_j. After mutual authentication between U_i and WD_j, a session key is generated using which secured communication takes place. The users can log in to with the steps given in Fig.6

STEP 1: If U_i is valid user then WD verifies the timestamp with $|T_1-T|<\Delta T$. Then $B_j=C_j\oplus A_j$, $X_j=h(K_{RW}||T_1||T_2)\oplus B_j$ are calculated and the parameters RIi,Di,Ei,UMi,IDj,Aj,Xj,T1,T2 are sent as request parameters to RA.

STEP 2: *RA* after receiving the request parameters will check for validation of timestamp using $|T_2-T|<\Delta T$. It would then calculates $A_j'=h(ID_j||K_R)$,$B_j'= C_j \oplus A_j'$, $B_j=X_j \oplus h(K_{RW}||\ T_1||T_2)$ for the validation of the condition $B_j==B_j'$. The parameters $<Q_{ij}, T_1, T_2, T_3>$are forwarded to WD_j if this condition holds.

STEP 3: WD_j after receiving the request parameters of U_i verifies the timestamp condition . Then generates session key with SK= h(a⊕b). It is generated with the help of the given operations like $Ai'= Q_{ij} \oplus h(A_j||K_{RW})$,$a=A_i' \oplus UN_i$, Generate nonce b and $X_{ij}=h(T_1||T_2||T_3||T_4||A_i'||ID_j) \oplus b$

STEP4: U_i will then generates session key with $b= X_{ij} \oplus h(T_1||T_2||T_3||T_4||A_i||ID_j)$,SK=h(a⊕b).

E) Biometric and Password update Phase

The legal users can replace their old password and old Biometrics with the new one very easily. To do so, U_i need to enter their old password and Biometrics.

STEP 1: The User U_i first gives the old password PWD_i' and Biometrics BM_i'.

STEP 2: The U_i calculates the hashed form of Password and Biometrics with $HID_i'=h(UID_i \ ||h_i) \oplus a_i$, $HPD_i'=h(PW_i||h_i) \oplus a_i$, η_i= Rep (BM_i, λ_i).

STEP 3: U_i will then get the stored values X_i, E_i, F_i and calculate the values of Y_i, Z_i using $p_i=H(HID_i||KUR)$,$q_i=H(HPD_i||KUR)$, $r_i=H(h_i||KUR)$, $m_i=p_i \oplus q_i$, $n_i=p_i \oplus r_i$. After U_i will check for the equality of $(n_i==n_i') \&\& (m_i==m_i')$.

STEP 4: The User can now give the new $NPWD_i$ and NBM_i and replaces the old one with the new values.

VI. IMPLEMENTATION AND FUNCTIONALITY ANALYSIS

A) Formal verification

This section gives the formal verification of the proposed authentication mechanism with the use of the commonly used AVISPA tool. This is to check the security of the scheme against various attacks like the replay attack, parallel session attack etc

AVISPA is a tool which can be operated easily with a push button and mainly used for validating the Internet security protocols automatically [30-35]. The protocols analyzed under the AVISPA tool need to be specified in a language, called HLPSL (High-Level Protocols Specification Language). HLPSL is a role-oriented language. A static analysis is performed in order to check the executability of the protocol, and then the protocol and the intruder actions are together compiled into an intermediate format (IF).

There are the following sections in OF:

- SUMMARY indicates that whether the tested protocol is safe, unsafe, or whether the analysis is inconclusive.
- DETAILS either explains under what condition the tested protocol is declared safe, or what conditions have been used for finding an attack, or finally why the analysis was inconclusive.
- PROTOCOL, GOAL, and BACKEND are the name of the protocol, the goal of the analysis and the name of the back-end used, respectively.
- After some comments and statistics, the trace of an attack (if any) is also printed in the standard Alice-Bob format.

AVISPA integrates different back-ends that implement a variety of state-of-the-art automatic analysis techniques [36].It implements four back-ends: On-the-fly Model-Checker (OFMC), Constraint Logic based Attack Searcher (CL-AtSe), SAT-based Model-Checker (SATMC) and Tree Automata based on Automatic Approximations for the Analysis of Security Protocols (TA4SP).

5.1.1Protocol Design in HLPSL

HLPSL is based on roles: the basic roles represent each participant role, and composition roles represent the scenarios of basic roles. Each role is independent of the others, which gets some initial information by parameters, and then communicates with the other roles by channels. In HLPSL, an intruder is always denoted by i and i is always modeled using the Dolev–Yao model [37] with the possibility for the intruder to assume a legitimate role in a protocol run. Furthermore, the role system defines a number of sessions, and a number of principals and some basic roles. The output format (OF) is produced by using one of the four back-ends. When the analysis of a protocol has been successful (by finding an attack or not), the output describes precisely what is the result, and under what conditions it has been obtained [38].

Some basic types supported in HLPSL are explained below for gaining detailed knowledge of protocol specification in HLPSL [36,41]:

- **agent** It represents the principal names. The intruder is always assumed to have the special identifier i.
- **public_key** It represents agents' public keys in a public-key cryptosystem. For example,given a public (respectively private) key KU, its inverse private (respectively public) key KR is obtained by inv KU.
- **symmetric_key** It represents the keys for a symmetric-key cryptosystem.
- **text** It is often used as nonces. These values can be used for messages. If Ri is of typetext (fresh), then Ri0 will be a fresh value which the intruder cannot guess.
- **nat** It represents the natural numbers in non-message contexts.
- **const** It represents constants.
- **hash_func** The base type hash_func represents cryptographic hash functions. The base type function also represents functions on the space of messages. It is assumed that theintruder cannot invert hash functions (in essence, that they are one-way).

The three phases of the proposed protocol-registration, login and authentication phases have been codes in HLPSL with the help of three roles-User, Registration Authority, Wearable Devices which is represented as Ui, RA, and WDj respectively. There are also other roles like session, goal, and environment.

```
% OFMC
% Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
C:\program1\SPAN\testsuite \programs\
wearables.if
GOAL
as_specified
BACKEND
OFMC
COMMENTS
STATISTICS
parseTime: 0.00s
searchTime: 0.09s
visitedNodes: 9 nodes
depth: 3 plies
```

Fig.7 Result analysis using OFMC

Fig.7 and Fig.8 shows the result obtained from the AVISPA tool. It had been obtained by the use of OFMC [39] and CL-AtSe backend. The major advantage of using OFMC backend is that it supports bounder number of execution and executes fast.

TABLE II FUNCTIONALITY FEATURES

Functional Features	Proposed scheme
FF1	✓
FF2	✓
FF3	✓
FF4	✓
FF5	✓
FF6	✓
FF7	✓
FF8	✓
FF9	✓
FF10	✓
FF11	✓
FF12	✓

```
CL-AtSe
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
TYPED_MODEL
 PROTOCOL
  C:\program1\SPAN\testsuite \
  programs\wearables.if
GOAL
  As Specified
BACKEND
  CL−AtSe
STATISTICS
     Analysed  : 8 states
  Reachable  : 0 states
  Computation: 0.00 seconds
  Translation: 0.14 seconds
```

Fig.8 Result analysis using CL−AtSe

A) Comparison of Functionality Features

An Informal analysis has been performed with the proposed scheme and other related schemes. TABLE III gives the comparison details of the Informal analysis. ✓ indicates that the scheme satisfies the given security feature.

VII. CONCLUSION

Wearable technology is gaining a significant notification in the recent years, especially in the field of healthcare and medical fitness. With its rapid emergence, it also faces severe security issues. The key challenge is legitimate authentication. An efficient Biometric based remote user authentication mechanism for wearable technology has been proposed. The proposed mechanism focuses only on local authentication. It poses low computational and communication time than other related schemes. It makes it adaptable for modern wearable devices.

FF1:	User anonymity preservation;
FF2:	mobile device stolen attack protection
FF3:	Wearable device stolen attack protection
FF4	offline password guessing attack protection;
FF5:	wearable device anonymity preservation;
FF6:	traceability preservation;
FF7:	denial-of-service attack protection;
FF8:	support of password/biometric update phase;
FF9:	support of replacing wearable devices phase.
FF10:	replay attack protection;
FF11:	man-in-the middle attack protection;
FF12:	impersonation attack protection;
✓:	scheme supports a feature or it is secure;
×:	scheme it does not support a feature or it is insecure.
N/A:	not applicable;

REFERENCES

[1] https://www.techopedia.com/definition/31206/wearable-device (accessed March 2018)
[2] http://www.wearabledevices.com/what-is-a-wearable-device/ (accessed March 2018)
[3] https://www.statista.com/statistics/487291/global-connected-wearable-devices/ (accessed March 2018)
[4] W. Liu, H. Liu, Y. Wan, H. Kong, and H. Ning, “The yoking-proof-based authentication protocol for cloud-assisted wearable devices,” Personal and Ubiquitous Computing, vol. 20, no. 3, pp. 469–479, 2016.
[5] S.Liu, S.Hu , J. Weng ,S. Zhu , and Z.Chen , “A novel asymmetric three-party based authentication scheme in wearable devices environment”, J Netw Comput Appl, vol.60, pp:144–54,2016 .
[6] D. Dolev and A. Yao, “On the security of public key protocols,” IEEE Transactions on Information Theory, vol. 29, no. 2, pp. 198–208, 1983.
[7] R. Canetti and H. Krawczyk, “Analysis of key-exchange protocols and their use for building secure channels,” in International Conference on the Theory and Applications of Cryptographic Techniques– Advances in Cryptology (EUROCRYPT 2001). Innsbruck (Tyrol), Austria: Springer, pp. 453–474,2001.
[8] R. Canetti and H. Krawczyk, “Universally Composable Notions of Key Exchange and Secure Channels,” in International Conference on the Theory and Applications of Cryptographic Techniques– Advances in Cryptology (EUROCRYPT 2002), Amsterdam, The Netherlands, pp. 337–351, 2002.

[9] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably Secure Authenticated Key Agreement Scheme for Smart Grid," IEEE Transactions on Smart Grid, 2016, DOI: 10.1109/TSG.2016.2602282
[10] D. Z. Sun, J. P. Huai, J. Z. Sun, J. W. Zhang, and Z. Y. Feng, "A new design of wearable token system for mobile device security," IEEE Transactions on Consumer Electronics, vol. 54, no. 4, pp. 1784–1789, 2008.
[11] William J. Long and Wei Lin, "An authentication protocol for wearable medical devices Emerging Technologies for a Smarter World (CEWIT)", in 13th International Conference and Expo on IEEE , 2017.
[12] D. He and S. Zeadally, "Authentication protocol for an ambient assisted living system," IEEE Communications Magazine, vol. 53, no. 1, pp.71–77, 2015.
[13] H.Y. Chien and S.B.Liu, "Tree-based RFID yoking proof. In: Proceedings of the international conference on networks security, wireless communications and trusted computing (NSWCTC 2009), pp. 550–553, 2009.
[14] F.P. Diez, D.S. Touceda, J.M.S. Camara, and S. Zeadally, "Toward self-authenticable wearable devices", IEEE Wirel Commun, Vol. 22, no.1, pp.36–43, 2017.
[15] R. Khan, R. Hasan , J.Xu ," SEPIA: secure-PIN-authentication-as-a-service for ATM using mobile and wearable devices", In: The 3rd IEEE international conference on mobile cloud computing, services, and engineering (MobileCloud), pp 41–50,2015.
[16] R.Amin, S.K.Islam , G.P.Biswas, K.M.Khan, and N. Kumar, " A robust and anonymous patient monitoring system using wireless medical sensor networks", Fut Gener Comput Syst, 2016. http://dx.doi.org/10.1016/j.future.2016.05.032 .
[17] Qi Jiang, Jianfeng Ma, Chao Yang , Xindi M, Jian Shen and Shehzad Ashraf Chaudhry, "Efficient end-to-end authentication protocol for wearable health monitoring systems", Computers and Electrical Engineering vol. 63, pp.182–195, 2017.
[18] Sravani Challa, Mohammad Wazid, Ashok Kumar Das, and Muhammad Khurram Khan,"Authentication Protocols for Implantable Medical Devices:Taxonomy, analysis, and future directions", IEEE Consumer Electronics Magazine,2018, Vol: 7, no.1, pp: 57 – 65.
[19] Hamed Arshad and Abbas Rasoolzadegan (2017).A secure authentication and key agreement scheme for roaming service with user anonymity. International Journal of Communication system,30(18)
[20] Karuppiah M, Saravanan R,"A secure authentication scheme with user anonymity for roaming service in global mobility networks",2015, Wirel Pers Commun ,vol.84(3), pp.:2055–2078
[21] Li, X., Sangaiah, A.K., Kumari, S. et al. ," An efficient authentication and key agreement scheme with user anonymity for roaming service in smart city", Pers Ubiquit Comput ,2017, vol. 21.
[22] Fan Wu, Xiong Li, Lili Xu, Saru Kumari, Marimuthu Karuppiah, Jian Shen ,"A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server", Computers & Electrical Engineering, Vol. 63,2017, Pp. 168-181.
[23] A.K. Das and A. Goswami , "A secure and efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care", J Med Syst, vol. 37, no.3, pp.:1– 16, 2013
[24] Sarkar P ,"A simple and generic construction of authenticated encryption with associated data". ACM Trans Inf Syst Secur ,2010, vol.13(4) pp.:33
[25] Stinson DR, "Some observations on the theory of cryptographic hash functions",Des Codes Crypt ,2006,38(2):259– 277
[26] Ashok Kumar Das, "A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks " ,Peer-to-Peer Netw. Appl.2014.
[27] Burnett, A., Byrne, F., Dowling, T., Duffy, A., "A biometric identity based signature scheme" Int. J. Netw. Security , 2007,vol.5 (3), pp.317–326.
[28] Dodis, Y., Reyzin, L., Smith, A., " Fuzzy extractors: how to generate strong keys from biometrics and other noisy data". In: Proceedings of the Advances in Cryptology (Eurocrypt'04), LNCS, 2004,vol. 3027, pp. 523–540.
[29] Ashok Kumar Das, Adrijit Goswami , "A robust anonymous biometric-based remote user authentication scheme using smart ", Journal of King Saud University – Computer and Information Sciences, 2015 , vol.27, pp.193–210
[30] Das, A. K , "A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks", Peer-to-Peer Networking and Applications, 2016, vol.9(1), pp. 223–244.
[31] Das, A. K., "A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor", International Journal of Communication Systems, 2015, pp.1–25.
[32] Das, A. K. "A secure and efficient user anonymity-preserving three-factor authentication protocol for large-scale distributed wireless sensor networks", Wireless Personal Communications, 2015, vol.82(3), pp. 1377–1404.
[33] Chatterjee, S., & Das, A. K., "An effective ECC-based user access control scheme with attributebased encryption for wireless sensor networks", Security and Communication Networks, 2015,vol.8(9), pp.1752–1771.
[34] Odelu, V., Das, A. K., & Goswami, A. , "A secure and efficient ECC-based user anonymity preserving single sign-on scheme for distributed computer networks", Security and Communication Networks, 2015, vol.8(9), pp.1732–1751.
[35] Lv, C., Ma, M., Li, H., Ma, J., and Zhang, Y. , "An novel three-party authenticated key exchange protocol using one-time key", Journal of Network and Computer Applications, 2013, vol. 36(1), pp. 498–503.
[36] AVISPA. Automated Validation of Internet Security Protocols and Applications. http://www.avispaproject.org/. Accessed January 2015.
[37] Dolev, D., & Yao, A., " On the security of public key protocols", IEEE Transactions on Information Theory, 1983, vol.29(2), pp.198–208.
[38] von Oheimb, D., "The high-level protocol specification language hlpsl developed in the eu project avispa. In Proceedings of APPSEM 2005 Workshop",2005,pp. 1–17
[39] Odelu, V., Das, A. K., & Goswami, A., " A secure effective key management scheme for dynamic access control in a large leaf class hierarchy", Information Sciences, 2014, vol.269, pp. 270–285.
[40] F. Hern´andez ´Alvarez, L. Hern´andez Encinas, C.S´anchez ´ Avila, "Biometric Fuzzy Extractor Scheme for Iris Templates", Security and Management,2009, http://digital.csic.es/bitstream/ 10261/15966/1 SAM3262.pdf (last accessed 25 January 2018)
[41] Ashok Kumar Das ,Anil Kumar, Sutrala Vanga , Odelu, Adrijit Goswami,"A Secure Smartcard-Based Anonymous User Authentication Scheme for Healthcare Applications Using Wireless Medical Sensor Networks",Wireless Personal Communications, 2017, vol. 94, no.3, pp 1899–1933.