BioWallet: A Biometric Digital Wallet

E. Benli, I. Engin, C. Giousouf, M. A. Ulak
Faculty of Computer and Informatics
Istanbul Technical University
34469, Maslak, Istanbul, Turkey
{benliel, engini, giousouf, ulak}@itu.edu.tr

Ş. Bahtiyar
Department of Computer Engineering
Boğaziçi University
34342, Bebek, Istanbul, Turkey
serif.bahtiyar@boun.edu.tr

Abstract— **People have used digital currencies to meet their online payment requirements in a more convenient, cheaper, and secure way. The currencies have been stored in digital wallets, where security is a significant challenge. In this paper, we propose a model that uses biometric methods to secure digital currencies within wallets. The proposed model improves both usability and security of payment transactions carried out with digital currencies, which are stored in wallets, by using fingerprints of users.**

Keywords- Digital currency; security; wallet; biometric.

I. Introduction

Recently, modern societies have become more connected than ever with the help of recent communication technologies. The connections have affected daily lives of people that have changed our habits. One of the most significant changes is our payment behavior, where payments shift from cash to digital money. This shift offers new benefits to corporations because the digital payment solutions have become more global. Therefore, the willingness to use such solutions has increased dramatically. Particularly, the research area of digital currencies has been given considerable attention. A digital currency is a currency that has neither physical representation nor belongs to a country. Nevertheless, it still has a value and allows individuals to make purchases or transactions with various amounts. For instance, the daily exchange of bitcoin may be $2 and $5 million USD. Recently, there are approximately $100 million bitcoins on the market [1].

The main issue about digital currencies is security. One of the significant challenges is the storage security of digital currencies that affects the anonymity of transactions. Existing storage systems have security vulnerabilities. This fact reduces the usability of digital currencies, which prevents the increase of online payment transactions. Some digital currency providers collaborate with third party security vendors to straighten the anonymity of transactions by enhancing security and trust. On the other hand, this approach does not provide complete trust since there is always a suspicion around what kind of security the third party provides related to the anonymity of transactions. This reduces trust in conventional digital currencies. Actually, some financial institutions use different security mechanisms to protect customers' data with the help of additional security mechanisms in the online environment, such as mobile and Web applications.

Wallets store digital currencies from where users obtain an address to use in order to make transactions. Simply, the sender must know the receiver's address in order to achieve a bitcoin transfer. Most of the time, third party organizations provide these addresses. Since the organizations can monitor transactions and they have all the critical information about users, anonymity and trust issues related to digital currency usage remain.

Most of the time, digital wallets are associated with specific hardware properties of computing devices to improve the security of the wallets for ensuring anonymity and trust. However, security usability is a challenge in those cases. For instance, if the device is lost, it is very hard or impossible to reach the coins within the wallet. Our motivation in this paper is the lack of usable security mechanisms that extend anonymity and trust for digital currencies. In this paper, we propose a conceptual model for securing credentials within digital wallets by using biometric methods. The model uses biometric sensors to reach biological properties of the users to increase usability. Particularly, we use data from fingerprint sensors to improve security usability of digital wallets for bitcoin like digital coins.

The reminder of the paper is organized as follows. Section II explains digital currencies and security. In Section III, we present our solution, BioWallet. Section IV is about the analysis of the proposed solution. Section V is devoted to conclusions and future works.

II. Security and Digital Currencies

There are various digital currencies, such as Bitcoin [1], Dogecoin [2], Mastercoin [2] and Litecoin [2]. Crypto currency is also used to refer to these currencies, since they have cryptographic properties. Bitcoin is a well-known and well-accepted digital currency. It is a distributed and open source digital currency system [1]. Bitcoin was designed by Satoshi Nakamoto in October, 2008. It addresses some crucial challenges, such as anonymity, double payment problem and illegal use of money. However, it does not provide a complete solution to these challenges [2][3]. Therefore, new digital currency systems similar to Zerocoin [1][4] have been developed.

Zerocoin [1], which was developed by Miers, solves some specific problems found in Bitcoin. It brings partial anonymity to transactions by hiding the senders' identity, but not the amount and the receivers' identity [4]. In addition, Zerocoin [1] tried to solve the double pay problem to ensure the integrity of digital currency systems. Although the structure of Zerocoin solves the double payment problem, it reduces the performance.

Ben et al. have introduced Zerocash [4] to solve the performance and anonymity problems of Zerocoin. They created DAP (Decentralized Anonymous Payment) scheme. Zerocash decreases the time of verification until 6 ms and hides the receiver identity by using DAP [4].

One of the most important parts of the digital currencies is wallets, since they allow users to store their bitcoins and transfer them whenever and wherever they desire. Although these wallets make the transaction process less challenging, they may be unprotected against thieves. For example, consider a user who is using a mobile bitcoin wallet to make his/her transactions. Someone can easily take that mobile device for a limited amount of time and send an amount of bitcoins to another bitcoin wallet account. The reason of this problem is the usage of traditional wallet systems that are working with just a password such as BlueWallet [9]. Therefore, it is obvious that a strong authentication mechanism is required for these wallet systems, especially for the people who desire to have it.

Hence, the biometric authentication systems are getting more common worldwide. Therefore many payment systems are shifting from traditional authentication methods to modern approaches like fingerprint, face recognition, ear recognition, and retina scan [6]. In personally identifiable authentication systems that contain critical data of the users, it is crucial to provide a strong access control mechanism to prevent unauthorized accesses to the confidential information related to financial information.

Bitcoin like cryptocurrencies still have security challenges. In 2011, intruders stole 25.000 bitcoins [1] that means we still have no strong access control for cryptocurrencies. On the other hand, Zerocoin has attempted to solve the double pay problem, which is one of the most essential challenges. In order to solve this problem, bigger sized spend proofs are used. As the block chain keeps the spend proofs, it may result in deployment problems [7]. In order to maintain the anonymity, Zerocoin uses zero-knowledge proof [7].

The protection of wallets where users keep their digital properties, such addresses and keys, is a significant challenge. Password based authentication methods are the common way to protect current digital wallets. On the other hand, passwords are prone to many attacks or simply they may be stolen. For instance, someone may make coin transactions from these wallets by taking possession of the passwords or device of the user.

Recent researches show that to get secret keys and passwords from a mobile device is a very easy process. Researchers have accomplished this using an ordinary magnetic probe to get the private key of some wallet applications [8]. This shows how vulnerable existing digital wallets are. One of the best ways to avoid this kind of problems is using biometric authentication methods, such as fingerprint and retina scan. [9].

BioWallet offers a new method for the specified problem. Bitcoin users can protect their information on storage by using the fingerprint based access control of BioWallet. Specifically, users need to enroll their fingerprints for the initial installation of the wallet. Moreover, a user must verify her fingerprint in every transaction. BioWallet improves the security of Zerocash that offers pure anonymity. We believe that the proposed solution extends the security of digital currency systems, particularly for crypto currencies.

III. BIOWALLET

One of the most useful methods to authenticate users is to use their biometric information. Almost all systems allow users to use their biometric information in terms of hardware. Additionally, the security of biometric methods is a proven fact [10][11][12].

In our model, users initially register their biometric credentials to the system. The information gathered from users is encrypted with 1024 or 2048-bits RSA (Rivest, Shamir, Adleman) keys and it is kept in server in order to protect the data. Figure 1 shows our model about secure registration process using fingerprint.

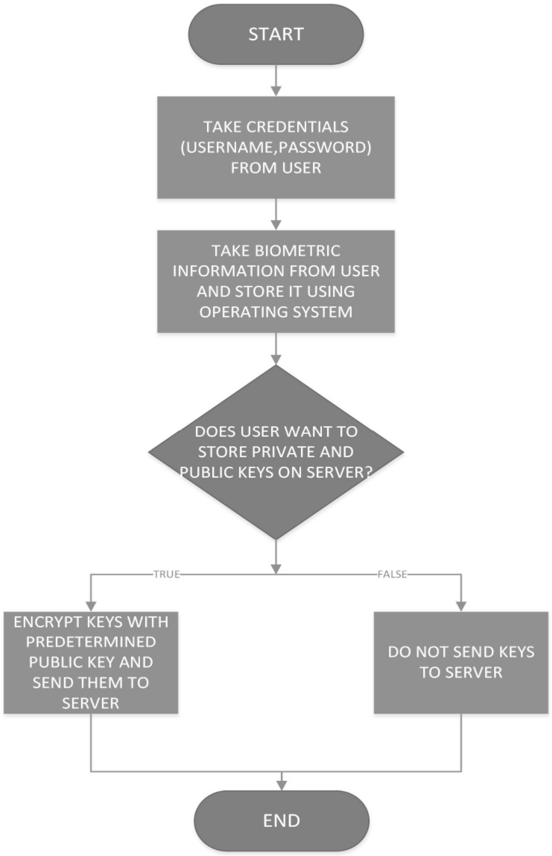
START
TAKE CREDENTIALS (USERNAME,PASSWORD) FROM USER
TAKE BIOMETRIC INFORMATION FROM USER AND STORE IT USING OPERATING SYSTEM
DOES USER WANT TO STORE PRIVATE AND PUBLIC KEYS ON SERVER?
TRUE
FALSE
ENCRYPT KEYS WITH PREDETERMINED PUBLIC KEY AND SEND THEM TO SERVER
DO NOT SEND KEYS TO SERVER
END

Fig. 1. Information gathering of users.

Below are the abbreviations we used in the encryption process.

PR_U : *Private key of user*
PU_U : *Public key of user*
PR_S : *Private key used in server*
PU_S : *Public key used in server*
$E(data, key)$: *Encryption of data with given key*
$D(cipher, key)$: *Decryption of cipher with given key*
$ciper = E(PR_U, PU_S)$
$PR_U = D(cipher, PR_S)$

After registration, in order to allow users to send bitcoins, we have two approaches. In the first approach, a user is authorized for a predetermined time (i.e. 10 minutes). In this manner, users are allowed to accomplish multiple transactions without approving their identities. However, it may be vulnerable against some attacks.

In the second approach, a user provides its identity for each transaction she initiates. This makes it harder for an attacker to steal coins. Figure 2 explains the flow of this approach. Here, we use two-phase authorization system in the model. In this way, we eliminate potential vulnerabilities emerged from using only biometric information.

During the process of sending bitcoins, a standard public key encryption is used. However, if a user loses his/her credentials (i.e. losing phone or logging out from the application), then he/she also loses the related keys.

When the user registers onto the system, a public-private keys pair is created. Then, the keys are sent to the server after encrypting them with a predetermined public key. The private key that is used to decrypt the encrypted public-private keys of user are kept on the server. Therefore, no one is able to reach the keys of the user.

A user may lose his/her device and he/she obtains a new device, where the user installs the wallet. When the user gives his/her credentials (username and password) and the answer of the security question, the system creates a new private and public key for the user. Since the server has the old encrypted version of private-public keys of the user and the private key to decrypt them, the system automatically sends the bitcoins left in the old account of the user to the new created account.

IV. ANALYSIS OF BIOWALLET

We compare BioWallet with existing wallets to show the advantages of the proposed solution. The first wallet system that we compare with BioWallet is BlueWallet. BlueWallet is a hardware device that uses Bluetooth technology. The device is a little mobile hardware box which contains input and output screens [9].

The most similar product is Case which is a bitcoin wallet that offers complete security in a hardware component that allows to spend or transfer bitcoins [13]. They claim that they do not save users' fingerprints directly in their database, but rather that the fingerprint patterns are stored and that helps to authenticate a user. The main lack of the product may be that it does not give chance to its users to reacquire their money when the users somehow lose them. Besides, Case uses a piece of hardware for performing all bitcoin operations. On the other hand, BioWallet uses a device built-in fingerprint scanner to scan fingerprints and keeps them on operating system. Therefore, it does not need any additional hardware but the smart phone that supports fingerprint scan.

There are many digital wallet systems, which store Bitcoin like cryptocurrencies by using only software solutions on Android or iOS. These options ensure diverse usage of personal smartphones as a digital wallet. The biggest advantage of mobile application wallets against any other wallet types is the availability when a user needs it. On the other hand, if there is no screen lock or another protection mechanism on smartphones, thieves can steal the smartphone and access any critical information. For example, one of the well-known wallet applications is Bitcoin Wallet. Although Bitcoin Wallet has some useful features like QR Code (Quick Response Code) scanning and more than one bitcoin receive address support, it does not have any security barrier against reaching the application except a single password.

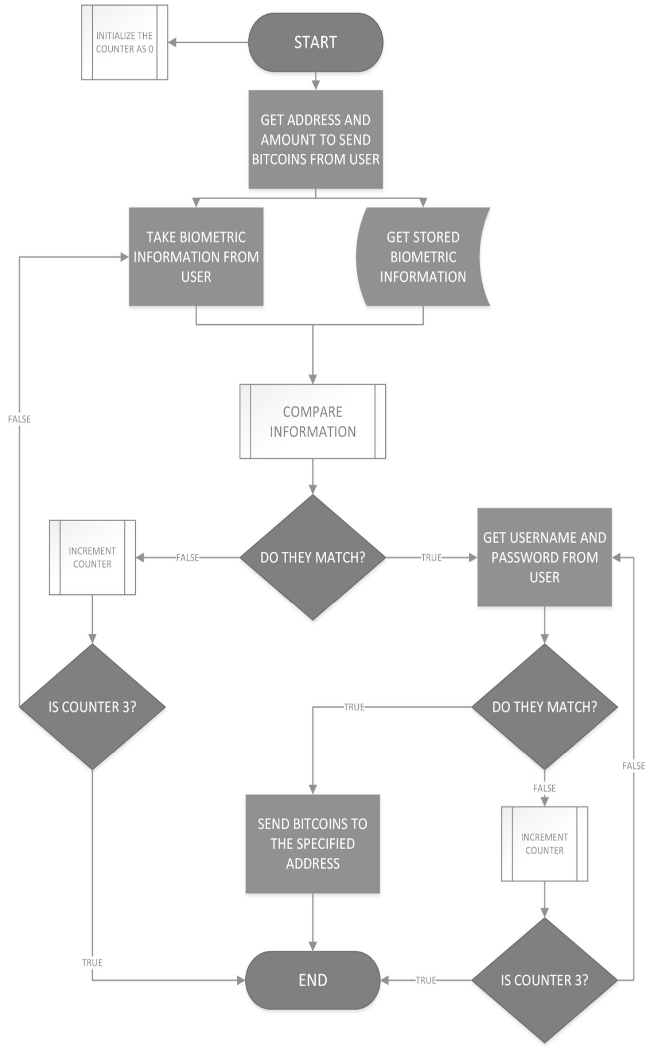
START
INITIALIZE THE COUNTER AS 0
GET ADDRESS AND AMOUNT TO SEND BITCOINS FROM USER
TAKE BIOMETRIC INFORMATION FROM USER
GET STORED BIOMETRIC INFORMATION
COMPARE INFORMATION
DO THEY MATCH?
FALSE
TRUE
INCREMENT COUNTER
GET USERNAME AND PASSWORD FROM USER
IS COUNTER 3?
FALSE
DO THEY MATCH?
TRUE
FALSE
SEND BITCOINS TO THE SPECIFIED ADDRESS
INCREMENT COUNTER
FALSE
TRUE
END
TRUE
IS COUNTER 3?

Fig. 2. Two phase authentication system

BioWallet protects the digital assets and transaction process with two-phase authentication system that employs fingerprint and password authentication. Additionally, BioWallet does not store any fingerprint data online to be able to preserve privacy. All personal data are stored locally. Based on the personal needs of a user, private and public keys can be stored at the cloud server in an encrypted way except fingerprint data. When users need to use a new device, the system sends user's money to the new device. Thus, digital wallet users can continue to use their digital money from the new device.

There is another kind of wallet for performing digital currency activities. It is called Web wallets where users can directly reach it from Web browser. Ordinary Bitcoin clients require at least 14 GB disk capacity and they need many hours to complete synchronization with block chain. Owing to Web wallets, no need for these requirements anymore. However, this kind of wallets are vulnerable from the server side. For example, 923 BTCs (Bitcoin) were stolen from OzCoin system [14].

TABLE I.
SUMMARY COMPARISON OF BIOWALLET AND OTHER WALLETS

Wallet Name	Fingerprint Authentication	Mobile Support	Basic Wallet Operations	Easy Transfer	Software Solution
BioWallet	✓	✓	✓	✓	✓
BlueWallet	×	✓	✓	✓	×
Case	✓	✓	✓	✓	×
Bitcoin Wallet	×	✓	✓	✓	✓
Web Wallets	×	×	✓	✓	✓
Desktop Wallets	×	×	✓	✓	✓

The last type of bitcoin wallets is desktop wallets. Desktop computers are safer than mobile computers or systems against physical theft. Moreover, almost all desktop computer systems have a system password at the beginning. Thus, fingerprint protection is not really solving security issues on personal computers when compared with the smartphones. That's why BioWallet is primarily created for mobile platform users. We compare BioWallet and other wallets in Table I.

V. CONCLUSION AND FUTURE WORK

Password based authentication mechanisms are inadequate for the protection of currencies within digital wallets. In this paper, we propose a solution that uses biometric methods to secure coins within digital wallets. A user can easily guard her digital coins by using BioWallet with her fingerprints that will extend the usability of digital currency.

As a future work, we will implement BioWallet. Moreover, we have been working to integrate other biometric methods to BioWallet, such as retina and face recognitions.

ACKNOWLEDGMENT

This work is supported by the Turkish State Planning Organization (DPT) under the TAM Project, number 2007K120610.

REFERENCES

[1] I. Miers, C. Garman, M. Green, and A. D. Rubin, “Zerocoin: Anonymous Distributed E-Cash from Bitcoin,” in 2013 IEEE Symposium on Security and Privacy (SP), 2013, pp. 397–411.

[2] F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," in *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2084-2123, third quarter 2016.

[3] S. Barber, X. Boyen, E. Shi, and E. Uzun, “Bitter to Better — How to Make Bitcoin a Better Currency,” in Financial Cryptography and Data Security, A. D. Keromytis, Ed. Springer Berlin Heidelberg, 2012, pp. 399–414.

[4] E. Ben-Sasson et al., “Zerocash: Decentralized Anonymous Payments from Bitcoin,” 349, 2014.

[5] http://www.coindesk.com/data/bitcoin-daily-transactions/. [Accessed: 18-Nov-2016].

[6] N. L. Clarke and S. M. Furnell, “Authentication of users on mobile telephones – A survey of attitudes and practices,” Computers & Security, vol. 24, no. 7, pp. 519–527, Oct. 2005.

[7] C. Garman, M. Green, I. Miers, and A. D. Rubin, “Rational Zero: Economic Security for Zerocoin with Everlasting Anonymity,” in Financial Cryptography and Data Security, R. Böhme, M. Brenner, T. Moore, and M. Smith, Eds. Springer Berlin Heidelberg, 2014, pp. 140–155

[8] D. Genkin, L. Pachmanov, I. Pipman, E. Tromer, and Y. Yarom, “ECDSA Key Extraction from Mobile Devices via Nonintrusive Physical Side Channels,” in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA, 2016, pp. 1626–1638.

[9] T. Bamert, C. Decker, R. Wattenhofer, and S. Welten, “BlueWallet: The Secure Bitcoin Wallet,” in Security and Trust Management, S. Mauw and C. D. Jensen, Eds. Springer International Publishing, 2014, pp. 65–80.

[10] V. Matyás Jr. and Z. Ríha, “Biometric Authentication - Security and Usability,” in Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security, Deventer, Netherlands, 2002, pp. 227–239.

[11] “Android 6.0 APIs | Android Developers.” [Online]. Available: https://developer.android.com/about/versions/marshmallow/android-6.0.html. [Accessed: 12-Nov-2016].

[12] “RSA Laboratories - Has the RSA algorithm been compromised as a result of Bernstein’s Paper?” [Online]. Available: http://www.emc.com/emc-plus/rsa-labs/historical/has-the-rsa-algorithm-been-compromised.htm. [Accessed: 19-Nov-2016].

[13] “Case - The world’s most secure and easy-to-use bitcoin wallet.” [Online]. Available: https://choosecase.com/faq.html. [Accessed: 18-Nov-2016].

[14] A. Gervais, G. O. Karame, V. Capkun, and S. Capkun, “Is Bitcoin a Decentralized Currency?,” *IEEE Security Privacy*, vol. 12, no. 3, pp. 54–60, May 2014