https://doi.org/10.2352/ISSN.2470-1173.2017.10.IMAWM-161

Multimedia Instant Messaging with Real-time Attribute-based Encryption

Xunyu Pan and Christopher Gill
Department of Computer Science and Information Technologies, Frostburg State University, Frostburg, Maryland, USA

Abstract

Today, Online Social Network (OSN) has emerged as the pervasive form of media connecting people from all over the world. Among the core functionalities associated with OSN, Instant Messaging (IM) plays a critical role in real-time communication between those virtual online communities. As the growth in IM usage continues, it has become the primary means of communication within business, education, and everyday life. Meanwhile, privacy management and data protection are issues that remain paramount to the future development of IM technology. In this work, we focus on the data protection and privacy management of group chat where multiple users simultaneously connect to a central server for real-time communications. We describe a novel multimedia IM system supporting user defined security control over real-time communication in a multiuser environment. The attribute-based encryption (ABE) is employed by the system to provide access control over transmitted user messages. Extensive experiments demonstrate that the new ABE key management mechanism provides a flexible and effective solution to data protection and privacy management for real-time online communication in multiuser environments.

Introduction

With the wide use of online social networking (OSN) applications, people around the world have become part of multiple individual online communities. Among many solutions for information exchange within these communities, Instant Messaging (IM) evolves as a very convenient and easy tool for communication between users on the Internet. Boasting a variety of features, IM has become the primary means of communication within business, education, and everyday life. Individuals can share their knowledge, opinions, and experiences with one another or even in a group meeting scenario. Due to the characteristics of high capability and extremely flexibility, IM can be implemented either as a stand-alone application or as an integrated component of OSN systems.

Recent techniques has focused on the development of security mechanisms for statically stored information on different OSNs. Meanwhile very little effort has been made to specifically address security concerns in regards to real-time IM communications. Although many third-party IM providers offer the privacy control over identification information such as name, birth date, and contact address for their users, these IM applications typically provide insufficient protection for individual users over their personal privacy such as political and religion views and sexual preference. Business and governmental employees may also have the concern regarding the exposure of business and even national security secrets when they use IM for online communication. As the consequence, the investigation of privacy management and data protection becomes the critical issues during the process of IM technology development.

Aiming to improve IM capability and flexibility, we focus on the data protection and privacy management in group chat scenarios where multiple users simultaneously connect to a central server for real-time communications. Note that the chat between two online parties is considered as a group chat between only two users. We describe in this paper a novel multimedia IM system supporting user defined security control over real-time communication in a multiuser environment. This chat program can be deployed as a communication platform in the business and government environments where the security of real-time data transmission is highly emphasized.

While most existing IM applications only prevent malicious third parties from gaining access to the communication with channel encryption, the proposed IM system provides real-time data protection and privacy management on the client side. To this end, we first introduce the attribute-based encryption (ABE) to provide flexible, user defined access control over real-time communication in various multiuser environments. In our system, the transmitted messages are encrypted with the sender's key which is specified by a set of attributes. Any user of our IM system can define such an attribute-based policy to decide who are allowed to decrypt the encrypted messages based on the identity of the receivers. In addition to the text-based messages, the proposed IM system also support secure transmission of audio, image, and other types of file format for the purpose of multimedia communications. Finally, the communication platform is implemented in the manner so that the central server does not collect sensitive messages and credentials from the individuals who are chatting using the program, adding another layer of defense to the information transmitted with our system.

We evaluate the performance of the developed multimedia IM system on secure transmission of instant messages in various multiuser environments. The message construction time at sender side and message interpretation time at receiver side are measured against user attribute with different sizes. Experimental results demonstrate that the new ABE key management mechanism helps IM users securely exchange information on many group chat occasions. The proposed IM system provides a flexible and effective solution to data protection and privacy management for real-time online communication in multiuser environments where strong information security is required.

Related Work

The rapid growth of OSN has attracted the attention of both academia and industry. OSN allows user to create profile, communicate with friends, publish and share multimedia information [1, 2, 3]. Meanwhile studies [4, 5, 6] have found that the privacy management become one of the central problems of OSN development. It was discovered [5] that many OSN providers share user data with third-parties such as advertisers and developers for the purpose of making profit.

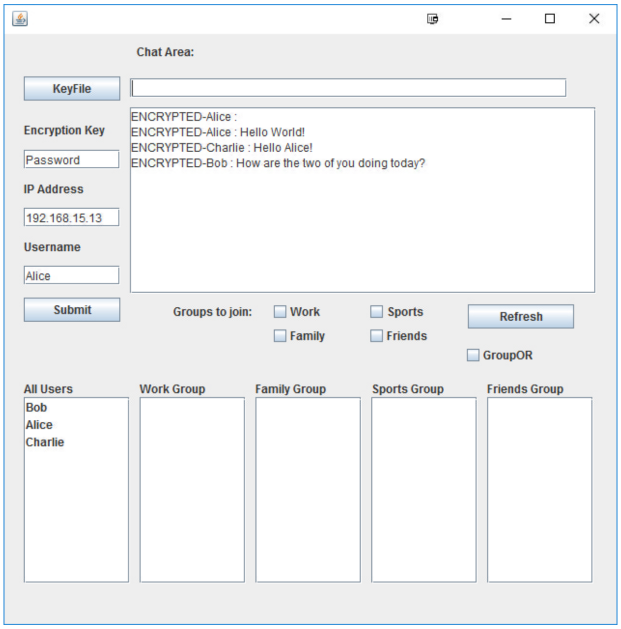
Facebook users for example usually share far more data than what they believe to have willingly shared [7]. The location data in users photographs can be leaked when they use the services of Flicker [8]. The social network between friends can also be exploited to infer the characteristics of users [9]. The authors of [10] employ a technique based on custom add-on in combination with web crawling to collect sensitive data from OSNs. Much effort has been put forth to solve these privacy management issues on OSNs. A mechanism is implemented in [11] to preserve much of the functionality of OSN by generating fake user data. The authors of [12] describe a novel technology used for verification of photos published through OSNs such as Facebook. A new architecture with client side data encryption and decryption is presented in [13] for protecting information on OSNs. An access control scheme based on social relationships is proposed in [14] to make sharing personal content easy and secure for OSNs. Moreover, the introduction of attribute-based encryption (ABE) [15, 16] further improves the security of privacy management of OSN. Similar to the attributed-based access control [17], ABE-based privacy management [18] makes sure that the access of user data is determined by the attributes assigned to users. More specifically, the ABE-based system binds encrypted data to access structures while secret keys contain attributes, which enhance the flexibility and expressive power of the system.

While the above described techniques enhance the security of static information stored in various OSNs, little effort has been made to specifically address security concerns on real-time IM communications. As an integrated part of many OSNs, IM plays an important role as a convenient tool for communication between users on Internet. Most current studies [19, 20] on IM security are focused on the channel encryption to prevent third-party from access to the multimedia messages transmitted between online users. However, very few studies have been done on the subject of IM user-end security, especially in many group chat scenarios.

Methods

We introduce in this section a novel multimedia IM system supporting user defined security control and group chat functionality. The goal of proposed IM system is to provide real-time data protection and privacy management on the client side. The system is designed to allow multiple IM users to decide whether to encrypt messages and to select the preferred user attributes. The IM system requires a central server to act as the hub for all communication between end users. Different from most existing IM systems, the central server of our IM system is *dumb* in the sense that it has no way to examine the content of any messages being sent beyond the information needed to forward these messages appropriately.

While the task for message receiving and forwarding is processed on the central server running in the background, IM users operate with Graphical User Interfaces (GUI) to send and view messages. The layout of GUI as shown in Figure 1 has input fields wherein a user can submit a user name, an IP address for connecting to central server, as well as an encryption key for secure communication. The GUI also provides users with input fields to select preferred attribute groups. The attribute group selection are operated under two different modes: (a). *AND Mode* (default mode): In this mode, only users enrolled in the exact same groups as the sending user can view the transmitted messages. (b). *OR Mode*: In this mode, users enrolled in any of the same groups but not all of the same as the sending user can view the transmitted messages.



Encryption Key: Password

IP Address: 192.168.15.13

Username: Alice

ENCRYPTED-Alice :
ENCRYPTED-Alice : Hello World!
ENCRYPTED-Charlie : Hello Alice!
ENCRYPTED-Bob : How are the two of you doing today?

All Users
Bob
Alice
Charlie

Figure 1. *The Graphical User Interface (GUI) of the proposed IM system.*

The core logic of the proposed IM system can be divided into four functional modules:

1. **Central Server**: The central server module is hosted on one computer over the Internet, and is the central node that all the IM users connect to and transmit messages to. Any message that the server receives is forwarded to all the users currently connected to the server.
2. **Message Transmission**: Messages are transmitted between IM users and the central server. The central server copies received messages and forwards them to all connected and authenticated users. This module by itself has no encryption protocols to limit whom can view messages. Hence users can send plaintext messages to all users connected to the central server.
3. **Message Encryption**: The encryption module is responsible for the attribute-based encryption implemented by the IM system to support privacy management. Messages are encrypted using a popular encryption algorithm and then transmitted to all the other users. Those users whom do not enter the correct key will not be able to, under any circumstances, view the original message. Users of this system can

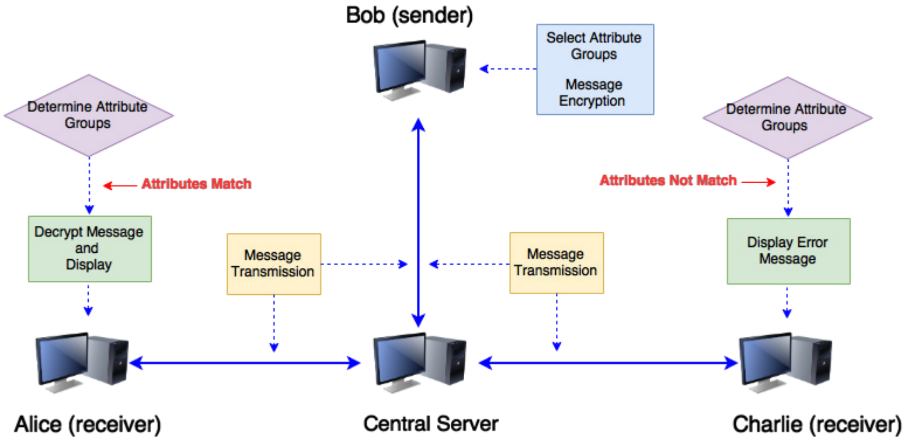


Figure 2. *High level logic overview of the described IM system: IM sender selects preferred user attributes and processes message encryption. A message is transmitted to central server and is further forwarded to all receivers. User attributes are matched between sender and receiver at receiver side. Depending on the attributes matching results, either decrypted message or error message is displayed for receiver.*

enter an encryption key or instead utilize a stored key file to generate an encryption key.

4. **User Attributes**: In addition to message encryption, multiple user attributes which represent the specific groups a user may belong to, are available for selection. A user can select to join some of these groups and view only messages sent from users in the same groups. The proposed IM system allows for user defined access control over the real-time messages. The user attributes module is independent from, and not reliant on the encryption that is in use by other aspects of the IM system.

Shown in Figure 2 is the high level logic overview of the above described IM system. IM sender selects preferred user attributes and processes message encryption. A message is transmitted to central server and is further forwarded to all receivers. User attributes are matched between sender and receiver at receiver side. Depending on the attributes matching results, either decrypted message or error message is displayed for receiver. The *Central Server* and *Message Transmission* modules serve for the message communication between IM users. The *Message Encryption* and *User Attributes* modules serve for the privacy management of the entire IM system.

Message Communication

The *Central Server* module plays a critical role in our attribute-based encryption IM system. It is responsible for the receiving, duplicating, and forwarding of all user messages transmitted in the network that constitute communication between the end users. Unlike most IM system, the *Central Server* in the proposed system does not examine the receiving messages and hence is unable to share any user messages or credentials with third-parties such as advertisers or developers, providing additional protection to the information transmitted with our system.

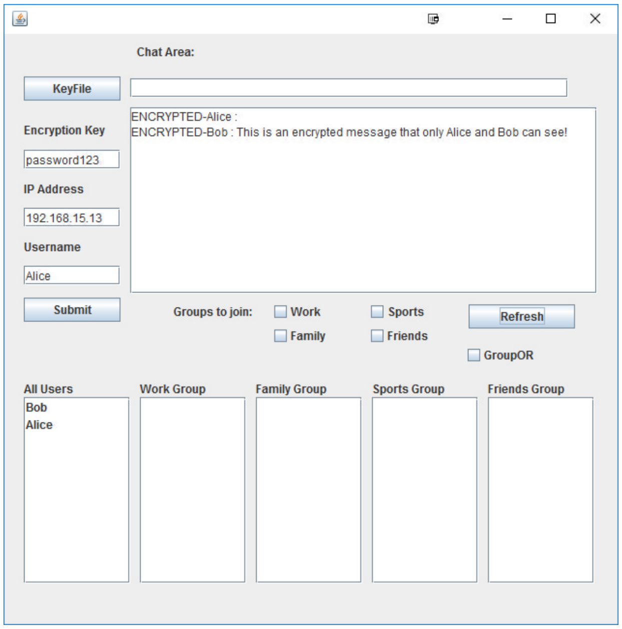
When designing an IM communication system, we typically first specify the Internet transport protocol supporting the content transmission of media data. It is well known that the Transmission Control Protocol (TCP) provides a more reliable data transfer service. Due to the high reliability requirement of the proposed ABE IM system, the TCP transport protocol is used exclusively. This is the primary duty of the *Message Transmission* module, sending the TCP data packets encapsulating user messages to the central server and further forwarding to other users. Those data packets can be encrypted, associated with attribute information, or simply be plaintext. The *Message Transmission* module ensures all data packets are transmitted without loss.

Privacy Management

Message encryption is important for communication security, without encryption on some level all communication details are visible on Internet. The *Message Encryption* module of the proposed IM system encrypt user messages using Advanced Encryption Standard (AES) [21]. Published by the National Institute of Standards and Technology (NIST) in 2001, AES is a symmetric block encryption algorithm that is intended to replace earlier algorithms for a wide range of applications. The technique is secure enough that the United States Government allows it to be used for the securing of classified and top secret data. Though AES is implemented as the encryption algorithm for messages transmitted in our system, any other encryption algorithm could also be used in this module. The data encryption is an independent process within the modules, and does not affect anything but the messages being transmitted by the system. Consequentially a user can choose to send either unencrypted messages or encrypted messages to other users at any time.

The transmitted messages are encrypted using AES with the encryption key provided by the sending user. Users can manually input an encryption key, a string of text which will be used as the cryptographic base. Alternatively, users can select any file on their computer as a *Key File* where the data of the file will be read and converted to a 100-character key used for message encryption. The advantage of using a *Key File* is that a user does not have to remember or memorize an encryption key.

The input of encryption key on the client side is optional as the sending user can choose to transmit either encrypted messages or unencrypted messages. If the sending user does provide an encryption key, all messages transmitted from the sending users are encrypted using AES algorithm with the provided encryption key.

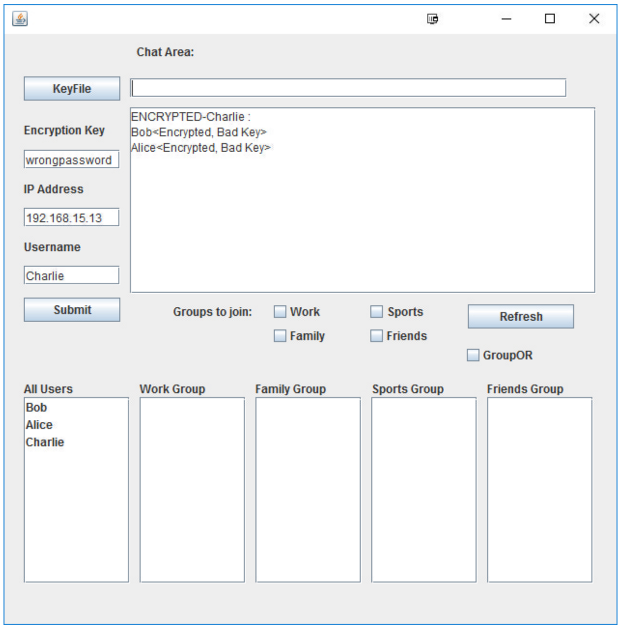


ENCRYPTED-Alice :
ENCRYPTED-Bob : This is an encrypted message that only Alice and Bob can see!

Encryption Key: password123
IP Address: 192.168.15.13
Username: Alice

All Users: Bob, Alice

Figure 3. Alice entered the same encryption key as Bob, she can view the encrypted messages he sends.



ENCRYPTED-Charlie :
Bob<Encrypted, Bad Key>
Alice<Encrypted, Bad Key>

Encryption Key: wrongpassword
IP Address: 192.168.15.13
Username: Charlie

All Users: Bob, Alice, Charlie

Figure 4. Charlie enter an incorrect encryption key, he cannot view what Alice and Bob are discussing.

As shown in Figure 3, these messages can only be displayed in the GUI where the receiving users entering the correct encryption key. Receiving users who do not enter the correct encryption key is unable to view encrypted messages as shown in Figure 4. On the other hand, the sending user can choose to send messages without providing any encryption key. In this scenario, all messages are transmitted as the form of plaintext and can be viewed by all receiving users as shown in Figure 5.

The *User Attributes* module aims to further enhance the security level by introducing attribute-based encryption. Users of the proposed IM system are allowed to join attribute groups to securely view messages sent from other users in the same groups, and are allowed to quickly switch between attribute groups for more flexible communication. The attribute information of a specific user is constantly updated and checked against the groups that the user is currently enrolled in. If two communication parties are belong to the same groups, both users are able to view the transmitted messages. Otherwise, the receiving user is unable to view these messages.

The attributes supported by our IM system include *Work*, *Family*, *Sports*, and *Friends*. IM users can optionally select to join one or multiple attribute groups. For instance, Alice, Bob, and Charlie are three users who organize a three-person group chat using the IM system. Suppose both Alice and Bob select to join the *Family* group as they are brother and sister in one family, at this moment, only Alice and Bob can view the messages sent by themselves while Charlie is unable to view their messages. Now if Bob further join the *Sports* group, any messages sent by Bob from this time point are hidden to Alice. Only users with same (*Family* AND *Sports*) attributes are able to view messages sent from Bob. This example shows that user attribute provides additional privacy control in multiuser environments where strong information security is required.

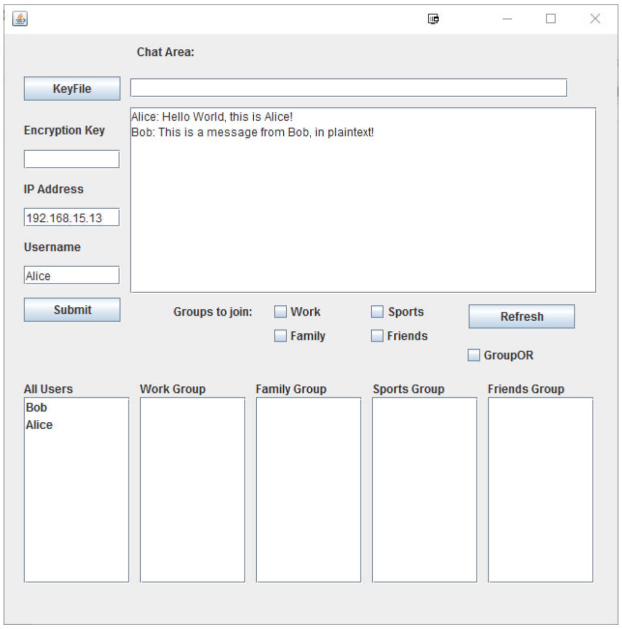
Note the proposed IM system also supports a *GroupOr* flag. If this flag is not marked, the system is running in *AND Mode*. As shown in Figure 6, only users enrolled in the exact same attribute groups as the sending user can view the transmitted messages. If this flag is marked, the system is running in *OR Mode*. In this mode, the semantics of logic for the user attributes is changed, allowing users enrolled in any of the same attribute groups but not all of the same as the sending user to view the transmitted messages.

The *Message Encryption* module and the *User Attributes* module can work together to provide higher level of data protection. As an additional layer of security, user messages may even be encrypted while still having user attributes, offering a user two layers of security within the IM system.

Results

The proposed Instant Messaging (IM) system is developed on Windows 10(X64) operating system. The standard Java JDK is used and all programming is performed within the Eclipse Development Environment. The AES encryption used for system development is implemented using standard javax.crypto package that is included with the standard Java Development Kit (JDK). The central server is run on Machine A which has an AMD FX-6300 6-core processor running at 3.5 GHz with 24 GB of memory. Machine B which is responsible for connecting to and sending all message to be examined has an Intel i5-3337U dual core processor running at 1.8 GHz with 8 GB of memory.

We evaluate the system performance with two measurements: *Construction Time* and *Interpretation Time*. The *Construction Time* measures the amount of time used for an IM sending client to process a message, which consists of attributes specification and message encryption. The *Interpretation Time* measures the amount of time used for an IM receiving client to process



Alice: Hello World, this is Alice!
Bob: This is a message from Bob, in plaintext!

Encryption Key:

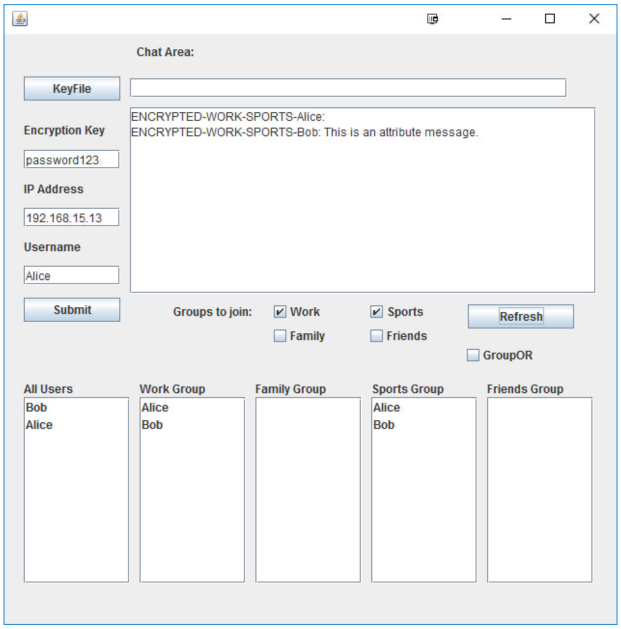
IP Address: 192.168.15.13

Username: Alice

Groups to join: □ Work □ Sports □ Family □ Friends □ GroupOR

All Users: Bob, Alice

Figure 5. From Alices perspective, plaintext message is transmitted if no encryption key is entered.



ENCRYPTED-WORK-SPORTS-Alice:
ENCRYPTED-WORK-SPORTS-Bob: This is an attribute message.

Encryption Key: password123

IP Address: 192.168.15.13

Username: Alice

Groups to join: ☑ Work ☑ Sports □ Family □ Friends □ GroupOR

All Users: Bob, Alice

Work Group: Alice, Bob

Sports Group: Alice, Bob

Figure 6. IM System in AND Mode*: Alice is enrolled in the exact same attribute groups as Bob and hence can view messages sent from him.*

a message, which consists of attributes matching and message decryption. Network latency is ignored as it is a variable and fluctuates with many factors such as the distance between IM users.

The *Construction Time* and *Interpretation Time* are measured for both non-encryption scenarios and encryption scenarios. We count the above two measurements with different sizes of user attribute, where each attribute is specified as a 5-character string. The sizes of user attribute used for testing include 0, 1, 10, 25, 50, 100, 200, 300, 400, and 500 attribute(s). 0 attribute refers no user attribute is specified. For each size of user attribute, 100 experiments are conducted. We take the average time of each set of experiments as the final result. As shown in Figure 7 and Figure 8, the overall *Construction Time* and *Interpretation Time* tend to increase for more user attributes. The results are expected as it takes more time for attribute-based encryption and decryption when more user attributes are involved.

Note that the message interpretation takes a significantly longer amount of time compared to message construction for a variety of reasons. The message interpretation process involves the parsing of received data strings, username extraction, attributes matching, and message decryption. The attributes matching is performed through the comparison of multiple arrays, a process which is exceptionally time consuming but necessary to ensure messages from all users are correctly interpreted.

Conclusions

Instant Messaging (IM) has become the primary means of communication within business, education, and everyday life. Individuals can share their knowledge, opinions, and experiences with one another due to a variety of features supported by existing IM applications. However, very little effort has been made to specifically address security concerns regarding real-time IM communications. In this work, we focus on the data protection and privacy management of group chat where multiple users simultaneously connect to a central server for real-time communications. We describe a novel multimedia IM system supporting user defined security control in a multiuser environment. To this end, we first introduce the attribute-based encryption (ABE) to provide flexible, user defined access control for real-time communication. The proposed IM system also support secure transmission of audio, image, and other types of file format for the purpose of multimedia communications. Finally, the communication platform is implemented in the manner so that the central server does not collect sensitive messages and credentials from the individuals who are chatting using the program. The proposed IM system provides a flexible and effective solution to data protection and privacy management for real-time online communication in multiuser environments where strong information security is required.

Our attribute-based encryption IM system is demonstrated to be secure and flexible for supporting real-time communication on Internet. Some potential improvements are achievable for the proposed system in the near future: (a). Employ automatic key distribution mechanism such as public key to enhance system security. (b). Instead of transmitting messages from one user to all connected users, the central server can choose specific receiving user based on user attributes and hence improve the system efficiency. (c). Integrate the IM system with existing Online Social Networks (OSNs) for more wide applications in the ever-expanding world of social networking. (d). Support more multimedia data formats for better user experiences. (e). Incorporate user attributes into the key generation for more reliable and flexible message encryption. The IM system is expected to be ultimately integrated into popular social networking applications to provide secure real-time message communication between users from various online communities.

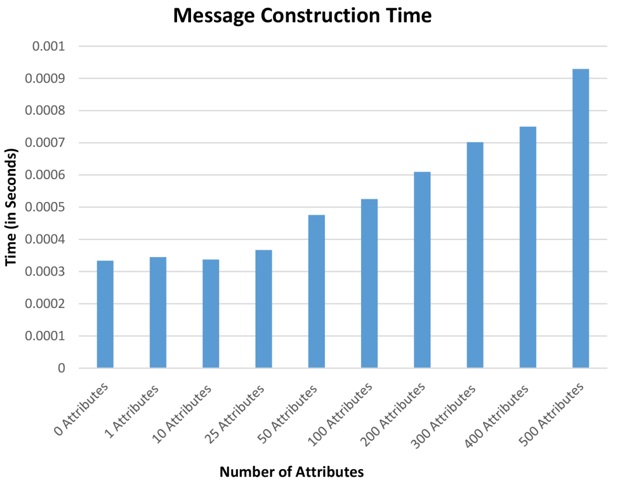


Figure 7. *Message construction time with different sizes of user attribute.*

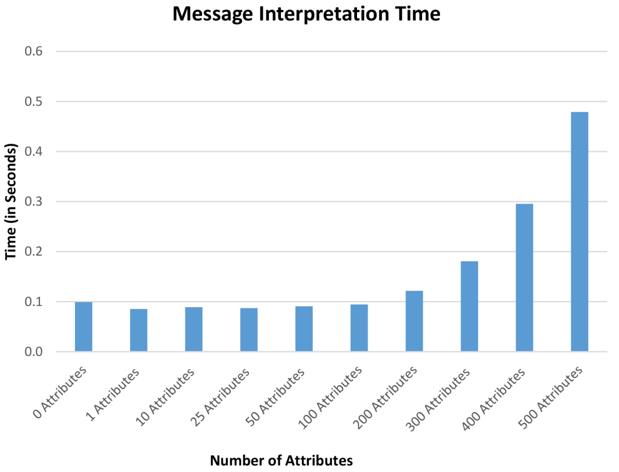


Figure 8. *Message interpretation time with different sizes of user attribute.*

Acknowledgements

This work was partially supported by the Frostburg State University President's Experiential Learning Enhancement Fund Program (PELEF) and by a FSU Foundation Opportunity Grant (# 30606).

References

[1] X. Pan, J. Wilson, M. Balukoff, A. Liu, and W. Xu, "Musical instruments simulation on mobile platform," in *IS&T Symposium on Electronic Imaging (IS&T-EI)*, (San Francisco, CA), 2016.

[2] X. Pan, T. Cross, L. Xiao, and X. Hei, "Musical examination and generation of audio data," in *SPIE Symposium on Electronic Imaging (SPIE-EI)*, (San Francisco, CA), 2015.

[3] X. Pan and K. Free, "Interactive real-time media streaming with reliable communication," in *SPIE Symposium on Electronic Imaging (SPIE-EI)*, (San Francisco, CA), 2014.

[4] A. Mislove, M. Marcon, P. K. Gummadi, P. Druschel, and B. Bhattacharjee, "Measurement and analysis of online social networks," in *Proceedings of the 7th ACM SIGCOMM Internet Measurement Conference, IMC 2007, San Diego, California, USA, October 24-26, 2007*, pp. 29–42, 2007.

[5] B. Krishnamurthy and C. E. Wills, "Characterizing privacy in online social networks," in *Proceedings of the first Workshop on Online Social Networks, WOSN 2008, Seattle, WA, USA, August 17-22, 2008*, pp. 37–42, 2008.

[6] B. Krishnamurthy, "A measure of online social networks," in *Proceedings of the First International Conference on COMmunication Systems And NETworks*, COMSNETS'09, (Piscataway, NJ, USA), pp. 190–199, IEEE Press, 2009.

[7] A. Acquisti and R. Gross, "Imagined communities: Awareness, information sharing, and privacy on the facebook," in *Privacy Enhancing Technologies, 6th International Workshop, PET 2006, Cambridge, UK, June 28-30, 2006, Revised Selected Papers*, pp. 36–58, 2006.

[8] S. Ahern, D. Eckles, N. Good, S. King, M. Naaman, and R. Nair, "Over-exposed?: privacy patterns and considerations in online and mobile photo sharing," in *Proceedings of the 2007 Conference on Human Factors in Computing Systems, CHI 2007, San Jose, California, USA, April 28 - May 3, 2007*, pp. 357–366, 2007.

[9] A. Korolova, R. Motwani, S. U. Nabar, and Y. Xu, "Link privacy in social networks," in *Proceedings of the 17th ACM Conference on Information and Knowledge Management, CIKM 2008, Napa Valley, California, USA, October 26-30, 2008*, pp. 289–298, 2008.

[10] M. Huber, M. Mulazzani, M. Leithner, S. Schrittwieser, G. Wondracek, and E. R. Weippl, "Social snapshots: digital forensics for online social networks," in *Twenty-Seventh Annual Computer Security Applications Conference, ACSAC 2011, Orlando, FL, USA, 5-9 December 2011*, pp. 113–122, 2011.

[11] S. Guha, K. Tang, and P. Francis, "NOYB: privacy in online social networks," in *Proceedings of the first Workshop on Online Social Networks, WOSN 2008, Seattle, WA, USA, August 17-22, 2008*, pp. 49–54, 2008.

[12] X. Pan and S. Lyu, "Region duplication detection using image feature matching," *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 5, no. 4, pp. 857–867, 2010.

[13] M. M. Lucas and N. Borisov, "Flybynight: mitigating the privacy risks of social networking," in *Proceedings of the 2008 ACM Workshop on Privacy in the Electronic Society, WPES 2008, Alexandria, VA, USA, October 27, 2008*, pp. 1–8, 2008.

[14] A. Tootoonchian, K. K. Gollu, S. Saroiu, Y. Ganjali, and A. Wolman, "Lockr: social access control for web 2.0," in *Proceedings of the first Workshop on Online Social Networks, WOSN 2008, Seattle, WA, USA, August 17-22, 2008*, pp. 43–48, 2008.

[15] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, pp. 457–473, 2005.

[16] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *2007 IEEE Symposium on*

Security and Privacy (S&P 2007), 20-23 May 2007, Oakland, California, USA, pp. 321–334, 2007.

[17] W. Stallings and L. Brown, *Computer Security: Principles and Practice*. Upper Saddle River, NJ, USA: Prentice Hall Press, 3rd ed., 2014.

[18] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin, "Persona: an online social network with user-defined privacy," in *Proceedings of the ACM SIGCOMM 2009 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, Barcelona, Spain, August 16-21, 2009*, pp. 135–146, 2009.

[19] A. Azfar, K. R. Choo, and L. Liu, "A study of ten popular android mobile voip applications: Are the communications encrypted?," in *47th Hawaii International Conference on System Sciences, HICSS 2014, Waikoloa, HI, USA, January 6-9, 2014*, pp. 4858–4867, 2014.

[20] J. Kim and J. W. Yoon, "Honey chatting: A novel instant messaging system robust to eavesdropping over communication," in *2016 IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2016, Shanghai, China, March 20-25, 2016*, pp. 2184–2188, 2016.

[21] "Fips pub 197, advanced encryption standard (aes)," 2001. U.S.Department of Commerce/National Institute of Standards and Technology.

Author Biography

Xunyu Pan received the B.S. degree in Computer Science from Nanjing University, China, in 2000, and the M.S. degree in Artificial Intelligence from the University of Georgia in 2004. He received the Ph.D. degree in Computer Science from the State University of New York at Albany (SUNY Albany) in 2011. From 2000 to 2002, he was an instructor with Department of Computer Science and Technology, Nanjing University, China. In August 2012, he joined the faculty of Frostburg State University (FSU), Maryland, where he is currently an Assistant Professor of Computer Science and the Director of Laboratory for Multimedia Communications and Security. Dr. Pan is the recipient of 2011∼2012 SUNY Albany Distinguished Dissertation Award and 2016 FSU Faculty Achievement Award in Teaching. His publications span peer-reviewed conferences, journals, and book chapters in the research fields of multimedia security, image analysis, medical imaging, communication networks, computer vision and machine learning. He is a member of the ACM, IEEE, and SPIE. (Corresponding Author: xpan@frostburg.edu)

Christopher Gill is currently working toward the B.S. degree in Computer Information Systems at Frostburg State University (FSU) in 2017. He intends to continue his education either through the pursuit of additional degrees, or through on the job training within the computer science industry.