This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMM.2018.2882744, IEEE Transactions on Multimedia

Emotion-aware Multimedia Systems Security

Yin Zhang, Yongfeng Qian, Di Wu, M. Shamim Hossain, Ahmed Ghoneim, Min Chen

***Abstract*—The interactive robot is expected to support emotion analysis, and utilize the deep learning and machine learning to provide users with continuous emotional care. However, it brings a great challenge to securely acquire sufficient data for emotion analysis that the privacy of emotional data should be adequately protected. To address the security issue, this paper proposes a security policy based on identity authentication and access control, to ensure the security certificate through the interactive robot or edge devices while the access control of private data stored in the edge cloud is adequately protected. Specifically, this paper adopts a polynomial-based access control policy and designs a secure and effective access control scheme. At the same time, this paper puts forward the identity authentication mechanism in view of edge cloud systems, which can reduce the computation overhead and authentication delay in a collaborative authentication of multiple edge clouds. The effectiveness of the proposed access control policy and identity authentication mechanism is verified by a actual testbed platform.**

***Index Terms*—Security analysis, Access control, emotion interaction, identity authentication, social robot**

I. Introduction

With the continued growth in demand of personalized services, the emotional care robot (also known as a social robot) is developed to provide emotional applications and services. In practical situation, a social robot collects the user's emotion data, social data and other data through various sensors. Furthermore, the multidimensional data analysis is supported by machine learning or deep learning, and the personalized emotional care is provided to the user.

However, the emotion robot, edge cloud and remote cloud stores a lot personal data generated through the interaction with the user. Thus, the data access control permission is critical for the user privacy protection. There are many researches on the access control and identity authentication of new-type network architecture, such as software-defined networks or cyber-physical systems (CPS). For instance, in [1], Klaedtke, *et al.* researched the access control policy of a software-defined network controller and designed a novel access control mechanism for different network resources and multiple safety demands. However, the existing approaches rarely consider the particularity of the social robot that it often collects various user's private information, so the implementation of the access control policy should be more important.

Furthermore, due to the fact the emotional robot often needs to interact with different edge computing nodes to obtain the computation or storage resources, the user authentication and privacy protection are particularly important [2].

However, in terms of the emotion-aware system, the access control and authentication for this system face the following challenges:

- **Lack of enough secure protection**: Due to the traditional robot system or in the traditional IoT system, the protection measures taken cannot meet the user's need for security protection. Taking identity authentication as an example, the selected identity information is only the user's ID, name or voice, etc., as the source of authentication information. However, in the emotional robot system, the user's emotion needs to be collected as a data source, so the user's emotion is also a key user privacy data. If this data can be used as part of identity authentication, it will be more personalized to protect the privacy of users.
- **Delay**: In general, the computing and storage capabilities of emotional robots are limited, but when the emotional robot interacts with the user, it collects a large amount of data from the user (such as the user's emotional data mentioned above). In order to better serve users, emotional robots will help analyze user data and provide good services in a timely manner by means of computing and storage resources in the nearby edge cloud. That is to say, when the emotional robot is working, or providing services to the user, or interacting with the user, the time delay required is as small as possible. Therefore, if you deploy these security measures, especially in the deployment of access control policies, you need to interact with the edge cloud. If you bring higher latency, the user experience will be reduced. For this reason, when considering the security issue of the emotion-aware multimedia system, pay special attention to the problem of time delay.

To address these challenges, we consider the unique features of edge cloud systems to further improve the polynomial-based access control policy, enable a full adaptation to the access control of *the emotional robot*, and accordingly enhance its security and performance. Meanwhile, a collaborative authentication is implemented to further reduce the required computation overhead of authentication in the edge cloud systems. Specifically, the main contributions of this paper are

Y. Zhang is with School of Information and Safety Engineering, Zhongnan University of Economics and Law, Wuhan 430073, China.

Y. Qian is with School of Computer Science, China University of Geosciences, Wuhan 430074, China.

D. Wu is with the School of Data and Computer Science, Sun Yat-Sen University, Guangzhou 510006 China, and also with the Guangdong Province Key Laboratory of Big Data Analysis and Processing, Guangzhou, 510006, China (e-mail: wudi27@mail.sysu.edu.cn)

M. S. Hossain is with the Department of Software Engineering, College of Computer and Information Sciences (CCIS), King Saud University, Riyadh 11543, Saudi Arabia. E-mail: mshossain@ksu.edu.sa

A. Ghoneim is with the Department of Software Engineering (SWE), College of Computer and Information Sciences (CCIS), King Saud University, Riyadh 11543, Saudi Arabia and with the Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shebin El-Koom 32511, Egypt. E-mail: ghoneim@ksu.edu.sa.

M. Chen is with School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMM.2018.2882744, IEEE Transactions on Multimedia

as follows.

- The security issues of a social robot are analyzed from two perspectives, i.e., 1) the identity authentication and access control; 2) the access control management and identity authentication management.
- An effective access control scheme for the emotion-aware robot is proposed to support the access control policy between the emotion-aware robot and the user or edge cloud node. The access control management involving the access permission update and upgrade is realized on the premise of untrusted edge cloud node, which is based on a polynomial-based access control policy.
- An identity authentication mechanism for the emotion-aware robot is proposed. This mechanism can provide a collaborative authentication scheme among the user, edge cloud, and emotion-aware robot, while the computation overhead of authentication is further reduced. This scheme solves the problem of the low efficiency caused by repeated authentication in the edge cloud system, further enhances the ability to resist to the attack based on identity information recovery, and reduces the probability of leakage of a user's sensitive data during the identity authentication process.

The remainder of this article is organized as follows. Section II introduces the related work focusing on the identity authentication and access control. Section III describes the architecture of a social robot and summarizes its security problems. Section IV introduces the proposed access control policy. Section V presents the identity authentication mechanism for the emotion-aware robot. Section VI introduces the experimental results. Finally, Section VII concludes this paper.

II. Related work

A. Access Control

With the continuous development of the Internet of Things, medical and health monitoring can be applied. In fact, the medical health monitoring system is similar to the emotion-aware multimedia system. Due to the frequent occurrence of a user's life-critical emergency in medical care, the access control that can be taken needs to fully consider these emergencies, so that the medical health monitoring system can respond in a timely manner. For example, in In [3], an adaptive access control strategy is proposed for the healthcare system, the authors. This scheme has designed two access control strategies for general and special situations. However, in this scenario, additional third parties are required to participate in the emergency, which makes it difficult to apply to the emotional robot interaction system. Because in this system, only emotional robots and users often happen, it is difficult for additional third parties to participate.

In the process of providing services to users in the emotion-aware multimedia system, cloud servers are often required to provide computing and storage resources to achieve a better service experience. For example, in [4], in term of multi-authority cloud, the author proposes an effective access control strategy and proves that the strategy is safe. In [5], the author proposes a strategy called "AnonyControl", which not only protects the privacy of user data, but also ensures that the user's identity information is protected. In [6], considering the web-based cloud service, a fine-grained access control strategy is proposed. At the same time, the cloud server can also control the access user. However, these strategies are not fully considered. In the emotion-aware multimedia system, the cloud service resources that need to be used frequently are the resources of the edge cloud. Because the edge cloud computing and storage resources are not as full as traditional cloud servers, there may be inefficiencies in implementing these access control policies.

In fact, there are many effective access control policies for cloud servers at this stage [7]. For example, an effective access revocation scheme is proposed in [7]. Experiments show that this scheme can effectively reduce computational and storage overhead. For the emotion-aware multimedia system, if you can design an access control strategy that saves cloud computing resources, it will greatly reduce the delay and give users a better experience. However, this method obviously

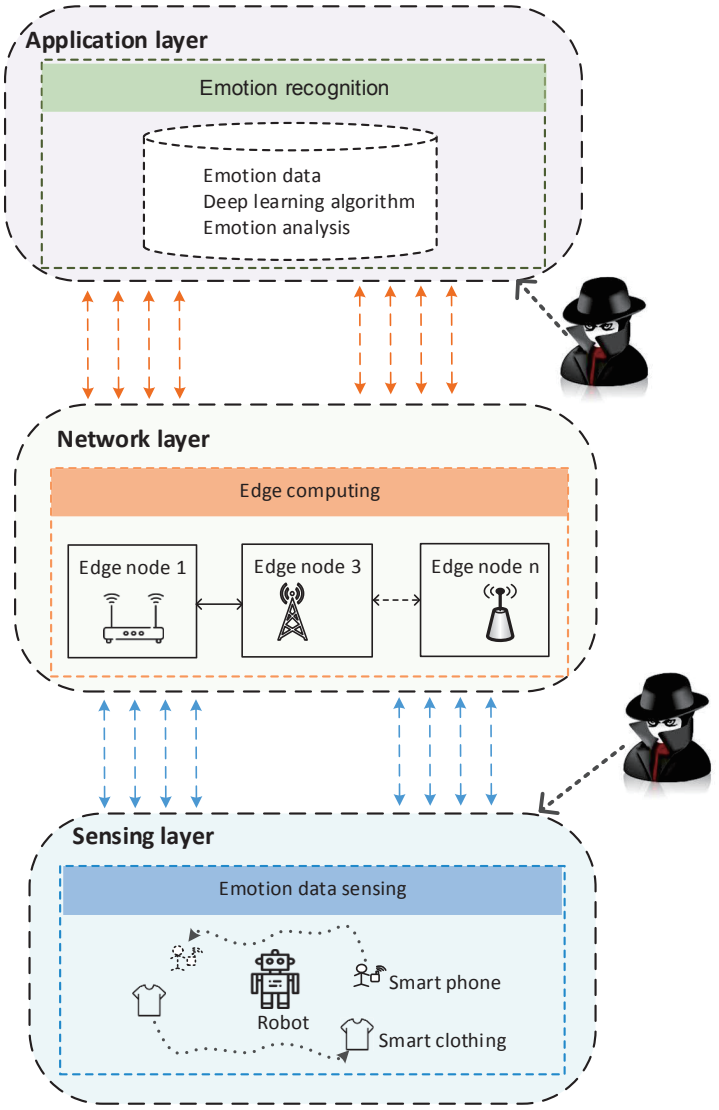

Fig. 1. Architecture of the emotion-aware multimedia system.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMM.2018.2882744, IEEE Transactions on Multimedia

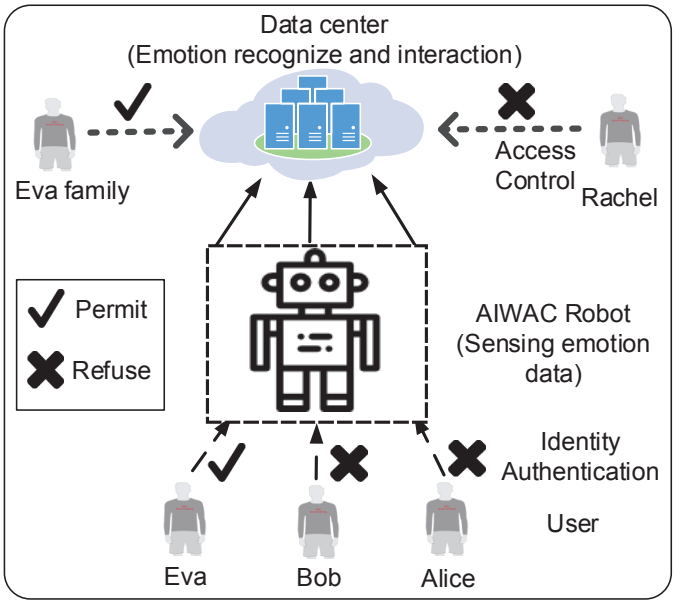

Fig. 2. Access control and authentication architecture of the emotion-aware multimedia system.

requires a trusted third party to participate in the operation and jointly implement the entire access control strategy.

B. Identity authentication

In the aspect of emotion-aware multimedia system, in this process, the identity of the user needs to be authenticated, so as to ensure the reasonable demand of legitimate users, the research shows the comprehensive investigation of the authentication protocol in the Internet of Things. In fact, there is now a lot of work on identity authentication [8], [9]. In cite he2015analysis. For example, in the field of helathcare, [9] uses modern cryptography theory to analyze that there is no suitable RFID authentication method at this stage to meet security needs. To this end, it is an urgent problem to be solved by using cryptography theory to design a better identity authentication mechanism. Especially for emotion-aware robots, it collects more data from users, which makes the interaction with the edge cloud more busy, and the more services are requested, and it is necessary to design a reasonable identity authentication mechanism. For the distributed mobile health cloud computing system, in [10], the authors introduce a cooperative authentication scheme that meets three different security and privacy protection requirements.

In addition to the authentication scheme in the traditional RFID-based IoT system, the authors proposed a new voice recognition mechanism in [11]. The system proposed in this article is called VoiceGesture and can accurately determine whether the sound is playback. However, applying this identity authentication mechanism to the emotion-aware multimedia system will bring greater challenges to the computing and storage capabilities of the edge cloud. This is because in the solution proposed by [11], the edge node needs to extract and store the voice information of the user who has authenticated the emotion-aware robot, which will occupy the storage resources with large edge cloud. Because the edge cloud itself has limited computing and storage resources, and provides computing services for the emotion-aware robot, this identity authentication scheme is difficult to apply to the emotion-aware multimedia system proposed in this paper. So in [12], the authors revisited the access control and authentication mechanisms for home IoT and found that the access control policies that users expect are different for different IoT capabilities. Therefore, when designing a practical IoT system, the designed access control and identity authentication also need to meet the diverse needs of users, especially in the emotion-aware multimedia system.

III. Secure issues in emotion-aware robot

A. Emotion-aware robot architecture

In Fig. 1, it shows the main components of the emotion-aware robot, which mainly includes three layers, i.e., sensing layer, network layer, and application layer.

- **Sensing Layer**: can continuously acquire user data, including physiological data and psychological data. The sensory data can used to analyze the user's emotions, and internal psychological status on a deeper level. Moreover, these data would form the multidimensional user-data information for different applications.
- **Network Layer**: mainly includes various network forward devices, such as a router, gateway, etc., which can transmit the user's data to the designated location.
- **Application Layer**: provides emotion-aware services and applications. In particular, the emotion-aware robot could provide the emotional care, health care, and various personalized applications, to upgrade the user experience. Advanced data analysis and learning techniques, such as machine learning and deep learning, are the essential to provide the cognition control system assisted by the remote cloud, to enable the emotion interactive robot to understand the user demand better and provide the corresponding service.

B. Security issues

With the development of the network technology, a series of security and privacy issues that should be addressed are presented in [13] [14]. For instance, the user identity information may be leaked, the edge cloud data could be falsified maliciously, and the access control permission of an edge cloud would be controlled [15], [16]. These issues could mainly considered from the following two aspects, i.e. the access control management and identity authentication management.

- **Access control management**. The emotion-aware robot systems often involve some complex computation tasks [17]. Due to the limited resources on the robot, these tasks should be transmitted to a nearby edge cloud that the edge cloud gains the user's sensitive information [18], [19]. In addition, the emotion-aware robot can provide a powerful emotional services because of the intelligent control system assisted by the remote cloud, which means

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMM.2018.2882744, IEEE Transactions on Multimedia

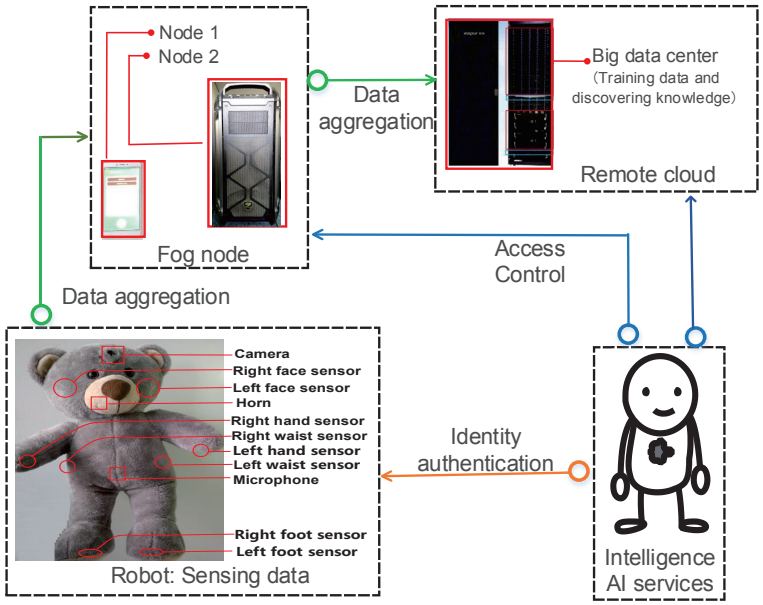

Fig. 3. Testbed illustration.

the user's data are stored on a remote cloud [20]. Thus, considering the data stored on an edge cloud or a remote cloud, it is important to develop a robust and reliable access control management [21].

- **Identity authentication management**. The emotion-aware robot must identify the user accurately that the poor identity authentication may cause failing to serve the true user better [22], [23], and even the data being collected by the malicious users [10], [24]. For instance, a malicious user may send the emergency call information after gaining the legal identity authentication. When the emotion-aware robot receives the request, it would believe it is a actual accident and send the alarm message.

IV. Access Control and Authentication for Emotion-Aware Robot

In view of above two aspects of access control and identity authentication management relevant to the emotion-aware robot, this section will introduce its security and privacy protection architecture, i.e., the access control and identity authentication.

A. Access control for emotion-aware robot

When an emotion-aware robot is applied to an edge cloud system, the resulting emotion-aware multimedia system needs to constantly interact with the edge cloud to access the data stored in the edge cloud to continuously provide emotional comfort to the user. service. However, the current edge-based access control strategies basically require trusted third parties to assist in the completion, and many research efforts assume that the edge cloud nodes are completely trusted [25], [26]. Due to the large number of edge clouds and their wide distribution, if you need additional third parties to help you complete the access control, it will bring a lot of inconvenience. In addition, since the calculation and storage resources of the edge cloud are limited and there are many interactions with the users, the acquired user information is also more, and the information relates to a lot of private information, such as name, user ID, and long-term user. Emotional and other data. If the edge cloud is maliciously attacked by an attacker, it will be easy to get this information from the user. Therefore, these all illustrate the need for a reasonable access control strategy to implement a deployment plan for an effective access control policy for the emotion-aware multimedia system.

Based on the above considerations, we utilize a polynomial access control policy in the emotion-aware robot environment, to adapt to the access control be used in the edge cloud environment . To be specific, the vector constituted by L permission is set as $V = (v_1, v_2, \cdots, v_L)$. For each user i, the following permission polynomial is built:

$$f_i(t) = \prod(t - v_i) = \sum_{i=0}^{i=L} s_i t^i \tag{1}$$

The maximum number of times of polynomial is denoted as θ_i and $\theta_i < i < L$. s_i denotes the the i-th plaintext vector. While judging whether an access permission of a user i meets the corresponding access control policy of an edge cloud node, it is only required to judge whether this access permission is the root of polynomial $f_i(t)$. This scheme can realize a safe and efficient access control policy management in the edge cloud environment and even more complex environment consisting of both edge cloud and remote cloud.

In addition, considering the situation multiple users interacting with the same emotion-aware robot, a more complex access control policy management should be implemented. The existing access control policy can only realize the access control of each device used by a single user with the nearby edge cloud, but it fails to support the access control management policy between multiple devices used by the same user

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMM.2018.2882744, IEEE Transactions on Multimedia

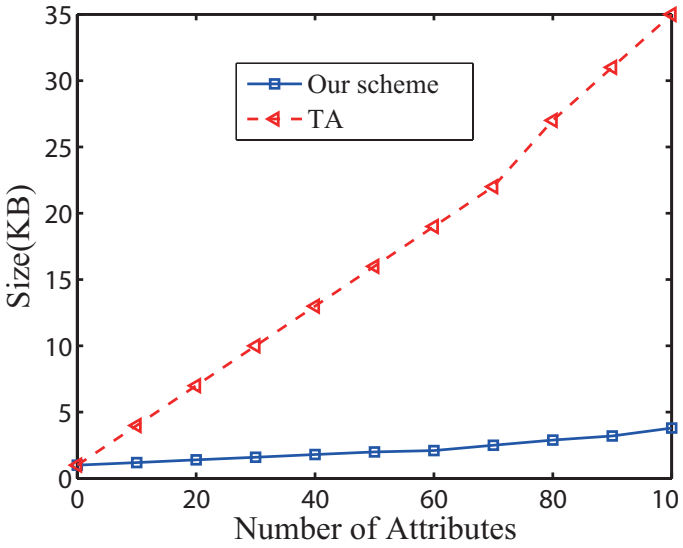

Fig. 4. The size of public key.

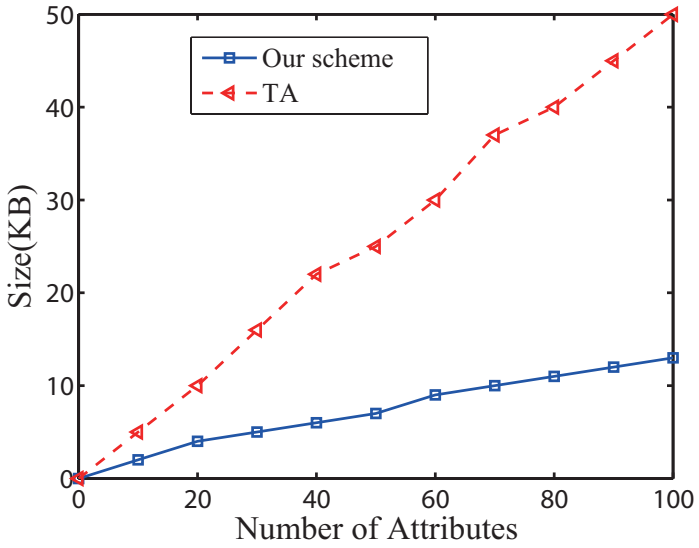

Fig. 5. The size of secret key.

or multiple devices used by many similar users and nearby edge cloud or remote cloud.

On this assumption, an edge cloud node can be enabled to save a device management sheet R. When a new device i (the device ID is ID_i) is added to the edge cloud node, then, the edge cloud node will generate the secret key $sk_i = H(ID_i)^a$, and send the public key $pk_i = H(ID_i)$ to the device i. Then, device i verifies whether it meets the following condition:

$$e(sk_i, f_p) = e(pk_i, h_p) \tag{2}$$

where $h_p = f_p^a$. While passing the validation, device i sets the password p_i of a device connected to the edge cloud, and the edge cloud ciphertext saves the device information (ID_i, sk_i, p_i). Similarly, when the other emotion interactive robot of the user is connected to the edge cloud node, data are still stored in table R using the above method, so as to realize the access control management between multiple devices of the user and the edge cloud node.

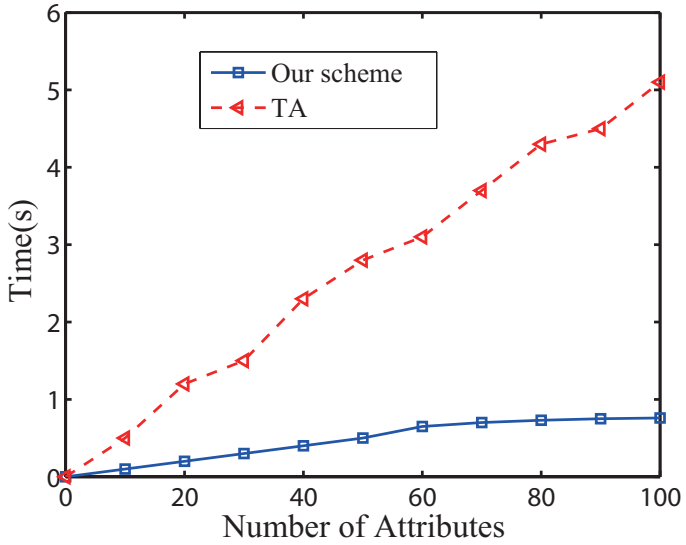

Fig. 6. Encrypt time vs number of attributes.

B. Identity authentication for emotion aware robot

Since the edge cloud can provide computing and storage services for the emotion-aware robot, it is especially important in the emotion-aware multimedia system proposed in this paper. However, for privacy protection, identity authentication is required when interacting with edge cloud nodes. At present, most of the edge cloud-based identity authentication mechanisms need to be authenticated with a single edge cloud node. However, due to the mobility of users and the distributed characteristics of edge cloud nodes, this poses challenges for users' identity authentication. Especially in terms of computing and communication, it will bring a lot of overhead, so it is also difficult to apply to the emotion-aware multimedia system.

Addressing to the issue, we combine with the collaborative authentication mechanism to realize the identity authentication of an emotion interactive robot. This method can realize the multiple edge clouds sharing the authentication results of an emotion-aware robot or a user in the edge cloud environment, and accordingly reduce the required computation overhead of authentication. To be specific, suppose there are m edge cloud nodes (i.e., $E = \{e_1, e_2, \cdots, e_m\}$) and m user signatures within a particular area, where the user signature includes the personal identity information on the user. The edge cloud node e_i randomly selects n_e user signatures for verification, $0 \leq n_e \leq n$. Suppose that the signature of n_e users is s_i, and the corresponding identity information is m_i respectively. After the edge cloud node e_i authenticates n_e user signatures, an integrated signature s_i is generated, including the verification result m_i of n_e user signatures, and (s_i, m_i) is sent to the adjacent edge cloud node. Thus, other edge cloud nodes only

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMM.2018.2882744, IEEE Transactions on Multimedia

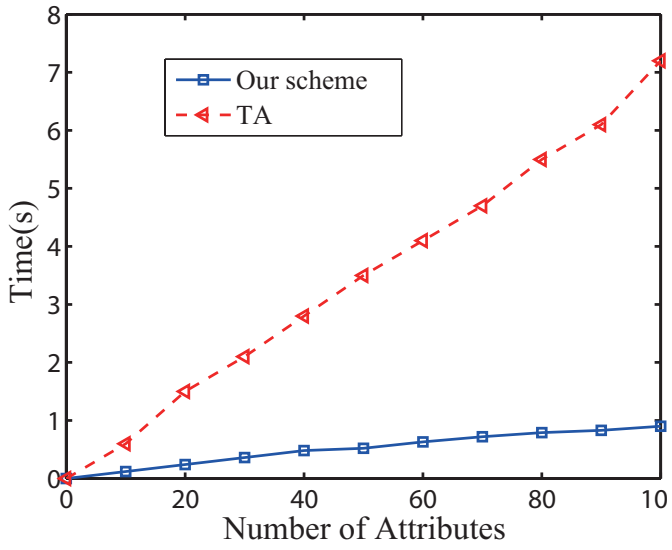

Fig. 7. Decryption time vs number of attributes.

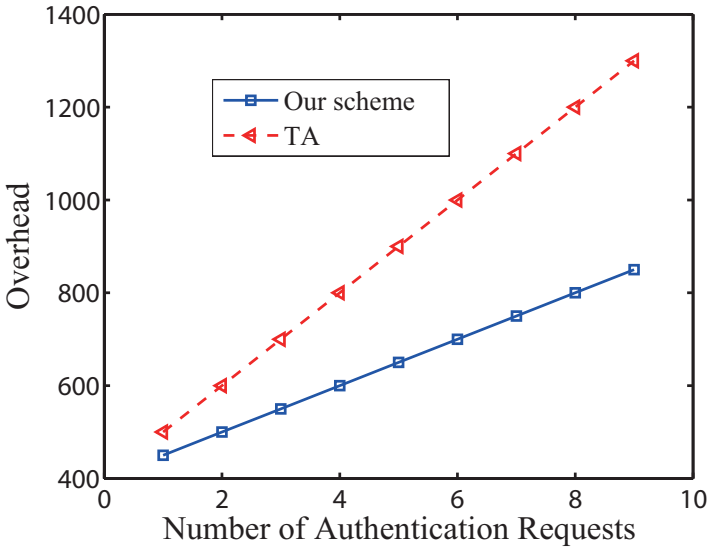

Fig. 9. Computation overhead vs number of authentication request.

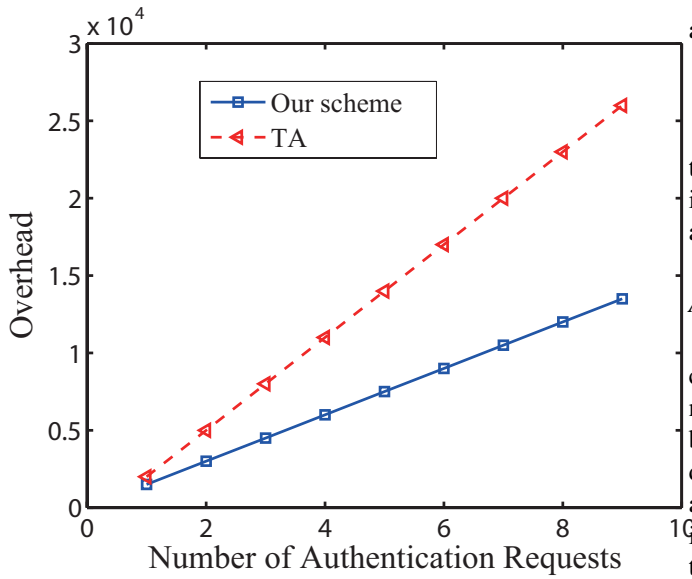

Fig. 8. Communication overhead vs number of authentication request.

need verification (s_i, m_i) and that user signature information without verification of the edge cloud e_i, rather than verifying each user signature repeatedly, so as the computation overhead of the edge cloud node is reduced greatly.

The identity privacy data in different application scenes are different in the edge cloud environment. For instance, in the emotion interaction environment, the user identity information does not consist of only the user's name and ID, but also the user's emotion, behavior, and habit. These data can indirectly gain the identity information of a user. At present, the existing identity information privacy protection scheme based on the edge can protect only the explicit information involving the user's name, family address, and ID, and rarely considers the implicit information such as emotion, behavior, and habit of a user. However, the seemingly insensitive data may be applied to the recovery attack of identity information.

V. Experiment and Evaluation

This section mainly introduces the experiment and evaluation using the the actual emotion-aware robot system, to validate the performance of the proposed identity authentication and access control.

A. Testbed platform

As shown in Fig. 3, the sensors on the robot are able to collect various data, which are fused and transmitted to the fog node and big data center through the network. Especially, the big data center is responsible for training data and knowledge discovery. The access control mainly occurred when the user accessed the fog node and remote big data center, while the identity authentication is used during the interaction between the user and emotion-aware robot.

B. Performance analysis

In the performance analysis, our proposed approach compares with the traditional approach. In the comparison of access control methods, we selected the traditional method as an access control policy that requires trusted third parties to assist and the edge cloud nodes are completely trusted. In identity authentication, the traditional method we choose is a single edge cloud authentication method. For the sake of simplicity, we simply write these traditional methods as TA. Specifically, it compares the change of public key size with the increasing number of attributes. As illustrated in Fig. 4, with the increasing of the number of attributes, the public key size of the traditional method is increased, while the public key size of our proposed approach always keeps at a lower level and the growth rate is slow.

The change of the size of the private key with the attribute base is analyzed either. As illustrated in Fig. 5, with the

increase of attribute number, the growth rate of private key size is faster in traditional method than our proposed approach, and its size keeps at a low level.

As illustrated in Fig. 4 and 5, our proposed approach can still maintain a lower size of public key and private key as the number of users increases or the number of attributes. It verifies that the approach proposed in this paper is easier to deal with a large number of users.

In Fig. 6, it shows the comparison about the change of encryption time with the increasing of the attribute number. Obviously, the proposed approach can quickly complete the encryption comparing with the traditional method, which means the method proposed in this paper can save the user's time and improve the user experience.

In Fig. 7, it shows the comparison about the change of decryption time with the increasing of the attribute number. As shown in Fig. 7, comparing with the traditional method, the method proposed in this paper can complete decryption in 1 second, when the number of attributes is range from 0 to 100. However, the delay of traditional method is a bit higher that when the number of attribution is 100, the decryption delay is about 8 second.

As shown in Fig. 8 and 9, the communication and computation overhead with increasing of authentication requests are analyzed respectively that the method proposed in this paper is much better than the traditional method.

VI. CONCLUSION

This paper presents an identity authentication and access control policy in view of the emotion-aware robot systems and summarizes the security issues by analyzing its architecture. This paper designs an identity information privacy protection with a small computation overhead that supports the collaborative authentication of an edge cloud node, while an universal access control scheme meeting the security requirement and supporting the edge cloud node and multiple devices of a single user is realized. Through the evaluation on the actual testbed, the performance of the collaborative identity authentication mechanism is better than that of the traditional approaches.

REFERENCES

[1] F. Klaedtke, G. O. Karame, R. Bifulco, and H. Cui, "Access control for sdn controllers," in *Proceedings of the third workshop on Hot topics in software defined networking*. ACM, 2014, pp. 219–220.

[2] Y. Chen, A. Machanavajjhala, M. Hay, and G. Miklau, "Pegasus: Data-adaptive differentially private stream processing," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2017, pp. 1375–1388.

[3] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving smart iot-based healthcare big data storage and self-adaptive access control system," *Information Sciences*, 2018.

[4] K. Yang and X. Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," *IEEE transactions on parallel and distributed systems*, vol. 25, no. 7, pp. 1735–1744, 2014.

[5] T. Jung, X.-Y. Li, Z. Wan, and M. Wan, "Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption," *IEEE transactions on information forensics and security*, vol. 10, no. 1, pp. 190–199, 2015.

[6] J. K. Liu, M. H. Au, X. Huang, R. Lu, and J. Li, "Fine-grained two-factor access control for web-based cloud computing services," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 3, pp. 484–497, 2016.

[7] E. Bacis, S. De Capitani di Vimercati, S. Foresti, S. Paraboschi, M. Rosa, and P. Samarati, "Mix&slice: Efficient access revocation in the cloud," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016, pp. 217–228.

[8] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication protocols for internet of things: a comprehensive survey," *Security and Communication Networks*, vol. 2017, 2017.

[9] D. He and S. Zeadally, "An analysis of rfid authentication schemes for internet of things in healthcare environment using elliptic curve cryptography," *IEEE internet of things journal*, vol. 2, no. 1, pp. 72–83, 2015.

[10] J. Zhou, X. Lin, X. Dong, and Z. Cao, "Psmpa: Patient self-controllable and multi-level privacy-preserving cooperative authentication in distributed m-healthcare cloud computing system," *IEEE Transactions on Parallel & Distributed Systems*, no. 1, pp. 1–1, 2015.

[11] L. Zhang, S. Tan, and J. Yang, "Hearing your voice is not enough: An articulatory gesture based liveness detection for voice authentication," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2017, pp. 57–71.

[12] W. He, M. Golla, R. Padhi, J. Ofek, M. Dürmuth, E. Fernandes, and B. Ur, "Rethinking access control and authentication for the home internet of things (iot)," in *27th USENIX Security Symposium (USENIX Security 18). USENIX Association, Baltimore, MD*, 2018.

[13] P. Derbez and P.-A. Fouque, "Automatic search of meet-in-the-middle and impossible differential attacks," in *Annual Cryptology Conference*. Springer, 2016, pp. 157–184.

[14] Y. Qian, Y. Jiang, J. Chen, Y. Zhang, J. Song, M. Zhou, and M. Pustišek, "Towards decentralized iot security enhancement: A blockchain approach," *Computers & Electrical Engineering*, vol. 72, pp. 266–273, 2018.

[15] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.

[16] K. S. Kim, M. Kim, D. Lee, J. H. Park, and W.-H. Kim, "Forward secure dynamic searchable symmetric encryption with efficient updates," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2017, pp. 1449–1463.

[17] Y. Qian, Y. Zhang, X. Ma, H. Yu, and L. Peng, "Ears: Emotion-aware recommender system based on hybrid information fusion," *Information Fusion*, vol. 46, pp. 141–146, 2019.

[18] X. Chen, L. Jiao, W. Li, and X. Fu, "Efficient multi-user computation offloading for mobile-edge cloud computing," *IEEE/ACM Transactions on Networking*, no. 5, pp. 2795–2808, 2016.

[19] L. Tong, Y. Li, and W. Gao, "A hierarchical edge cloud architecture for mobile computing," in *INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications, IEEE*. IEEE, 2016, pp. 1–9.

[20] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Information sciences*, vol. 305, pp. 357–383, 2015.

[21] Y. A. Younis, K. Kifayat, and M. Merabti, "An access control model for cloud computing," *Journal of Information Security and Applications*, vol. 19, no. 1, pp. 45–60, 2014.

[22] I. Butun, M. Erol-Kantarci, B. Kantarci, and H. Song, "Cloud-centric multi-level authentication as a service for secure public safety device networks," *IEEE Communications Magazine*, vol. 54, no. 4, pp. 47–53, 2016.

[23] H. Liu, H. Ning, Q. Xiong, and L. Yang, "Shared authority based privacy-preserving authentication protocol in cloud computing," *IEEE Transactions on Parallel & Distributed Systems*, no. 1, pp. 1–1, 2015.

[24] L. Cheng, D. M. Divakaran, A. W. K. Ang, W. Y. Lim, and V. L. Thing, "Fact: A framework for authentication in cloud-based ip traceback," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 604–616, 2017.

[25] J. Ni, K. Zhang, X. Lin, and X. Shen, "Securing fog computing for internet of things applications: Challenges and solutions," *IEEE Communications Surveys & Tutorials*, 2017.

[26] P. Garcia Lopez, A. Montresor, D. Epema, A. Datta, T. Higashino, A. Iamnitchi, M. Barcellos, P. Felber, and E. Riviere, "Edge-centric computing: Vision and challenges," *ACM SIGCOMM Computer Communication Review*, vol. 45, no. 5, pp. 37–42, 2015.