International Journal of Latest Trends in Engineering and Technology
Special Issue SACAIM 2016, pp. 169-175
e-ISSN:2278-621X

ENCRYPTION OF DATA WITH BIOMETRIC IN M-COMMERCE

Manoj M[1], Vineet Stewart Lasrado[2] and CG Thomas[3]

Abstract- Protecting information is the process of Information security, it secures its availability, integrity, and privacy. The users of Mobile have increased drastically where users prefer to store data in the mobile so that they can use data wherever they go. In the present era of smartphones, we see that security has been given more priority than other aspects, since then the use of Biometrics came into existence. Biometric helps an individual to secure the data more efficiently. In this, we are going to discuss how biometric and encrypted data can be used in M-Commerce at the time of payment.

Keywords: Fingerprint, Biometric, smartphone, M-Commerce

I. INTRODUCTION

In the recent years, the use ofsmartphones is in the higher scale. Also with this, the use of online shopping has increased [1]. This integrates user's Biometric features into key generation process based on theSHA-1 algorithm so that the process is not known to the hackers who won't have thesame Biometric traits[2][3]. Here we are taking the Bio-Metric data of the user, device ID, and the credentials, which will be encryptedand stored locally. When the users try to pay through M-Commerce app users will be asked to verify himself by using the biometric device at the time of payment, once the device senses the biometric itallows the user tothe payment procedure and also credentials will be decrypted [4]. This will be validated with the user's input credentials and the stored credentials. This helps the user to pay safely through M-Commerce.

II. EXISTING ALGORITHM

SHA1Encryption Algorithm[5][6].

Step 1: Append Padding Bits

Message is "padded" with a 1 and as many 0's as necessary to bring the message length to 64 bits fewer than an even multiple of 512.

Step 2: Append Length

64 bits are appended to the end of the padded message. These bits hold the binary format of 64 bits indicating the length of the original message.

[1] *Aloysius Institute of Management and Information Technology, Mangaluru, Karnataka, India*
[2] *Aloysius Institute of Management and Information Technology, Mangaluru, Karnataka, India*
[3] *Aloysius Institute of Management and Information Technology, Mangaluru, Karnataka, India*

Step 3: Prepare Processing Functions

SHA1 requires 80 processing functions defined as:

f(t;B,C,D) = (B AND C) OR ((NOT B) AND D) (0 <= t <= 19)

f(t;B,C,D) = B XOR C XOR D (20 <= t <= 39)

f(t;B,C,D) = (B AND C) OR (B AND D) OR (C AND D) (40 <= t <=59)

f(t;B,C,D) = B XOR C XOR D (60 <= t <= 79)

Step 4: Prepare Processing Constants

SHA1 requires 80 processing constant words defined as:

K(t) = 0x5A827999 (0 <= t <= 19)

K(t) = 0x6ED9EBA1 (20 <= t <= 39)

K(t) = 0x8F1BBCDC (40 <= t <= 59)

K(t) = 0xCA62C1D6 (60 <= t <= 79)

Step 5: Initialize Buffers

SHA1 requires 160 bits or 5 buffers of words (32 bits):

H0 = 0x67452301

H1 = 0xEFCDAB89

H2 = 0x98BADCFE

H3 = 0x10325476

H4 = 0xC3D2E1F0

Step 6: Pseudo Code

For loop on k = 1 to L

(W(0),W(1),...,W(15)) = M[k] */* Divide M[k] into 16 words */*

For t = 16 to 79 do:

W(t) = (W(t-3) XOR W(t-8) XOR W(t-14) XOR W(t-16)) <<< 1

A = H0, B = H1, C = H2, D = H3, E = H4

For t = 0 to 79 do:

TEMP = A<<<5 + f(t;B,C,D) + E + W(t) + K(t) E = D, D = C,

C = B<<<30, B = A, A = TEMP

End of for loop

H0 = H0 + A, H1 = H1 + B, H2 = H2 + C, H3 = H3 + D, H4 = H4 + E

End of for loop

Limitations:

- Has known security vulnerabilities
- The key can be hackedby the hacker with various forms of hacking.

III.PROPOSED ALGORITHM

A SHA1 with device ID Encrypted

Step 1: Take the Input from the fingerprint sensor, and the value obtained from it store it in a string has a Message.

Step 2: Append Padding Bits

Message is "padded" with a 1 and as many 0's as necessary to bring the message length to 64 bits fewer than an even multiple of 512.

Step 3: Append Length

64 bits are appended to the end of the padded message. These bits hold the binary format of 64 bits indicating the length of the original message.

Step 4: Prepare Processing Functions

SHA1 requires 80 processing functions defined as:

f(t;B,C,D) = (B AND C) OR ((NOT B) AND D) (0 <= t <= 19)
f(t;B,C,D) = B XOR C XOR D (20 <= t <= 39)
f(t;B,C,D) = (B AND C) OR (B AND D) OR (C AND D) (40 <= t <=59)

f(t;B,C,D) = B XOR C XOR D (60 <= t <= 79)

Step 5: Prepare Processing Constants

SHA1 requires 80 processing constant words defined as:

K(t) = 0x5A827999 (0 <= t <= 19)
K(t) = 0x6ED9EBA1 (20 <= t <= 39)
K(t) = 0x8F1BBCDC (40 <= t <= 59)
K(t) = 0xCA62C1D6 (60 <= t <= 79)

Step 6: Initialize Buffers

SHA1 requires 160 bits or 5 buffers of words (32 bits):

H0 = 0x67452301
H1 = 0xEFCDAB89
H2 = 0x98BADCFE
H3 = 0x10325476
H4 = 0xC3D2E1F0

Step 7: Pseudo Code….

For loop on k = 1 to L
(W(0),W(1),...,W(15)) = M[k] */* Divide M[k] into 16 words */*
For t = 16 to 79 do:
W(t) = (W(t-3) XOR W(t-8) XOR W(t-14) XOR W(t-16)) <<< 1
A = H0, B = H1, C = H2, D = H3, E = H4
For t = 0 to 79 do:
TEMP = A<<<5 + f(t;B,C,D) + E + W(t) + K(t) E = D, D = C,
C = B<<<30, B = A, A = TEMP
End of for loop
H0 = H0 + A, H1 = H1 + B, H2 = H2 + C, H3 = H3 + D, H4 = H4 + E
End of for loop

Step 8: Encrypt the device ID

Acquiring the device ID and encrypting the device ID with sha1 algorithm

Step 9: Concatenating both the keys

Take the encrypted fingerprint key and the encrypted device ID key concatenate them as

a single string.

Step 10: Store the String
Store the string in the phone database.

Advantages of this Algorithm

- The data of the fingerprint will be encrypted with SHA1 Algorithm.
- The unique Device ID will be encrypted with SHA1 Algorithm.
- Produces a longer hash value.
- Both the encrypted keys will be concatenated and will be stored as a string.

IV. EXPERIMENT AND RESULT

The evaluation for the experiment "Encryption of data with Biometric in M-Commerce" has been achieved by using a smartphone with a fingerprint sensor. The experiment was performed using the Android Studio 2.1 platform. The experiment was tested in a smartphone consisting Android 6.1 Operating System with 6GB of memory and powered with 1.6GHz Qualcomm Snapdragon 820 a Quad-Core processor.

The experiment was performed by various users and appropriate results wereobtained. The userof the smartphone saved the fingerprint in the phone, the user opens the app and he is asked to authenticate his fingerprint to proceed further. According to the instruction the user verified the fingerprint and he was authenticated, as a test we kept the values of the encrypted device ID and encrypted fingerprint keyand a string of both concatenated was also obtained. Same procedure but different user whose fingerprint was not stored was tested and he got the message that the fingerprintcannot be recognized. In such cases the user can tap fingerprint sensor three times andthe input appears which tells user to use the security code which is stored at the time of registration of any app. If both the process is unsuccessful then the user won't be authenticated to the further payment procedure in a M-Commerce application.

The proposed algorithm was tested using fingerprint of the smartphone owner and also it was tested when the fingerprint was not stored in the device. The test cases where successful in both the cases. The tested results are as follows:

(a)

Figure 1:(a)Interface of the fingerprint screen.

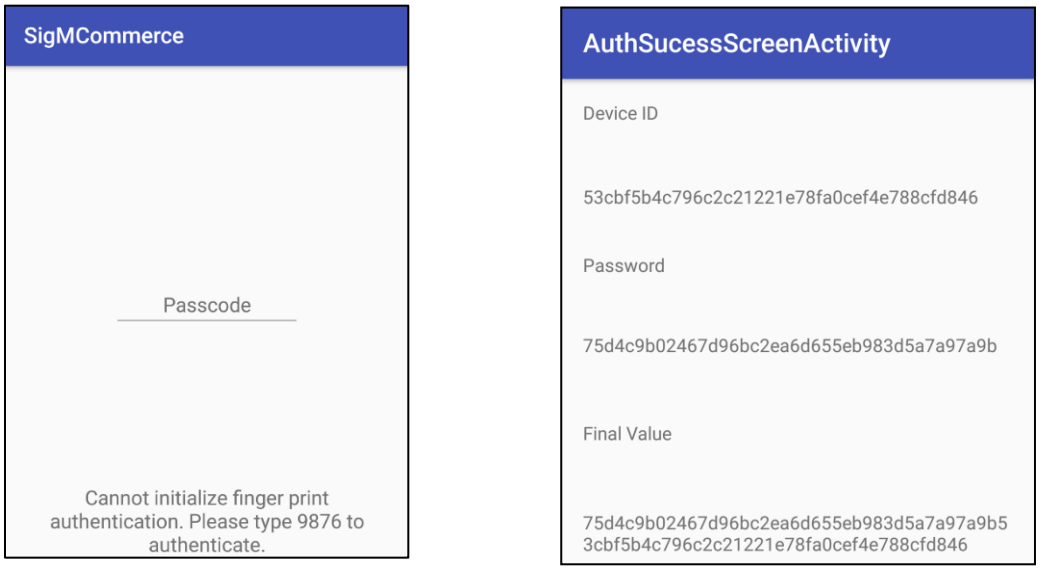
The Figure 1(a) portraits us the Interface that will occur to the user before he proceeds to the payment procedure. It tells the user to scan his fingerprint. If the fingerprint is matched, then the user is authenticated to the payment procedure.

Figure 2: (a) Encrypted key of Device ID with SHA1 Algorithm. (b)Encrypted key from the input of the Fingerprint value ([B@d205f44) [7]. (c)Concatenated string of key(b) and key(a). (d) Image after the fingerprint is matched successfully.

(a) (b)

Figure 3: (a) Error message if the finger is moved fast on the fingerprint sensor. (b) Error message cannot recognize the fingerprint

In figure 3 (a) the user moved his finger from the sensor too fast so the error was shown and told the user to try again to enter the payment procedure.In figure 3 (b) shows an error message suppose the fingerprint which is sensed is not matching the stored fingerprint from the device.



(a) (b)

Figure 4: (a) Passcode if fingerprint doesn't match. (b) The final result after encryption of the passcode.

Figure 4 (a) This option is appeared when the fingerprint is not matching with saved fingerprint or a phone without a fingerprint sensor. The passcode entered by the user will be encrypted with SHA1 Algorithm and will be concatenated with the device ID key (i.e. same has the figure 2 (c)). Figure 4 (b) This image displays the encrypted Device ID, Password and the final concatenated String. The Final value is concatenated first 40 characters of the encrypted password and then 40 characters of the encrypted Device ID.

V.CONCLUSION

Using this Algorithm, company which provides the app with this module can ensure users of company that security level will be high. The user will have to register their fingerprint and a password at the time of app registration and this helps them to securely transact online. Once the user has registered the fingerprint he can view the products and add items to the cart or if it's a banking app he adds all the details. At the time of payment, the user will be asked to scan his finger and authenticate himself. Suppose the fingerprint doesn't match he will be asked to add the registered password, this helps the user to buy the items safely and also no other person can use the app because at the time of payment the owner has to be authenticated. The same can be

used in mobile banking apps at the time of payment the app will verify whether it's the appropriate user. This approach helps people from not being attacked by the hackers.

VI.FUTURE WORK

In the future work of this topic, we will be concentrating towards the decryption of the encrypted data and authenticate the user to complete his transaction successfully.

REFERENCES

[1] Gagandeep Nagra, CBD Belapur, Gopal "An study of Factors Affecting on Online Shopping Behavior of Consumers"International Journal of Scientific and Research Publications, Volume 3, Issue 6, June 2013.

[2] http://findbiometrics.com/solutions/biometric-sensors-detectors/.

[3] Filip Orság ,Martin Drahanský "Biometric Security Systems: Fingerprint and Speech Technology".

[4] Colin Soutar, Danny Roberge , Alex Stoianov, Rene Gilroy, and B.V.K. Vijaya Kumar from Bioscrypt Inc "Biometric Encryption™".

[5] http://cs.winona.edu/lin/cs435/Presentations/SECURE%20HASHING%20ALGORITHM.ppt.

[6] http://www.herongyang.com/Cryptography/SHA1-Message-Digest-What-Is-SHA1.html.

[7] https://developer.android.com/reference/android/hardware/fingerprint/package-summary.html