ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 8, Issue 3, March 2019

Security Protocol using ALTA for Implantable Medical Devices Deployment

G.Sethuram Rao, K.Aruna, S.Mahesha Sree, S.Shasimithra

Assistant Professor, Department of Electronics and Communication Engineering, Velammal Institute of Technology, Chennai, India

UG Student, Department of Electronics and Communication Engineering, Velammal Institute of Technology, Chennai, India

UG Student, Department of Electronics and Communication Engineering, Velammal Institute of Technology, Chennai, India

UG Student, Department of Electronics and Communication Engineering, Velammal Institute of Technology, Chennai, India

ABSTRACT: In this artificial intelligence dependent world, advantages and disadvantages of the technologies have equal foot. The transmission of data in medical field has a major drawback in security and privacy. Security plays a vital role in medical field as there can be adverse events. Implantable Medical Devices (IMD) is a man-made implantable device that helps in monitoring and treats the physiological conditions of human (temperature sensor for body temperature and pacemaker for heart beat rate). In our proposed system, we use IMD to monitor the conditions of the patient. In case of any abrupt changes in the monitored values, it records and sends the information to the controller node. This node collects the information and sends to the doctor through an access point. We can even send the data to the friends, relatives and trusted authority of patient's choice. Now by knowing the condition of the patient, doctor can prescribe the patient at right time even from a remote distance. This communication is allowed only after the mutual authentication between the user and the nodes by providing a secret session key. The security verification is done using Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. This scheme provides security to known attacks. We use Attack Localization Task Allocation (ALTA) providing hash key to increase the security. The practical demonstration is performed in NS2 simulation tool. Performance analysis of the proposed scheme with existing schemes is done using AWK graph.

KEYWORDS: Implantable Medical Devices (IMD), Controller node, mutual authentication, AVISPA tool, ALTA, NS2 simulation, AWK graph.

I. INTRODUCTION

Implantable Medical Device (IMDs) is a man-made device which monitors and treats the physiological conditions within the human body. Different types of IMDs are available they are brain neurosimulator, pacemaker, gastric implant etc. Even cochlear implant provides remote monitoring and treatment to patient under severe medical conditions. Information and communication technology (ICT) facilitates the information exchange of IMDs and provide them to communicate with each other. It has an ability to collect the health related data and send to nearby Controller Node (CN) using communication technology i.e. Bluetooth, ZigBee etc. And then CN node is connected to internet using access point. A user (for example Doctor, trusted authority etc.) can access the data from CN after a successful mutual authentication.

However, in this technology developed world an attacker can exploit the vulnerabilities in the IMDs. The attacker can be a replay attacker, middle attacker or an impersonation attacker. To avoid these attacks there is a strong need to

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 8, Issue 3, March 2019

design a secure remote user authentication scheme for IMDs by which the controller node of the patients IMD and user can mutually authenticated each other. The both entities establish a secrete session key for future communications.

In addition, the formal security verification is done using the widely accepted AVISPA tool which secure against the replay and man in the middle attack. The practical implementation is also done using NS2 simulations tool to measure the impact of the scheme on network performance parameters such as end-to-end delay and throughput.

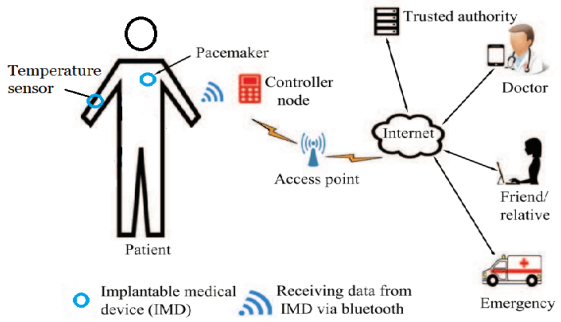

Fig. 1. Network model of IMDs communication environment

II. LITERATURE SURVEY

Secure access to a programmer with no constraint on power or computational ability is provided by the IMDs. It did not provide non-traceability property, session key and security towards replay and man-in-the middle attacks [1].
A scheme to secure cardiac IMDs uses Wireless Identification and Sensing Platform (WISP). They provide solution to extend the battery life and authentication using biometric keys for secured communication. It did not provide anonymity and non-traceability property [2]. Heterogeneous cryptosystems (symmetric and non-symmetric) is used to provide different levels of security. Their protocol consists of two stages. They are global authentication (between BSN and CA) and local authentication (between BSN and BS). It did not provide anonymity property [3]. Authentication scheme for Ambient Assisted Living (AAL) helps in tele-health care services. It uses assistive robotics (home service robots) [4]. Secure scheme for IMD Guard provides ECG based key establishment without prior shared secrets and access control mechanism to protect spoofing attacks [5]. A survey of existing techniques, which improves security and privacy in IMDs and BANs [6]. The human values and the security issues associated with the IMDs are provided [7]. ElGamal elliptic curve cryptography based RFID authentication schemes is provided. It has fast computation, less memory, power consumption and saving bandwidth. Computational cost and real-time experimentation is not suitable [8]. A lightweight and adaptive anonymous authentication scheme for inter-WBAN communication selects adaptive relay during authentication and key agreement process to ensure energy efficiency and security effectiveness. This is not efficient during emergency situation [9]. Healthcare system (HES) collects medical data from WBANs and transmits them through wireless sensor network to wireless personal area networks (WPANs) via a gateway. HES involves the GSRM (Groups of Send-Receive Model) scheme to ensure privacy and feedback the results automatically. HES did not monitor or analyze sudden diseases [10]. IMDs collects the change from the patient body and send it to the controller node. The security is provided by AVISPA tool, which implements High Level Protocol Specification Language scheme. Only after mutual authentication between the user and the nodes, the data can be accessed [11].

III. PROPOSED SYSTEM

In this section, we present a three-factor remote authentication protocol namely smart card; password; biometrics. This protocol is for the implantable medical devices communication environment, which uses the Elliptical Curve Cryptography (ECC). It is an approach to public key cryptography based on algebraic structure of elliptic curves over the finite fields.

ECC is applicable for many tasks like key agreement, pseudo-random generators and so on. Indirectly, they are used for the encryption by combining key agreement with symmetric encryption scheme elliptic curve is a plane curve over

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 8, Issue 3, March 2019

a finite field which consists of the points satisfying y^2=x^3+ax+b along with the point at infinity. For better understanding, we have a short view about two basic operations, such as point addition and point multiplication. With two distinct points P and Q addition is defined as the negation of the point resulting from the intersection of the curve, E and the straight line defined by the points P and Q, giving the point R=P+R. Point multiplication can be computed through repeated addition. This is a fully exponential approach to computing the multiplication. ECC is powerful. Calculating public key from known private key and base point is easy. But extracting private key from known public key and base point is not easy. This problem is called Elliptic Curve Discrete Logarithm Problem (ECDLP).

The network model presents the user whose body is implanted with implantable medical devices IMDs, such as pacemaker and temperature sensor. These IMDs monitor the patient's health condition and provides the service to the patient based on their symptoms. The patient is the user denoted as *Ui*. IMDs have wireless communication feature (like Bluetooth) using which they can send the patient's information data to the nearby controller node, say *CNj*, which collects the data securely. If there is a user wanted to access the real-time data from a particular controller node *CNj* for monitoring and diagnosis, we require mutual authentication between the user *Ui* and the control node *CNj*, then the establish session key to each other for future communication with security.

NOTATIONS USED IN PAPER

Notation	Description
U_i, MD_i	i^{th} user and his/her mobile device
CN_j	j^{th} controller node
IMD_l	l^{th} implantable medical device
TA	Trusted authority
ID_i, PW_i, BIO_i	U_i's identity, password and biometric information
ID_{TA}, ID_{CN_j}	Identities of trusted authority and controller node
RID_i, RID_{CN_j}	Pseudo identities of U_i and CN_j
N	1024-bit secret number of TA
r_i, r_j	160-bit random nonces of U_i and CN_j
RTS_{CN_j}	Registration timestamp of CN_j
T_i	Generated current timestamp
ΔT	Maximum transmission delay associated with a message
$Gen(\cdot)$	Probabilistic generation procedure used in fuzzy extractor
$Rep(\cdot)$	Deterministic reproduction procedure used in fuzzy extractor
σ_i	Biometric secret key of U_i
τ_i	Public reproduction parameter of U_i
t	Error tolerance threshold used in fuzzy extractor
$E_p(a,b)$	A non-singular elliptic curve: $y^2 = x^3 + ax + b \pmod p$ over a prime finite field Z_p (Galois field $GF(p)$) with $a, b \in Z_p^*$ are constants with $4a^3 + 27b^2 \neq 0 \pmod p$
$k.P$	Elliptic curve point multiplication; $k \in Z_p^*$ & $P \in E_p(a,b)$
$h(\cdot)$	Collision-resistant cryptographic hash function
$\|\|$, $\oplus$	Concatenation and bitwise XOR operations

We use random nonce and current timestamps to protect from replay attack against an active adversary. So we assume that all the network entities are synchronized with their clocks.

The proposed scheme consists seven phases. They are

1. *Pre-Deployment Phase*

A Trusted Authority is responsible for controller node *CNj* and devices *IMDl* registration to their deployment in the deployment fields (Hospital). For the deployment, at first the trusted authority selects a unique secret number N for every *CNj* and along with it the IMD'S attached in the body and then it calculates the pseudo identity for both the *CNj* and the IMDs. Finally it stores the information in the memory of *CNj* for deploying in the deployment field. To generate a pair wise key, a polynomial based protocol is used which is univariate.

Post-Deployment Phase: After the pre deployment phase, where once the IMD's and *CNj* are deployed, the first process in this phase is to establish a pair wise secret key. This is done by means of using the pre-loaded information which is stored in the memory during the previous phase. For the pair wise secret key to be established the *CNj* sends pseudo identity to IMD and then the IMD computes the shared key and hence it securely communicates.

2. *User- Registration Phase*

It deals with the registration procedure of the user *Ui*, to access information from the *CNj*. A trusted authority is required for registration. The doctor needs to register at the TA. It might be either the secure channel or the person. For registering, first the doctor selects an identity and sends to TA and after receiving reply, it sends registration reply

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 8, Issue 3, March 2019

message to the doctor. Then the doctor selects a password of their choice and applies the biometric at the sensor to generate a biometric key.

3. Login Phase

For the login phase the doctor has to perform the following process. At first the doctor inputs his or her ID and password into the mobile device (MD). The MD extracts the biometric key provided if the hamming distance between the original biometric and the recent biometric is less than the error tolerance threshold value. If the verification is correct then login takes place, else it is terminated.

4. Authentication And Key Agreement Phase

T1 when the condition |T1-T1*| < ΔT, ΔT is the highest transmission delay. In case, timeline matches controller node *CNj* computes and verifies the signature. After the computation controller node compute the session key and shared with user. After that *CNj* sends the authentication reply via public channel. After authentication reply, if it does not hold, user will suddenly cancel the connection. Then user checks if the condition holds *CNj* is authenticated by *Ui*. Then *Ui* will generate the timestamp and send acknowledgement message via open channel. After receiving the message from the *Ui*, *CNj* will check the readiness. In case if the condition holds *CNj* will calculate. If it does not hold, then it will terminate the connection immediately. Or else Ui and CNj collect the same session key for secure communication.

5. Password And Biometric Update Phase

Here we are using password and biometric update facility in which, the user will able to change their password and biometric without involving TA for the security reason at any time. User will input their identity; password to their mobile devices also imprints their biometric information to the sensor *MDi.* User who passes password and biometric verification and they make a start for password and biometric update procedure or else the update process will be suddenly terminated. User will provide a new password and biometrics, if they want to change the old biometric information. If the user does not want to change their biometric they can keep their old biometric. The new biometric will be taken as old one.

6. Dynamic Controller Node Addition Phase

Here the trusted authority will perform the Dynamic controller node addition. The trusted authority allocates a new special identity which is varied from the identities of existed controller node. Trusted authority will also compute polynomial share in GF.

7. Dynamic IMD Addition Phase

Another new Implantable Medical Devices is used to employ a new IMD to replace an existing IMD. The trusted authority will able to generate a different identity and calculate the similar pseudo identity and also the polynomial share. Them it will be stored in the memory of trusted authority. In controller node there will be no need to update the polynomial share. Only the trusted authority wants to inform the controller node about the deployment of implantable medical devices. It can determine the pair wise key with the controller node as *SKimd*. At last it starts secure communication using the determined key *SKimd* by the help of post deployment phase.

IV. SECURITY ANALYSIS

The possible known attacks are shortly discussed below to which the proposed system is secure.

1. Replay Attack

Replay or playback attack is a network attack in which a valid data transmission is maliciously repeated or delayed either by originator or an adversary person who intercepts and resends the data. In other words, it is an attack on a security protocol using replay of messages from a different context into the intended context, thereby fooling the user that they have successfully completed the protocol run. In the proposed scheme, during the login and authentication and key agreement phases, the messages Msg1, Msg2 and Msg3 are exchanged between *Ui* and *CNj* with different current timestamps T1, T2 and T3. If an adversary node intercepts these messages, the validity of timestamps will fail and the messages will be treated as the old messages. Hence, our scheme provides protection against replay attack.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 8, Issue 3, March 2019

2. *Man-in-the Middle Attack*

MITM is where the attacker makes independent connection with the victims, secretly relays and possibly alters the messages between two parties who believe they are directly communicating with each other. Authentication is the best way to prevent MITM. The attacker will not know the secret key; hence no modification can be done. Thus our scheme provides protection against MITM.

3. *Privileged-Insider and Offline Password Guessing Attack*

The privileged user of the trusted authority, who maybe an internal attacker can obtain the pseudo identities of *Ui* during registration phase. In addition, if the mobile device is lost or stolen after the completion of the registration, the attacker cannot find the correct password. Thus security is preserved in this attack also.

4. *User Impersonation Attack*

Impersonation is a tool to gain access to the network for any fraud. Calculating public key from known private key and base point is easy. But extracting private key from known public key and base point is not easy. This problem is called Elliptic Curve Discrete Logarithm Problem (ECDLP). Thus even if the attacker sends a valid login request to the control node, attacker do not know the secret biometric key, private key and correct password. Thus the security is maintained in this case too.

5. *Controller Node Impersonation Attack*

If an attacker sends a valid authentication reply message to the user for the message sent during authentication and key establishment phase, due to ECDLP, attacker will never know the secret key.

6. *Session Key Security*

Session key is a single-use symmetric key used for encrypting all messages in one communication session. During the login and authentication & session key agreement phases, *Ui* sends the message Msg1 to *CNj*. Then *CNj* replies Msg2 to *Ui*, which in turn sends the acknowledgment message Msg3 to *CNj*. In all these messages session key *SKij* is protected by the one-way hash function. Moreover, without the knowledge of short-term secrets such as random noncore and rj, and long-term secrets, Attacker cannot compute session key SKij. As a result, the proposed scheme provides session key security.

7. *Anonymity and Untraceability*

If an attacker intercepts the message Msg during the login and authentication & key agreement phases. Due to usage of random nonce and current timestamps, secret key and private session key becomes dynamic and “unique” in all messages for each session. It also does not directly include user and control node identification. Hence, the proposed scheme preserves both anonymity and non-traceability properties.ind the correct password. Thus security is preserved in this attack also.

8. *Resilience Against Controller Node Physical Capture Attack*

By physically capturing a controller node, attacker can extract the information from its memory using power analysis attacks. Note that all pseudo controller node identity and pseudo personality RID are distinct for all the controller nodes, and these are generated by the Trusted Authority. Therefore, attacker can only find the session key. Then, compromise of a controller node does not help in attacking the communications among the user and other non-compromised controller nodes. Hence, our scheme is unconditionally secure against controller node physical capture attack.

9. *Denial-of-Service Attack*

If a legal user *Ui* enters incorrect identity and/or Password during login phase, it is locally verified. The login request is sent to the controller node only after successful verification. As a result, the proposed scheme is secure against such Do’s attack. Stolen device attack - If mobile device is lost or stolen, attacker can extract all information. To guess password and identification, attacker has to know both secret key and the private session key. Thus the proposed system is secured to stolen mobile device attack.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 8, Issue 3, March 2019

V. FORMAL SECURITY VERIFIVATION USING AVISPA

a) Higher Level Protocol Specification Scheme

The security protocol in the role-based expressive formal language, called the High Level Protocol Specification Language (HLPSL). HLPSL is translated into the intermediate format (IF) using the translator, called HLPSL2IF. If is a lower-level language than HLPSL and is read directly by the back-ends to the AVISPA tool.

There are four back ends in AVISPA tool: 1) On-the-fly Model- Checker (OFMC); 2) Constraint-Logic-based Attack Searcher; 3) SAT-based Model-Checker (SATMC) and 4) Tree Automatic based on Automatic Approximations for the Analysis of Security Protocols (TA4SP).

Finally, the back ends produce the output format (OF), which precisely tells whether the protocol is safe or unsafe. If it is unsafe, the OF also lists the attack trace. In HLPSL, each entity in the network (user U, the TA and controller node CN) is implemented in a role. Apart from these basic roles, we have other two mandatory roles, called session, and goal and environment. Each role contains global constants and a composition of one or more sessions, where the intruder may play some roles as legitimate user. For the replay attack checking, OFMC checks whether the legitimate agents can execute the specified protocol by performing a search of a passive intruder. For the Dolev - Yao model check, this back-end also checks whether there is any man-in-the middle attack possible by the intruder. We have simulated the proposed scheme using the Security Protocol animator for AVISPA (SPAN) for the OFMC and CLAtSe back-ends since these back ends supports bitwise XOR operation.

b) Attack Localization Task Allocation

In our Attack Localization Task Allocation techniques we implemented the SHA512 hash key techniques. In these SHA512 is better than SHA 1 and latest SHA 256. The length of the key is increases the security are also increases. Secure Hashing Algorithms, also known as SHA algorithm that consists of bitwise operations, modular additions, and compression functions. The hash function then produces a fixed size string that looks nothing like the original. These algorithms are designed to be one-way functions, meaning that once they're transformed into their respective hash values, it's virtually impossible to transform them back into the original data. A few algorithms of interest are SHA-1, SHA-2, and SHA-5, each of which was successively designed with increasingly stronger encryption in response to hacker attacks. SHA-0, for instance, is now obsolete due to the widely exposed vulnerabilities. A common application of SHA is to encrypting passwords, as the server side only needs to keep track of specific user's hash value, rather than the actual password. This is helpful in case an attacker hacks the database, as they will only find the hashed functions and not the actual passwords, so if they were to input the hashed value as a password, the hash function will convert it into another string and subsequently deny access. Additionally, SHA exhibit the avalanche effect, where the modification of very few letters being encrypted cause a big change in output; or conversely, drastically different strings produce similar hash values. This effect causes hash values to not give any information regarding the input string, such as its original length. In addition, SHAs are also used to detect the tampering of data by attackers, where if a text file is slightly changed and barely noticeable, the modified file's hash value will be different than the original file's hash value, and the tampering will be rather noticeable.

VI. PRACTICAL PERSPECTIVE:NS2 SIMULATION STUDY

NS (version 2) is an object-oriented, discrete event driven network simulator written in C++ and OTcl. NS is for simulating local and wide area networks. The NS project is now a part of the VINT project that develops tools for simulation results display, analysis and converters that convert network topologies generated by well-known generators to NS formats.

The following parameters are used in stimulation

- No of Nodes: 11
- Frequency: 50Hz
- Routing Protocol: DSDV
- Antenna: Omni Antenna
- Channel: Wireless Channel

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 8, Issue 3, March 2019

The pattern of data transmission in WIFI network is viewed in the NS2 stimulator. The algorithm used for this is as follow

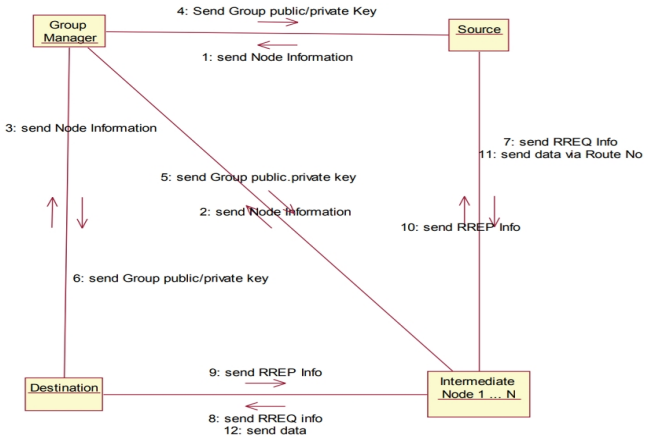

Fig. 2. Algorithm for the data transmission (viewed in NS2)

VII. RESULT

In order to measure the impacts of proposed scheme with the existing scheme, we calculate some performance parameters and store in the database as trace in hexadecimal form. These data help in graph formation using AWK language (language used in cricket to show the position of the ball). The parameters we include are end-to-end delay, loss, throughput, channel frequency, drop node frequency, source frequency, destination frequency and protocol frequency. We have a buzzer to indicate the sudden change in patient's health condition. An application is created in the mobile to update the patient's information.

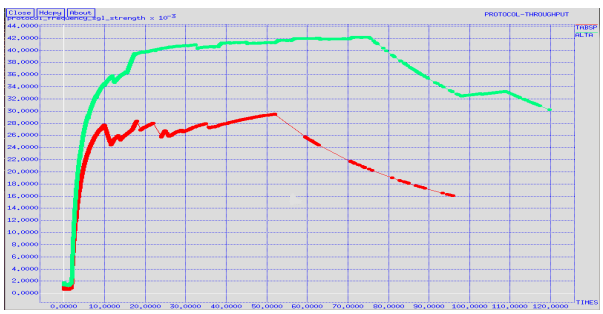

Fig. 2. Throughput comparison graph between HLPSL and ALTA

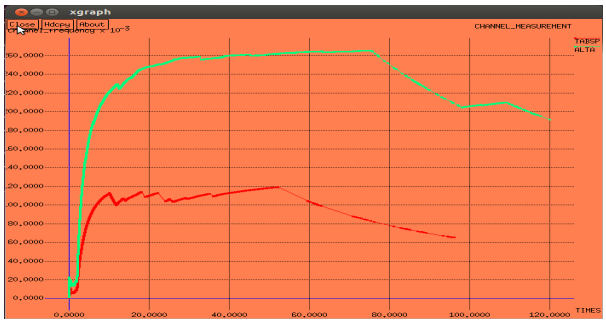

Fig. 3. Channel frequency comparison between HLPSL and ALTA

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 8, Issue 3, March 2019

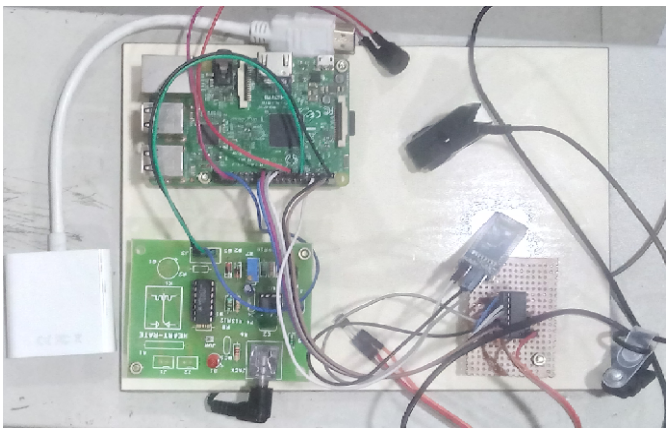

Fig. 4. Raspberry pi kit with heart rate sensor, pulse sensor, Bluetooth module, buzzer and ADC

VIII. CONCLUSION

In this paper, we introduce ALTA technique scheme is used to improve the communications having the hash key value for each data as followed by SHA1. The IMD treats and monitors a physiological condition of human body. As well as it facilities a doctor for a remote consultation on the basis of human health data which is collected by IMDs. However, wireless communication raises serious threats in the IMD deployment. A remote user authentication scheme has been proposed, through which a user (Doctor) and a controller node can be mutually authenticated each other and establish a session key for their future secure communication. Additionally, a comparative graph has been produced between exciting and proposed scheme which has a high level security base.

REFERENCES

[1] X. Li, J. Niu, S. Kumari, F. Wu, and K. K. R. Choo, "A robust biometrics based three-factor authentication scheme for Global Mobility Networks in smart city," Future Generation Computer Systems, 2017, DOI: 10.1016/j.future.2017.04.012.

[2] D. He and S. Zeadally, "Authentication protocol for an ambient assisted living system," *IEEE Communications Magazine*, vol. 53, no. 1, pp. 71–77, 2015.

[3] D. He and S. Zeadally, "An Analysis of RFID Authentication Schemes for IOT in Healthcare Environment Using Elliptic Curve Cryptography," *IEEE Internet of Things Journal*, vol. 2, no. 1, pp. 72– 83, 2015.

[4] D. He, N. Kumar, J. Chen, C. C. Lee, N. Chilamkurti, and S. S. Yeo, "Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks," *Multimedia Systems*, vol. 21, no. 1, pp. 49–60, 2015.

[5] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "SoK: Security and Privacy in IMD and BAN," in IEEE Symposium on Security and Privacy, San Jose, USA, 2014, pp. 524–539.

[6] D. He, N. Kumar, J. H. Lee, and R. S. Sherratt, "Enhanced threefactor security protocol for consumer USB mass storage devices," *IEEE* Transactions on Consumer Electronics, vol. 60, no. 1, pp. 30–37, 2014.

[7] N. Ellouze, M. Allouche, H. Ben Ahmed, S. Rekhis, and N. Boudriga, "Securing Implantable Cardiac Medical Devices: Use of Radio Frequency Energy Harvesting," in 3rd International Workshop on Trustworthy Embedded Devices, Berlin, Germany, 2013, pp. 35–42

[8] C. S. Jang, D. G. Lee, J.-w. Han, and J. H. Park, "Hybrid Security Protocol for Wireless Body Area Networks," *Wireless Communications and Mobile Computing*, vol. 11, no. 2, pp. 277–288, 2011.

[9] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *IEEE INFOCOM*, Shanghai, China, 2011, pp. 1862–1870.

[10] T. Denning, A. Borning, B. Friedman, B. T. Gill, T. Kohno, and W. H. Maisel, "Patients, Pacemakers, and Implantable Defibrillators: Human Values and Security for Wireless IMD," in SIGCHI Conference on Human Factors in Computing Systems, ser. CHI '10. Atlanta, Georgia, USA: ACM, 2010, pp. 917–926.

[11] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proximity-based Access Control for Implantable Medical Devices," inProceedings of the 16th ACM Conference on Computer and Communications *Security (CCS 2009)*, Chicago, USA, 2009, pp. 410–419.

[12] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541–552, 2002.