BioPay: Your Fingerprint is Your Credit Card

Fahad Alsolami,

Ph.D. in Engineering Concentration in Security
Information Technology Department
Faculty of Computer and Information Technology
King Abdulaziz University, Saudi Arabia

Abstract
In recent years, credit and debit cards have become a very con- venient method of payment. The growing use of card pay- ments, hereafter referred to as credit cards, is evident in the daily use with many applications, such as withdrawing money from an Automated Teller Machine (ATM) and making pay- ments in a store. Online payment has been very common these days, where the transaction is made across a great distance, al- lowing for online shopping. This has increased chance of credit cards experiencing a risk of cybersecurity attacks, particularly if the transaction amount is big enough. Another problem that arises is the potential fraud should a thief try to impersonate the credit card owners identity. To overcome these obstacles, we propose a BioPay scheme that uses the fingerprint biotoken to replace the current plastic credit card. The BioPay scheme uses the biometric data (fingerprint), revocable fingerprint bioto- kens (Biotope), and Bipartite token to provide high authenti- cation, non-repudiation, security and privacy for all payment transactions including money withdrawal from an ATM. The BioPay scheme collects biometric data (i.e. fingerprint) from users and embeds four-digit authentication numbers inside the encoding biometric data (i.e. fingerprint), finally distributing them over clouds. In the payment/withdrawal process, a user provides his/her fingerprint to complete the transaction. Bio- Pay scheme insures that the transaction process performs on an encrypted form to provide security and privacy for the cus- tomers bank information. Our experiment shows that BioPay has comparable accuracy and significant performance gain for performing the transaction process.

Keywords:
BioPay, Fingerprint, . Automated Teller Machine (ATM), security and privacy

1. Introduction

With the spread of e-commerce, many attacks are made against credit cards, debit cards, and other forms of online transac- tion; this has become so prevalent that securing card payments (hereafter referred to as credit cards) or inventing a new way of payment is no longer an alternative; it is a necessity. The credit card market is huge, containing 4000 firms and 75 mil- lion consumers [1]. The current bank credit card market is not enough for competition [1]. Recently, multiple payment tech- nologies have come into existence beside the credit card, such as Apple pay, Samsung pay, etc., both as a reaction for busi- ness revaluation and due to the increase of online e-commerce [24].

A study presents proof that consumers are willing to buy more when using a credit card payment [5]. A study evaluates the common use of credit card among college students in the United Sates, looking at habits for buying and attitudes towards money [2]. This leads to researchers inventing a programmable credit card that can access one or more credit accounts across multiple credit card companies [8]. Finally, another convenient invention is the use of a mobile payment device [13]. In sum, credit card payment system and other payment technologies, such as Apple Pay and Samsung Pay, provide convenient pay- ment methods while improving the e-commerce market.

Despite the great advantages of credit card and new payment technologies, security and privacy are still highlighted con- cerns for banks and customers. The most common concern is fraud, where the credit card information is impersonated. Many secure schemes are proposed in literature to improve the secu- rity and privacy. Whitworth [17] invents a credit card resistant fraud system using encryption that encrypts credit card on com- puting devices. Bezos et al [4] invents a secure method of com- municating credit cards over a non-secure network where the exchanging message between the merchant and customer con- tains a portion of each credit card numbers. Then the customer confirms in a return message which credit card can be used. Wong et al [7] invents a method to secure a credit card trans- action over the internet by inserting a user key into the user ac- count with a permutation variable. In each use, the permutation variable is changed, and the algorithm generates a new number. During the verification process, the permutation variable must be valid at the time of use. Stanfield et al [11] invents a dynamic card verification on credit transaction by requiring a card veri- fication value (CVVs) be provided from a secure wallet, which is software on the client side. This CVVs is used when no physical card is presented while shopping. Even though these schemes have solved many issues in credit card systems and financial transactions, other issues remain research challenges.

In this paper, we propose the BioPay scheme, which pro- vides security and privacy for customers bank information and for all bank transactions. The BioPay scheme is a new payment or/and a new ATM withdrawal tool for financial transactions, which uses a fingerprint as a credit card, since fingerprint data is unique where no two persons have the same fingerprint pat- tern. The BioPay scheme has many purposes such as payment online, payment in person, and withdrawal from an ATM, and is more convenient that

Manuscript received December 5, 2025
Manuscript revised December 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.12.5

makes it so a user does not need to carry a credit card. Specifically, our contribution is to design, imple- ment, and evaluate a BioPay scheme that uses the revocable fingerprint biotokens (Biotope) [30] and Bipartite token [31] to create a BioPay token. During the enrollment operation, Bio- Pay encodes the biometric data (i.e. fingerprint). Then, BioPay embeds an authentication code (i.e. a four-digit number) in- side the encoded fingerprint data. BioPay then distributes these tokens over the clouds. In the payment/withdrawal operation, BioPay matches the fingerprint data of a user in the encoded mode against the gallery token that is already saved in the sys- tem. If the matching is true, the BioPay scheme asks the user to enter his/her authentication code (i.e. the four-digit number). If the authentication code is true, the BioPay scheme sends an- other code as a text message through a user phone, providing second factor authentication. Finally, the BioPay scheme ver- ifies the second factor authentication; if found to be true, a user can perform his/her transaction operation (payment on- line, payment in person, and/or using ATM).

The rest of this paper is organized as follows: in section 2, we briefly describe previous related work. The objectives of BioPay are given in section 3. Our proposed BioPay algo- rithm is presented in section 4. In section 5, the description of the experimental design is given. The experimental evaluation and results are provided in section 6. Finally, the conclusion is drawn in section 7.

2. Background

2.1 Credit Card System Fraud

Fraud is the most pressing issue in credit card systems and bank transactions. Many schemes have been introduced in literature to detect fraud in a credit card system. Chan et al [3] provides a survey, evaluates the fraud detection techniques, and proposes a method that combines a fraud detector with a "cost model" to get significant results. They divide the large data set into small subsets and apply data mining technique to generate classifiers in parallel. Brause et al [6] presents a credit card fraud de- tection system by using a data mining technique with a neural network to achieve anti-fraud against credit cards. They apply data mining and a neural network algorithm on a given credit card transaction database to discover fraud attempts. Flitcroft et al. [10] invents a secure method that provides remote access a limited use number to reduce chances of credit card fraud. The access requires user authentication and another entry to validate the user. Wang et al [12] uses secondary verification to improve the accuracy of fraud detection. Then they perform an optimization experiment by applying the secondary verification using different threshold values. Carcillo et al [14] proposes a scalable real-time fraud finder (SCARFF) which implements machine learning with big data tools like Spark. The result of their experiment shows accurate fraud detection with a scalable system. Finally, Wang et al [15] uses distributed deep learning for credit card fraud detection which provides end-to-end privacy.

2.2 Credit Card System Authentication

Fingerprint data has long been an authentication tool in credit card systems. Gottfried et al [16] invents remote credit card authentication system by using a fingerprint authentication at the point of sale. Then the credit card company verifies the probe fingerprint by the gallery fingerprint stored in the database. The communication between the point of sale and the central database is in encryption form. Baratelli [18] invents a smart card with a fingerprint integrated reader. When a user inserts the smart card into a reader/writer, the scan machine asks for a user fingerprint. Then the smart card compares the user finger- print and give the matching result. If the matching is true, the card is enabled, and the user can access to information. Smith [19] invents a biometric anti-fraud plastic card, which requires a user to use his/her fingerprint for authentication. The plastic credit card compares the probe fingerprint against the gallery fingerprint stored in the plastic credit card. If the matching is true, the card is enabled, and the user can access informa- tion. Oshima et al [20] invents a card settlement method using a portable electronic device that has a fingerprint sensor. Chou et al [21] invents a card-type biometric that includes a biometric sensor to read the biometric data of a user and includes an op- erating/processing system to process the biometric data. Harris [22] invents an intelligent credit card system to improve biometric reading and other operations in a credit card system. Vogel et al [25] invents a flexible card with a fingerprint sensor and circuit chip to manage the communication with the finger- print sensor. Muley et al [26] presents an ATM system that uses fingerprint identification for money transactions that requires the ATM to have a fingerprint scanner. GieBmann [27] pro- poses a survey about the history of digital/electronic payment from credit cards to Apple Pay and blockchain technology. It discusses the understanding of technical and infrastructure for all payment schemes. Bhandari et al [28] proposes a literature survey about using fingerprint data as an authentication tool in ATMs to prevent fraud attacks. Thakur et al [29] proposes a scheme that uses a fingerprint scanner in a smartphone for se- curing the online transaction. They use the Android platform for their experiment. Even though these schemes have been introduced in literature as authentication tools for credit card system, they do not close the gap for using a biometric data in secure way.

3. Objectives of BioPay Scheme

The main goal of the BioPay scheme is to explore a new technology for payment by introducing fingerprint data to replace the current standard of the credit card. In this section, we ex- plore the objectives of BioPay scheme in non-repudiation, au- thentication, privacy, and security.

3.1 Non-Repudiation and Authentication

The BioPay scheme uses fingerprint data to achieve its goal in non-repudiation and authentication. During a payment and/or withdrawal operation from an ATM, a user must pro- vide his/her fingerprint, so a user cannot deny his/her transac- tion operation later. Thus, the BioPay scheme providing non-repudiation. Concerning authentication, fingerprint data is considered the highest authentication tool, so the bank/financial organization can verify who signed, meaning that the person who performs the payment operation is the right/authenticated person. The BioPay scheme requires a user to enroll his/her fingerprint data and then requires it be presented again at the time of payment. This allows the bank/financial organization system to verify and prove all transactions.

3.2 Security and Privacy

The BioPay scheme provides security and privacy, not only for user transaction information, but also for the fingerprint data itself. The BioPay scheme uses revocable fingerprint biotokens (Biotope) [30] to encrypt the transformation data of fingerprint. Thus, the BioPay scheme does not use fingerprint raw data, which provides security and privacy to the fingerprint data it- self. Moreover, the BioPay scheme creates a token for each user. Because this token is revocable and has expiration time, the BioPay scheme can delete the token if it has been hacked and/or expired. A new token is then created without needing to take the fingerprint data again for usability.

4. Design of BioPay Scheme Algorithm

4.1 Enrollment Operation

The enrollment operation, when a user registers for a BioPay token, is comparable to a customer getting his/her credit card from the bank, so we explain the scenario in those terms. First, a customer must be present in the bank, so the bank's agent can use the BioPay scheme to take the customer's fingerprint data. Second, the BioPay scheme algorithm follows the standard NIST Bozorth Matcher Algorithm [32] to create minutia points, a minutia points file, and a gallery pair table. Third, the BioPay scheme algorithm follows the revocable fingerprint biotokens (Biotope) [30] to transform the biometric data into stable data and then encrypt the transformation data to have a BioPay token for this customer. Fourth, the BioPay scheme re- quests the customer to enter a four-digit secret number. This number is like the four digits of a credit card used for authentication. Fifth, the BioPay scheme follows the Bipartite token [31] to hide the four digits inside the customer's BioPay token. Then the BioPay scheme sets the expiration data for the customer gallery BioPay token. Also, the customer enters his phone number to use as a second authentication.

After completing all these steps, the customer receives his/her gallery BioPay token and can use it for all bank activities, including money withdrawal from an ATM, payment in a store, and payment online. Finally, the BioPay scheme stores the BioPay tokens for all customers in the bank system either locally or in the cloud.

Fig. 1 Overview of the BioPay scheme architecture, which is considered to replace the current standard, which is a credit card. Each BioPay token has similar information as actual credit card such as expiration data, four digits for authentication, and a second factor authentication as a customer phone number where the BioPay scheme sends authentication messages.

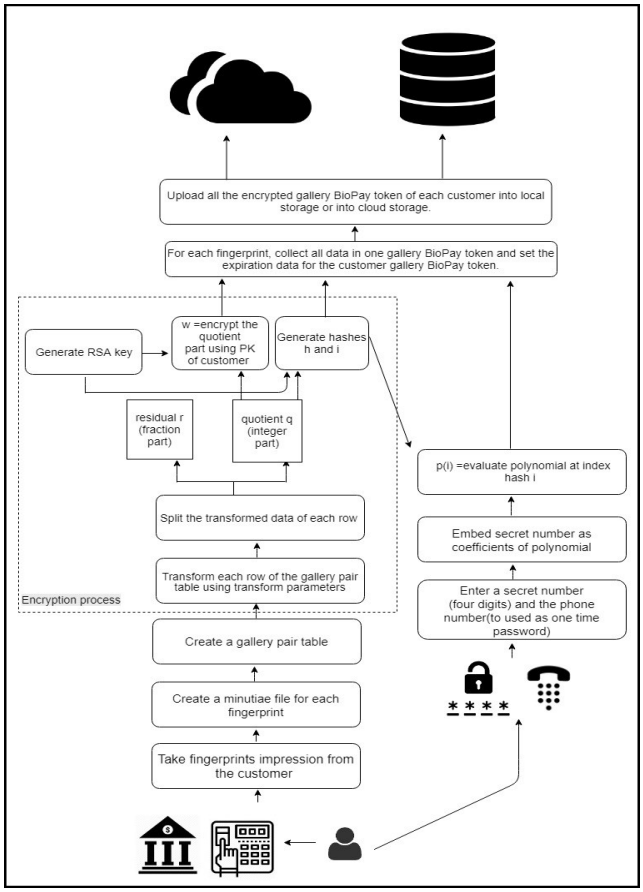

Fig. 2 Enrollment operation of BioPay scheme.Matching Operation

When using the matching operation that relies on the BioPay token for all bank activities, this operation is similar to a cus- tomer who needs to withdraw money from ATM, pay in store,or pay for online shopping. We explain in terms of the scenario where a customer needs to withdraw money from ATM. First, at the ATM, the BioPay scheme asks the customer to scan his/her fingerprint to start. Second, the BioPay scheme follows the same steps in enrollment operation to create minutiae points, a minutiae point file, a pair-table, and a pair-table trans- formation; the transformation data is encrypted, and a BioPay token is created. Third, the BioPay scheme matches the probe BioPay token against the gallery BioPay token that is stored in the system. If the authentication is successful, the BioPay scheme releases the four digits that have been stored inside the BioPay token from the gallery BioPay token; at the same time, the customer is asked to enter his/her four digits to compare the two numbers for authentication. Fourth, if the authentication is successful, the BioPay scheme sends a random number as a text message to the customer phone and asks him/her to enter this number as a second factor authentication. Finally, if the authentication is successful, the customer is considered authenticated and he/she is the right customer, so the BioPay scheme lets the customer withdraw money from ATM.

5. Experiment Design

Our experiment is designed to mimic a real-life scenario where a user can use his/her fingerprint to perform an online payment. First the user enrolls his/her fingerprint in a bank or financial organization, so the BioPay scheme can create a token for each user. During the payment operation, the user provides his/her fingerprint data for matching to complete the transaction. Our experiment compares our scheme Bio- Pay against two baselines: the revocable fingerprint biotokens (Biotope) [30] and Cloud-ID-Screen [33]. We conduct our experiment in the AWS cloud, so we use EC2 for computation and S3 for storage. We connect EC2 with S3 by using the Python boto library. We use the C++ and Python programming languages. BioPay scheme uses the fingerprint dataset called (FV C2002Db2 a) [34]. Finally, we did our experiment for twenty runs and calculated the average.

6. Experimental Evaluation

In the BioPay experiment. we seek to prove that if we use fingerprints instead of credit card during the payment process, we improve speed while getting comparable accuracy as com- pared to the two baselines. To test our hypothesis, we conduct two experiments, accuracy and performance, and we evaluate our results to draw our conclusion.

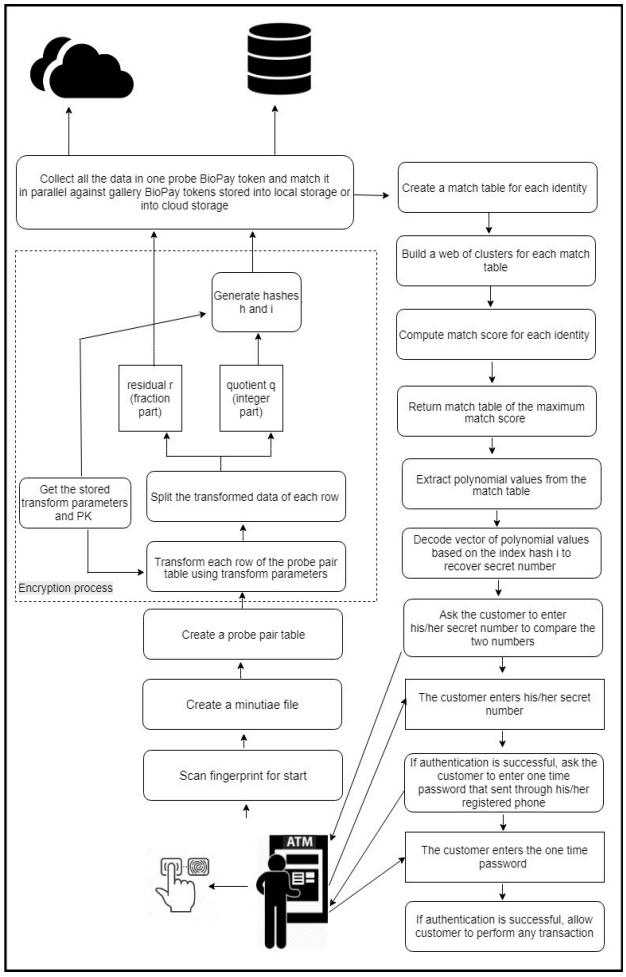

Fig. 3 Matching operation of BioPay scheme.

6.1 Accuracy Experiment

In the accuracy experiment, we need to evaluate BioPay scheme for the false accept rate (FAR) and for the genuine accept rate (GAR). Then we compare this result against the two baselines to determine how accurate the BioPay scheme is. The ROC curve results indicate that the GAR is equal to 97 and the FAR is equal to zero, a promising result that supports our hypothesis claim. Figure 4 shows the GAR and FAR results of the BioPay scheme comparing to the two baselines Bipartite Biotoken and Cloud-ID-Screen.

6.2 Speed Evaluation

In our performance experiment, we pick one user and compare his/her fingerprint against all records stored in the dataset. We did the comparison twenty times and took the average. Finally, we compared our result with the two baselines.

The performance results of BioPay demonstrate our scheme accomplished its goal with promising results. The P-value and t-test rejected the null hypothesis, which claim that the two baselines are better than BioPay scheme. This rejection of null hypothesis supports our hypothesis and proves our claim.

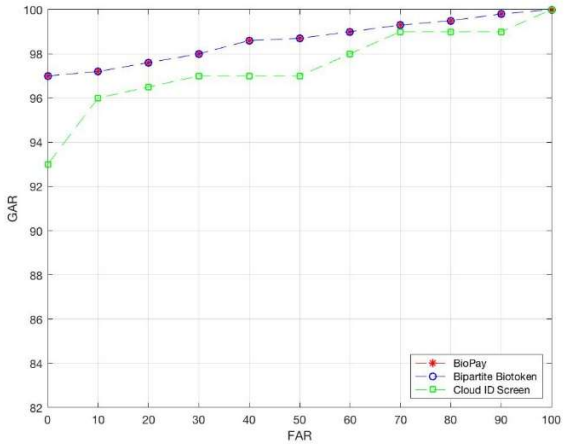

Fig. 4 The ROC curve shows the GAR and FAR comparison between the BioPay scheme and the two baselines Bipartite Biotoken and Cloud-ID-Screen.

7. Conclusion

In conclusion, to improve customer convenience by not requir- ing a credit card be carried, the software BioPay token can be used at any time with a provided fingerprint. For security and privacy, the BioPay cannot be stolen because the fingerprint is needed for authentication, and the BioPay does not use the fingerprint raw data, instead using the encryption of the trans-formation data of fingerprint. Moreover, the BioPay invention system has three level of security: fingerprint authentication, four-digit authentication, and the random number sent through a customer's phone as a text message acting as second authen-tication.

References

[1] L. M. Ausubel, "The failure of competition in the credit card market.," The American Economic Review, pp. 50– 81, 1991.

[2] J. A. . Roberts and E. Jones, "Money attitudes, credit card use, and compulsive buying among American col- lege students.," Journal of consumer affairs, vol. 35, no. 2, pp. 213–240, 2001.

[3] P. K. . Chan, Distributed data mining in credit card fraud detection. 1999.

[4] J. P. . Bezos, "Secure method and system for communi- cating a list of credit card numbers over a non-secure net- work.," U.S. Patent, vol. 5, 2 1998.

[5] D. . Prelec and D. Simester, "Always leave home without it: A further investigation of the credit-card effect on will- ingness to pay.," Marketing letters, vol. 12, no. 1, pp. 5– 12, 2001.

[6] T. L. . Brause and M. Hepp, ""Neural data mining for credit card fraud detection." Tools with Artificial Intelli- gence," 1999.

[7] J. Y. . Wong and R. L. Anderson, "System for secured credit card transactions on the internet.," U.S. Patent, vol. 5, 9 1999.

[8] R. S. . Wallerstein, "Programmable credit card.," U.S. Patent, vol. 5, 12 1996.

[9] S. H. . Wynn, "Programmable multiple company credit card system.," U.S. Patent, vol. 5, 1 1999.

[10] D. I. . Flitcroft and G. O'donnell, "Credit card system and method.," U.S. Patent, vol. 7, 7 2009.

[11] G. T. . Stanfield and J. Vacca, "Dynamic card verification values and credit transactions.," U.S. Patent, vol. 8, p. 29, 10 2013.

[12] B. C. . Wang and J. Chen, ""Credit card fraud detection strategies with consumer incentives." Omega(2018)."

[13] T. W. . Markison, "Credit card imaging for mobile pay- ment and other applications.," 2012.

[14] F. . Carcillo, "SCARFF: A scalable framework for streaming credit card fraud detection with spark.," Infor- mation fusion, vol. 41, pp. 182–194, 2018.

[15] Y. . Wang, "Privacy Preserving Distributed Deep Learn- ing and Its Application in Credit Card Fraud Detection." 2018 17th. 2018.

[16] O. . Gottfried, "Remote credit card authentication sys- tem.," U.S. Patent, vol. 6, 8 2001.

[17] B. . Whitworth, "Fraud resistant credit card using encryp- tion, encrypted cards on computing devices.," U.S. Patent Application, vol. 9, no. 764.

[18] P. J. . Baratelli, "Smart card with integrated fingerprint reader.," U.S. Patent, vol. 6, 12 2001.

[19] R. . Smith, “Biometric anti-fraud plastic card.,” U.S. Patent Application, vol. 11, no. 233.

[20] S. . Oshima, “Card settlement method using portable elec- tronic device having fingerprint sensor.,” U.S. Patent Ap- plication, vol. 10, no. 542.

[21] B. C. . Chou, “Card-type biometric identification device and method therefor.,” U.S. Patent, vol. 7, 9 2008.

[22] S. C. . Harris, “Intelligent credit card system.,” U.S. Patent, vol. 7, 4 2008.

[23] O. . Ogbanufe and D. J. Kim, Comparing fingerprint- based biometrics authentication versus traditional authen- tication methods for e-payment. 2018.

[24] K. . Vogel and J. L. Shaffer, “Flexible card with finger- print sensor.,” U.S. Patent, vol. 9, 10 2017.

[25] A. . Muley and V. Kute, Prospective solution to bank card system using fingerprint. 2018.

[26] “Digital Payment 1971/2014: From the Credit Card to Apple Pay.",” Administration & Society, vol. 50, no. 9, pp. 1259–1279, 2018.

[27] S. . Bhandari and Z. K. Mundargi, “A Review on Securing ATM System Using Fingerprint.,” 2018.

[28] M. R. S. . Thakur and K. Kakde, "Securing Online Trans- actions Using. 2018.

[29] W. J. S. . Boult and R. Woodworth, “Revocable finger- print biotokens: Accuracy and security analysis.,” Com- puter Vision and Pattern Recognition, vol. 2007, 2007.

[30] . W. J. Scheirer and T. E. Boult, Bipartite biotokens: Def- inition, implementation, and analysis,. 2009.

[31] “User’s guide to non-export controlled distribution of nist biometric image software,,” 2004.

[32] B. A. . Alsolami and T. Boult, Cloud-ID-Screen: Secure fingerprint data in the cloud. 2018.

[33] A. K. J. . D. Maltoni and S. Prabhakar, “Handbook of fingerprint recognition,,” 2009.