Enhancing Security in Smart Watches using Identity Based Cryptography

Prasanth S
Computer Science and Engineering
Dr.Mahalingam College of Engineering and Technology (Affliated to Anna University)
Pollachi,India
prasanthudt97@gmail.com

Sarika V G
Computer Science and Engineering
Dr.Mahalingam College of Engineering and Technology
(Affliated to Anna University)
Pollachi,India
sarikavenugopal98@gmail.com

Gokul Krishna Moorthy P
Computer Science and Engineering
Dr.Mahalingam College of Engineering and Technology
(Affliated to Anna University)
Pollachi,India
16bcs311@gmail.com

***Abstract*— The main objective is to enhance the security in wearable devices as similar to smart watches by preventing the brute force attack. We attain this objective using the Identity based encryption method. This type of encryption strategy allows us to prevent unauthorized access as it uses a unique ID for authentication. A unique ID that has been generated prevents the brute force attacks by sending the hash code to the user's mail when someone enters the password as wrong more than 3 times for that particular ID. As it uses a unique ID for its authentication, It has been termed as ID-Based Cryptography. This process is done using the secured hash algorithm (SHA-256) where a unique hash code is generated each time to authenticate the user during Each Login attempts. It has the count of all Login attempts and when the Incorrect Login attempts count reach to that of three, It request a user for a unique hash code that has been sent to their mail id.**

Previously, the data in wearable devices are secured using hardware based encryption but that doesn't prevent the brute force attack that has been performed by anonymous users. Hence, we use this Identity based encryption to overcome that disadvantage.

Keywords— *ID-Based Cryptography, Identity based encryption, Secured Hash Algorithm (SHA-256), Brute force attack*

I. INTRODUCTION

The project's main scope is to enhance security in terms of wearable devices. Here in case of wearable devices, we are enhancing security in terms of smart watches. Smart watches have several data's such as their walking distance, heart bit rate and also their fitness data. As they are the unique measurements of a particular people and its mandatory to save their data in a highly secured manner , As there also exists a previous method based on HBE (Hardware – Based Encryption). An anonymous user can easily access the data by means of Brute Force Attack. Brute Force Attack is the attack where user can access to the login by multiple irregular attempts. We are following a method named ID-Based Cryptography. The term ID-Based is a encryption based on their identity. Here ID is generated for all users, Based on their unique Id. They can login using their unique ID and the password that has been generated has been checked for all the attempts of login. So as it is sending a Unique Hash code to that of User's mail id. As each users have their own unique ID that has been sent to their mail id . It's termed as ID – Based Cryptography. When the hash code entered by the user remains correct, It allows the user to generate the data by clicking on the Generate button. Now the fitness and the heart beat data that has been generated , has been generated up for the corresponding users. The design and development of wearable biosensor systems for health monitoring has garnered lots of attention in the scientific community and the industry during the last years.

In this work, we develop a enhanced security in smart watches using Identity Based Cryptography. In summary our contributions include

- To enhance the security in smart watches in order to protect the data of the individual users.
- To prevent the brute force attacks in smart watches using SHA-256 algorithm.
- To generate hash code to ensure the security of the system.

II. RELATED WORK

In order to ensure the authentication, the system processes a set of incorrect login parameters, In case if it produces as a result as Email and Password is mismatched or the user has been enrolled previously. Then there is a case, where the anonymous user can perform the Brute force attack and can crack their passwords. In order to avoid those issues , during the attempt of signup in order to verify whether there exists any unique id for a user during the attempt of login. We are sending a reset password link to the corresponding users mail id to check whether the mail id belongs to a particular user or not. After the registration process, the user can have a login and for each login attempts the user is provided with that of the OTP.

As by means of OTP verification from their mail id, (i.e.,) they follow the ID-Based Cryptography encryption strategy. Now the user can be ensured that there will be no anonymous user can make a brute force attack.

And Finally, the user can be ensured that there is no anonymous authentication for their account. And it follows a method called ID – Based Encryption.

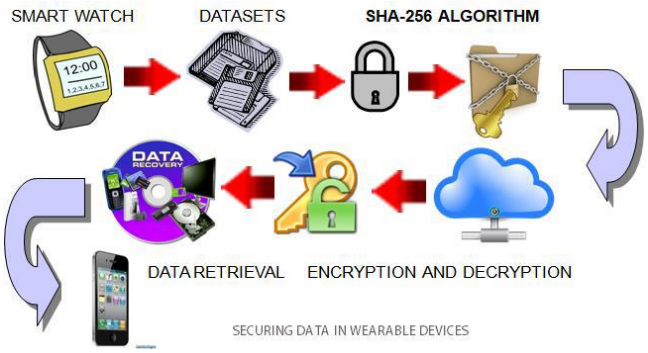

Fig. 1. Block Diagram of Enhancing Security in Wearable Devices

III. BACKGROUND

A. *Preprocessing of Input Data*

In order to check whether the login password that has been set by the user at the time of registration, matches with the password that has been attempted by the user during every login attempt. The algorithm that has been implemented is SHA-256 Algorithm. For the verification process, these data are generally maintained by means of Firebase. During each login attempts, it has been ensured that either password matches or not. Similarly, when the user account seems successfully created, it does not verify for the same mail id for the next time.

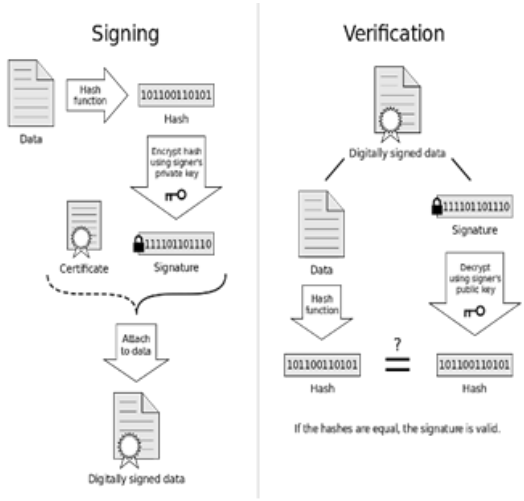

Fig. 2. Implementation of SHA Algorithm

B. *ID Based Cryptography*

The first implementation of identity-based signatures and an email-address based public-key infrastructure (PKI) was developed by Adi Shamir in 1984,which allowed users to verify digital signatures using only public information such as the user's identifier. Under Shamir's scheme, a trusted third party would deliver the private key to the user after verification of the user's identity, with verification essentially the same as that required for issuing a certificate in a typical PKI.

Identity-based systems allow any party to generate a public key from a known identity value such as an ASCII string. A trusted third party, called the private key generator (PKG), generates the corresponding private keys. To operate, the PKG first publishes a master public key, and retains the corresponding master private key (referred to as master key). Given the master public key, any party can compute a public key corresponding to the identity ID by combining the master public key with the identity value. To obtain a corresponding private key, the party authorized to use the identity ID contacts the PKG, which uses the master private key to generate the private key for identity ID.

Fig. 3. Secure Data Sharing One To One

C. *Implementation of ID Based Cryptography*

Here the Unique ID is sent to that of user's mail id. By means of unique mail id, the user can be able to identify his/her Own ID. An account is authenticated by means of the user's Unique ID which can be encrypted as a public key. It is called as ID – Based Cryptography.

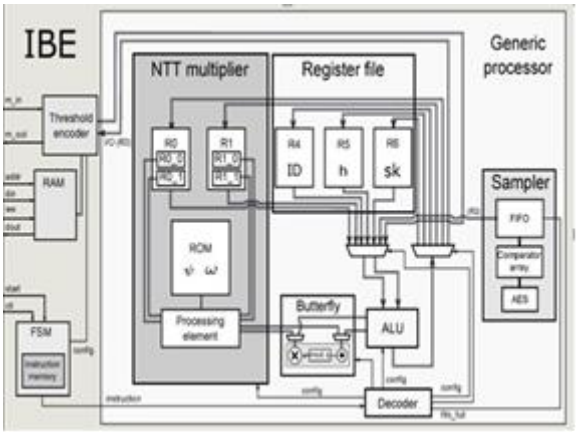

Fig. 4. Implementation of ID-Based Encryption

An identity-based encryption scheme enables the efficient distribution of keys in a multi-user system. Such schemes are particularly attractive in resource constrained environments where critical resources such as processing power, memory and bandwidth are severely limited. This research examines

the first pragmatic lattice-based IBE scheme presented by Ducas, Lyubashevsky and Prest in 2014 and brings it into the realm of practicality for use on small devices. This is the first standalone ANSI C implementation of all the software elements of the scheme with improved performance.

D. Extraction of Smart Watch Datasets

Here the system compares the datasets based on their fitness data that is generated from the smartwatch. Fitness data is generated for each and every milli seconds. When the data is successfully generated, it compares the results with that of the upcoming data. And finally, it produces a health care results of the user. The sample dataset I attached for the reference.

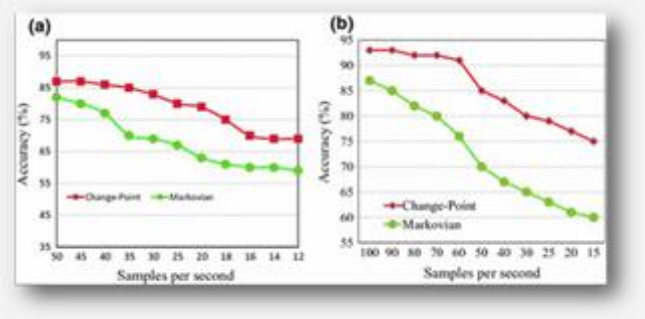

Fig. 5. Smartwatch Sample Datasets

E. Activation Function

In Step 1, the standard deviation of the Gaussian distribution from which f, g are generated is set to σf = 1.17p q 2N and is chosen so that E[||b1||] = 1.17√q. We have used a CDT Sampler in Step 2 to generate polynomials f, g from a discrete Gaussian distribution DN,σf over Rq. In Step 3, ||B˜ f,g||, the Gram Schmidt Norm of Bf,g, is computed, where Bf,g is a basis of the NTRU lattice associated to f, g (h = g ∗ f −1 mod q). If ||B˜ f,g|| > 1.17√q, the algorithm returns to Step 2 as the Gram-Schmidt Norm needs to be small enough so the basis can form a short trapdoor for sampling elements. In Step 5 the Extended Euclidean Algorithm is used to compute ρf , ρg∈ R and Rf , Rg∈ Z such that ρf · f = Rf and ρg · g = Rg. If GCD(Rf , Rg) 6= 1 or GCD(Rf , q) 6= 1, the algorithm returns to Step 2. Next, the algorithm computes u, v ∈ Z such that: u · Rf + v · Rg = 1. These integers are obtained from the Extended Euclidean algorithm (this extended version keeps track of the coefficients). In step 8, F = qvρg and Q = −quρf is computed so that f ∗G−g∗F = q, a condition needed to find a short basis. Next k = j F ∗f¯+G∗g¯ f∗f¯+g∗g¯ m is computed and F and G are reduced: F = F − k ∗ f and G = G − k ∗ g. The final steps generate and output the keys.

Polynomial h = g ∗ f −1 mod q is the master public key and defines a lattice Λh,q. Matrix B = A(g) −A(f) A(G) −A(F) is the master secret key and is a short basis for Λh,q. A is an anti-circulant matrix defined previously in Section 1.2. Key Generation is the most intensive component of the DLP-IBE scheme due to the arithmetic involving multiple-precision polynomials.

The Gram-Schmidt Norm is a property of the basis. It is the maximum of the norms (moduli) of the vectors in the Gram-Schmidt orthogonalization of the basis.

$$\text{GS Norm of } B = ||B||\tilde{} = \max i\in I \, ||\tilde{}bi|| \qquad (1)$$

The obvious way to compute the Gram-Schmidt Norm would be to compute the norms of each of the vectors and take the maximum.

IV. EVALUATION

A. Dataset

These datasets were generated by respondents to a distributed survey via Amazon Mechanical Turk between 03.12.2016-05.12.2016. Thirty eligible Fit bit users consented to the submission of personal tracker data, including minute-level output for physical activity, heart rate, and sleep monitoring. Individual reports can be parsed by export session ID (column A) or timestamp (column B). Variation between output represents use of different types of Fit bit trackers and individual tracking behaviors / preferences.

Id	Activity Date	Total Steps	Total Distance	Tracker Distance
1	3/25/2016	11004	7.11	7.11
2	3/26/2016	17609	11.55	11.55
3	3/27/2016	12736	8.53	8.53
4	3/28/2016	13231	8.93	8.93
5	3/29/2016	12041	7.85	7.85
6	3/30/2016	10970	7.16	7.16
7	3/31/2016	12256	7.86	7.86
8	4/01/2016	12262	7.87	7.87
9	4/02/2016	11248	7.25	7.25
10	4/03/2016	10016	6.37	6.37
11	4/04/2016	14557	9.8	9.8

Table.1. Fitness Datasets based on Daily Activities

B. Evaluation Metric

Cognitive Walkthrough is a method of testing user interface without user. When start testing use case we answer question Q0: “What does the user want to achieve?”

To determine level of usability of application we will go through use case step by step and at each step we raise questions.

Heuristic Evaluation is a method of testing that identifies usability problems in UI design. Application is tested if it follows the following heuristics.

C. *Experiments & Results*

Store the passwords using a function like **password_hash()** so that they're far more secure than being stored plain text (a huge no-no). This will generate unique salt each time so yes the hash will be different each time.

To validate the password the user is logging in with against the stored password, use **password_verify()** and pass it the password they posted and the stored hash from the database. The function will take care of the salt and comparison. This is the function that I think you might've missed when reading about password hashing.

A way to auto-generate key values is to specify your column as a type of uniqueidentifier and DEFAULT using NEWID() or NEWSEQUENTIALID(). Unlike IDENTITY, a DEFAULT constraint must be used to assign a GUID value to the column.NEWID() randomly generates a guaranteed unique value based on the identification number of the server's network card plus a unique number from the CPUclock. In contrast, NEWSEQUENTIALID() generates these values in sequential order as opposed to randomly.

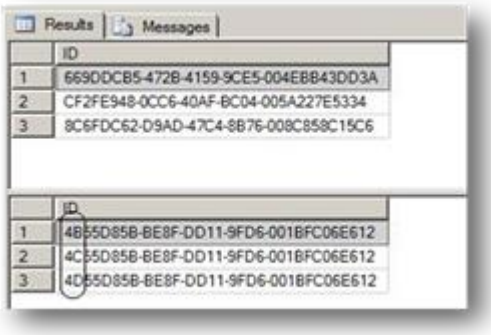

Fig. 6. Separate hash code for ID

1) 24/7 Heart Rate : Charge 3 uses the most advanced heart rate sensors and algorithms to uncover meaningful insights on your heart.

2) All Day Calorie Burn : Know how many calories you are really burning and use what you learn to reach your goals.

V. CONCLUSION

Thus from the above results, the system achieved the security of smart watch datasets using SHA-256 Algorithm for login authentication and for retrieving a particular id data ID-Based Encryption method is used. Now this system can withstand brute – force attack in a efficient manner. A user results can be processed without any delay and user can compare the results also with their previous results.

References

[1] Alexandros Pantelopoulos and Nikolaos G. Bourbakis,"A Survey on Wearable Sensor-Based Systems for Health Monitoring and Prognosis,"IEEE, vol. 40,pp.4-8 , 2010.

[2] Tommie W. Singleton,"The use of encryption in IT control and in the security of data and information,"University of Alabama at Birmingham,vol. 35924, pp. 4-8, 2011.

[3] Ke Wan Ching and Manmeet Mahinderjit Singh, "Wearable Technology Devices Security and Privacy Vulnerability Issues,"School of Computer Sciences,vol. 8, pp. 22-26, 2016.

[4] Marci Meingast, Tanya Roosta, Shankar Sastry, "Security and Privacy Issues with Health Care Information Technology," Department of Electrical Engineering and Computer Sciences,vol. SaC.14.4, pp. 5454-5457, 2016.

[5] Jingwei Liu Member of IEEE, Zonghua Zhang, Xiaofeng Chen Member of IEEE, and Kyung Sup Kwak Member of IEEE, "Certificateless Remote Anonymous Authenticationn Schemes for Wireless Body Area Networks,"IEEE, vol. 145, no. 5-6, 2013.

[6] Girish,Phaneendra"Identity Based Cryptography and Comparision with Traditional Public Key Encryption,"The National Institute of Engineering,Vol.5(4),pp.552-5524,2014.

[7] Ms. S.Padma 1, Dr.D.C.Joy Winnie Wise 2, Mr. S. Malaiarasan3, Ms. N. Rajapriya4, "Ensuring Authenticity and Revocability for Wireless Body Area Network using Certificateless Cryptography," "International Research Journal of Engineering and Technology (IRJET), "Vol.03,pp. 1712-1714, 2016.

[8] Sharvari Dixit1, Archana Gaikwad2, Snehal Gaikwad3, Shweta A.Shanwad4, "Public Key Cryptography Based Lossless and Reversible Data Hiding in Encrypted Images," SPPU, Bhivarabai Sawant Institute of Technology & Research, Pune, 2016.

[9] "Smartwatch Algorithm for Automated Detection of Atrial Fibrillation,"[Online]. Available:http://www.onlinejacc.org/. [Accessed May 2018].

[10] "Health at Hand – A systematic view of smart watch uses at health,"[Online]. Available: https://www.sciencedirect.com. [Accessed Oct 2016].

[11] "Healthcare Applications of Smart Watches,"[Online]. Available: https://www.ncbi.nlm.nih.gov [Accessed Nov 2016].

[12] "Smartwatches," [Online]. Available:https://www.researchgate.net [Accessed Apr 2015]

[13] "5 Reasons smartwatchneed security," [Online]. Available: https://www.techbeacon.com