Đề xuất giải pháp bảo mật dữ liệu riêng tư trong xếp hạng tín dụng của các ngân hàng thương mại ở Việt Nam

Đinh Trọng Hiếu **Nguyễn Thị Thu Trang**
Khoa Hệ thống thông tin quản lý, Học viện Ngân hàng

Xếp hạng tín dụng khách hàng (hay còn được gọi là chấm điểm tín dụng) được đánh giá là một trong những khâu quan trọng nhất giúp các ngân hàng thương mại (NHTM)/ tổ chức tín dụng (TCTD) phòng ngừa và hạn chế rủi ro trong hoạt động tín dụng. Tuy nhiên, việc tiếp cận tới các thông tin của khách hàng phục vụ cho việc chấm điểm tín dụng, đặc biệt là những thông tin mang tính chất riêng tư, nhạy cảm là điều không hề đơn giản. Thậm chí, kể cả khi khách hàng đồng ý cho các NHTM/TCTD sử dụng dữ liệu của mình thì việc lưu trữ, quản lý dữ liệu đó theo đúng quy định cũng hết sức phức tạp. Bài báo này, chúng tôi đề xuất một giải pháp cho phép các NHTM/TCTD xếp hạng tín dụng khách hàng trong khi hạn chế tối đa việc chia sẻ dữ liệu của khách hàng giữa các bên liên quan. Giải pháp này

A solution to secure private data in credit scoring for commercial banks in Vietnam

Abstract: Credit rating (also known as credit scoring) is considered as one of the most important steps to help commercial banks and credit institutions prevent and limit risks in credit activities. However, access to customer information for credit scoring is not simple, especially confidential and sensitive information. Even if the customer agrees to let the commercial banks or credit institutions use their data, the storage and management of such data in accordance with the regulations is also very complicated. In this paper, we propose a solution that allows commercial banks/credit institutions to calculate customer credit score while minimizing the sharing of customer data among stakeholders. Our solution helps protect the privacy and confidentiality of all parties.

Keywords: credit scoring, security, private data, banking

Hieu Trong Dinh
Email: hieudt@hvnh.edu.vn
Trang Thi Thu Nguyen
Email: trangntt83@gmail.com
Organization of all: Faculty of Management Information Systems, Banking Academy of Vietnam

[1] Bài báo được thực hiện trong khuôn khổ Đề tài khoa học cấp Học viện Ngân hàng: "Nghiên cứu ứng dụng giải pháp khai phá dữ liệu đảm bảo tính riêng tư trong phân tích dữ liệu NHTM Việt Nam", do Thạc sỹ Vũ Duy Hiến làm chủ nhiệm cùng nhóm thành viên thực hiện, Mã số: DTHV.02/2019.

Ngày nhận: 28/04/2020 *Ngày nhận bản sửa: 14/05/2020* *Ngày duyệt đăng: 15/00/2019*

ISSN 1859 - 011X

được kỳ vọng sẽ giúp các thông tin riêng tư và bí mật của các bên được bảo vệ an toàn hơn.
Từ khóa: bảo mật, dữ liệu riêng tư, xếp hạng tín dụng

1. Giới thiệu

Trong lĩnh vực tài chính- ngân hàng (TC-NH), hoạt động xếp hạng tín dụng khách hàng là đánh giá về rủi ro tín dụng, chất lượng tín dụng, khả năng và thiện chí của chủ thể đi vay trong việc đáp ứng các nghĩa vụ tài chính một cách đầy đủ và đúng hạn (Reserve, 2007). Hoạt động này được đánh giá là một trong những khâu quan trọng nhất giúp các NHTM và TCTD phòng ngừa và hạn chế rủi ro trong hoạt động tín dụng. Hiện nay, đối với các NHTM cổ phần (NHTMCP) ở Việt Nam như Vietcombank, BIDV, Vietinbank, công cụ xếp hạng tín dụng phổ biến nhất được sử dụng là chấm điểm tín dụng theo mô hình được tư vấn bởi chuyên gia (Dinh & Kleimeiera, 2007; Lê & Đặng, 2016; Nguyễn, 2019).

Để phục vụ cho hoạt động xếp hạng tín dụng, mỗi khách hàng cần phải cung cấp nhiều thông tin, bao gồm cả thông tin mang tính riêng tư như: thu nhập cá nhân, tổng số dư nợ hiện tại, các gói bảo hiểm nhân thọ tham gia, cước di động hàng tháng... cho các NHTM/TCTD. Những dữ liệu, thông tin này thường được chia sẻ từ phía các bên sở hữu (ví dụ: CIC, công ty bảo hiểm nhân thọ, công ty viễn thông, cơ quan thuế…) dưới sự đồng ý của khách hàng.

Mặc dù việc sử dụng, lưu trữ và bảo vệ dữ liệu thông tin riêng tư của cá nhân đã được quy định trong Điều 21 (Hiến pháp, 2013), Nghị định 117 (Chính phủ, 2018), Thông tư số 18 (NHNN, 2018), Khoản 2 Điều 46 của Luật Giao dịch điện tử năm 2005 (Luật GDĐT, 2005), Điều 72 của Luật Công nghệ thông tin năm 2006 (Luật CNTT, 2006), Mục 2 bảo vệ thông tin cá nhân của Luật An toàn thông tin mạng năm 2015 (Luật ATTTM, 2015), tuy nhiên các vụ việc nghiêm trọng làm lộ thông tin cá nhân của khách hàng vẫn xảy ra, đồng thời cũng không thể ngăn ngừa các tổ chức, cá nhân sử dụng dữ liệu khách hàng vào mục đích trái phép. Bên cạnh đó, việc sử dụng "chéo" dữ liệu khách hàng giữa các bên liên quan càng làm tăng nguy cơ rò rỉ các thông tin nhạy cảm và bí mật. Vì vậy, nhiệm vụ bảo vệ tính riêng tư cho dữ liệu khách hàng trong quá trình xếp hạng tín dụng là rất cấp thiết và phù hợp với tình hình thực tiễn hiện nay.

Tính đến nay, cùng với sự phát triển của hướng nghiên cứu phân tích dữ liệu ngân hàng đảm bảo tính riêng tư (Meints & Möller, 2004; Abbe, Khandani, & Lo, 2012), một vài kết quả nghiên cứu bảo vệ tính riêng tư cho thông tin khách hàng trong quá trình xếp hạng tín dụng đã được giới thiệu.

Elli Androulaki đã đề xuất trong (Androulaki, 2011) công cụ chấm điểm tín dụng khách hàng bảo vệ tính riêng tư với sự hợp tác giữa một ngân hàng và các tổ chức liên quan tới điểm tín dụng của khách hàng. Với kỹ thuật ẩn danh, giải pháp này đã giúp cho ngân hàng cập nhật điểm tín dụng của khách hàng dựa trên dữ liệu của khách hàng được gửi trực tiếp từ các tổ chức đối tác.

Trong nghiên cứu (Ralf Stecking and Klaus B. Schebesch, 2015), các tác giả đã giới thiệu mô hình chấm điểm tín dụng khách

hàng dựa trên kết quả phân lớp dữ liệu khách hàng sẵn có với ràng buộc đảm bảo tính riêng tư. Phương pháp xác định điểm tín dụng sử dụng kỹ thuật khai phá dữ liệu này được áp dụng khá phổ biến trên thế giới, tuy nhiên lại chưa được áp dụng ở Việt Nam- nơi mà điểm tín dụng vẫn được xác định chủ yếu thông qua ý kiến của chuyên gia.

Gần đây, Wang và cộng sự (Wang, Chen, & Feng, 2018) đã đề xuất công cụ chấm điểm tín dụng khách hàng trên môi trường đám mây trong khi vẫn bảo vệ được dữ liệu riêng tư của khách hàng. Trong nghiên cứu này, các bên sở hữu dữ liệu khách hàng liên quan tới điểm tín dụng sẽ tải dữ liệu khách hàng (đã được mã hóa) lên máy chủ (đám mây). Việc chia sẻ này rất dễ gây mất an toàn nếu bên sở hữu khóa mật mã thông đồng với địch thủ.

Trong bài báo này, chúng tôi đề xuất một giải pháp cho phép các NHTM/TCTD xếp hạng tín dụng khách hàng trong khi hạn chế tối đa việc chia sẻ trực tiếp dữ liệu của khách hàng giữa các bên liên quan. Cụ thể, giải pháp của chúng tôi kỳ vọng đạt được những mục tiêu như sau:

- Dữ liệu khách hàng do các bên sở hữu được giữ bí mật đối với ngân hàng.

- Khách hàng và các đối tác sở hữu dữ liệu khách hàng không khai thác được công thức tính điểm tín dụng của ngân hàng.

Nội dung chính của bài báo được tổ chức như sau: phần 2 nhằm cung cấp cơ sở lý thuyết để xây dựng giải pháp đề xuất. Ngoài trình bày chi tiết giải pháp này, phần 3 chứng minh tính chính xác và phân tích tính riêng tư của giao thức đề xuất.

2. Cơ sở lý thuyết

Trong phần này, chúng tôi nhắc lại các yêu cầu của bài toán chấm điểm tín dụng đảm bảo tính riêng tư và một số kết quả trong lý thuyết mật mã như: Hệ mã hóa ElGamal, thuật toán Shanks's baby-step giant-step, giao thức tính tích vô hướng bí mật và giao thức tính tổng bí mật. Đây là những cơ sở lý thuyết được chúng tôi sử dụng làm nền tảng để xây dựng giải pháp đề xuất.

2.1. Phát biểu bài toán

Ngoài những dữ liệu của khách hàng không thuộc loại riêng tư và nhạy cảm, chúng tôi giả sử rằng NHTM sử dụng thêm thuộc tính "bí mật và riêng tư" (A_1, A_2, ..., A_k) làm căn cứ xếp hạng tín dụng cho khách hàng. Ví dụ: *mức thu nhập, nhóm nghề nghiệp, số dư nợ tín dụng, bảo hiểm nhân mạng*.

Một khách hàng C với các đặc trưng tương ứng (c_1, c_2, ..., c_k) được xếp hạng như sau:

- Với mỗi đặc trưng c_i của thuộc tính A_i: C nhận được điểm $Mark_i$ theo thang điểm và hệ số mà B quy định.

- Tổng điểm tín dụng cho khách hàng C là Mark (C) = $\sum_{i=1}^{k} \mathbf{Mark_i(C)}$.

- Ngân hàng B căn cứ vào bảng quy đổi để biết hạng tín dụng của C và từ đó quyết định cho X vay hay không.

Chúng tôi khái quát bài toán xếp hạng tín dụng khách hàng có đảm bảo tính riêng tư như sau:

- Ngân hàng xét mỗi thuộc tính A_i thành các nhóm đặc trưng (A_i^1, ..., $A_i^{m(i)}$) và điểm tương ứng cho mỗi nhóm là ($mark_i^1$, ..., $mark_i^{m(i)}$) cho mỗi trường hợp. Ví dụ: thuộc

tính *Bảo hiểm nhân mạng* được Ngân hàng phân thành năm nhóm đặc trưng: *> 100 triệu; 50-100 triệu; 50-100 triệu; < 30 triệu; Không có,* với điểm tương ứng là 100, 75, 50, 25, 0.

- B công bố thông tin chi tiết (A_i^1, ..., $A_i^{m(i)}$) cho tất cả đối tác và giữ bí mật ($mark_i^1$, ..., $mark_i^{m(i)}$).

- Các đối tác không tiết lộ các đặc trưng c_i của khách hàng mà họ nắm giữ. Một đối tác có thể nắm giữ nhiều đặc trưng.

Ngân hàng B cần tính được tổng số điểm C đạt được và xếp hạng tín dụng cho C.

Tương tự như những bài toán phân tích dữ liệu đảm bảo tính riêng tư khác, bài toán này có thể giải quyết bằng hai phương pháp cơ bản là: phương pháp biến đổi ngẫu nhiên (Randomization) và phương pháp tính toán bảo mật nhiều thành viên (Secure Multiparty Computation- SMC). Tuy nhiên, phương pháp SMC được ưa chuộng hơn vì tính chính xác của kết quả đầu ra và tính riêng tư của dữ liệu người dùng được đảm bảo chắc chắn. Vì vậy, giải pháp của chúng tôi được xây dựng theo phương pháp thứ hai này.

2.2. Hệ mã hóa ElGamal

Phần này trình bày về hệ mã hóa ElGamal (ElGamal, 1985). Đây là cơ sở nền tảng để xây dựng giải pháp đề xuất.

Cho G là một nhóm cyclic cấp g với phần tử sinh , trong đó các bài toán logarit trong G là khó giải. Khóa bí mật x ϵ [1, q - 1] và khóa công khai tương ứng là $h = g^x$.

Ở bước mã hóa, người gửi sử dụng khóa công khai h để tính toán bản mã C cho bản rõ M như sau: anh ấy chọn ngẫu nhiên giá trị k ϵ [1, q - 1] và tính bản mã $C = (C_1 = M.h^k, C_2 = g^{k)}$.

Để giải mã, người nhận sử dụng khóa bí mật x theo công thức $M = C_1 . (C_2^x)^{-1}$.

Theo giả thuyết Diffie-Hellman quyết định (decisional Diffie–Hellman (DDH) assumption), hệ mã hóa ElGamal kể trên an toàn (Boneh, 1998).

2.3. Thuật toán Shanks's baby-step giant-step

Trong lĩnh vực số học và đại số, thuật toán Shanks's baby-step giant-step (Shanks, 1971) được sử dụng để giải quyết hiệu quả hơn các bài toán logarit rời rạc so với giải thuật vét cạn. Thuật toán này được trình bày ở Hình 1.

Chú ý rằng, nếu giá trị x cần tìm bị giới hạn bởi giá trị n ($x \leq n << q$) thì thuật toán trên sẽ hiệu quả hơn bởi vì giá trị n sẽ được thay thế bởi giá trị .

2.4. Giao thức tính tích vô hướng bí mật

Phần này giới thiệu giao thức tính tích vô hướng bí mật hai thành viên tương tự trong (Goethals, Bart and Laur, Sven and Lipmaa, Helger and Mielikainen, Taneli, 2004).

Giả sử X có vector bí mật $X = (x_1, x_2, ..., x_k)$ và Y có vector bí mật tương ứng $Y = (y_1, y_2, ..., y_k)$. X và Y mong muốn tính tích vô hướng $S = \sum_{i=1}^{k} x_i y_i$ trong khi mỗi bên không tiết lộ vector bí mật của mình.

Trước khi thực hiện giao thức, X lựa chọn các tham số của hệ mã hóa ElGamal (g, p, q, x, $h = g^x \bmod p$) trong đó X giữ khóa bí mật x cho riêng mình và công bố khóa công khai h cho Y. Để cho tiện theo dõi, chúng

Hình 1. Thuật toán Shanks's baby-step giant-step

- **Input:** Một nhóm cyclic G bậc q có phần tử sinh g và một phần tử y trong G
- **Output:** Một giá trị x thỏa mãn $g^x = y$

$m \leftarrow \lceil \sqrt{q} \rceil + 1$

forall j **where** $0 \leq j < m$ **do**

  Compute g^j and store the pair (j, g^j) in a hash table

Compute g^{-m}

$\beta \leftarrow y$

forall i **where** $0 \leq i < m$ **do**

  if β is the 2^{nd} element of any pair in the hash table **then**

    return $x = i.m + j$

  else $\beta \leftarrow \beta . g^{-m}$

Nguồn: (Shanks, 1971)

Hình 2. Giao thức tính tích vô hướng bí mật

Input: X có vector $(x_1, x_2, ..., x_k)$ và Y có vector tương ứng $(y_1, y_2, ..., y_k)$
Output: X có giá trị u, Y có giá trị v sao cho: u = $\sum_{i=1}^{k} x_i y_i + v$

Bước 1: X tính $E(g^{x(1)}), ..., E(g^{x(k)})$ rồi gửi cho Y

Bước 2: Y tính các giá trị sau: $(E(g^{x(1)}))^{y(1)} \bmod p, ..., (E(g^{x(k)}))^{y(k)} \bmod p$

Chọn ngẫu nhiên v và tính $m = (E(g^v). \prod_{i=1}^{k}(E(g^{x(i)}))^{y(i)} \bmod p$

Gửi m lại cho X

Bước 3: X tính K = D(m)

Thực thi thuật toán Shank's baby-step giant-step để tính u thỏa mãn $g^u = K$

Nguồn: (Goethals, Bart and Laur, Sven and Lipmaa, Helger and Mielikainen, Taneli, 2004)

tôi sử dụng ký hiệu E(m) thay cho phép mã hóa dữ liệu m sử dụng khóa công khai h và ký hiệu D(c) thay cho phép giải mã lấy dữ liệu gốc từ bản mã c sử dụng khóa bí mật .

Giao thức tính tích vô hướng bí mật được trình bày trong Hình 2.

Phân tích giao thức trên, ta có $E(g^{x(i)})^{y(i)} \bmod N^2 + E(g^{x(i)\ y(i)})$ nên:

$m = (E(g^v). \prod_{i=1}^{k}(E(g^{x(i)}))^{y(i)} \bmod p) \bmod p$

$= (E(g^v). \prod_{i=1}^{k} E(g^{x(i)\ y(i)})) \bmod p$

$= E\ (g^{v + \sum_{i=1}^{k} x_i y_i})$

Suy ra $K = g^{v + \sum_{i=1}^{k} x_i y_i}$. Và vì vậy $u = v + \sum_{i=1}^{k} x_i y_i + v$.

Hơn thế nữa, X không để lộ vector của mình vì mỗi đặc trưng x_i đã được mã hóa thành $E(g^{x(i)})$, và Y cũng giữ bí mật vector của mình do tất cả các đặc trưng y_i đã được "ẩn giấu" trong giá trị m.

2.5. Giao thức tính tổng bí mật

Phần tiếp theo mô tả lại giao thức tính tổng bí mật (Hình 3) được lấy từ giao thức A-V dựa trên hệ mã hóa ElGamal của Hao và cộng sự trong các nghiên cứu (F. Hao, P. Y. Ryan, P. Zieli´nski, 2010).

3. Đề xuất giải pháp xếp hạng tín dụng khách hàng đảm bảo thông tin riêng tư

Trong mục này, phần đầu sẽ mô tả giải pháp tính xếp hạng tín dụng khách hàng đảm bảo tính riêng tư. Phần tiếp theo sẽ phân tích và chứng minh tính riêng tư và sự đúng đắn toán học của giải pháp được đề xuất.

3.1. Giải pháp xếp hạng tín dụng khách hàng đảm bảo thông tin riêng tư

Trước khi thực hiện quy trình xếp hạng tín dụng khách hàng có đảm bảo tính riêng tư đối với khách hàng, ngân hàng và các đối tác lựa chọn các tham số cần thiết. Như đã trình bày ở trên, một đối tác có thể nắm giữ nhiều đặc trưng quan trọng của khách hàng. Tuy nhiên, để cho dễ hiểu và cũng không làm mất tính tổng quát, giả sử rằng mỗi thuộc tính được sở hữu bởi đối tác (bao gồm cả khách hàng).

Để tính được điểm tín dụng cho, đầu tiên giao thức tính tích vô hướng bí mật được sử dụng giữa mỗi cặp: B với vector bí mật đầu vào là $\vec{s_i} = (s_i^1, \dots, s_i^{m_i})$ và đối tác P_i với vector bí mật đầu vào là $\overrightarrow{vec_i} = (0, \dots, 0, 1, 0, \dots 0)$; trong đó s_i^j là ***"điểm*trọng số"*** cho nhóm đặc trưng thứ j đối với thuộc tính A_i và giá trị "1" trong $\overrightarrow{vec_i}$ đứng vị trí thứ k nếu như khách hàng C thuộc nhóm đặc trưng thứ k đối khi xét tới thuộc tính A_i. Kết quả đầu ra của giao thức này là đạt được giá trị u_i và P_i có được giá trị v_i thỏa mãn $u_i = v_i + \vec{s_i}.\overrightarrow{vec_i}$. Dễ thấy, giá trị tích vô hướng bí mật chính là điểm (trên 100) của khách hàng C đạt được khi chấm thuộc tính A_i. Quay lại ví dụ về thuộc tính *Bảo hiểm nhân mạng* ở trên, các nhóm (> 100 triệu; 50-100 triệu; 30-50 triệu; < 30 triệu; Không có) có điểm tương ứng là (100, 75, 50, 25, 0) và trọng số của thuộc tính này là thì ; nếu C mua gói bảo hiểm nhân mạng là 80 triệu thì $\overrightarrow{vec_i} = (0,1,0,0,0)$. Tiếp theo, B sẽ hợp tác cùng các đối tác P_i thực thi giao thức tính tổng bí mật để tính được giá trị $\sum v_i$. Cuối cùng, tính giá trị S = $(\sum u_i - \sum v_i) \div 100$ chính là điểm tín dụng của khách hàng C.

Giải pháp bảo vệ thông tin riêng tư của khách hàng trong quá trình xếp hạng tín

Hình 3. Giao thức tính tổng bí mật

Input: Mỗi đối tác P_i sở hữu một giá trị bí mật v_i ($i = \overline{1,n}$)

Output: Ngân hàng B tính được giá trị tổng $s = \sum_{i=1}^{k} v_i$ trong khi P_i không tiết lộ v_i

Bước 1: Mỗi P_i chọn $\frac{\sum_{j=1}^{i-1} g^{x_j}}{\sum_{j=i+1}^{n} g^{x_j}}$ ật x_i rồi gửi khóa công khai $g^{x(i)}$ cho B

Bước 2: B tính $X_i = \frac{\sum_{j=1}^{i-1} g^{x_j}}{\sum_{j=i+1}^{n} g^{x_j}}$ rồi gửi lại cho P_i

Bước 3: Mỗi P_i tính $m_i = g^{v(i)}. X_i^{x(i)}$ rồi gửi lại cho B

Bước 4: B tính $K = \prod_{i=1}^{n} m_i$

Thực thi thuật toán Shank's baby-step giant-step để tính s thỏa mãn $g^s = K$

Nguồn: (F. Hao, P. Y. Ryan, P. Zieli´nski, 2010)

Hình 4. Giải pháp bảo vệ thông tin riêng tư của khách hàng trong quá trình xếp hạng tín dụng

Bước 1: B lần lượt hợp tác tính tích vô hướng bí mật với mỗi đối tác P_i
B đạt được giá trị bí mật u_i và P_i có được giá trị bí mật v_i
Bước 2: B hợp tác với các đối tác P_i để tính tổng bí mật $\sum v_i$
Bước 3: B tính giá trị $S = (\sum u_i - \sum v_i) \div 100$ và quy đổi hạng tín dụng cho C dựa trên S.

Nguồn: ?

dụng được đề xuất như trình bày trong Hình 4.

3.2. Phân tích giải pháp đề xuất

3.2.1. Chứng minh tính đúng đắn

Để chứng minh giải pháp đề xuất mô tả trong Hình 4 xếp hạng tín dụng chính xác cho khách hàng C, chúng ta sẽ chỉ ra rằng giá trị S là tổng điểm tín dụng mà C nhận được. Hay nói cách khác, ta chứng minh kết quả điểm tín dụng tính theo giải pháp đề xuất (Hình 4) bằng đúng kết quả tính điểm tín dụng thông thường (nhưng không đảm bảo tính riêng tư).

Thật vậy, ta có:

$$S = \frac{\sum u_i - \sum v_i}{100} = \frac{\sum (u_i - v_i)}{100} = \sum \frac{(\vec{s_i}.\vec{vec_i})}{100}$$

Như đã đề cập, tích vô hướng $\vec{s_i}.\vec{vec_i}$ chính là điểm (trên 100) của khách hàng C đạt được khi xét thuộc tính A_i. Vì thế, S chính là tổng điểm tín dụng của C.

3.2.2. Phân tích tính riêng tư

Trong phần này, chúng tôi sẽ chỉ ra rằng dữ liệu riêng tư của mỗi bên tham gia vào giải pháp đều được giữ bí mật.

Ta thấy rằng khi kết thúc các bước tính toán trong Hình 4, ngân hàng B chỉ đạt được tổng điểm tín dụng của C trong khi dữ liệu của C được nắm giữ bởi P_i không cần tiết lộ.

Tiếp theo, chúng ta xét trường hợp tất cả đối tác P_i thông đồng chống lại B: do tất cả các vector riêng tư của ngân hàng B (trong công thức tính điểm tín dụng) đều được mã hóa bởi hệ mã hóa ElGamal sử dụng khóa công khai của B và tổng điểm tín dụng S của C chỉ được biết bởi một mình B nên địch thủ không thể khai thác được gì.

4. Kết luận

Trong nghiên cứu này, việc chấm điểm tín dụng vẫn sử dụng công thức tổng có trọng số với trọng số do ngân hàng quyết định. Tuy nhiên, thay vì phải lưu trữ và tính toán trên những thông tin của khách hàng (không đảm bảo tính riêng tư), giải pháp được đề xuất đưa ra phương thức chấm điểm tín dụng mà khách hàng không cần công khai các thông tin riêng tư của mình dựa trên các công cụ mã hóa. Vì vậy, giải pháp này có thể đảm bảo phía lưu trữ dữ liệu đặc trưng của khách hàng không cần tiết lộ các thông tin riêng tư, nhạy cảm, còn phía ngân hàng không cần công bố chi tiết phương pháp xếp hạng tín dụng, nhưng vẫn đạt được kết quả đầu ra chính xác ■

Tài liệu tham khảo

1. Abbe, E. A., Khandani, A. E., & Lo, A. W. (2012). Privacy-preserving methods for sharing financial risk exposures. American Economic Review.
2. Androulaki, E. (2011). A Privacy Preserving ECommerce Oriented Identity Management Architecture. COLUMBIA UNIVERSITY.
3. Boneh, D. (1998). The Decision Diffie–Hellman Problem. Proceedings of the Third Algorithmic Number Theory Symposium, (pp. 48-63).
4. Chính phủ. (2018). Nghị định 117/2018/NĐ-CP ngày 11/9/2018 của Chính phủ.
5. Dinh, T. H., & Kleimeiera, S. (2007). Credit scoring for Vietnam's retail banking. International Review of Financial Analysis.
6. ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE transactions on information theory, 31(4), 469-472.
7. F. Hao, P. Y. Ryan, P. Zieli´nski. (2010). Anonymous voting by two-round public. IET Information Security.
8. Goethals, Bart and Laur, Sven and Lipmaa, Helger and Mielikainen, Taneli. (2004). On private scalar product computation for privacy-preserving data mining. International Conference on Information Security and Cryptology (pp. 104-120). Springer.
9. Hiến pháp. (2013). Điều 21. Hiến pháp năm 2013 của nước Cộng hòa xã hội chủ nghĩa Việt Nam.
10. Lê, T. T., & Đặng, T. V. (2016). Xếp hạng tín dụng khách hàng thể nhân tại. Tạp chí tài chính.
11. Luật ATTTM. (2015). Mục 2 Bảo vệ thông tin cá nhân . Luật an toàn thông tin mạng năm 2015.
12. Luật CNTT. (2006). Điều 72. Luật công nghệ thông tin năm 2006.
13. Luật GDĐT. (2005). Điều 46. Luật giao dịch điện tử năm 2005.
14. Meints, M., & Möller, J. (2004). Privacy Preserving Data Mining: A Process Centric View from a European Perspective.
15. Nguyễn, H. C. (2019). Một số đề xuất nhằm nâng cao hiệu quả xếp hạng tín dụng. Nâng cao chất lượng thu thập thông tin và chấm điểm tín dụng cho khách hàng cá nhân tại các tổ chức tín dụng.
16. Ngân hàng Nhà nước (2018). Thông tư số 18/2018/TT-NHNN của Ngân hàng Nhà nước.
17. Ralf Stecking and Klaus B. Schebesch. (2015). Classification of credit scoring data with privacy constraints. Intelligent Data Analysis .
18. Reserve, B. o. (2007). Report to the Congress on credit scoring and its effects.
19. Shanks, D. (1971). Class Number, a Theory of Factorization, and Genera. Proc. of Symposia in Pure Mathematics (pp. 415-440). AMS.
20. Wang, J., Chen, Y., & Feng, X. (2018). Privacy-Preserving Credit Scoring on Cloud. International Conference on Cloud Computing and Security.