American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-13, Issue-8, pp-78-80
www.ajer.org
Research Paper Open Access

Application And Security of GAN in Mobile Payment

Ke Xu
Department of E-Commerce, Shenzhen Tourism College, Jinan University

ABSTRACT :*Mobile payment is an important part of current e-commerce, and its security plays an important role in the current mobile payment. GAN has a broad application prospect in the field of mobile payment. In this paper, the principle and application of GAN are introduced, and the application of GAN in mobile payment is explained in detail. Finally, the application of GAN in mobile payment is analyzed from the aspect of security.*

KEYWORDS *GAN, Mobile payment, Security threats;*

Date of Submission: 06-08-2024 Date of acceptance: 17-08-2024

I. INTRODUCTION

In recent years, the rapid development of artificial intelligence technology, its application field is more and more extensive, Generative adversarial network (GAN) technology is one of them. GAN is a kind of neural network architecture of generative model. Generation model refers to the use of models to generate new cases based on existing samples, such as generating a new set of similar but slightly different photos based on an existing photo collection. GAN is a generative model trained using two neural network models. One of them, called a "generator" or "generative network" model, learns to generate new usable cases. The other, called a "discriminator" or "discriminator network," can learn discrimination-generated cases and real cases. The two models (in the game theory sense) are in a state of competition, with the generator trying to fool the discriminator, and the discriminator dealing with both the generated case and the actual case[1]. The generative model can be learned to generate new cases as needed.

GANs can automatically generate corresponding outputs by observing the distribution of input data without introducing prior knowledge, thus producing some complex images or models that cannot be represented by real data. In recent years, GAN has made great progress in many fields. GAN can be used to generate realistic digital images, speech and natural language. In the field of machine learning, GANs are used to train large deep learning models.

In recent years, third-party payment trading platforms have become the medium connecting retailers, consumers and banks, and the development of Internet finance and e-commerce has enabled people to transact and buy and sell without leaving their homes[2]. Mobile payment has become a new payment method, which is efficient and saves time and effort. But this method of payment also brings new security problems such as transaction fraud. With the rapid development of mobile payments and digital currencies, people are paying more attention to payment security. This paper introduces the basic principle of GAN, analyzes the application of GAN in mobile payment, and finally makes a security analysis and summary.

II. PRINCIPLE OF GAN

The basic principle of GANs is: GANs use the adversarial training between the generator and discriminator, so that the generator and discriminator reach a balance to some extent, and the generator will eventually map a new sample data into a new feature space through training, while the discriminator will map a new feature into the known sample data through learning. This enables GANs to greatly reduce the amount of computation when dealing with large data sets, and to extract more important information from high-dimensional feature Spaces.

In generative models, GANs need to train the discriminant ability by training the antagonism between generators and discriminators. The generator uses the probability distribution from the original sample data as input, while the discriminator generates the sample data using the generation model. Therefore, the generator constantly learns a distribution similar to the target data from the original data during the training process and maps this distribution into a feature space similar to the target data. This allows the generator and discriminator to constantly optimize each other during training so that there is a balance between them.

Many machine learning systems look at some kind of complex input (for example, an image) and produce a simple output (such as a label like "cat"). By contrast, the goal of a generative model is just the opposite: take a small piece of input - perhaps a few random numbers - and produce a complex output, such as an image of a realistic-looking face. Generative adversarial networks (GANs), a machine learning architecture proposed by Ian Goodfellow at the University of Montreal in 2014 and introduced only a few years ago, have been a subject of great interest in machine learning[3].

The idea of a machine "creating" realistic images from scratch may seem magical, but GANs use two key tricks to turn vague, seemingly impossible goals into reality.

One is to use random components. This is easy to understand: it doesn't make much sense to build a system that produces the same result every time it is run. Thinking in terms of probability also helps to translate the problem of generating images into a natural mathematical framework. Selecting images uniformly and randomly will only produce noise. However, we want the system to know which images are likely to be faces and which are not. Mathematically, this involves modeling the probability distribution of images, that is, a function that tells us which images are likely to be faces and which are not. This kind of problem (modeling a function on a high dimensional space) is exactly what neural networks are designed to solve.

The key idea of GANs is to build two competing networks: a generator and a discriminator. Generators try to create random composite outputs (for example, images of faces), while discriminators try to distinguish those outputs from real outputs (for example, a database of celebrities). The hope is that as the two networks face off, they will both get better and better - eventually forming a network of generators that produce real-world output.

In summary: Generative adversarial networks are neural networks that learn to select samples from a special distribution (the "generative" part of the name), and they do this by setting up competitions (hence the name "adversarial").

III. APPLICATION OF GAN

GANs can be used in many fields, including image and audio generation, object detection, data enhancement, and more. In terms of image generation, GAN can generate realistic images, including faces, landscapes, buildings, etc. In terms of audio generation, GANs can generate a variety of sounds, such as music synthesis and natural language processing. In object detection, GANs can be used to detect objects in images, such as faces, as well as the relative positions and orientations between objects. In terms of data enhancement, GANs can be used to improve the quality of images, including synthesizing new images and improving existing ones. In the financial field, GAN mainly focuses on the synthesis of financial tabular data and financial time series[4].

GAN, as a powerful deep learning framework, show great potential for data analysis in multiple domains. Taking mobile payment as an example, this paper discusses two main applications of GANs in this field: one is to generate fake data to simulate payment services, and the other is to use GANs for transaction analysis and authentication. These innovative applications facilitate cooperation between mobile payment service providers and third parties such as banks, and open up new possibilities for mobile payment security and efficiency.

The collection of user information in the field of mobile payment is very important. The mobile payment system can obtain the basic information of the user, such as name, gender and contact information, by entering the mobile phone number and other information. This type of information collection is popular in an increasingly privacy-conscious environment. By using GANs to generate simulated data, mobile payment system providers can quickly obtain user information while complying with privacy protection regulations to ensure user data security.

Model training is also important in the field of mobile payment, through which the system can intelligently judge the user account status and provide users with unique personalized transaction suggestions. Through the training of the generated adversarial network, the model's ability to understand and predict user behavior has been improved, thus enhancing the intelligence and security of the mobile payment system.

All in all, generative adversarial network has a broad application prospect in the field of mobile payment. By using GAN technology, the mobile payment system can more effectively process user information, realize intelligent transaction analysis and identity authentication, provide users with a safe and convenient payment experience, and also bring new vitality and innovation to the development of the mobile payment industry. These applications demonstrate the potential and advantages of GAN in the field of mobile payment, and point out the direction for the future development of mobile payment.

IV. GAN SECURITY ANALYSIS

All in all, generative adversarial network has a broad application prospect in the field of mobile payment. By using GAN technology, the mobile payment system can more effectively process user information, realize intelligent transaction analysis and identity authentication, provide users with a safe and convenient payment experience, and also bring new vitality and innovation to the development of the mobile payment industry. These applications demonstrate the potential and advantages of GAN in the field of mobile payment, and point out the direction for the future development of mobile payment.

Due to the breakthrough of big data and artificial intelligence and other technologies, people's information is very easy to leak, which also leads to fraud crimes in the process of using online transactions. The security of GAN is mainly reflected in the difference between the generated image and the real image. Attackers can exploit these gaps for fraudulent activities. At present, the application of GAN in mobile payment is mainly through the adversarial training of real images and generated images, and then the known generated data is used to optimize the training data, so as to produce virtual photos with high similarity. GANs can generate images of high quality, so they can also be the target of malicious attackers. The security problems of the mobile payment system mentioned in this paper mainly include the following aspects: (1) the security of the mobile terminal; (2) User authentication problem; (3) Mobile payment information leakage problem; (4) User privacy issues.

In view of the above mentioned mobile payment security problems, this paper puts forward some corresponding solutions to ensure that the security threats faced by mobile payment can be effectively prevented and dealt with.

a. Strengthen device security measures: Users should regularly update the operating system and application programs and install the latest security patches and antivirus software to reduce the risk of malware intrusion.

b. Use a secure connection: Avoid using public wireless networks for sensitive operations during mobile payments.

c. Adopt multi-factor authentication: Introduce biometric technology, SMS verification code and other multi-factor authentication methods to improve the security of user authentication.

d. Periodically change passwords: Users are encouraged to use complex passwords and change passwords periodically to make cracking difficult.

e. Encrypted data transmission: Use end-to-end encryption technology to avoid man-in-the-middle attacks.

f. Data isolation: Effective isolation of sensitive user information from payment data.

V. CONCLUSION

The application of GAN technology in the security of mobile payment has made some progress, but there are still some security problems to be solved. First of all, there is no good solution to the security problems brought by GAN technology in mobile payment applications. Secondly, the images and videos generated by GAN technology in mobile payment applications are maliciously used by criminals, thus causing damage to the mobile payment system. In order to avoid such attacks, GAN technology should be further perfected, and its security and accuracy should be improved through model training. When the model reaches a certain level of training, it can be used for security defense against attacks and anti-detection, so as to improve the security and reliability of the mobile payment system itself and better serve the mobile payment system.

REFERENCES

[1]. Zeng Xiaoyan. Generated against the application of network in cross-border payment fraud recognition [D]. East China normal university, 2023. The DOI: 10.27149 /, dc nki. Ghdsu. 2023.001328.)

[2]. Zhang Hao. Research on Online transaction anti-fraud method based on Generative adversarial network [D]. Beijing university of information science and technology, 2021. DOI: 10.26966 /, dc nki. GBJJC. 2021.000024

[3]. Zhao. Structured data unbalanced classification based on the generated against network [D]. Southwest university of finance and economics, 2019. The DOI: 10.27412 /, dc nki. Gxncu. 2019.001938.

[4]. Cui Yihao, Liu Sen, Ye Guangnan). Emergent against network application in financial data [J/OL]. Journal of network and information security, 2024, (03) : 156-174 [2024-08-09]. http://kns.cnki.net/kcms/detail/10.1366.TP.20240801.1543. 008.html.