Research on Identity Authentication Method Based on Negative Logic System

Yexia Cheng[1,2,3(✉)], Yuejin Du[1,2,4(✉)], Jin Peng[3(✉)], Jun Fu[3], and Baoxu Liu[1,2]

[1] Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
chengyexia@iie.ac.cn
[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China
[3] Department of Security Technology, China Mobile Research Institute, Beijing, China
pengjin@chinamobile.com
[4] Security Department, Alibaba Group, Beijing, China
yuejin.dyj@alibaba-inc.com

Abstract. With the rapid development of computer and network, new technologies and services such as mobile Internet, Internet of Things, cloud and artificial intelligence have arisen and changed people's life. The identity authentication is a must for these services. To solve the problem, identity authentication system and method based on negative logic system (NLS) is proposed in the paper. NLS is introduced to improve security in the essence of attack and defense. Security mechanisms based on NLS are proved effective to increase attack cost and strengthen defense ability. So NLS-based identity authentication system and method in the cloud environment are designed. Meanwhile, the corresponding converters, distributed storage, distributed detectors and authentication are proposed. The proposed method can improve security and provide identity authentication for cloud, IoT, etc. The theoretical performance analysis proves that it is feasible and effective.

Keywords: Negative Logic System · Attack and defense · Identity authentication · Cloud security · Secure accessing · Internet of Things

1 Introduction

With the rapid development of computer and network, new technologies and services are being generated, evolved and promoted constantly, bringing great convenience and changes to people's life. Of which, mobile Internet, Internet of Things, cloud and artificial intelligence are all becoming the rising topics. Concerning to these technologies and services, the identity authentication is the precondition to guarantee secure accessing. Taking cloud environment as an example, it has some features and advantages such as broadband interconnection, resource pool sharing, flexible configuration, on-demand services, etc. However, while providing services and sharing resources in an open cloud environment, how to ensure the confidentiality, integrity, and availability

X. Yun et al. (Eds.): CNCERT 2018, CCIS 970, pp. 3–15, 2019.
https://doi.org/10.1007/978-981-13-6621-5_1

of system resources and user's data in the cloud is an important issue, and identity authentication is a premise guarantee to achieve this goal.

The researchers have already taken some studies on identity authentication. At present, Ghosh et al. focus on NFC and biometric algorithms [1]. Chien proposes video recognition technology [2]. Hu et al. point out the privacy protection using images and identity information [3]. And some other researchers propose the identity based encryption [4–10]. Of which, the identity based encryption is a new tendency for identity authentication. Urbi et al. propose PUF+IBE scheme, which contains the identity authentication algorithm for Internet of Things devices and its connection and protocol process based on elliptic curve [4]. In the field of aviation aircraft, a layered identity-based authentication IBV scheme is proposed. Wu et al. talk about the mobile device authentication and key agreement protocol based on elliptic curve [5]. Yuan et al. propose identity-based identification, mobile identity identification solutions based on IBI [6].

Although the research on identity authentication are more and more, there is a common problem on it, that is all the researches are based on positive logic system. It means that the user account authentication and other information are all stored in the identity authentication system based on positive logic system. Once the user's account is leaked or stolen, the attacker can make use of the acquired user information to access to the system and resources. Even worse, the attacker uses it as a springboard for taking deep cyber attack and penetration, which is a great security risk for the whole system. In addition, the security bottleneck of identity authentication lies in the selection of the authentication algorithm, which is the attacker's focused attack goal. If the authentication algorithm is attacked, the security of the entire cloud environment is hard to guarantee. Furthermore, the existing identity authentication technology does not involve the elements of a distributed cluster in the cloud environment, which has certain limitations in adaptability and scalability.

In order to solve the above problems, we propose the negative logic system (NLS) and take research on the method of identity authentication based on negative logic system in this paper. The identity authentication system and method based on negative logic system is proposed in the paper. NLS is introduced to improve security in the essence of attack and defense. Security mechanisms based on NLS are proved effective to increase attack cost and strengthen defense ability. So NLS-based identity authentication system and method in the cloud environment are designed. Meanwhile, the corresponding converters, distributed storage, distributed detectors and authentication are proposed. The proposed method can improve security and provide identity authentication for cloud, IoT, etc. The theoretical performance analysis proves that it is feasible and effective.

Our Innovations and Contributions. In this paper, there are some innovations and contributions. One of which is the negative logic system. The other is the security attack and defense mechanisms based on negative logic system. The third is the identity authentication method based on negative logic system. And the last is the method of converters and distributed storage based on NLS as well as the method of distributed detectors and authentication based on NLS.

The rest of this paper is organized as follows. Section 2 introduces the motivation. Section 3 proposes negative logic system. Section 4 presents security attack and defense mechanisms based on negative logic system. Section 5 proposes the identity authentication system and method based on NLS. Finally, in Sect. 6 we draw the conclusion of this paper.

2 Motivation

The existing security attack and defense mechanisms are based on the security attack and defense mechanisms of the positive logic system (PLS), that is to say, the state description of the security attack and defense is positive to the logic description of the security attack and defense. Hence, in the PLS-based security attack and defense mechanisms, the information is same and equal for both offensive and defensive sides. The essence of security attack and defense is the cost and expense of both offensive and defensive sides taken while attacking and defending. On the basis of information equivalence, the degree of confrontation, the superiority and inferiority status and the active and passive situation of both offensive and defensive sides can only rely on the cost and expense of cyber attack and defense tactics.

Therefore, the disadvantage of the existing PLS-based security attack and defense mechanisms is the limitation of offensive and defensive information equivalence. Firstly, on the basis of PLS, information is a one-to-one correspondence. Relatively speaking, the attacker can use a large number of attack groups to achieve an attack. The attack group here is a broad group that includes both the actual attacker population and any host, device, or computer network system that can be used in the network. Secondly, the existing attack and defense mechanisms increase the cost of information network defense side relatively. When it comes to the network or system of defensive side, it can be protected and defended by the defensive side only. For the decentralized or centralized attack methods and attack groups, only by strengthening the protection system of the defense side, can it be possible to defend against the attacker's attack, so that the defense cost and expense is much greater.

In order to solve the disadvantage of the existing mechanisms, the security attack and defense mechanisms based on negative logic system are innovatively proposed in the paper. That's the motivation of this paper. The NLS-based security attack and defense mechanisms can break the situation of information equivalence between offensive and defensive sides, so as to achieve that the information for both offensive and defensive sides is not equal, and then increase the cost and expense of cyber attacks, and meanwhile reduce the cost and expense of cyber defense.

What's more, the method of using the negative logic system for identity authentication is also proposed innovatively. And this NLS-based identity authentication method can be applied not only in the cloud environment but also in the Internet of Things (IoT) environment, which is of great significance to secure accessing.

3 Negative Logic System

We innovatively propose the negative logic system in the cyber security area together with the security attack and defense mechanisms based on negative logic system as well as the principle and method of our negative logic system.

Principle and Method of Negative Logic System. The principle and method of our negative logic system is described as follows.

The negative logic system is the opposite logic to the positive logic [11–17], and the corresponding relationship is 1:N mode, i.e. a one-to-many relationship. As for the formal language description, it can adopt the normal binary, octal, decimal, or hexadecimal formats, and it can also use the state number of the practical applications as well, for example, the state number of the application is N, then it can use N bases. Therefore, its formal language description method is flexible and can be selected according to the requirements.

We take the actual state number as an example to give the formal language description and definition of negative logic system. Assuming that there are n kinds of states in a system, which are defined as $S_1, S_2, S_3, \ldots\ldots, S_n$. Let $S = \{S_1, S_2, S_3, \ldots\ldots, S_n\}$, so that for any state $S_i \in S$, in which $i \in \{1, 2, 3, \ldots\ldots, n\}$, the negative logic value of S_i is any one of the states in S except S_i. That is to say, $NLS(S_i) \stackrel{def}{=} \{S_j | S_j \in S, S_j \neq S_i, j \in \{1, 2, 3, \ldots\ldots, n\}\}$.

The method of NLS is illustrated in following Fig. 1.

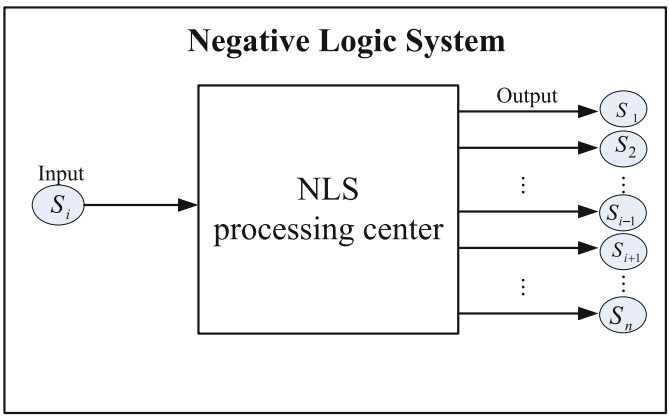

Fig. 1. Method of NLS

According to the above Fig. 1, the method of NLS is combined with input, NLS processing center and output.

As for input item, it is the value for inputting, which is transferred to the NLS processing center. The input value can be data information formatted in binary base, data information formatted in decimal base, data information or text information formatted in hexadecimal base, etc.

As for NLS processing center, it includes NLS processing mechanisms, the choosing and the transforming of number bases, selecting algorithm, calculation method, etc. Its main function is to determine the negative logic values according to the input and give result to the output part. For example, when the input is S_i, the negative logic values are in the following sets $\{S_1\}, \{S_2\}, \cdots, \{S_{i-1}\}, \{S_{i+1}\}, \cdots, \{S_n\}$.

As for output item, one of the negative logic values will be output randomly according to the selecting method and the calculation method set in the NLS processing center and even the time the input value being inputted into the NLS processing center. Taking the above example, one of $\{S_1\}, \{S_2\}, \cdots, \{S_{i-1}\}, \{S_{i+1}\}, \cdots, \{S_n\}$ may be outputted as the actual output value, such as S_2 at this moment. So the negative logic system result for S_i at the moment is S_2.

4 Security Attack and Defense Mechanisms Based on Negative Logic System

The structure of security attack and defense mechanisms based on negative logic system is shown in Fig. 2 below. It is comprised of the attack module, NLS module and defense module.

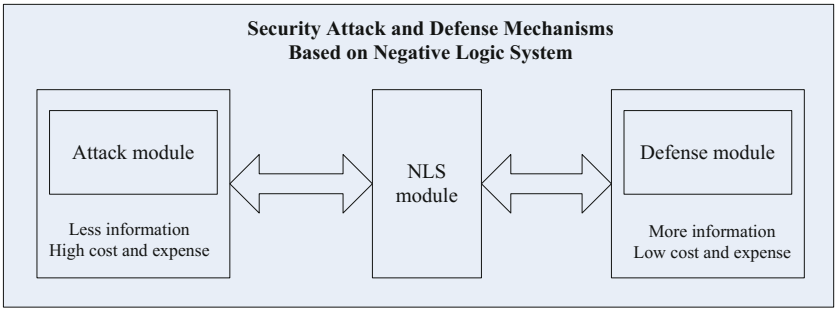

Fig. 2. Security attack and defense mechanisms based on NLS

In Fig. 2, we can see that attack module under the NLS-based security mechanisms is with less information so that the cost and expense to take an attack is much higher than ever PLS-based security mechanisms.

NLS module is the negative logic system and it is implemented according to the principle described in Fig. 1.

Defense module is under the NLS-based security mechanisms and its information is much more so that the cost and expense to take defense is much lower than ever PLS-based security mechanisms.

The performance analysis of security attack and defense mechanisms based on NLS is presented as follows.

According to the NLS principle and method, and combing with the security attack and defense mechanisms based on NLS, it is assumed that the number of states of a

system is n, which are defined as $S_1, S_2, S_3, \ldots\ldots, S_n$. Let $S = \{S_1, S_2, S_3, \ldots\ldots, S_n\}$, so based on NLS, there are $n-1$ possible kinds of negative logic value for any state $S_i \in S$, such as $\{S_1\}, \{S_2\}, \cdots, \{S_{i-1}\}, \{S_{i+1}\}, \cdots, \{S_n\}$. Therefore, in order to get the value of S_i, at least $n-1$ different values after data de-duplicating must be given. And by combing and analyzing, the value of S_i can be computed. Compared to the PLS, to get the value of S_i requiring only 1 value, the space of NLS is much greater than PLS. As for the entire system space, the space of PLS is n, while the space of NLS is $n(n-1)$. When a logic value is given, the probability of a successful PLS judgment is $\frac{1}{n}$, while the probability of a successful NLS judgment is $\frac{1}{n(n-1)}$.

In the security attack and defense mechanisms based on NLS, the defense side knows the number of all the states as well as the scope of the whole system space. It is therefore that the information for the defense side is much more than the attack side, and the cost and expense that needed to take is much lower.

However, as for the attack side in the security attack and defense mechanisms based on NLS, objectively speaking, the whole system security space is greatly expanded at first. It is expanded to the second power relationship for NLS from the linear relationship for PLS. Secondly, in the actual attack and defense, the attack side doesn't know or cannot get known of the number of all states such as n, so that, even if the attacker obtains k kinds of different logical values, the attacker cannot know how many times it still needs to get the correct information he wants when he doesn't know n. Thus, the complexity and difficulty of the attack is greatly increased. It is therefore that the information for the attack side is less than the defense side, and the cost and expense required for the attack side is much higher and more.

From the viewpoint of the essence of security attack and defense, the essence of the attack lies in the cost and expense of taking attack, while the essence of the defense lies in the cost and expense of taking defense. From the above performance analysis, we can know that the security attack and defense mechanisms based on NLS can essentially increase the cost and expense required for the attack and reduce the cost and expense required for the defense. The security attack and defense mechanisms based on NLS are of important practical value and significance in the field of security.

5 Identity Authentication System and Method Based on Negative Logic System

Based on the proposed negative logic system, we propose NLS-based identity authentication. The NLS-based identity authentication system and method can be applied not only in the cloud environment but also in the Internet of Things environment, which is of great significance to secure accessing. Here we take cloud environment as a specific application scene. And we will give out the identity authentication system and method based on NLS in the cloud environment as well as the method of converters and distributed storage based on NLS, and the method of distributed detectors and authentication based on NLS.

Firstly, we compare our NLS-based identity authentication system and method with the existing identity authentication system and method.

The existing identity authentication system and method are all based on positive logic system. It means that the user account authentication and other information are all stored in the identity authentication system based on positive logic system. Once the user's account is leaked or stolen, the attacker can make use of the acquired user information to access to the system and resources. Even worse, the attacker uses it as a springboard for taking deep cyber attack and penetration, which is a great security risk for the whole system. In addition, the security bottleneck of identity authentication lies in the selection of the authentication algorithm, which is the attacker's focused attack goal. If the authentication algorithm is attacked, the security of the entire cloud environment is hard to guarantee. Furthermore, the existing identity authentication method and system does not involve the elements of a distributed cluster in the cloud environment, which has certain limitations in adaptability and scalability.

The identity authentication system and method based on negative logic system can break the situation of information equivalence between offensive and defensive sides from the essence. The information for both offensive and defensive sides of identity authentication system is not equal. It can increase the cost and expense of cyber attacks of the system, and meanwhile reduce the cost and expense of cyber defense of the system. Besides, this NLS-based identity authentication method can be applied not only in the cloud environment but also in the Internet of Things (IoT) environment, etc., which is of great significance to secure accessing. And according to the theoretical performance analysis in Sect. 4, it proves that it is feasible and effective.

5.1 Identity Authentication System Based on NLS in the Cloud Environment

The system structure of identity authentication system based on NLS in cloud environment is shown as follows, in Fig. 3.

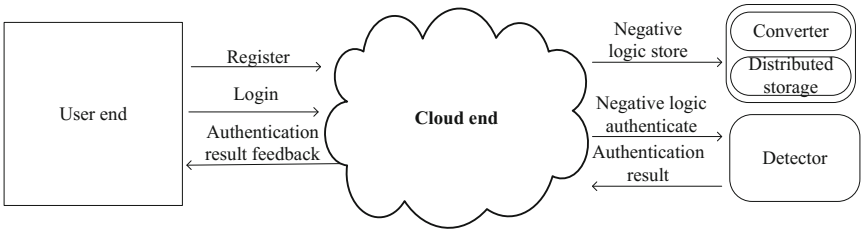

Fig. 3. System structure of identity authentication system based on NLS in the cloud environment

As is illustrated in Fig. 3, the system structure is comprised of user end, cloud end, converter, distributed storage and detector. The procedure of the system mainly contains two periods, one of which is the period of user registering, the other of which is the period of login authenticating.

(1) **User Registering Period**

In user registering period, at first, the user end is used to send register information to the cloud end.

The cloud end receives the register information from the user end and obtains the set of user identity information based on the negative logic system through the negative logic converter, and then distributes the negative logic-based identity information set by the distributed storage.

The converter is used to receive the information from cloud end and transform the information to the negative logic presentation and then obtain the set of NLS-based identity information.

The distributed storage is used for receiving identity information from the converter and distributing them to storage.

(2) **Login Authenticating Period**

In the login authenticating period, the user end is used for sending user's login information to the cloud end and receiving the authentication result from the cloud end.

The cloud end can receive the login information set sent from user end and then transport the login information set to the detector so as to take distributed detection and then get the authentication result. Besides, the cloud end receives the authentication result and then feedbacks the identity authentication result to the user end.

The detector is used to receive the login information from the cloud end and take distributed detection. The authentication result can be concluded according to the comparison of the number of matched detector with the maximum number of tolerances. After that, the authentication result is outputted to the cloud end.

5.2 Identity Authentication Method Based on NLS in the Cloud Environment

The following Fig. 4 describes the method of identity authentication based on NLS in the cloud environment.

According to the above Fig. 4, the method of identity authentication based on NLS in the cloud environment includes the following steps.

Step 1: User's registration requesting. The user end sends request to the cloud end with the user's registration information.

Step 2: User's registration information obtaining. The cloud end obtains user's registration information.

Step 3: Identity information transforming. Extract corresponding information from registration information, and transform identity information based on NLS to obtain the corresponding NLS-based identity information set. For example, there are n kinds of NLS-based identity information. Concerning with the information, only when not less than m kinds of different identity information are obtained at the same time, then the identity information of the user can be authenticated. Here, m is the maximum number of tolerances to authenticate.

Step 4: Distributed storing. Distribute the n kinds of NLS-based identity information to distributed storage.

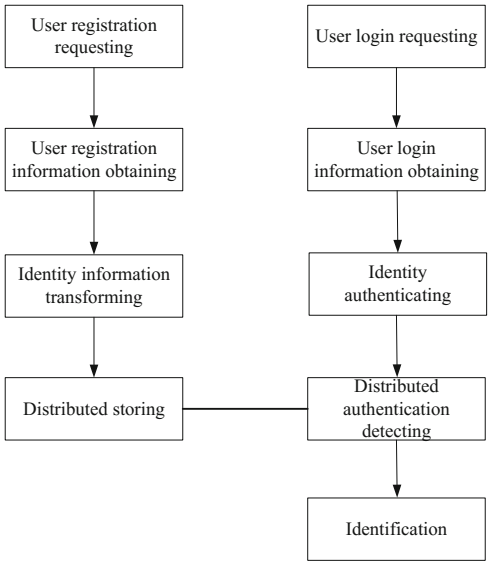

Fig. 4. Method of identity authentication based on NLS in the cloud environment

Step 5: User login requesting. The user end sends request to the cloud end with the user login information set.
Step 6: User login information obtaining. The cloud end obtains user login information set.
Step 7: Identity authenticating. The cloud end begins identity authenticating procedure.
Step 8: Distributed authentication detecting. Distributed detect the user login information set. Assuming that user login information set contains t kinds of different identity information. By detecting based on NLS, the number of matched detectors will be figured out, e.g. the number is k. Then compare k with the maximum number of tolerances m. Only when $k \geq m$, the user information can be gotten, otherwise the user information cannot be gotten.
Step 9: Identification. According to the result of Step 8, the identification is taken out.

5.3 Method of Converters and Distributed Storage Based on NLS

As in the above, we can know that, the method of converters and distributed storage is of great importance to the identity authentication based on NLS. So Fig. 5 shows the specific method of converters and distributed storage based on NLS.

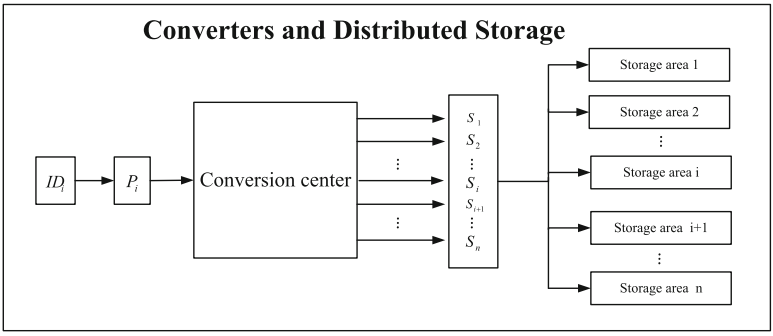

Fig. 5. Method of converters and distributed storage based on NLS

We can see from Fig. 5 that the method procedure of converters and distributed storage based on NLS includes five components. For the first thing, input the user's registration information, for example the user's registration information is written as ID_i. For the second thing, obtain the user's original identity information, which is written as P_i.

For the third thing, the conversion center, which is based on NLS, is the main function and component. Assuming that the user's registration information is ID_i and the related original real identity information is 1 kind, denoted as P_i, the corresponding non-real identity information is n kinds, written as $S_1, S_2, S_3, \ldots\ldots, S_n$. Let $T = \{P_i, S_1, S_2, S_3, \ldots\ldots, S_n\}$, then as for user's registration information ID_i, the corresponding NLS-based identity information set is $T' = T - \{P_i\}$, i.e. $T' = \{S_1, S_2, S_3, \ldots\ldots, S_n\}$. The conversion result will be outputted to the next component, receiving the identity information set T' based on NLS of ID_i, that is $\{S_1, S_2, S_3, \ldots\ldots, S_n\}$.

And for the last thing, the identity information set T' based on NLS of ID_i is distributed to different storage area, such as storage area $1, 2, \cdots,$ i, $\mathrm{i}+1, \cdots,$ n.

5.4 Method of Distributed Detectors and Authentication Based on NLS

The procedure of distributed detectors and authentication based on NLS is shown in Fig. 6. It is the distributed detecting and authenticating based on negative logic system, in which, the maximum number of tolerances is m, that is to say, the identity information of the user can be authenticated with at least m kinds of different identity information.

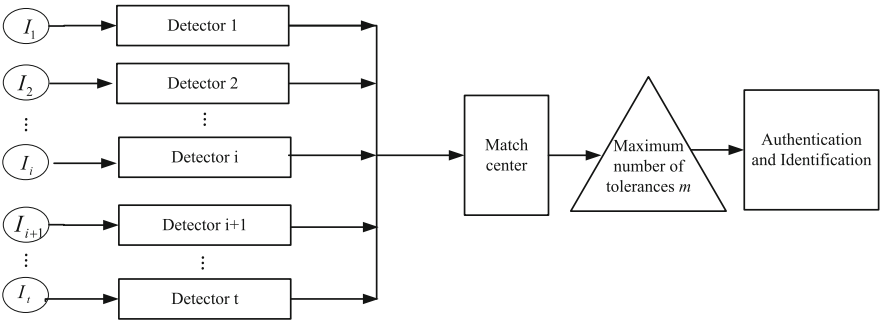

Fig. 6. Method of distributed detectors and authentication based on NLS

In Fig. 6, we get the user's login information set and extract different elements as $I_1, I_2, \cdots, I_i, I_{i+1}, \cdots, I_t$. Then we transfer them to distributed detectors.

In the detectors, let the obtained value and elements correspond to different distributed detectors, such as detector $1, 2, \cdots$, i, $\mathrm{i}+1, \cdots$, n. Meanwhile, take the detection of the t kinds of different identity information $I_1, I_2, \cdots, I_i, I_{i+1}, \cdots, I_t$ based on NLS and judge whether it belongs to the corresponding NLS-based identity information set T' of user's registration information ID_i, for which $T' = T - \{P_i\}$, and at the same time, $T' = \{S_1, S_2, S_3, \ldots\ldots, S_n\}$. Simply speaking, judge whether it belongs to the element of set T'. After that, feedback the result to the mach center. Then the match center calculates the number of matched detectors, denoted as k. And compare k with the maximum number of tolerances m. Finally, according to the result of the comparison, we take identity authentication, judging whether the user is a legal user. Only when $k \geq m$, the user's real original information can be gotten and the user begins to access to the resource in the cloud and use the resource, otherwise the user's real original information cannot be gotten, hence the user can't login and can't access to the resource in the cloud.

6 Conclusion

In this paper, identity authentication system and method based on negative logic system is proposed to solve the problem of identity authentication, NLS is introduced to improve security in the essence of attack and defense. Security mechanisms based on NLS are proved effective to increase attack cost and strengthen defense ability. So NLS-based identity authentication system and method in the cloud environment are designed. Meanwhile, the corresponding converters, distributed storage, distributed detectors and authentication are proposed. The proposed method can improve security and provide identity authentication for cloud, IoT, etc. The theoretical performance analysis proves that it is feasible and effective.

Acknowledgement. This work is supported by the National Natural Science Foundation of China (No. 61702508 and No. 61602470) and Strategic Priority Research Program of Chinese Academy of Sciences. This work is also supported by Key Laboratory of Network Assessment Technology at Chinese Academy of Sciences and Beijing Key Laboratory of Network Security and Protection Technology.

References

1. Ghosh, S., Majumder, A., Goswami, J., Kumar, A., Mohanty, S.P., Bhattacharyya, B.K.: Swing-Pay: one card meets all user payment and identity needs: a digital card module using NFC and biometric authentication for peer-to-peer payment. IEEE Consum. Electron. Mag. **6**(1), 82–93 (2017)
2. Chien, H.-Y.: Efficient authentication scheme with tag-identity protection for EPC Class 2 Generation 2 version 2 standards. IJDSN **13**(3) (2017)
3. Hu, G., Xiao, D., Xiang, T., Bai, S., Zhang, Y.: A compressive sensing based privacy preserving outsourcing of image storage and identity authentication service in cloud. Inf. Sci. **387**, 132–145 (2017)
4. Urbi, C., et al.: PUF+IBE: blending physically unclonable functions with identity based encryption for authentication and key exchange in IoTs. IACR Cryptology ePrint Archive 2017, 422 (2017)
5. Wu, L., Zhang, Y., Xie, Y., Alelaiw, A., Shen, J.: An efficient and secure identity-based authentication and key agreement protocol with user anonymity for mobile devices. Wirel. Pers. Commun. **94**(4), 3371–3387 (2017)
6. Yuan, Y., Zhao, J., Xi, W., Qian, C., Zhang, X., Wang, Z.: SALM: smartphone-based identity authentication using lip motion characteristics. In: SMARTCOMP 2017, pp. 1–8 (2017)
7. Wu, L., Zhang, Y., Choo, K.K.R., He, D.: Efficient and secure identity-based encryption scheme with equality test in cloud computing. Future Gener. Comput. Syst. **73**, 22–31 (2017)
8. Xie, Y., Wu, L., Shen, J., Alelaiwi, A.: EIAS-CP: new efficient identity-based authentication scheme with conditional privacy-preserving for VANETs. Telecommun. Syst. **65**(2), 229–240 (2017)
9. Yang, A., Tan, X., Baek, J., Wong, D.S.: A new ADS-B authentication framework based on efficient hierarchical identity-based signature with batch verification. IEEE Trans. Serv. Comput. **10**(2), 165–175 (2017)
10. Teh, T.-Y., Lee, Y.-S., Cheah, Z.-Y., Chin, J.-J.: IBI-Mobile Authentication: a prototype to facilitate access control using identity-based identification on mobile smart devices. Wirel. Pers. Commun. **94**(1), 127–144 (2017)
11. Buchman, D., Poole, D.: Negative probabilities in probabilistic logic programs. Int. J. Approx. Reason. **83**, 43–59 (2017)
12. Ori, L., João, M., Yoni, Z.: Sequent systems for negative modalities. Log. Univ. **11**(3), 345–382 (2017)
13. Thomas, S.: Decidability for some justification logics with negative introspection. J. Symb. Log. **78**(2), 388–402 (2013)
14. Norbert, G.: A sequent calculus for a negative free logic. Stud. Logica. **96**(3), 331–348 (2010)

15. Nikodem, M., Bawiec, M.A., Surmacz, T.R.: Negative difference resistance and its application to construct boolean logic circuits. In: Kwiecień, A., Gaj, P., Stera, P. (eds.) CN 2010. CCIS, vol. 79, pp. 39–48. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13861-4_4
16. Lee, D.-W., Sim, K.-B.: Negative selection algorithm for DNA sequence classification. Int. J. Fuzzy Logic Intell. Syst. **4**(2), 231–235 (2004)
17. Duccio, L., Franco, M.: An operational logic of proofs with positive and negative information. Stud. Logica. **63**(1), 7–25 (1999)