

Constructional Cyber Physical System: An Integrated Model

Tzer-Long Chen¹, Chien-Yun Chang², Yung-Cheng Yao³ and Kuo-Chang Chung^{4,*}

¹Department of Finance, Providence University, Taichung, Taiwan

²Department of Fashion business and Merchandising, Ling Tung University, Taiwan

³Department of Communication Engineering, National Penghu University of Science and Technology, Penghu, Taiwan

⁴Department of Marketing and Logistics Management, National Penghu University of Science and Technology, Penghu, Taiwan

*Corresponding Author: Kuo-Chang Chung. Email: d9732004@gmail.com

Received: 16 December 2020; Accepted: 21 January 2021

Abstract: Artificial intelligence, machine learning, and deep learning have achieved great success in the fields of computer vision and natural language processing, and then extended to various fields, such as biology, chemistry, and civil engineering, including big data in the field of logistics. Therefore, many logistics companies move towards the integration of intelligent transportation systems. Only virtual and physical development can support the sustainable development of the logistics industry. This study aims to: 1.) collect timely information from the block chain, 2.) use deep learning to build a customer database so that sales staff in physical stores can grasp customer preferences, and 3.) integrate Generative Adversarial Network analysis and logistics truck delivery route analysis. This study will introduce new logistics technology development and innovative smart service structure, covering front-end Internet of Things sensing, mobile application apps, and back-end massive data analysis platform to promote the self/intelligence of logistics. Artificial intelligence for customer preference analysis is used, and images are automatically distributed through the system to reduce labor costs and increase sales. The proposed method is feasible, and it also achieves the push system of information transmission in transportation. Thus, logistics transportation cost transmission is reduced, thereby intelligently pushing self-promotion in marketing activities.

Keywords: Artificial intelligence; integration of intelligent transportation systems; deep learning

1 Introduction

Nowadays, the development of e-commerce has moved towards Online to Offline (O2O) integration. It has become a mainstream for consumers to conduct mobile shopping through mobile phones or computers. This approach has made shopping a quick and convenient experience; thus, e-commerce platforms combine with physical stores to adopt a multichannel approach for product promotion. O2O integration can achieve the goal of omni-channel marketing. While consumers can make purchases at any time and place in the virtual market, the physical stores can provide consumers with services, such as logistics, pick-up, and



This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

product experience. This approach can fully combine the advantages of O2O to maximize profits and diversify customer base. The main customer base of traditional marketing includes the peripheral business districts and shop consumption customers. The influence is limited to the customers in the business district. With O2O integration, the source of customers can be diversified, and the physical stores can combine multiple e-commerce players to allow more diversified product distribution channels. When an online brand establishes a physical channel, three disadvantages are found compared with the virtual market, as follows: 1.) costs of rent, 2.) surplus inventory, and 3.) product profit. The major problem is the lack of control on the sales of goods, leading to the stockpiles of slow sale products occupying the showroom space and causing invalid inventory. In the virtual market, goods can only be viewed from photos or video clips; consumers cannot actually experience or learn more about the content of the goods.

In view of this, virtual and physical integration can incorporate the convenience of virtual market and the actual experience of physical stores. To construct a complete virtual and physical integration project and allow the industry to set up physical stores based on their business strategies, BlockChain technologies can be employed to link the data from various platforms, such as: sales data, inventory status, etc. In addition to online product recommendations, such as recommendations on social media, or e-mails, etc., physical stores can analyze customer needs through the recommendation system to strengthen customer relationships. Thus, the system needs to accurately analyze customer consumption needs to improve sales performance. However, the current recommendation system can only recommend products online for a single information platform. Physical stores thus cannot connect and aggregate the membership data on various information platforms; the system thus cannot accurately analyze consumer behavior. The precision marketing through the analysis of consumer behavior across e-commerce operators is the only path to Retail 4.0 era. Therefore, to establish capacities in consistent experience, the firms need to integrate data from various platforms and observe customer consumption behaviors through third-party channels to achieve data availability.

Brent [1], the recommendation system was mainly based on social networks. Christidis et al. [2] the recommendation system will recommend related products based on personalized interests. Up to present, in addition to understanding personal interest products, it can increase sales through recommending different products based on the similarity of customers' preferences. Smart contract [2] is a special protocol used when formulating a contract in the blockchain. It is mainly used to provide verification and execution of the conditions set in the smart contract. It can automatically execute various steps in the transaction of virtual and physical integration application. When the consumer chose the product and made the payment, the smart contract can execute in accordance with the terms set in the content, which can ensure the implementation of each item; the consumer can also understand the status of shipment. The employment of smart contract in a virtual and physical integration is conducive to transaction efficiency, high security, and high contract customization. This study mainly constructed a virtual and physical integration application based on BlockChain to make virtual/physical information consistent and used deep learning technology to build a recommendation system to build a recommendation system and a marketing system. Through this study, the e-commerce operators can realize virtual and physical integration application.

The construction of a customer marketing system was proposed. Each customer has different product preferences; thus, the system generates a set of mosaic based on the customer's preference and sends it to the customer. If the sales staff can grasp the customers' consumption behavior and predict their purchase time, then the overall sales volume can be increased. A customer marketing system using blockchain information was developed. It is used to analyze customer consumption patterns through deep learning algorithms and predict customer product shopping cycles. The proposed smart contract also combines the pickup models of a physical store and automatically notifies the sales staff and customers. A customer marketing system based on deep learning was constructed using long short-term memory (LSTM) to

analyze consumer consumption patterns and GAN to generate picture. The system needs to collect information from the blockchain from time to time for analysis. In addition to analyzing the customers' own consumption behavior, the customer marketing system in the study can judge the customer's product preferences on the basis of the similarity with other customers when the initial customer data are small. The forecast time cycle of purchasing and the analysis of future product trends were also established. A marketing system is developed, and the data of O2O were integrated to allow a more diversified business marketing strategy and customer base to increase the overall sales volume. This study uses a customer marketing system to construct different customers' product preferences. Using this system can reduce the time for customers to choose products and allow manufacturers to accurately target customer needs. This study uses deep learning to judge customer needs from the blockchain and establishes a marketing system that is very helpful to both consumers and manufacturers.

2 Related Work

Dongyuan et al. [3] mainly proposed that photos can be used offline to identify and mark the people in the photos. Through the method in Dongyuan et al. [3], the people in the photos can be learned offline to promote social activities and construct one's own social circle. Guoyi et al. [4] concluded that customer management system is contributory to managing long-term loyal customers. The study mentioned that customer loyalty is not mainly based on brand factors. The major factor includes the value and promotion measures. Therefore, the customer management system needs to propose the best promotion measures based on customer preferences. Qing et al. [5] is mainly an O2O integration case study. Firms convert physical stores into customer service centers and establish e-commerce platforms for product sales. The sales volume indicates that O2O integration is feasible. Wenjie et al. [6] used big data to analyze customer loss; the systems reduce customer loss rate. Adnan et al. [7] considered genetic algorithms to predict the probability of telecommunication user loss; the proposed method helps to retain telecommunications users. Junliang et al. [8] analyzed the relationships between products and customers, between markets and products, and between innovative technology and products. The analysis can help the firms to find potential customers and is contributory to firm's future development.

Qiang et al. [9] used bilateral LSTM to carry out the production and control time of each stage in the wafer production line, which facilitate maintenance by helping to determine whether there are errors in the wafer production process. Kangil et al. [10] converted the carbon dioxide and other gases in automobile exhaust into wavelet coefficients and then used the wavelet coefficients, through LSTM, to predict the air quality in the city and the amount of vehicle exhaust gas. Irfan et al. [11] employed LSTM to predict the environmental factors in the city, such as: air, water, etc.; the LSTM prediction results is contributive to environmental improvement by the government. The telecommunications industry constantly analyzes the conditions of potential customers and customer loss; through LSTM, Yang-Jie et al. [12] conducted the prediction of telecommunication customer loss, which helps the telecommunications industry propose more favorable promotion measures to retain customers and reduce the customer loss.

Qiang et al. [13] proposed the application of generative adversarial networks (GAN) in computer vision; GAN helps to synthesize high-quality images and reduces the occurrence of defects in the synthesized images. Fiona Schweitzer et al. [14] overcame the two major problems in GAN: 1. Semantic misjudgment, and 2. the defects in the synthetic image. Therefore, this study adds a self-learning method to train the GAN in its accuracy in semantic analysis and continuously correct the errors in synthetic image generation to perfect the composite images. Jieying et al. [15] proposed the Encoder Guided Generative Adversarial Network algorithm to enhance the fidelity of the facial conditions in real photos and synthesized sketches; quantity experiments showed that the method proposed in the study can help

enhance the fidelity of the synthesized photos. Yali et al. [16] proposed that DualAttn-GAN method can effectively enhance the perfection of the text in the composite photo and avoid compromising the photos and visual effect when synthesizing the text and images. Jaihyun et al. [17] used cycle-consistent Generative Adversarial Networks to enhance the presentation of texture in synthetic photos. Donghua et al. [18] mainly used GAN for speech synthesis to improve the smoothness of speech pronunciation and the perfection of natural pronunciation.

This study mainly employed BlockChain to integrate the virtual and physical data and adopted LSTM to carry out the customer purchase cycle; social network software was then used to push the marketing advertisement images generated by GAN. The method introduced in the study facilitated automatic marketing to increase the firm's sales volume.

3 Background

This section introduces the system architecture of this study and Bilinear Pairings.

3.1 System Model

The system architecture of this study is shown in Fig. 1. The customer consumption data of both e-commerce and physical operations are stored in BlockChain. Customer relationship system will automatically predict every customer behavior. LSTM is employed as the prediction method to predict the cycle of customer consumption pattern, and machine learning is employed to conduct classification judgement. Promotion commodities are found from the classification; then, GAN is used to synthesize the images of promotion commodities and their prices. The images are later disseminated through social software media. The system mainly conducts automated marketing based on AI; automated marketing can help reduce the labor costs and increase the firm's product sales. The sales system based on AI can help promote the sales strategies of O2O integration.

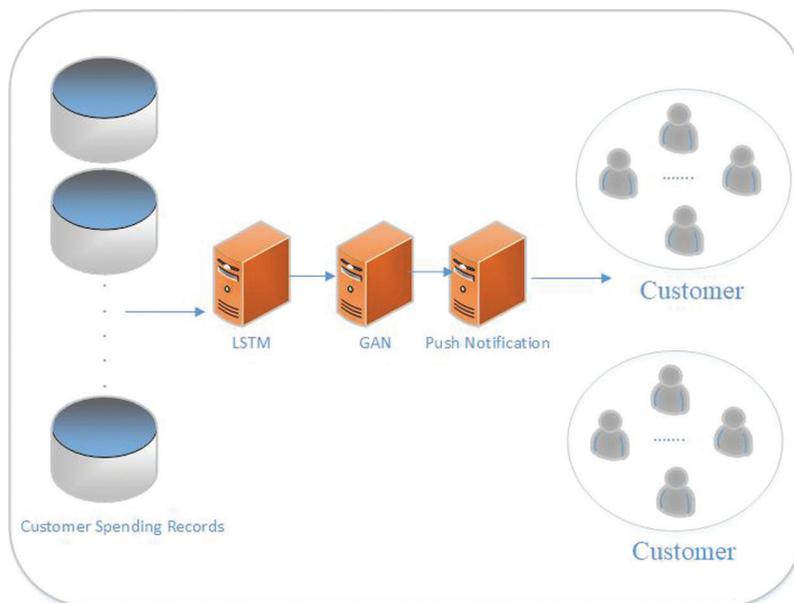


Figure 1: System diagram

3.2 Bilinear Pairings

The study employed Bilinear Pairings technology to construct the network security mechanism of BlockChain, which enhance the fast search and security of BlockChain. Suppose G_1 and G_2 are, respectively, additive and multiplicative groups and apply the prime order q ; suppose P, Q is G_1 's generator, and the bilinear mapping is $e : G_1 \times G_1 \rightarrow G_2$. The features of bilinear pairing are as follows:

1. Bilinear: $e(aP, bP) = e(P, P)^{ab}$, $e(a \cdot P + b \cdot P + c \cdot P, P) = e(a \cdot P, P)e(b \cdot P, P)e(c \cdot P, P)$, for all $PP \in G_1$ and $a, b, c \in \mathbb{Z}_q^*$.
2. Non-degeneracy: $Q \in G_1$ such that $e(Q, Q) \neq 1$.
3. Computable: There exists an efficient algorithm to compute $e(Q, Q)$ for all $Q \in G_1$.

In Scott [19], the Bilinear Pairings encryption technology was implemented, and the data volume of G_1 and q are 161 bits and 160 bits respectively. This study employed ID-based cryptography (IBC) [20,21] which is mainly based on Bilinear Pairings technology. IBC can construct a Common session key for both parties, which can be used by both parties to encrypt and decrypt information symmetrically.

4 The Proposed Scheme

This section described 4.1 BlockChain search; 4.2 LSTM product prediction; and 4.3 GAN image generation.

4.1 BlockChain Data Search

First, each store use IBC to encrypt customer transaction data and transmit customer-related data to the BlockChain. The data are $M = SK_u(MD) || ID_{a,O_1} || ID_{n,C_1} || H(MD) || \dots || TS$. Next, the server will verify the authenticity of the message and then encrypt it with the server's private key. The cipher text is $\mathcal{PR}_{ID_{a,C_1}}(M) || ID_{a,C_1} || \dots || TS$. Should anyone want to verify the authenticity of the message, he/she only needs to use the server's public key and then use the IBC to decrypt and verify the integrity, and then they can learn whether the message in the BlockChain is correct. Marketing staff will then conduct blockchain search based on the customer's real ID. Since the customer transaction data is also stored in the firm's server, the blockchain can be used to find customer data from different servers and the blockchain Hash value and time stamp (TS) can be compared to determine whether it is the same data; search and judge whether it belongs to $ID_{a,C}$ data. After comparing the blockchain Hash value and TS to determine whether it is the same data, the data collected is $GL_{ID_{a,C_u}}$.

After collecting consumer data, data analysis is required. The system mainly analysis the following information of consumers: 1. Consumption amount; 2. Frequency of consumption; 3. Methods of payment; 4. Categories of product purchased. The system will analyze the consumption amount to understand the average value and change of the purchase amount each time, which is calculated as follows:

(1) The consumer's ID_{a,C_u} consumption amount each time is $AC_{ID_{a,C_u}}^i$. First, the average value is calculated as

$$AVGAC_{ID_{a,C_u}} = \frac{\sum_{i=1}^n AC_{ID_{a,C_u}}^i}{n}. \quad (1)$$

(2) Next, calculate the change of consumption amount; the system employs the variance to calculate. The calculation is

$$VARAC_{ID_a,C_u} = \frac{\sum_{i=1}^n (AC_{ID_a,C_u}^i - AVGAC_{ID_a,C_u})^2}{n}. \quad (2)$$

Next, the number of data is used as consumption frequency ((CS_{ID_a,C_u})). The system will calculate the most frequent method of payment used and take it as the method of payment ((PC_{ID_a,C_u})). The purchased product category is sorted in ascending order and calculated as $CP_{ID_a,C_u}' = \text{SORT}_{\max \rightarrow \min}(CP_{ID_a,C_u})$. The system analyses consumers' data to improve the accuracy of deep learning. The customer marketing system constructed in this study provides marketers to understand customer preferences and their consumption status so that they can conduct related promotion activities, such as special offers for upscale consumers or regular customers. After data analysis, the information $AVGAC_{ID_a,C_u} || VARAC_{ID_a,C_u} || CS_{ID_a,C_u} || PC_{ID_a,C_u} || CP_{ID_a,C_u}'$ will be transmitted to LSTM for deep learning analysis.

4.2 LSTM Commodity Prediction

This study employed Long Short-Term Memory (LSTM) to conduct predict the sales of products. The calculation is as follows:

1. The study collects the daily sales volume of each product as $X_i = \{X_1, X_2, X_3, \dots, X_t\}$.
2. First, calculate the input part $i_t = \text{sigm}(W_{X_i}X_t + W_{h_i}h_{t-1})$, where h_{t-1} is the upper hidden layer, W_{X_i} and W_{h_i} are parameter matrix, and sigm is calculated as $\text{sigm}(z) = \frac{1}{1 + e^{(-z)}}$.
3. Next, calculate the forget gate as $f_t = \text{sigm}(W_{X_f}X_t + W_{h_f}h_{t-1})$, where W_{X_f} and W_{h_f} are parameter matrix.
4. Next, calculate the output layer as $h_t = o_t \odot \tanh(c_t)$, where \odot is the product, \tanh is the hyperbolic tangent function, o_t is calculated as $o_t = \text{sigm}(W_{X_o}X_t + W_{h_o}h_{t-1})$, $c_t = f_t \odot c_{t-1} + i_t \odot \tilde{c}_t$, $\tilde{c}_t = \tanh(W_{X_c}X_t + W_{h_c}h_{t-1})$.

Next, the system will calculate the expected sales volume of each product the next day. On one hand, one can understand the product sales status for review or related promotion activities.

The study predicts the purchase cycle of customers and automatically notify high frequency customers the related promotion on the frequently purchased products to encourage customers to visit the physical stores and make further purchase and experiment. In addition, this study constructs future sales forecasts of products, using LSTM for prediction. The study takes product purchase time to sequence the daily sales volume to forecast the future product sales; so that the firms can have a better handle on the product sales and inventory to facilitate the dispatch.

4.3 Generation of GAN Images

The study first establishes a fixed term database CSQl. CSQl will create comments corresponding to the predicted value of the output layer, such as: high consumption regular customers, credit card payment, purchasing skin care products, etc.; then, the analysis is as follows:

1. The first-order eigenvalue calculation model is z_l , and the calculation is $z_l = P_u \times q_i$, where P_u is the consumer and q_i is the consumption information.
2. Suppose the predicted value is calculated as $a_l = \sigma(w_l \times z_l)$, where w_l is the weight, and a_l is the output of the hidden layer predicted value.

3. The system inputs P_u and q_i into the hidden layer for calculation. The calculation is as follows.:

$$\begin{aligned} z_1 &= P_u \times q_i \\ z_2 &= \sigma_2(w_2z_1 + b_2) \\ z_3 &= \sigma_3(w_3z_2 + b_3) \\ &\dots\dots \\ z_H &= \sigma_H(w_Hz_{H-1} + b_H) \end{aligned}$$

4. Next, hyperbolic tangent, Rectified Linear Unit, and excitation function are employed. The gradient of Rectified Linear Unit is a constant $\lambda \in (0, 1)$, The calculation is as follows:

$$f(z_H) = \begin{cases} z_H, & \text{if } z_H > 0 \\ \lambda z_H, & \text{if } z_H \leq 0 \end{cases}$$

5. The predicted value after the input of the input layer is a^H ; the calculation formula is $a^H = \sigma(w_Hz_{H-1} + b_H)$.
6. The system will correspond to the word database CSQL according to the predicted value a^H , and output the results to the Web for display.

The establishment of a customer marketing system in this study helps marketers to have better understanding of consumer preferences. Although many POS systems today can list customer transaction details, it is difficult for marketers to grasp customers from transaction details in a short time. Therefore, this study proposes a customer marketing system which adopts deep learning to extract feature values and displays them on the Web through predictive values that correspond to relative words, which helps marketers better understand, from the results, customer spending habits and preferences. The system integrates the transaction details of the virtual market and can better grasp the customer needs to achieve the goal of virtual and physical (O2O) integration. To provide customers with more special offers, the system uses GAN for image synthesis technology. The system presets the background image as fi_i , the product object image as ri_i , and the product title as ti_i . The system then uses GAN for image synthesis. After detecting every customer's preference, the system will assemble the product images into a mosaic and forward it to the customer to improve the customer's return rate and sales contribution.

5 Experiment Results

The study performed LSTM prediction using a total of 1,000 customer data. As shown in Fig. 2, the prediction accuracy of the study is 98%. It can be understood from Fig. 2 that the method proposed in this study can precisely predict the time a customer makes the next purchase which help the system to automatically notify customers the latest marketing scheme. As it is shown in Fig. 3, this study first employed GAN for face synthesis training. The results showed that the face synthesis effect is very effective. Next, the study synthesized products on sale and the text of marketing scheme. The results showed that the GAN proposed in the study helps to synthesize product pictures and the texts. It can be learned from the experiment results that the method proposed in this study can effectively achieve the marketing function by predicting and reusing synthesized pictures. As shown in Fig. 4.

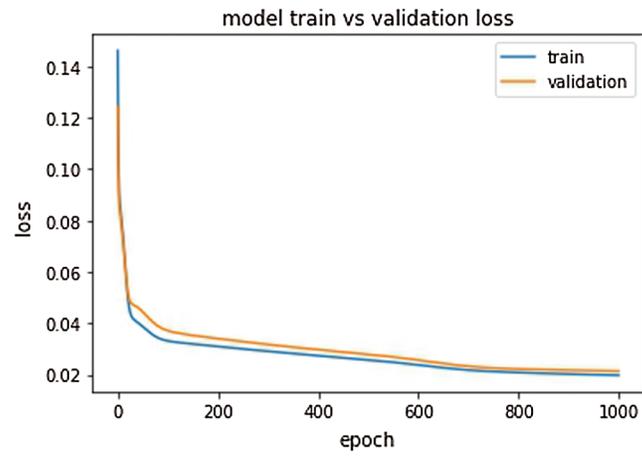


Figure 2: LSTM predicts consumption accuracy

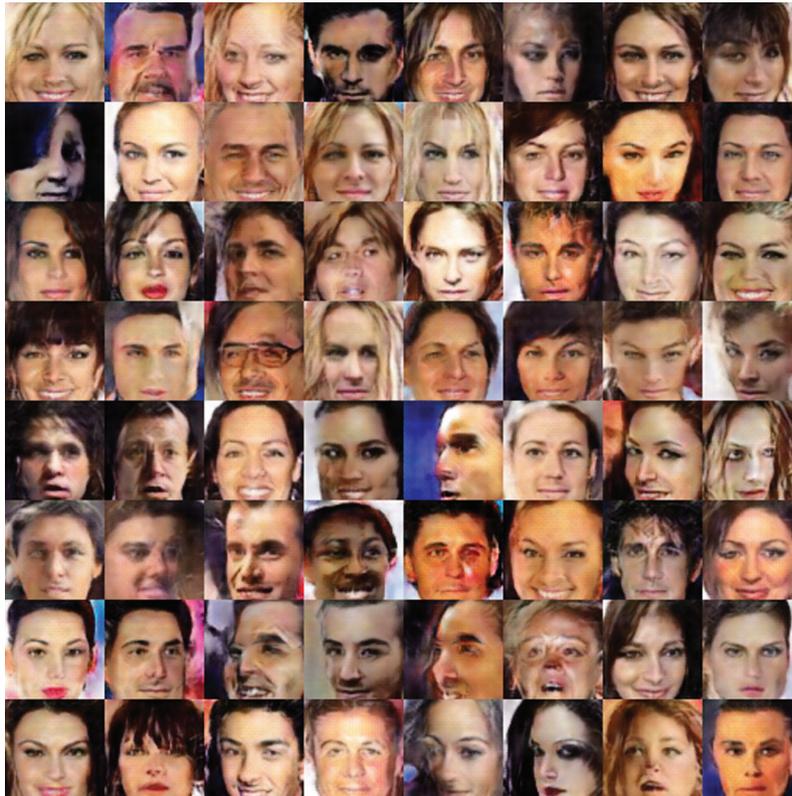


Figure 3: Human face picture synthesis



Figure 4: Synthesized picture of the discount product

6 Conclusions

Nowadays customer shopping has moved from traditional stores to online shopping. Many customers make online purchase through mobile devices. Under the competition of e-commerce, if you can grasp the customer's consumption interest and cycle, you can get the customer's willingness to buy your products. This study proposed a marketing customer system which mainly uses LSTM for cycle prediction to understand a customer's purchasing cycle; then uses GAN to perform marketing product synthesis and pushes the message through social media or SMS. According to the experiment results, the LSTM prediction accuracy is about 98%. From the results, it can be learned that the method proposed in the study is feasible; the method proposed in the study can help stores conduct smart marketing and improve their product sales performance.

Acknowledgement: The authors would like to thank Intelligent Automation & Soft Computing for their help in preparing this manuscript for publication.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: All authors declare that they have no conflicts of interest to report regarding the present study.

References

- [1] D. Brent, "The value of heterogeneous property rights and the costs of water volatility," *American Journal of Agricultural Economics*, vol. 99, no. 1, pp. 73–102, 2017.
- [2] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
- [3] L. Dongyuan, S. Jitao, C. Zhineng, X. Min and M. Tao, "Who are your "real friends: Analyzing and distinguishing between offline and online friendships from social multimedia data," *IEEE Transactions on Multimedia*, vol. 19, no. 6, pp. 1299–1313, 2017.
- [4] C. Guoyi and Z. Jiansheng, "Performance evaluation of customer knowledge management competence based on Balanced Scorecard," *2013 6th Int. Conf. on Information Management, Innovation Management and Industrial Engineering*, Xi'an, China, 2014.
- [5] Y. Qing, H. Lihua and X. Yunjie, "Role of trust transfer in E-commerce acceptance," *Tsinghua Science & Technology*, vol. 13, no. 3, pp. 279–286, 2008.

- [6] B. Wenjie, C. Meili, L. Mengqi and L. Guo, "A big data clustering algorithm for mitigating the risk of customer churn," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 3, pp. 1270–1281, 2016.
- [7] A. Adnan, A. Sajid, A. Awais, N. Muhammad, H. Newton *et al.*, "Comparing oversampling techniques to handle the class imbalance problem: A customer churn prediction case study," *IEEE Access*, vol. 4, pp. 7940–7957, 2016.
- [8] W. Junliang, Z. Jie and W. Xiaoxi, "Bilateral LSTM: A two-dimensional long short-term memory model with multiply memory units for short-term cycle time forecasting in re-entrant manufacturing systems," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 748–758, 2017.
- [9] Z. Qiang, L. Feng, L. Fei and L. Qiang, "Vehicle emission forecasting based on wavelet transform and long short-term memory network," *IEEE Access*, vol. 6, pp. 56984–56994, 2018.
- [10] K. Kangil, K. Dong-Kyun, N. Junhyug and K. Minhyeok, "Stable forecasting of environmental time series via long short term memory recurrent neural network," *IEEE Access*, vol. 6, pp. 75216–75228, 2018.
- [11] U. Irfan, R. Basit, K. M. Ahmad, I. Muhammad Imran and I. Saif, "A churn prediction model using random forest: analysis of machine learning techniques for churn prediction and factor identification in telecom sector," *IEEE Access*, vol. 7, pp. 60134–60149, 2019.
- [12] Y. J. Cao, L. L. Jia, Y. X. Chen, N. Lin, C. Yang, B. Zhang, Z. Liu, X. X. Li and H. H. Dai, "Recent advances of generative adversarial networks in computer Vision," *IEEE Access*, vol. 7, pp. 14985–15006, 2018.
- [13] W. Qiang, F. Huijie, Z. Linlin and T. Yandong, "Deeply supervised face completion with multi-context generative adversarial network," *IEEE Signal Processing Letters*, vol. 26, no. 3, pp. 400–404, 2019.
- [14] S. Fiona Schweitzer, A. Ellis, H. Van den and H. Erik-Jan, "There's more than one perspective to take into account for successful customer integration into radical new product innovation: A framework and research agenda," *IEEE Transactions on Engineering Management*, vol. 67, no. 3, pp. 813–829, 2020.
- [15] Z. Jieying, S. Wanru, W. Yahong, X. Ran and L. Feng, "Feature encoder guided generative adversarial network for face photo-sketch synthesis," *IEEE Access*, vol. 7, pp. 154971–154985, 2019.
- [16] C. Yali, W. Xiaoru, Y. Zhihong, L. Fu, X. Peirong *et al.*, "Dualattn-GAN: text to image synthesis with dual attentional generative adversarial network," *IEEE Access*, vol. 7, pp. 183706–183716, 2019.
- [17] P. Jaihyun, H. David. and K. Hanseok, "Fusion of heterogeneous adversarial networks for single image dehazing," *IEEE Transactions on Image Processing*, vol. 29, pp. 4721–4732, 2020.
- [18] W. Donghua, D. Li, W. Rangding, Y. Diqun and W. Jie, "Targeted speech adversarial example generation with generative adversarial network," *IEEE Access*, vol. 8, pp. 124503–124513, 2020.
- [19] M. Scott, "Computing the Tate pairing," *Proc. of the Cryptographers Track at the RSA Conf.*, pp. 293–304, 2005.
- [20] P. S. L. M. Barreto, H. Y. Kim, B. Lynn and M. Scott, *Proc. of the 22nd annual Int. cryptology Conf., Proc. of the Cryptographers Track at the RSA Conf.*, 2020.
- [21] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *Proc. of the Int. Cryptology Conf.*, 2001.