Energy Engineering

Tech Science Press

DOI: 10.32604/ee.2022.020873

ARTICLE

An Improved Biometric Fuzzy Signature with Timestamp of Blockchain Technology for Electrical Equipment Maintenance

Rao Fu[1,*], Liming Wang[2], Xuesong Huo[2], Pei Pei[2], Haitao Jiang[3] and Zhongxing Fu[4]

[1]State Grid Xuzhou Power Supply Company of Jiangsu Electric Power Co., Ltd., Xuzhou, 221000, China

[2]State Grid Jiangsu Electric Power Co., Ltd., Nanjing, 211000, China

[3]State Grid Jiangsu Electric Power Co., Ltd., Research Institute, Nanjing, 211103, China

[4]State Grid Yancheng Power Supply Company of Jiangsu Electric Power Co., Ltd., Yancheng, 224000, China

[*]Corresponding Author: Rao Fu. Email: 1806000365@139.com

Received: 16 December 2021 Accepted: 18 February 2022

ABSTRACT

The power infrastructure of the power system is massive in size and dispersed throughout the system. Therefore, how to protect the information security in the operation and maintenance of power equipment is a difficult problem. This paper proposes an improved time-stamped blockchain technology biometric fuzzy feature for electrical equipment maintenance. Compared with previous blockchain transactions, the time-stamped fuzzy biometric signature proposed in this paper overcomes the difficulty that the key is easy to be stolen by hackers and can protect the security of information during operation and maintenance. Finally, the effectiveness of the proposed method is verified by experiments.

KEYWORDS

Blockchain technology; fault diagnosis of electrical equipment; biometric fuzzy signature; timestamp; deep learning technology

1 Introduction

Due to increasing energy consumption, electric power systems have grown larger and more complex than ever before to meet the increasing demand for energy and its storage. In this regard, the concept of an electric Internet of Things (IoT) is utilized to connect various devices and people in the power system together in order to realize the effective management of the power system. However, most of the devices and people in the power system are distributed in the electric IoT, which makes for the difficult management of either the IoT or the connected people. Therefore, how to securely protect the huge amount of device-related data in the electric IoT is still a challenging problem.

As a distributed ledger platform, blockchain technology can provide a more secure protection to solve this problem due to its decentralization, traceability, immutability, and currency properties [1]. Until now, blockchain technology has been widely deployed in the electric IoT for a variety of purposes, including market transactions, operations management, and system security [2]. In the application of market transactions, blockchain technology is used to solve the trust crisis between users in the context of the energy market. For example, a micro-grid electricity transaction credit consensus mechanism based on blockchain technology is proposed in [3]. Furthermore, a self-manageable

electric vehicle charging transaction model based on blockchain technology is proposed to ensure the reasonable distribution of energy [4]. Furthermore, a photovoltaic trading scheme based on blockchain incentives is proposed, which allows users to conduct self-transactions with ease [5].

In regard to power grid transaction management, blockchain technology can be used to solve the associated problems, such as high cost and low efficiency, as well as to realize the safe and stable operation of energy system. For instance, in relation to the field of distribution network, a model of intelligent transaction and collaborative dispatching of energy internet based on blockchain technology is established to provide solutions for the efficient and safe operation of the energy internet [6]. Moreover, blockchain technology can also make great contributions in regards to demand-side response. For example, a blockchain-based automatic demand response approach for local area network energy storage systems has been developed [7].

In addition, the asymmetric encryption algorithm and data storage technology contained in the blockchain technology can also be integrated into any system in order to effectively avoid the leakage of system information and to further ensure the security of user information. In [8], a new transaction method and a multi-energy complementary secure transaction model are introduced that better solve both of the information security problems in energy transactions [9].

In a power system, there are huge amounts of electrical equipment including power generation, substation, transmission, distribution, and electrical machinery [10]. It is critical to maintain this electrical infrastructure on a regular basis [11]. Since power infrastructure is generally distributed across entire systems, blockchain technology can also be competent regarding the maintenance of power infrastructure [12]. Generally, during the regular maintenance of power infrastructure, a large amount of information on power infrastructure operation and maintenance will be collected and stored on various blockchains [13]. When consumers log in to their accounts, however, attackers or hackers may be able to intercept the passwords they use [14]. Once people lose or disclose their secret keys, they will lose all their information on the blockchain, which will create a significant threat to the stability and security of the power system itself [15]. Therefore, it is necessary to build a secret key management system to prevent attacks from malware that steal secret keys, thus ensuring the security of information on the blockchain.

The digital password account is used in the traditional manner of solving the problem. In this instance, hackers can easily acquire the account's secret key. Furthermore, users must fill out account details while logging into the blockchain system. Therefore, it has low security and poor efficiency. By using the biometric digital signature to generate the secret key, however, the secret key can be generated by people's biological characteristics automatically. What's more, the secret key in the key management server will be deleted after finishing the transactions in the blockchain system. As a result, the security and ineffectiveness of the system are improved. However, it does remain easy in this scenario for a hacker to attack the sensor and steal the face picture to replay the old data. In order to solve this further problem, this paper proposes an improved biometric fuzzy signature with a timestamp, which can ensure the security of a secret key. Thus, the hacker cannot steal the key secret from the key management server, and the security of the system is further improved as a result.

In general, a biometric digital signature is used to generate the secret key for improving security. After finishing any transactions in the blockchain system, the secret key in the key management server will be deleted. As a result, the hacker will be unable to obtain the key secret from the key management server. However, it is easy for a hacker to attack the sensor and steal the face picture to replay the old data. In order to solve this problem, this paper proposes an improved biometric fuzzy signature with a timestamp, which can ensure the security of the secret key.

The main contributions of this paper are summarized as follows:

1. Blockchain technology is used to manage the devices and people in the power system, protecting the huge amount of device-related data in the electric IoT.
2. To create a verification system based on the biometric fuzzy signature and add a timestamp in the process of feature extraction, preventing the hackers from stealing the user's secret key and replaying the old data to log into the system.
3. By using deep learning technology, the accuracy and efficiency of face recognition in the system are further enhanced.

The remainder of this paper is organized as follows: In Section 2, basic knowledge of blockchain and digital signatures based on biometrics are described. In Section 3, the proposed biometric fuzzy signature and timestamp are explained and built upon. In Section 4, four specific cases in power system equipment operation and maintenance are analyzed to verify the security and reliability of the system. In Section 5, the summary of the full paper is given.

2 Blockchain Basics

2.1 Overview of Blockchain System

Since Nakamoto first proposed bitcoin using blockchain technology in mid-2008, the blockchain technology has gradually developed in various aspects. As a collection of various technologies, blockchain technology can be divided into a data layer, a network layer, a consensus layer, an incentive layer, an application layer, etc.

In the data layer, the hash function in cryptography is mainly used to construct a data structure like hash chain for storing transactions or data [16]. In the network layer, it uses a peer-to-peer (P2P) network without a central node to complete the dissemination and diffusion of data [17]. In the consensus layer, it uses the consensus algorithm and other technologies in the distributed system to realize the consensus of distributed nodes, and stores the consensus redundantly in multiple distributed nodes in the form of hash chain, which is difficult to tamper with.

Different blockchain applications are implemented through different application layer protocols and get different functions and characteristics, so they can be applied to different fields. Among them, there are two types of blockchain configuration, namely the public type and permissioned type [18]. For the public type blockchain configuration, a certain number of nodes can be freely used [19]. In other words, the distributed ledger and transactions are public to any participants. In order to guarantee the transaction from untrusted participants, consensus algorithms such as proof of work (POW) are required [20]. In regard to permissioned type blockchain configuration, the transaction approval process only uses the specified nodes, since ledger data may be disclosed outside of the network. In such a system, digital signatures are used for user authentication and transaction generation, and users must pay great attention to the management of secret keys.

Fig. 1 demonstrates the general configuration of the blockchain system. As shown in Fig. 1, each block in the blockchain system consists of two parts: a block header and a block body. The value of the hash and pre-hash of the block and the timestamp are stored in the block header. The detailed data of blocks such as transaction information is stored in the block body. Since blocks are linked with hash one by one, hash can be regarded as the unique identifier of blocks. The association between different blocks depends on their hash and pre-hash. The pre-hash value of each block is equal to the hash value of the previous block.

In the blockchain, a more complex hash algorithm is adopted, which converts the transaction records and other data information into hash value strings through a series of complex calculations.

Because the hash algorithm has the characteristics of one-way, the output can be obtained from the input, but it is almost impossible to push back the input through the output, and the hash value will change greatly for any input, even if it is a small change. Therefore, each block of the blockchain is processed by a hash algorithm, which makes the information on the blockchain difficult to be tampered with, so the security of the information is greatly improved.

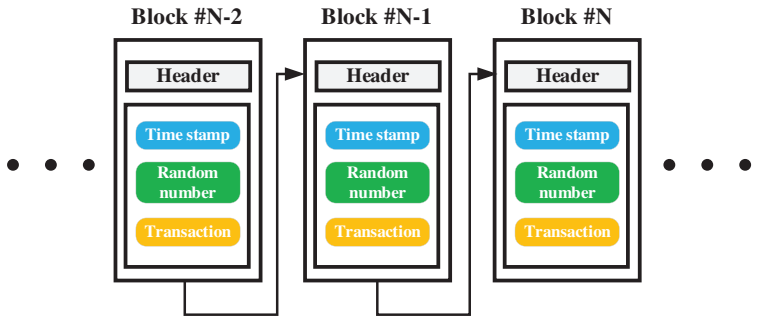

Figure 1: The diagram of the blockchain system

2.2 Application of Blockchain to Electrical Equipment Maintenance

Personnel management and unified certification and control technology of power secondary equipment are the key realizations of this project. The technical scheme will connect the network management system, work ticket system, personnel database system, face recognition system, and other systems in the power system in series to provide AAA service based on the blockchain for secondary power equipment. The deployment architecture is as follows (Fig. 2).

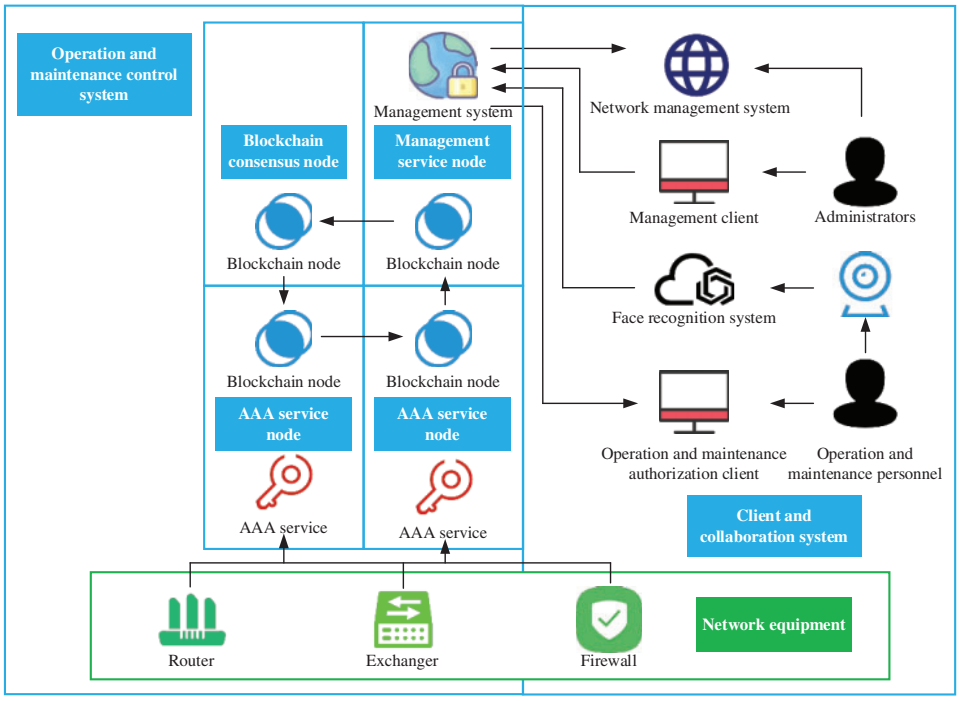

Figure 2: System deployment architecture

As demonstrated in Fig. 3, the operation and maintenance personnel information uplink process consists of: the administrator signs and authorizes the operation and maintenance personnel data and submits it to the information-sharing system for signature verification and audit. After the signature verification and audit are passed, the system signs and adds the signed data to the data source. At the same time, the data summary block is generated and added to the data summary chain.

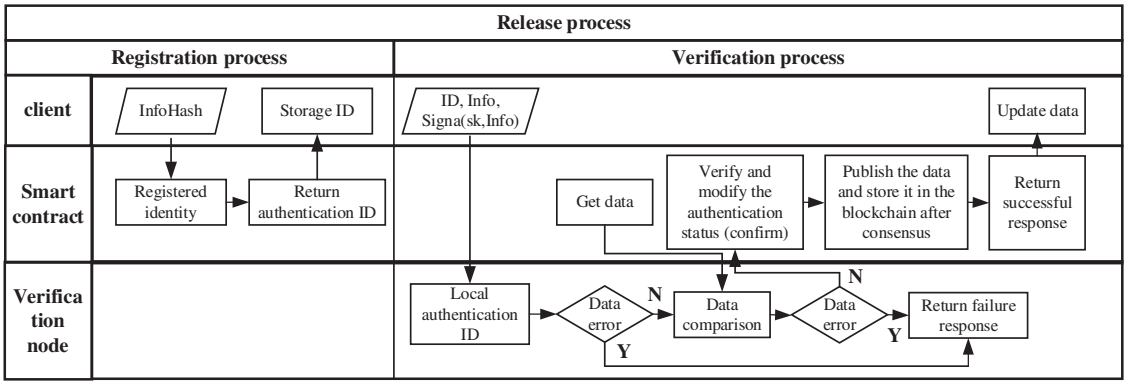

Figure 3: Key management system on the server-side

As shown in Fig. 4, the corresponding data of block structure and personnel information includes login name, authentication status, authentication time, login device IP, end-user IP, session status, session duration, access time, off time, etc.

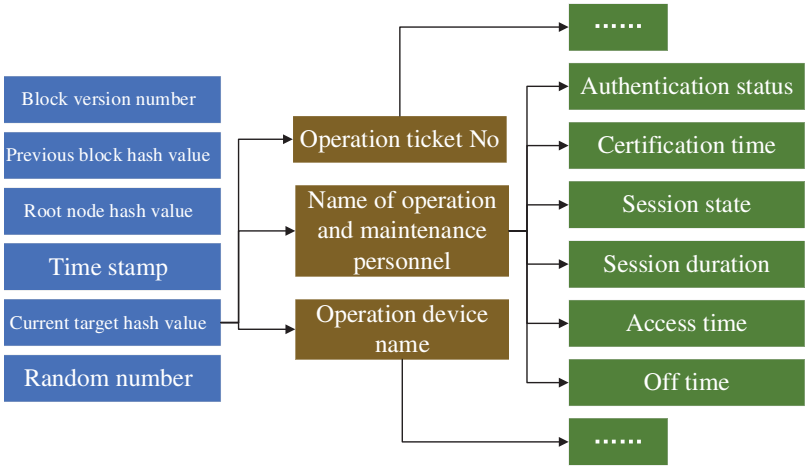

Figure 4: Key management system on the server-side

2.3 Biometric Fuzzy Signature

Fig. 5 demonstrates the key management system on the server-side in the blockchain system. First, the user sends a transaction request to the key management server. After that, the user provides a digital signature for the transaction key, and finally, the transaction is implemented in the blockchain system. The generated keys are usually stored in the key management server. As alluded to in the aforementioned discussions, blockchain is hard to be tampered with. Therefore, the user or users secret key is one of the attacked targets from hackers. As shown in Fig. 2, once the user's secret key is stolen

by hackers, they can replace the user in the transaction process, making transaction requests, forging digital signatures, and creating fake transactions, which will lead to the leakage of the user's individual information and loss of accompany benefits. In serious cases, the leakage of keys will even affect the security of the whole system.

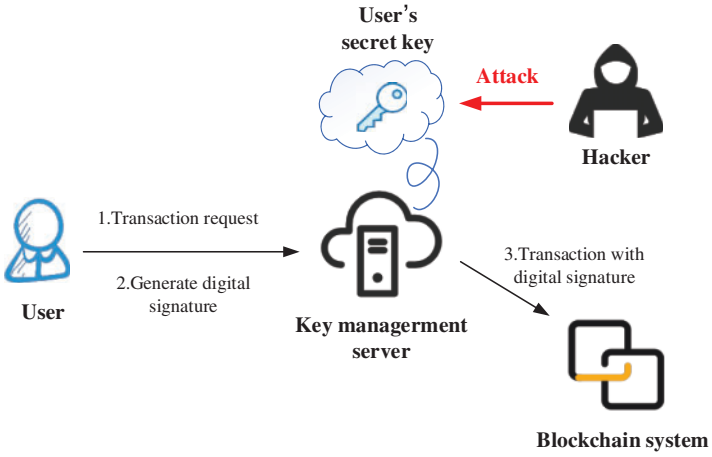

Figure 5: Key management system on the server side

In order to overcome this problem, a biometric fuzzy signature is used. However, biological information received from biosensors may result in a system misjudgment due to measurement errors. Thus, a fuzzy extractor is generally used to fix the discrepancy caused by measurement errors. The obtained key features are then used as a digital signature, which can be used to replace the traditional password key.

Since the management devices such as a key management server is vulnerable to hackers or can be attacked by malware, which can possibly cause a loss of security keys, a solution is looked for. According to the signature method, the key is generated based on the biometric information provided by users at the input side each time. Therefore, the signature method reduces the risk of key theft to a certain extent.

2.4 Security Issues of Key Management

In this section, we summarize the problems in the application of blockchain technology to the process of facial recognition-based transactions. As shown in Fig. 6, the blockchain transaction based on facial recognition adds a sensor to the traditional method. The main role of this sensor is to collect the input face images from the user side, while the biometric features on the facial images are later extracted by the feature extractor. After the system identifies and confirms the user's identity, a digital signature is provided by the user for key generation. Finally, the transaction is completed in the blockchain system.

There is still a risk of hacking in the above transaction process. Since the traditional biometric authentication system will release the key as soon as it detects that the fit between the input biometric and the registered biometric during the identification process is within the error tolerance. Even if keys generated by the biometric signature are deleted after use, hackers still have opportunities to attack the sensor, then they steal facial pictures uploaded by users, and subsequently obtain the biometric information to replay old data, as shown in Fig. 6.

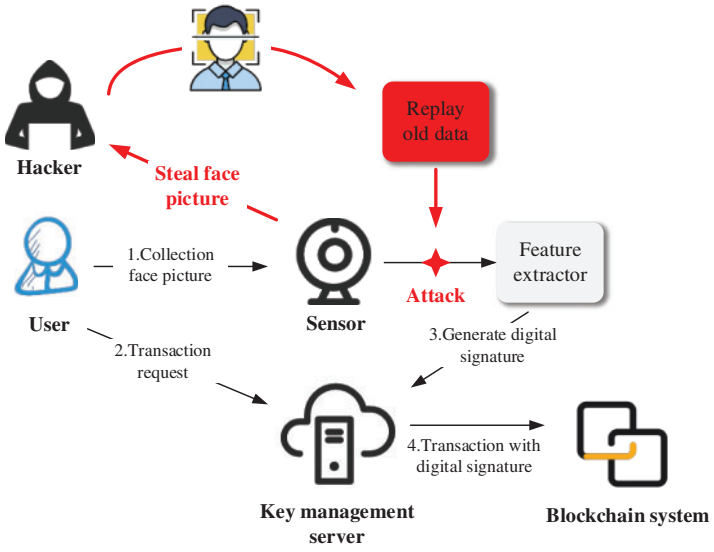

Figure 6: The schematic diagram of blockchain transaction based on face recognition

The validity of transactions on the blockchain is achieved by the system checking the match between the biometric and the key. Therefore, if the user loses or leaks the key, it will lead to vicious transactions caused by the leakage of information stored on the blockchain, which may break the trust within the current market trading environment. Due to a special way of combining the key with the biometric features, the security of the key will directly determine the security of the system. Therefore, once the security of the key has a major problem, it will drag and implicate the security of the system in question as well.

3 The Proposed Method

For a long time, it has been understood that biometric systems are vulnerable to some hardware and software attacks. By presenting attack detection technology, the physical attack on biosensors can be overcome to a certain degree or extent. On the other hand, using biometric template protection technology can prevent a group of important software attacks too. However, as shown in Fig. 6, it is easy for hackers to steal the user's photos by attacking the sensor. Then, the hackers replay the old photos (old data) to impersonate the user login interface. As shown in Fig. 7, an innovative method is proposed in this paper. Adding a timestamp in the process of feature extraction can well solve the attack of hackers stealing old photos. Because each photo is stamped with a time stamp, the time when the hacker uses the photo again is not matched with the time when the photo is obtained, so the hacker cannot pass the face recognition process.

3.1 Blockchain System Based on Timestamp and Face Recognition

Deep learning (DL) technology develops rapidly nowadays. In the field of face recognition, the DL techniques have also been applied to some extent. In this paper, compared with other proposed methods, more advanced DL-based face recognition techniques, namely ResNet50 and ArcFace, are used in the blockchain transaction process.

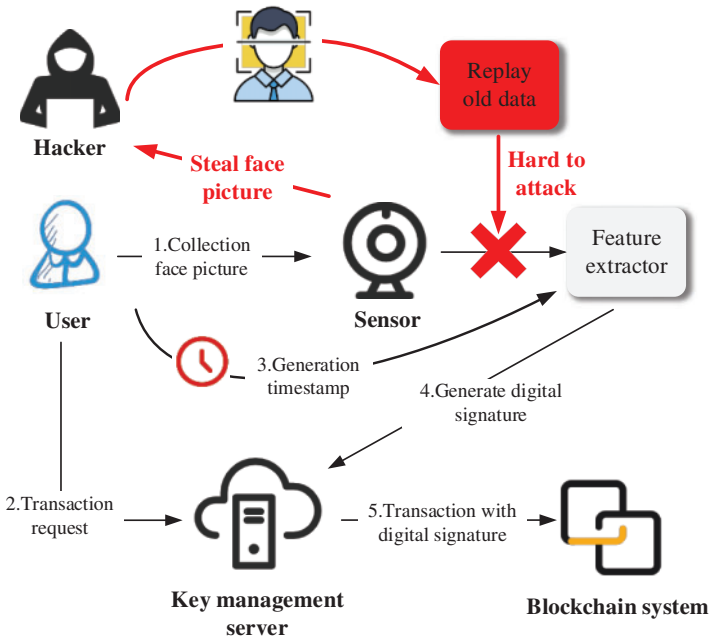

Figure 7: The schematic diagram of blockchain transaction based on face recognition and timestamp

The depth of the network is one of the important parameters of a neural network. Because CNN can extract low/mid/high-level features, the more layers the network possesses means that richer features can be extracted to different levels too. Moreover, the deeper the network is, the more abstract the features extracted are, and the more semantic information it in turn has. However, simply increasing the number of layers of the network does not improve the performance of neural networks indefinitely either.

This problem has been solved to a considerable extent by normalized initialization and intermediate normalization layers, which allow networks with tens of layers to begin converging for stochastic gradient descent (SGD) with backpropagation.

In addition, another problem occurs, namely the degradation problem. Although the number of layers of the network increases, the accuracy of the training set is saturated or even decreases. This cannot be explained as overfitting, because overfitting should be shown to perform better on the training set. The degradation problem illustrates that deep networks cannot be optimized well quite simply. In summary, the ResNet has been proposed. It uses a connection method called "shortcut connection".

The main difference between ordinary neural networks and deep residual networks is that deep residual networks have many bypass branches to connect the input directly to the later layers, so that the later layers can learn the residuals directly. These branches are called shortcuts. The ResNet solves this problem to some extent by directly bypassing the input information to the output to protect the integrity of the information, so that the whole network only needs to learn part of the input and output differences, simplifying the learning goal and difficulty.

In the biometric cryptosystem, the main feature is the existence of public data related to the stored biometric template, which is called auxiliary data. Because the biometric credentials of legitimate users are different, the auxiliary data helps to correctly reconstruct the key. The comparison of keys

is encrypted, so the biometric cryptosystem is used for biometric template protection. The template security method based on a biometric cryptosystem is also known as the method based on auxiliary data. Biological encryption mainly includes key binding and key generation. Key binding means that the key is bound with the biometric template to generate auxiliary data. During authentication, the query biometrics and stored auxiliary data are used to retrieve the key; key generation refers to the biometric template used to generate keys and auxiliary data, which are not necessarily stored in the database. During authentication, the secondary data uses query biometrics to assist in retrieving the key.

Fig. 8 illustrates the flow of face recognition. As can be seen from the figure, first, the camera collects the video stream at the input for pretreatment. The image or video collected by the camera contains a large amount of background information, which is invalid information that can interfere with face recognition. Therefore, it is necessary to pretreat the information in the collected video streams. The neatly arranged face images obtained after pretreatment will be used to extract face features. Then, the facial recognition system recognizes the extracted face information. Joseph Redmon proposed Yolo (you only look once) algorithm in 2015 and developed Yolo V3 version in 2018. Yolo V3 uses a single network structure to predict the object category and location while generating candidate regions.

The coordinate decoding formula of Yolo V3 is as follows:

$$b_x = \sigma\left(t_x\right) + c_x \tag{1}$$

$$b_y = \sigma\left(t_y\right) + c_y \tag{2}$$

$$b_w = p_w e^{t_w} \tag{3}$$

$$b_h = p_h e^{t_h} \tag{4}$$

where $\left(t_x, t_y, t_w, t_h\right)$ are prediction target, and $\left(b_x, b_y, b_w, b_h\right)$ are real coordinates, the above equation is the transformation from predicted target to real coordinates.

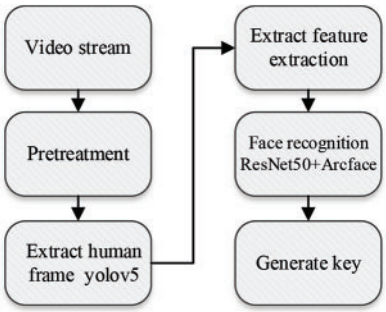

Figure 8: The flowchart of face recognition

Yolo V5 is the latest version and is widely used currently. Yolo V5 is a single-stage target detection algorithm. The algorithm adds some new improvement ideas onto the basis of Yolo V4, which greatly improves its speed and accuracy. In the paper, the Yolo V5 algorithm is used to extract the human frame and the facial recognition technology in the application of the recognition process is ResNet50+ArcFace, which is based on advanced deep-learning technology. In the transaction based on blockchain, after the results are obtained from the face recognition system, the key is generated by the transaction system for the final transaction.

3.2 Pretreatment and Face Recognition

Pretreatment is the first step of almost all computer vision technologies. First, the target to be processed needs to be detected in the image before continuing the next task. Face detection is a specific target detection belonging to target detection. Face detection is a technology to extract faces from images containing faces. It includes two parallel steps: location and classification. It is necessary to obtain the exact position of faces while judging whether there are actually faces in the image. Generally, the face image or video collected by the camera contains a lot of irrelevant background information. If you want to operate the face, you need to detect the face and preprocess it to get the aligned face image. Early face detection technology is mainly based on traditional image features and classifiers, which are slow and inaccurate. In recent years, with the emergence of deep learning, there have been many face detection algorithms based on deep learning, which have high accuracy and fast speed, and can achieve high accuracy in many difficult scenes, such as dense scenes, small faces, occlusion and so on. Considering that the faces in the data set used in this subject are relatively easy to detect, fast, and easy to operate, this paper chooses to use the open-source Dlib toolkit for facial detection. The facial detection interface provided by the Dlib toolkit includes the traditional cascade detection method based on hog feature, as well as the deep learning method based on convolutional neural network, The method based on CNN has high speed and accuracy. In the process of this experiment, the method based on CNN is used for facial detection, and the face is successfully detected in all the pictures in the data set.

In order to make our algorithm run in real-time, we choose directional gradient histogram (HOG) as the face detector. This method is first used for human body detection, and then specially used for face recognition. The algorithm first performs a gray-scale transformation on the image, because facial recognition does not need color. Then, the image is divided into multiple connected regions, and the edge direction histogram of each connected region is calculated. Then the sliding window is used to train the classification algorithm support vector machine (SVM) in both positive and negative aspects. In particular, a method called hard negative mining is used to train an SVM classifier by using the feature vectors obtained from positive and negative samples.

Once the face is detected in the image, we use a convolutional neural network (CNN) to encode the latter. FaceNet is introduced and trained on LFW. The accuracy of the recognition task is 99.63% and 95.12% on YouTube faces dB. After training, the CNN can generate 128 measurements for each person, that is, embedding, which is particularly suitable for our target, because when the images are different, the difference displayed is very small, but the objects are the same. This method was born from facial recognition. Because of our interest in authentication, we are not interested in the nature of the proposed transaction.

4 Result

4.1 Security Policy Implementation

The safety protection of electric power information systems is divided into two stages: Subsystem Protection, and Internet Protection. Below the chain link, Information security relies on hardware isolation in each independent link. Generally, the security hardware is independent of the mobile intelligent terminal. It has a separate system, namely an independent operating environment, to protect the authentication data security of users and provide random number generation, certificate requests and external information signature services. Hardware isolation systems cannot be compromised by network hackers, so fake identity attacks are what you need to be aware of at this stage. On the

Blockchain network, the Consensus mechanism can protect the preset user authentication information from hacker attacks.

However, due to the complexity of the power system, existing security measures cannot entirely avoid risks from within. Especially when the operator information is stolen and used to log in to the system and conduct illegal operations, the security system lacks effective means for identification. In response to this problem, we added facial recognition to the security system to prevent operator information from being stolen. The subsystem is also able to avoid hacker attacks by proofreading work ticket information and personnel information with time stamps. The effectiveness of the protection strategy can be proved through experiments.

4.2 The Experiment Platform

Our experiments took place on a machine whose OS is Windows 10, with 1 CPU and 16 GB RAM. All functions are implemented in Python. Components, i.e., the blockchain network, virtual substations, and all services are deployed in local servers. Our program is based on the Python Flask framework. Flask is a web framework, it is a Python module that lets us develop web applications. It has a small and easy-to-extend core: it is a microframework that doesn't include an ORM (Object Relational Manager) or such features. It does have many interesting features like URL routing, and a template engine. It is a WSGI web app framework.

4.3 Block Information Structure

This article proposes a late-blockchain system with a timestamp which aims to enhance the part before uplink. We detail it in the applications of the power grid for the verification of confidentiality and practicality. In this model, we set a timestamp verification code. When logging in, the operator must apply for an operation ticket and sign in within the time, otherwise, they will be judged as invalid by the system. Compared with traditional blockchains, this architecture reduces the risk of being attacked in a pre-chain stage, which tends to be neglected.

The operation of equipment maintenance involves different sections such as a dispatching department, a maintenance department, and various substations. As shown in Fig. 9, the information of operator, equipment, and operation ticket mainly compose the block which supports major functions of power system operations. The generation of the message block is firstly launched by dispatching departments. This process will invoke the operation ticket generation system that includes mission objective, operator, and specific mission time. Specific mission time is a key certificate that will be employed to verify whether the task execution time is consistent within operation ticket. The maintenance department will read the operator information and dispatch operator according to the message block. The substation will verify the target equipment and accept operation requests. In addition to the function parts above, the message block also contains information about a blockchain and computer systems. Only some important data is encrypted to improve the encryption speed.

4.4 Face Recognition

To ensure the safety of the power system, the process of operation needs PPK which is generated from each operator's face feature matrix and timestamp individually. The generation of these keys is retrieved by each operator in its local node and called by the face recognition service in the Substation Management Service Centers. They are thus generated off-chain and sent to key management servers via blockchain transition. Public keys are handed out to selected organizations, while private keys are only stored in trusted partners.

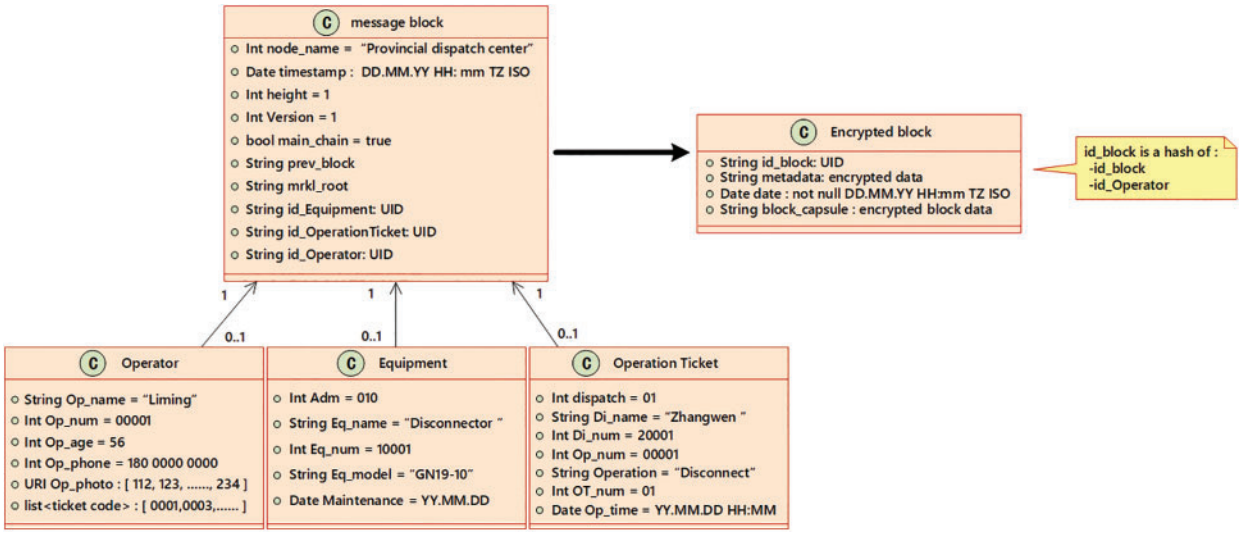

Figure 9: Blockchain information integration and important information encryption

For contrast purposes, we set two sets of normal experiments and two sets of abnormal values. In the normal experiment, the operator is recognized by whose feature matrix and timestamp are identified by dynamic PKI logs in the system and is allowed to pass. The third person failed to find the account when the circumstance is not in condition. The fourth person is a simulated hacker attack, stealing the same photos but is not prescribed with the wrong timestamp, the system detects and intercepts it to prevent access.

4.5 Functional Verification

In the experiment, the verification process is shown in Fig. 10 and the procedure is as follows:

(1) Scan face into the substation management system or portable verification device

The first procedure is to log into the system, operators should scan the face into the substation management system or portable verification device to input facial information into the system. As shown in the first line of Fig. 10, the image of the first and second operators is normal, while the image of the third operator in the system is not distinct enough due to the lack of light.

(2) Extract image features and add timestamps

The system collects the operator's facial image information, converts the color image into digital information, and waits for the system verification. At the same time, the system records the current time, and converts it into digital information as a timestamp. As shown in the second line of Fig. 10: the image data of red, green, and blue are input into one block. Then, they are combined with the timestamp and merged into a new grey block, waiting to be verified with the original given value in the system.

Figure 10: Login verification effect of operation and maintenance personnel

(3) Verify time stamps and perform face recognition

The block composed of facial image information and timestamps is used to generate a secret key, which is verified with the original given value in the system. The verification process

consists of two parts is as follows: first, compare the facial image digital information in the key block with the image digital information previously stored in the system. If the verification fails, it is proved that the user does not have permission to use the power equipment and this verification process fail. If the verification of face image information is correct, go to the next verification step, and compare the timestamp information in the key block with the time information stored in the original system. If the timestamp is appropriate, it indicates that the operator has passed the identity verification. If the timestamp is not of the proper condition, it indicates that the verification has failed. In a word, only when the two parts of the verification process are correct, can the operator pass the test of sorts and be accepted.

(4) Return the result and upload on the blockchain

After the system verification, the relevant data information of an operator is finally returned, such as the amount equipment operated and used, the operator's name, operation ticket, and other information. The result of this identity verification is then displayed. As shown in line 4 of Fig. 10, the first and second operators passed the verification, while the third operator failed since the light was too dim. Although the fourth operator's facial recognition verification was successful, the timestamp did not conform to the given range of the timestamp in the original blockchain. So he fails to pass the verification and a warning is returned.

Through the experiment, data processing and personnel registration have verified the defensive capabilities of the timestamp blockchain by simulating attacks caused by third-party theft and the subsequent data leakage. While ensuring security, the speed of identity verification has not been decreased.

5 Conclusions

In this paper, a novel blockchain system which is based on facial recognition and timestamp procedures is proposed. The advantages and innovations of the system are as follows:

(1) By using a biometric fuzzy signature, this system can prevent the hackers from stealing the user's secret key.

(2) Adding a timestamp to the process of feature extraction can solve the problem that hackers replay the old data to impersonate the user login interface.

(3) Deep learning technology is used in this system. After training, the CNN can generate 128 measurements for each person which enhance the accuracy and efficiency of face recognition.

In order to verify the performance of the system, four experimental samples are set up. Through experiments, it is proved that the system can successfully recognize the wrong face information and can effectively prevent hackers from replaying old data to attack the system.

In future research, we will focus on the following aspects:

(1) To realize the monitoring of the running state of the power system equipment by blockchain.

(2) Research new energy current affairs trading strategy on blockchain technology.

(3) Test system reliability in real power system.

Funding Statement: This research was funded by science and technology project of State Grid JiangSu Electric Power Co., Ltd. (Research on Key Technologies of power network security digital identity authentication and management and control based on blockchain, Grant No. is J2021021).

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

References

1. Wang, Y. Z., Chen, J. L., Wang, X. (2019). *Smart contract*. Beijing, China: Electronic Industry Press.
2. Ding, W., Wang, G. C., Xu, A. D., Chen, H. J., Hong, C. (2018). Research on key technologies and information security issues of energy blockchain. *Proceedings of the CSEE, 38,* 1026–1034.
3. Qin, J., Sun, W., Li, Z., Zhu, Y. (2020). Credit consensus mechanism for microgrid blockchain. *Automation of Electric Power Systems, 44(15),* 10–18.
4. Jin, Z. G., Wu, R. Q., Li, G., Yue, S. (2019). Transaction model for electric vehicle charging based on consortium blockchain. *Power System Technology, 43,* 4362–4370.
5. Qi, B., Xia, Y., Li, B., Li, D., Zhang, Y. et al. (2019). Photovoltaic trading mechanism design based on blockchain-based incentive mechanism. *Automation of Electric Power Systems, 43(9),* 132–139.
6. Gong, G., Zhang, T., Wei, P., Su, C., Wang, H. (2019). Research on intelligent trading and cooperative scheduling system of energy internet based on blockchain. *Resources Environment & Engineering,* 1278.
7. Yang, X., Zhang, Y., Lu, J., Zhao, B., Huang, F. T. et al. (2017). Blockchain-based automated demand response method for energy storage system in an energy local network. *Proceedings of the CSEE, 37(13),* 3703–3716.
8. She, W., Gu, Z., Yang. X. (2019). A model of multi-energy complementation and safety transaction on heterogeneous energy blockchain. *Power System Technology, 43(9),* 3193–3201.
9. Li, B., Cao, W., Lu, C. (2018). Security management and technique support for multi-level DR bidding under untrusted environment based on blockchain. *Proceedings of the CSEE, 38(8),* 2272–2283.
10. Arab, A., Tekin, E., Khodaei, A., Khator, S. K., Han, Z. (2016). System hardening and condition-based maintenance for electric power infrastructure under hurricane effects. *IEEE Transactions on Reliability, 65(3),* 1457–1470. DOI 10.1109/TR.2016.2575445.
11. Callou, G., Sousa, E., Maciel, P., Tavares, E., Araujo, C. et al. (2010). Impact analysis of maintenance policies on data center power infrastructure. *IEEE International Conference on Systems, Man and Cybernetics*, pp. 526–533. Istanbul, Turkey: IEEE.
12. Li, J. F., Lu, X., Zhang, D., Sheng, J. (2021). A review on the blockchain technique applied in cloud energy storage power system. *IEEE 6th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA)*, pp. 415–422. Chengdu, China: IEEE.
13. Kumar, N. M., Chand, A. A., Malvoni, M., Prasad, K. A., Mamun, K. A. et al. (2020). Distributed energy resources and the application of AI, IoT, and blockchain in smart grids. *Energies, 13(21),* 5739.
14. Thukral, M. K. (2021). Emergence of blockchain-technology application in peer-to-peer electrical-energy trading: A review. *Clean Energy, 5(1),* 104–123. DOI 10.1093/ce/zkaa033.
15. Li, W., Liu, Z., Song, J. (1998). Enhancement of electric power system security using network topology reconstruction-A bibliographical survey. *Automation of Electric Power Systems*, 22. X7–66.
16. Yang, Y., Zhang, X., Yu, J., Zhang, P. (2017). Research on the hash function structures and its application. *Wireless Personal Communications, 94(4),* 2969–2985. DOI 10.1007/s11277-016-3760-4.
17. Barolli, L., Xhafa, F. (2010). JXTA-overlay: A P2P platform for distributed, collaborative, and ubiquitous computing. *IEEE Transactions on Industrial Electronics, 58(6),* 2163–2172. DOI 10.1109/TIE.2010.2050751.

18. Jin, L. J. (2011). System in the RSA asymmetric encryption algorithm. *Electronic Design Engineering, 11(10)*.
19. Lu, C., Hu, Z. (2010). A security routing algorithm of P2P network based on asymmetric nested encryption. *2010 Second International Conference on Information Technology and Computer Science*, pp. 17–20. Kiev, Ukraine, IEEE.
20. Ametrano, F. M. (2016). *Bitcoin, blockchain, and distributed ledger technology*. Social Science Electronic Publishing.