Research on User Safety Authentication Based on Biometrics in Cloud Manufacturing

Xiaolan Xie[1,2], Xiao Zhou[3(✉)], and Yarong Liu[1,2]

[1] College of Information Science and Engineering,
Guilin University of Technology,
Guilin 541004, Guangxi Zhuang Autonomous Region, China
[2] Guangxi Universities Key Laboratory Fund of Embedded Technology and Intelligent Information Processing, Guilin University of Technology,
Guilin 541004, China
[3] College of Mechanical and Control Engineering,
Guilin University of Technology,
Guilin 541004, Guangxi Zhuang Autonomous Region, China
2485782688@qq.com

Abstract. Cloud manufacturing is a use of the network and cloud manufacturing services platform, according to user requirements organize manufacturing resources online (manufacturing cloud), and provide users a new network manufacturing model with various on-demand manufacturing services. Through the design of user access security authentication model, using biometric technology to ensure the access security of users in the cloud environment, to prevent malicious users access to illegal. The point set topological group fractal changing algorithm is used to encrypt biometric information acquired by biometrics, which provides more guarantee for the security authentication of users.

Keywords: Cloud manufacturing · Security authentication · Biometrics
Point set topological group fractal changing algorithm

1 Introduction

Cloud manufacturing technology integrates existing networked manufacturing services technology with cloud computing, cloud security, high-performance computing, networking and other technologies [1]. Cloud manufacturing achieve unified, centralized, intelligent management of all kinds of manufacturing resources (manufacturing hard equipment, computing systems, software, models, data, knowledge, etc.) and provide the available, Immediate, on-demand, safe, reliable, quality and cheap service for the life cycle process. User security certification is the first concern of cloud manufacturing system. In the cloud manufacturing system architecture, the application layer is directly oriented to the user, and the security authentication of the user access is directly related to the security of cloud manufacturing [2, 3]. Biometric identification technology is used to identify biometric and encrypt them at the same time, so as to ensure the user's information security. Biometric cryptography implements the unity of the person's digital identity (who he is) and the physical identity of the person (who he really is).

G. Sun and S. Liu (Eds.): ADHIP 2017, LNICST 219, pp. 50–55, 2018.
https://doi.org/10.1007/978-3-319-73317-3_7

Key is the most important part of encryption [4]. Point set topological group fractal changing algorithm combined with biological feature information to generate key. At the same time, the biometric points such as face, voice and fingerprint are used as the data source of fractal change, which is unique, and further improves the security of the encryption system [5].

2 Related Introduction

2.1 Cloud Manufacturing

Cloud manufacturing is the enterprise manufacturing resources as the research object, for the purpose of realizing dynamic combination and efficient utilization of resources. Through the Internet of things, Internet technology to achieve comprehensive connectivity and intelligent perception of manufacturing resources; through virtualization technology to build virtual resources cloud pool, and realize the virtualization and service of manufacturing resources. Build a cloud manufacturing service platform with the support of network technology. Publish the personalized requirements of the cloud requester to the manufacturing resource to the platform. Conducting a fast and efficient resource intelligent search and matching by cloud service. The dynamic reconfiguration and utilization of manufacturing resources are rapidly realized by the cloud provider and achieve a new service-oriented network manufacturing model with three win-win situation by cloud request side, cloud service providers and cloud providers.

2.2 Biometrics and Its Risks

When users enter the cloud manufacturing system or access the system resources of different protection levels, the system needs to use some authentication methods to carry out security. Biometric technology is unique individual identification techniques that can be sampled and measured for biological characteristics. Biometric features are acquired by biometrics. There is a risk of biometric information protection, once the user's biometric information was leaked, stolen or tampered with, such as fingerprints or facial features, due to the fixed and only has the biological characteristics, it is difficult to conduct similar password reset remedial measures will likely cause great losses to the users. Therefore, biometric encryption is critical.

2.3 Point Set Topological Group Fractal Changing Algorithm

Firstly, the image data set division, after the division of the subset of hash operations as a random key input, and then get the fractal changing loop operation, the coordinate values of the sub set points after loop operation are obtained, the final output of the pseudo random sequence. The flowchart of the point set topological group fractal changing algorithm is shown in Fig. 1.

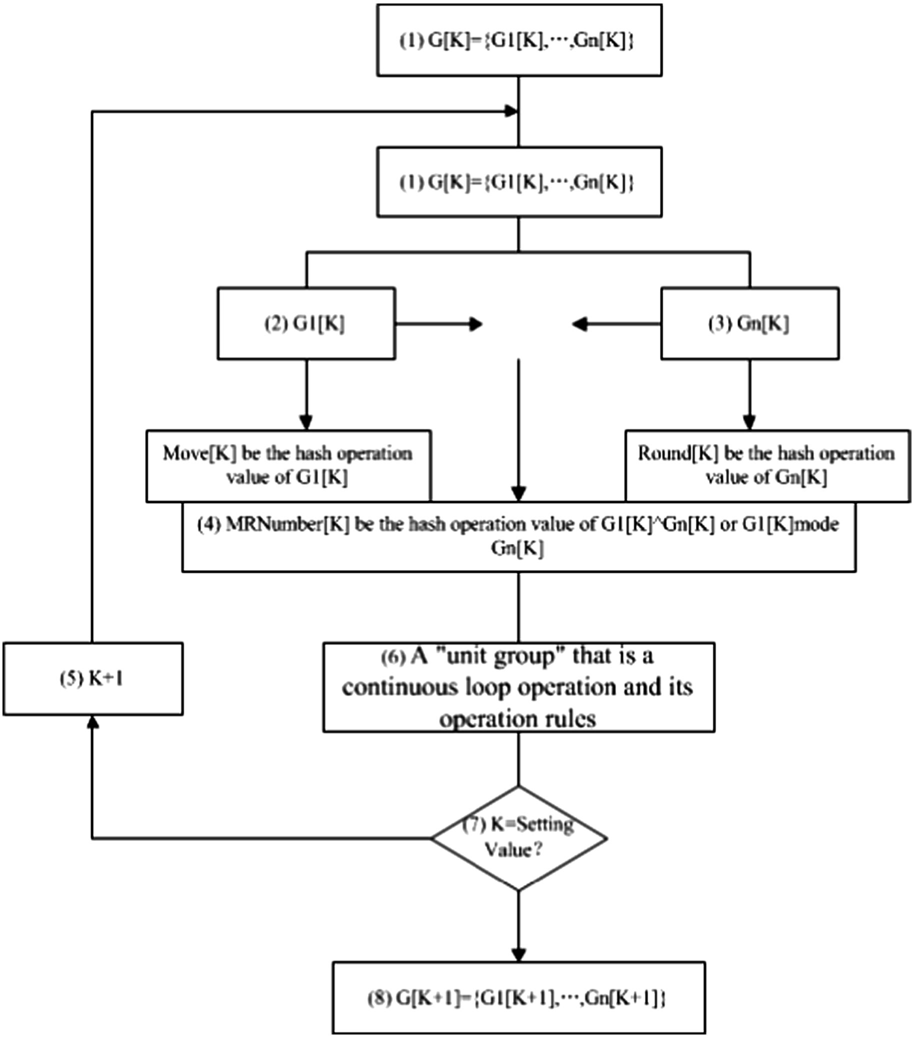

(1) G[K]={G1[K],···,Gn[K]}
(1) G[K]={G1[K],···,Gn[K]}
(2) G1[K]
(3) Gn[K]
Move[K] be the hash operation value of G1[K]
Round[K] be the hash operation value of Gn[K]
(4) MRNumber[K] be the hash operation value of G1[K]^Gn[K] or G1[K]mode Gn[K]
(5) K+1
(6) A "unit group" that is a continuous loop operation and its operation rules
(7) K=Setting Value?
(8) G[K+1]={G1[K+1],···,Gn[K+1]}

Fig. 1. The flowchart of the point set topological group fractal changing algorithm

3 User Access Security Authentication Design Model in Cloud Manufacturing

The architecture of cloud manufacturing system mainly includes physical resource layer, cloud manufacturing, virtual resource layer, cloud manufacturing core service layer, application interface layer and cloud production application layer. Users in different industries need to access and use various cloud services of cloud manufacturing systems only through cloud manufacturing portals, various user interfaces (including mobile terminals, PC terminals, dedicated terminals, etc.). The two layers in the cloud manufacturing architecture are connected to the outside world, directly to the user. User access security authentication is divided into the user which is bound to platform command access security authentication and the user which is bound to client access security authentication. The authentication process is shown in Fig. 2.

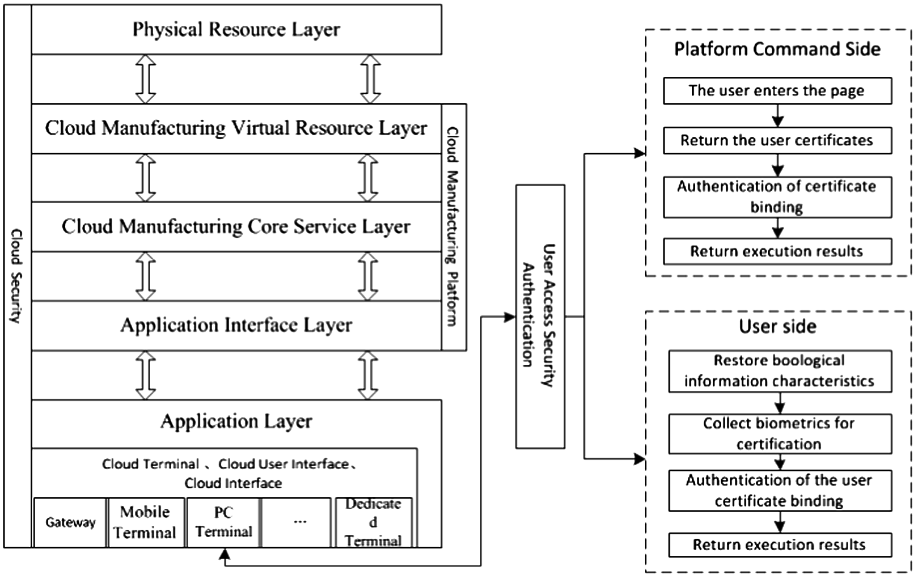

Physical Resource Layer
Cloud Manufacturing Virtual Resource Layer
Cloud Manufacturing Core Service Layer
Application Interface Layer
Application Layer
Cloud Terminal 、Cloud User Interface、
Cloud Interface
Gateway
Mobile Terminal
PC Terminal
...
Dedicated Terminal
Cloud Security
Cloud Manufacturing Platform
User Access Security Authentication
Platform Command Side
The user enters the page
Return the user certificates
Authentication of certificate binding
Return execution results
User side
Restore boological information characteristics
Collect biometrics for certification
Authentication of the user certificate binding
Return execution results

Fig. 2. User access security authentication model in cloud manufacturing

When the user which is bound to platform command access security authentication. First of all, the cloud management platform based on user login web page user information to pass user certificates. If the user does not have a certificate to store user security information, the certificate is returned to the user and pass commands to collect biological information features of users. Then, perform the trusted pattern recognition technology and the certificate signature binding authentication and returns the result of the execution. At last, enters the other service process. If there is a certificate of user security information locally, the binding authentication is performed directly.

When the user which is bound to client access security authentication, client return a certificate‘s biometric information, then according to public key which is associated with biometric information. The biometric information feature template is restored by using the information characteristic associated with the private key. The platform issues commands to collect user information characteristics. Then, perform the trusted pattern recognition technology and the certificate signature binding authentication and returns the result of the execution. The cloud management platform analyzes binding authentication information, determines the user access, and then provides services.

4 Biological Feature Information Encryption Instance Simulation

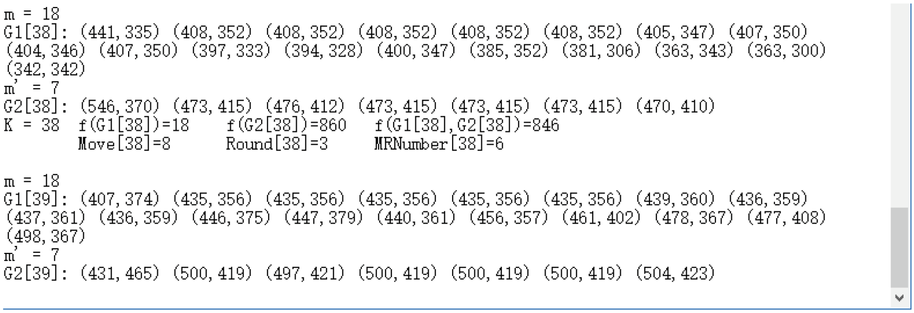
4.1 Point Set Topological Group Fractal Changing Algorithm Instance Running

Safety certification process Manufacturing System in the cloud access users are required in the use of biometric technology to read the biological characteristics, biological characteristics of information security also have a risk. In this paper, we use the point set topological group fractal changing algorithm. Taking the fingerprint image of a network public database as a reference example, the random key generation is completed by using the point set topological group fractal changing algorithm.

Run the program, select a fingerprint image to open. The simulation fill in 38, so perform 38 units Point set topological group fractal changing arithmetic operations, the operation of the contents recorded in the "mmlog" file.

4.2 Generate Point Set Topological Group Fractal Changing Operation Value

Open the file "mmlog" by G1[K] and Gn[K] display set a series of data collection G[K]. From the beginning to the end, it is shown that each set of data is not the same, showing great variability and randomness (Fig. 3).



```
m = 18
G1[38]: (441,335) (408,352) (408,352) (408,352) (408,352) (408,352) (405,347) (407,350)
(404,346) (407,350) (397,333) (394,328) (400,347) (385,352) (381,306) (363,343) (363,300)
(342,342)
m' = 7
G2[38]: (546,370) (473,415) (476,412) (473,415) (473,415) (473,415) (470,410)
K = 38  f(G1[38])=18    f(G2[38])=860   f(G1[38],G2[38])=846
        Move[38]=8      Round[38]=3     MRNumber[38]=6

m = 18
G1[39]: (407,374) (435,356) (435,356) (435,356) (435,356) (435,356) (439,360) (436,359)
(437,361) (436,359) (446,375) (447,379) (440,361) (456,357) (461,402) (478,367) (477,408)
(498,367)
m' = 7
G2[39]: (431,465) (500,419) (497,421) (500,419) (500,419) (500,419) (504,423)
```

Fig. 3. "mmlog" file content

The range of K the value is 1–38.

Move[K], Round[K], MRNumber[K] numerical range is also from Move[1] = 6, Round[1] = 4, MRNumber[1] = 3, to perform 38 units point set topological group fractal changing arithmetic operations, show Move[38] = 8, Round[38] = 3, MRNumber[38] = 6.

From the file set G[2] series data of G1[2] and G2[2] composed, to set G[39] series data of G1[39] and G2[39] composed, 38 set of G[K] changing data. The first set is the initial data.

5 Conclusion

This paper designs a user access security authentication model in cloud manufacturing, and applies biometric identification technology to user security authentication, which provides security for users to secure access in cloud manufacturing. At the same time, this paper uses the algorithm of point set topological group fractal changing. The biometric information is encrypted by biometric identification technology, and the security key is generated by combining the data of biological features to protect the user's information security, and further protect the security authentication of users in cloud manufacturing. This article has carried on the research safety certification of user in cloud manufacturing, and to ensure the safety of user data such as intrusion detection techniques do not study, this is should pay attention to the subsequent cloud manufacturing safety problems in the research, but also need to carry out research on infrastructure safety and operation management of safety, strengthen the security of cloud manufacturing system. However, the technology of intrusion detection and other technologies to ensure the security of user data has not been studied. This should be the focus of attention in the follow-up research of cloud manufacturing safety. Meanwhile, it also needs to study infrastructure and security, operations management security. To strengthen cloud manufacturing security protection system.

Acknowledgements. This research work was supported by the 'Ba Gui Scholars' program of the provincial government of Guangxi and Guangxi Universities key Laboratory Fund of Embedded Technology and Intelligent Information Processing (Guilin University of Technology).

References

1. Wu, D., Greer, M.J., Rosen, D.W., et al.: Cloud manufacturing: strategic vision and state-of-the-art. J. Manuf. Syst. **32**(4), 564–579 (2013)
2. Wang, X.V., Xu, X.W.: An interoperable solution for cloud manufacturing. Robot. Comput.-Integr. Manuf. **29**(4), 232–247 (2013)
3. Zureik, E., Hindle, K.: Governance, security and technology: the case of biometrics. Stud. Polit. Econ. Soc. Rev. **73**, 113–137 (2016)
4. Moulay, E., Baguelin, M.: Meta-dynamical adaptive systems and their applications to a fractal algorithm and a biological model. Physica D Nonlinear Phenomena **207**(1–2), 79–90 (2005)
5. Hosaka, T.: On boundaries of Coxeter groups and topological fractal structures. Tsukuba J. Math. **35**(2), 153–160 (2009)