

An Authorized Identity Authentication-based Data Access Control Scheme in Cloud

Jian Shen, Dengzhi Liu, Qi Liu, Baowei Wang, Zhangjie Fu

School of Computer & Software, Nanjing University of Information Science & Technology, China

s_shenjian@126.com, liudzd@foxmail.com

Abstract—Cloud computing is a newfound service which has a rapid growth in IT industry recent years. Despite it has a huge contribution to the development of the technology and society, the cloud still exists some security deficiencies to block its development such as data leakage, illegal access and privacy risks. Hence, access control and user authentication is very important in cloud environment. Some related access control schemes has been proposed to solve the security problems in cloud, however, the high computation cost is a crucial factor in practical use. In this paper we propose a novel lightweight identity authentication-based access control scheme for cloud, due to adopt an authorized agency to assist the authentication and key distribution, this scheme is more efficient and practical than the related work.

Keywords—Cloud computing; access control; user authentication; security; authorized agency

I. INTRODUCTION

Cloud computing is originally developed from distributed computing, it can be defined as a type of parallel and distributed system which has many interconnected computers or servers [1][2]. Cloud computing is a promising technology which attracts researchers, academicians and computing industries in great extent because of its computing capability to deliver shared cloud objects dynamically. In cloud computing all the objects are stored remotely on untrusted cloud servers and accessed by users via Internet [3][4][5]. Hence, ensuring only legal users to access the data is very important in cloud security. Access control is a vital solution to deal with determining which user has what access rights towards an object. That is the aim of an access control scheme is to protect the resources against unauthorized or illegal access by the users [6].

In security community the current researches of the access control is classified into three types: Role Based Access Control (RBAC), User Based Access Control (UBAC) and Attribute Based Access Control (ABAC). However, the traditional UBAC is not suitable for the cloud environment. Because in UBAC the access control list (ACL) [7] is attached to the data, which decided who are authorized to access the data. Whereas in the cloud there would be many users and these users are dynamic, if adopts UBAC to control data access, it will result in higher computation and communication burden, and above all the access control list is difficult to manage. In RBAC the users are classified based on roles of individual users [8]. The cloud data can be accessed by the users who possess the matching roles. These roles are defined

by the system. This data access control scheme is often used in an organization such as enterprise, company or hospital. In ABAC the users are given the attributes and the data has some access policies, which are decided by the data owners [9]. Only users with a valid set of the attributes to satisfy the access policy can access the data. The attribute based encryption used in the cloud data access control often classified into two types, which are KP-ABE [10][11] and CP-ABE [12][13]. In KP-ABE data access control scheme each user's key is associated with an access policy and each ciphertext is related to attributes, on the contrary to the KP-ABE, in CP-ABE data access control scheme, each user's key is associated with attributes and each ciphertext is related to an access policy.

In this paper we propose a novel lightweight authentication-based access control scheme, which is designed by exclusive-or operations, string concatenation and hash functions. Therefore, this scheme has lower computation cost. Moreover, the main computing work is transferred to the authorized agency, hence, the computation of the user side and the server side is lower than the related authentication scheme for cloud.

This paper is organized as follows: In Section 2, the related work of a traditional user authentication scheme and a related cloud user authentication scheme are presented in detailed. The proposed authentication-based access control scheme is shown in Section 3. In Section 4 the security analysis of the proposed scheme is shown in detailed. Then we conclude this paper in Section 5.

II. RELATED WORK

This section gives a detailed introduction of the related traditional user authentication scheme and the cloud user authentication scheme.

A. User Authentication

In [14] Wang et al. proposed an identity-based authentication scheme. This scheme is based on hash and exclusive or operations, thus, it has less computation costs. The notations uses in their scheme are shown in TABLE 1, this scheme is divided into the registration phase and the mutual authentication phase.

1) The Registration Phase

Step 1. The user sends ID_i and PW_i to the server for the registration.

Step 2. The server will compute $N = h(PW_i) \oplus h(X) \oplus ID_i$ and

TABLE 1. THE NOTATIONS

U_i	The user i
ID	The identity of the user
S	The remote server
PW_i	The password of user i
$h(\bullet)$	A secure one-way hash function
$\oplus$	XOR operation
γ	The secret value in user's smart card
X	The secret value kept by the server
TS	The timestamp

store $\{h(\bullet), N_i, \gamma\}$ in a smart card. Then, the server sends the smart card to the user in a secure channel.

2) The Mutual Authentication Phase

Step 1. To log in the server, the user computes $CID_i = h(PW_i) \oplus h(N_i \oplus \gamma \oplus TS) \oplus ID_i$ using the smart card. Then, the user sends $\{ID_i, CID_i, N_i, TS\}$ to the server.

Step 2. The server checks the timestamp TS . If TS is not valid, then the server denies the user.

Step 3. If the TS is valid, then the server will compute $h'(PW_i) = CID_i \oplus h(N_i \oplus \gamma \oplus TS) \oplus ID_i$ and $ID'_i = N_i \oplus h(X) \oplus h'(PW_i)$. If $ID_i = ID'_i$, then the server allows the user's login.

Step 4. The server will compute $a' = h(h(PW_i) \oplus \gamma \oplus TS)$ and send $\{a', TS'\}$ to the user.

Step 5. The user checks the timestamp TS . If TS is valid, then the user computes $a = h(h(PW_i) \oplus \gamma \oplus TS)$ and checks if $a = a'$. If they are equal, then the user ensures that the server is legal.

B. User Authentication for Cloud

In [15] Yang et al. proposed a new user authentication scheme on multi-server environments for cloud computing. This scheme has less computation costs and it can be applied to multi-server environments. The notations uses in their scheme are shown in TABLE 2, this scheme is divided into the registration phase and the mutual authentication phase.

1) The Registration Phase

Step 1. The mobile user sends ID_u and PW_u to the ID provider. Then, the ID provider computes $A = h(ID_u || x) \oplus PW_u$ and sends it to the mobile user in a secure channel.

Step 2. The user sends IDS_i to the ID provider. Then, the ID provider computes $B = h(h(ID_u || x) || IDS_i)$ and sends it to the server in a secure channel.

2) The Mutual Authentication Phase

Step 1. The user generates N to computes $D = h(B || TS) \oplus N$ and $C = h(N \oplus TS)$. Then, the user sends (D, C, TS) to the server.

Step 2. The server checks if ΔTS is valid or not. If ΔTS is valid, then the server will compute $N' = h(B || TS) \oplus D$ and $C' = h(N' \oplus TS)$.

Step 3. If $C' = C$, then the server ensures that the mobile user is valid. Then, the server computes $SK = h(N' || TS || C' || TS')$ and $KC = h(C' || SK || TS')$, then it will send (KC, TS') to the user.

TABLE 2. THE NOTATIONS

ID_u	User's identity
PW_u	User's password
IDS_i	Server's identity
$ $	String concatenation operation
$h(\bullet)$	One-way hash function
$\oplus$	Exclusive-or operation
N	random number
x	Secret key of the ID provider
TS	Timestamp generated by the mobile user
TS'	Timestamp generated by the server
ΔTS	Time difference of the timestamp

Step 4. The user checks if ΔTS is valid or not. If it is valid, then the user computes $SK' = h(N || TS || C || TS')$ and $KC' = h(C || SK' || TS')$. If $KC = KC'$, then the user ensures that server is valid.

III. PROPOSED SCHEME

We assume that there are four roles in this proposed scheme, which are the cloud server, the use, the data owner and the authorized agency. The cloud server is responsible for providing services for users and storing the data of the data owner, the authorized agency is a trust third party whose duty is to generate the public and secret key, security parameters and distribute an identity ID to the authorized users and cloud servers. The proposed scheme is divided into six phases, including the request phase, the confirmation phase, the authorization and outsourcing phase, the agency response phase, the authentication phase and the data retrieval phase. The notations used in this scheme are listed in detailed in the TABLE 3.

A. The Request Phase

Step 1. The user and cloud server generates a random number N_c and N_u firstly.

Step 2. The user and the cloud server generates ID request $ID_{r,c}$ and $ID_{r,u}$.

Step 3. The user and cloud server sends $\{ID_{r,c}, N_c\}$ and $\{ID_{r,u}, N_u\}$ to the authorized agency respectively.

B. The Confirmation Phase

Step 1. After received the ID requests of the user and the cloud server, the authorized agency will check its legitimacy and then generates an ID or not.

Step 2. The authorized agency generates public key PK , which will be used to encrypt the data.

Step 3. The authorized agency will send $\{ID_u, ID_c, PK\}$ to the data owner.

TABLE 3. THE NOTATIONS OF THE PROPOSED SCHEME

ID_c, ID_u	The identity of the cloud server and the user
$ID_{r,c}, ID_{r,u}$	The identity request of the cloud server and the user
$ID_{a,c}, ID_{a,u}$	The authorized cloud server and the authorized user
N_c, N_u	The random number chosen by the cloud and the user
k	A security parameter chosen by the authority
$\oplus$	XOR operation
$h(\bullet)$	A secure one-way hash function
$\parallel$	String concatenation operation
TS_c, TS_u	Timestamp of the cloud and the user
PK, SK	Public and secret key
R_u	The user's data retrieval request
ACK	The acknowledgement of the data is successfully stored in the cloud

C. The Authorization and Outsourcing Phase

Step 1. The data owner will utilize the PK to encrypt the data and then outsource the encrypted data to the cloud server.

Step 2. If the cloud successfully receives the encrypted data, it will send an acknowledgement ACK to the data owner.

Step 3. According to the ID received from the agency, the data owner will judge it can access the data or not. If the user and the server pass the verification, the data owner will send an authorized confirmation of the user and the server $\{ID_{a,u}, ID_{a,c}\}$ to the authorized agency.

D. The Agency Response Phase

Step 1. The authorized agency generates a security parameter k and timestamp TS for user and server.

Step 2. The authorized agency computes $A=h(ID_u \parallel k) \oplus N_u$ and $B=h(ID_c \parallel k) \oplus N_c$.

Step 3. The authorized agency then sends $\{B, k, TS_u, SK\}$ and $\{A, k, TS_c\}$ to the user and server respectively.

E. The Authentication Phase

1) User Authentication Phase

Step 1. The user sends $\{ID_u, TS_u, N_u\}$ to the cloud server.

Step 2. After received the parameter combination, the server will check the TS_u is valid or not. If TS_u is valid then the server will compute $P_u=A \oplus N_u$ and $P_u'=h(ID_u \parallel k)$.

Step 3. If $P_u=P_u'$, the user is confirmed to pass the authentication, otherwise, the server ensures this user is illegal and reject it login.

2) Server Authentication Phase

Step 1. The cloud server sends $\{ID_c, TS_c, N_c\}$ to the user.

Step 2. After received the parameter combination, the user will check the TS_c is valid or not. If TS_c is valid then the user will compute $P_c=A \oplus N_u$ and $P_c'=h(ID_c \parallel k)$.

Step 3. If $P_c=P_c'$, the cloud server is confirmed to pass the authentication, otherwise, the user ensures this server is illegal and will not access this server.

F. The Data Retrieval Phase

Step 1. The user sends identity and data retrieval request $\{ID_u, R_u\}$ to the cloud server.

Step 2. According to the received $\{ID_u, R_u\}$, the server will confirm it is the legal user or not.

Step 3. If it is the legal user, the cloud server will response the data retrieval request to send the corresponding encrypted data to the user.

Step 4. The user will utilize the SK to decrypt the data.

Fig. 1 shows the architecture and the main process of the proposed scheme. Due to this scheme is constructed by the one-way hash functions, string concatenation operations and XOR operations so it will bring lower computation cost. In addition, the main authentication computations are transferred to the authorized agency, hence, the user side and server side will save much computation resource and the verification time will be shortened, which will bring much actual use value. Therefore, the proposed scheme is more efficient in practical data access control for cloud computing.

IV. SECURITY AND PERFORMANCE ANALYSIS

In this section, we analyze the security of the proposed scheme from some possible attacks. Moreover, in order to show this scheme's lower computation of the user side and the server side, we also give a comparison of the proposed scheme and the related schemes in the performance analysis.

A. Security Analysis

1) Replay Attack

Assume that an attacker intercepts the communications between the cloud server and the user in the authentication phase, and this attacker can obtain $\{ID_u, TS_u, N_u\}$. In order to login the server, this attacker will re-send $\{ID_u, TS_u, N_u\}$ to the server, however, the attacker will not be authenticated, which is because in the authentication information the timestamp TS_u and the random N_u is not a constant, in every authentication phase this two parameters are different. It is the same situation when the attacker can obtain $\{ID_c, TS_c, N_c\}$. Therefore, the replay attack is infeasible in this proposed scheme.

2) Eavesdropping

During the communication process an adversary may try to obtain the secret information through eavesdropping, this is a common security problem to threat a system. In the proposed system, although an attacker can get the secret key of a decrypted data, he/she cannot get the encrypted data, because the user must pass the authentication phase and he/she can obtain the encrypted data. Therefore, the proposed scheme is resistant to eavesdropping.

3) Impersonating Attack

Assume that an attacker wants to impersonate a legal user to log in the server, and he/she generate a correct timestamp to send to the server. However, this illegal user cannot pass the authentication phase, because he/she is not possessing a correct random number N_u to ensure $P_u=P_u'$. The illegal server

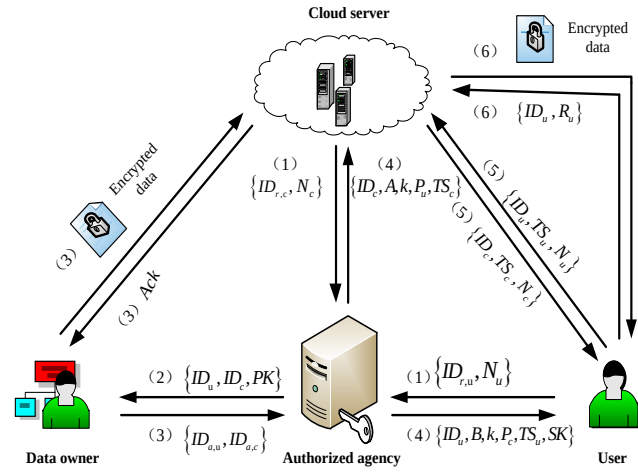


Figure 1. The architecture and the process of the proposed scheme

to impersonate a legal server is not successful to pass the authentication, the reason is the same in the illegal user authentication process.

4) Man-In-The-Middle Attack

Our scheme is resistant to man-in-the-middle attack. We assume an attacker wants to modify the P_u or P_c to meet their own fake or overdue parameter. In the proposed scheme, the $P_u = A \oplus N_u$ and $P_c = A \oplus N_u$. If wants to modify the P_u or P_c , the adversary must possess the random parameter and the security parameter k , however, it is impractical because these two parameters are not the same in every authentication round, they are randomly generated by the agency. That is, the adversary cannot modify the true P_u or P_c . Therefore, the man-in-the-middle attack is infeasible for the proposed scheme.

5) Forward Security

In this scheme, the different user's identity is different, the ID_u is generated by the agency. In the user authentication phase, we assume an adversary obtains the TS_u and random number N_u , he/she wants to use these two parameters to make an illegal user authenticated by the server, however, the $ID_u || k$ is protected by the one-way hash function $h(\bullet)$, the illegal user will not pass the authentication because the $P_u \neq P_u'$. Similarly, in the server authentication phase, it is the same situation. Therefore, this scheme is resistant to forward security.

B. Performance Analysis

TABLE 4 shows the computation comparison of the proposed scheme and the Yang et al.'s scheme in the user side and server side respectively. According to TABLE 4, the computation cost of the proposed scheme is lower than Yang et al.'s scheme in the user side and server side.

V. CONCLUSION

In this paper we propose an identity authentication-based data access control scheme for cloud computing. Due to this scheme uses XOR and hash function to conceal the parameter and authenticate the identity, hence, the proposed scheme has low computation cost. Moreover, this scheme transfers the

TABLE 4. COMPUTATION COMPARISON

scheme	Yang et al.'s scheme[15]		Proposed scheme	
	User	Server	User	Server
XOR (X)	2	2	1	1
Hash Function (H)	4	4	1	1
Concatenation Operation (C)	6	6	1	1
Computation cost	$2X+4H+6C$	$2X+4H+6C$	$1X+1H+1C$	$1X+1H+1C$
Total Costs	$4X+8H+12C$		$2X+2H+2C$	

main computation to the authorized agency, therefore, this scheme is more efficient than other access control schemes. According to the security analysis, this scheme is practical in real world application for data access control in the cloud.

ACKNOWLEDGMENT

This work is supported by the National Science Foundation of China under Grant No. 61300237, No. U1405254, No. 61232016, No.61373133 and No. 61300238, the National Basic Research Program 973 under Grant No. 2011CB311808, the Basic Research Programs (Natural Science Foundation) of Jiangsu Province (BK20131004), the Natural Science Foundation of Jiangsu province under Grant No. BK2012461, the research fund from Jiangsu Technology & Engineering Center of Meteorological Sensor Network in NUIST under Grant No. KDXG1301, the research fund from Jiangsu Engineering Center of Network Monitoring in NUIST under Grant No. KJR1302, the research fund from Nanjing University of Information Science and Technology under Grant No. S8113003001, the 2013 Nanjing Project of Science and Technology Activities for Returning from Overseas, the Prospective Research Project on Future Networks under Grant No. BY2013095-4-04, the CICAET fund, Scientific Support Program of Jiangsu Province (BE2012473) and the PAPD fund.

REFERENCES

- [1] W. Liu, "Research on Cloud Computing Security Problem and Strategy", *International Conference on Consumer Electronics, Communications and Networks (CECNet)*, 2012, pp.1216 – 1219.
- [2] F. Sabahi, "Cloud Computing Security Threats and Responses", *International Conference on Communication Software and Network (ICCSN)*, 2011, pp. 245-249.
- [3] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data", *IEEE Transactions on Parallel and Distributed Systems*, (DOI: 10.1109/TPDS.2015.2401003), 2015.
- [4] Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, "Mutual Verifiable Provable Data Auditing in Public Cloud Storage", *Journal of Internet Technology*, vol. 16, no. 2, 2015, pp. 317-323.
- [5] Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving Efficient Cloud Search Services: Multi-keyword Ranked Search over Encrypted Cloud Data Supporting Parallel Computing", *IEICE Transactions on Communications*, vol. E98-B, no. 1, 2015, pp.190-200.

- [6] M. V. Thomas and K. C. Sekaran, "An Access Control Model for Cloud Computing Environments", *International Conference on Advanced Computing, Networking and Security (ADCONS)*, 2013, pp. 226-231.
- [7] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage", *Proceedings of NDSS*, 2003, pp. 131-145.
- [8] L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving secure role-based access control on encrypted data in cloud storage", *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, 2013, pp. 1947-1960.
- [9] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure Scalable and Fine-Grained Data Access on Cloud Computing", *Proceedings of IEEE INFOCOM*, 2010, pp.1-9.
- [10] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. De Panafieu, and C. R'afols, "Attribute-based encryption schemes with constant-size ciphertexts", *Theoretical Computer Science*, vol. 422, pp. 15-38, 2012.
- [11] J. Han, W. Susilo, Y. Mu, and J. Yan, "Privacy-preserving decentralized key-policy attribute-based encryption", *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 11, 2012, pp. 2150-2162.
- [12] C. Hong, M. Zhang, and D. G. Feng, "AB-ACCS: A Ciphertext Access Control Method for Cloud Storage", *Computer Research and Development*, 2010, pp. 259-265.
- [13] G. Z. Sun, Y. Dong, and Y. Li, "Access Control Based on CPABE for the Data Stored in the Cloud", *Journal on Communications*, 2011, pp. 146-152.
- [14] Y. Wang, J. Liu, F. Xiao, and J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme", *Computer Communications*, vol. 32, no. 4, 2009, pp. 583-585.
- [15] J. Yang, Y. Chang, and C. Huang, "A User Authentication Scheme on Multi-Server Environments for Cloud Computing", *International Conference on Information, Communications and Signal Processing (ICICS)*, 2013, pp. 1-4.



Jian Shen received the M.E. and Ph.D. degrees in Computer Science from Chosun University, Korea, in 2009 and 2012, respectively. Since late 2012, he has been a professor at Nanjing University of Information Science and Technology, Nanjing, China. His research interests include computer networking, and information security systems.



Dengzhi Liu received the B.S. degree in 2014 and is currently working toward the M.E. degree at Nanjing University of Information Science and Technology, Nanjing, China. He focuses on the security and privacy issues in cloud environment. His current research interests are fine-grained cloud data access control, privacy preserving search schemes in cloud and auditing protocols for cloud storage.



Qi Liu (M'11) received his BSc degree in Computer Science and Technology from Zhuzhou Institute of Technology, China in 2003, and his MSc and PhD in Data Telecommunications and Networks from the University of Salford, UK in 2006 and 2010. His research interests include context awareness, data communication in MANET and WSN, and smart grid. His recent research work focuses on intelligent agriculture and meteorological observation systems based on WSN.



Baowei Wang received his B.S. and Ph.D. degrees in Computer Science from Hunan University in 2005 and 2011, respectively. He is currently working as a lecturer in School of Computer and Software, Nanjing University of Information Science and Technology. His research interests include steganography, wireless networks and securing ad hoc network



Zhangjie Fu is a visiting scholar of Computer Science and Engineering at State University of New York at Buffalo. He received his PhD in computer science from the College of Computer, Hunan University, China, in 2012. He is currently an associate professor at Department of Computer and Software, Nanjing University of Information Science and Technology, China. His research interests include Cloud and Outsourcing Security, Digital Forensics, Network and Information Security. His research has been supported by NSFC, PAPD, and GYHY. Zhangjie is a member of IEEE, and a member of ACM.