MJoSHT
Malaysian Journal of Science, Health & Technology
[mjosht.usim.edu.my]

USIM

Article

Location-Based Cryptographic Techniques for Data Protection

Nur Syafiqah Mohd Shamsuddin[1,a] and Sakinah Ali Pitchay[1,b, 2]

[1]*Faculty of Science & Technology, Universiti Sains Islam Malaysia (USIM), 71800 Nilai, Negeri Sembilan, Malaysia*
E-mail: [a]syafiqah.mohdshamsuddin@gmail.com, [b]sakinah.ali@usim.edu.my

[2]*CyberSecurity and System Research Unit, Islamic Science Institute, Universiti Sains Islam Malaysia (USIM), 71800 Nilai, Negeri Sembilan, Malaysia*
E-mail: sakinah.ali@usim.edu.my

***Abstract*— Data protection has become one of the significant issues in cloud computing when end users must rely on their cloud providers for security purposes. Cloud providers never guarantee the security of data. One of the best ways to overcome this issue is to have the data encrypted before it reaches the cloud servers. Cryptographic becomes a common mechanism used to transmit data securely in open networks, but there are also some challenges to implement encryption internally due to key management. Either the keys are vulnerable towards any security attacks such as HTTP-focused-brute-force attack during transmit over the network, in case of the keys are kept at the user site, or keys are missing if the device is stolen. Thus, location-based encryption adds another layer of security on top of existing encryption method. Location-based encryption enhances security by implementing location information into the encryption and decryption process to counter the possible problems. Location coordinates are used as a key for encrypting the data and the cipher text can only be decrypted if and only the decrypted location is matched with the location that has been computed with the key. In this paper discuss on location-based encryption technique that has been implemented in previous works which are asymmetric, symmetric and hybrid algorithm followed by its strengths and weaknesses. This paper finds that majority of the researchers used hybrid algorithm to implement their location-based encryption instead of using the asymmetric algorithm or hybrid algorithm alone because the hybrid algorithm has fast computation of symmetric algorithm and high security of asymmetric dual keys.**

***Keywords*— Cryptographic techniques; Data protection; Data security; Location-based encryption.**

I. INTRODUCTION

Organizations around the world have invested heavily in information technology to protect their critical assets, including their precious data and the most commonly encountered method of practicing data security was the use of encryption, where digital data were encrypted and therefore rendered unreadable to unauthorized users and hackers. However, encrypted data are still vulnerable towards some attack such as brute-force and mathematical encryption attacks [1]. Besides, key management of locating the encryption key can become another issue if it is located either at the user site nor the server site. If it is located at the user site, such as at the user device, there is a possibility of the device being stolen or misplaced, making the key available towards the stealer. As a result, the encrypted data are possible to be encrypted once the unauthorised user found the key from the stolen device. To overcome this scenario, location-based encryption is implemented by integrating location information into encryption and decryption processes. Location-based encryption or geo-encryption is referred as any method of encryption where the information, were encrypted and can be decrypted at only a specific location [1]. Geo-encryption is an enhancement of conventional cryptography process where it provides another security layer on the available encryption protocol using the recipient location information to generate the encryption key [2], [3]. The original information will not be revealed if there is any attempt to decrypt the data at other locations as the encrypted file will can be only decrypted back if the location of decryption is matched with the location information inside the generated key.

II. CRYPTOGRAPHIC TECHNIQUES

Cryptography is a secret of writing where it enables people to send or store sensitive information in the form of unreadable or non-understandable language [3]. In location-based encryption, it builds from established cryptographic algorithm techniques which are asymmetric algorithm and symmetric algorithm. However, a lot of the existing works implements geo-encryption using both of the cryptographic techniques at the same time known as hybrid algorithm [4].

A. Asymmetric Algorithm Technique (Public-key Cryptography)

Asymmetric algorithm or also known as public key cryptography was an algorithm that used public key to encrypt and decrypt the data. One of the keys can be shared with everyone which is called as 'public key', used to encrypt the data while the other key is called as 'secret key' will be kept secret, used to decrypt the encrypted data [5]. In location-

based encryption, Rivest-Shamir-Adleman Algorithm (RSA) was found as the strongest public key available encryption method and the most used technique by the researchers [6]. The difficulty of factoring large prime numbers gives extra strength, as well as, extra security towards the algorithm [1]. Table 1 shows existing works on location-based encryption that used asymmetric algorithm technique.

TABLE I
EXISTING WORKS ON LOCATION-BASED ENCRYPTION THAT USED ASYMMETRIC TECHNIQUE

No	Existing works	Technique	Advantages	Disadvantages
1.	[7]	RSA	Strong protection against location spoofing.	Too small grid space cause wrong geo-lock.
2.	[8]	RSA	Assure secure data access.	Exposed to mathematical attack and brute force attack.

B. Symmetric Algorithm Technique (Private-key Cryptography)

Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are some of the symmetric algorithm techniques that are widely used due to its fast algorithm [1]. Symmetric algorithm has a better performance compared to asymmetric based on these two reasons, speed and vulnerability [5]. It is 1000 times faster than asymmetric algorithm because it uses a mutual key for both of its encryption and decryption process [9]. Table 2 summarizes the existing works on location-based encryption that used symmetric algorithm.

TABLE II
EXISTING WORKS ON LOCATION-BASED ENCRYPTION THAT USED SYMMETRIC TECHNIQUE

No	Existing works	Technique	Advantages	Disadvantages
1.	[10]	DES	Effective and practical for data transmission against location spoofing.	Decryption successful rate decreased.
2.	[11]	DES	Effective transmission between mobile client..	Decryption successful rate decreased.
3.	[12]	DES	Message access optimized only to specific area.	MAC ID changed if device rooted, upgrade version or factory reset.
4.	[13]	Modified AES	Low algorithm complexity.	Missing mix column transformation.
5.	[14]	AES	Straightforward and less effort for administrative overhead.	-
6.	[15]	DES	Privilege setting available.	High budget to afford anti-spoof device.
7.	[16]	AES	Available for multimedia files.	-
8.	[17]	AES	Good defence against cryptanalytic attack.	-
9.	[18]	AES	Best suit for mobile application.	Need velocity as additional parameter.

C. Hybrid Algorithm Technique

In terms of computational and implementation, it was very fast when using a symmetric algorithm, but slower when using an asymmetric algorithm due to difficulty in its computational. However, there is also another problem with symmetric algorithm which is how to securely exchange the secret key to each end and keep them secure after that. For this reason, asymmetric algorithm is used to encrypt the secret key and perform the key exchange to the other end as it offers very high security [19]. Therefore, a combination of symmetric and asymmetric encryption is used, called hybrid algorithm. The public key algorithm is used to secure and distribute session keys while the symmetric encryption is used to encrypt the information. Table 3 summarizes the related existing works that used hybrid algorithm for implementing their location-based encryption.

TABLE III
EXISTING WORKS ON LOCATION-BASED ENCRYPTION THAT USED SYMMETRIC TECHNIQUE

No	Existing works	Technique	Advantages	Disadvantages
1.	[1]	RSA & AES	Support location-based data encryption	Hard to meet same mapping function output
2.	[2]	Not stated	Support mobility	Low decryption ratio
3.	[5]	RSA & AES	Protected against location spoofing	Too small grid space cause wrong geo-lock
4.	[20]	Not stated	Support moving decryption zone	Increasing message queue cause low decryption ratio
5.	[21]	Not stated	Skip mapping function	Limited toleration distance
6.	[22]	Not stated	Support dynamic toleration distance	Decryption failed if movement too fast
7.	[23]	Not stated	Support mobility	Low rate of decryption
8.	[24]	RSA & AES	Limit data access to specific room	High cost of anti-spoof and GPS device

9.	[25]	AES for symmetric, not stated for asymmetric	Low energy, high packet delivery ratio	Possible attack spoofing and replay network
10	[26]	AES for symmetric, not stated for asymmetric	Prevent unauthorized access in cloud	Challenging data access control
11	[19]	RSA & AES	Customer can access account from anywhere	Person need to stay stable during transaction
12	[27]	RSA & AES	Accurate user location	Challenging access control
13	[28]	Not stated	Very accurate results	Expensive and difficult computational technique

III. DISCUSSION

There are three main algorithm techniques used in location-based encryption, which are asymmetric, symmetric and hybrid algorithms. There is also a work that used classical cryptography, which is the permutation cipher algorithm [29]. It proposed a method that applied to images, however this work has a major drawback where the decrypted image was totally distorted. Figure 1 shows that the asymmetric algorithm alone was not commonly practiced by the researchers due to complexity in factoring large prime numbers. Nevertheless, asymmetric algorithm offers high security which made the decryption process more complicated compared to symmetric algorithm. This leads to the notion of the hybrid algorithm as the most frequently used technique in location-based encryption due to fast computation of symmetric algorithm and high security of asymmetric dual keys.

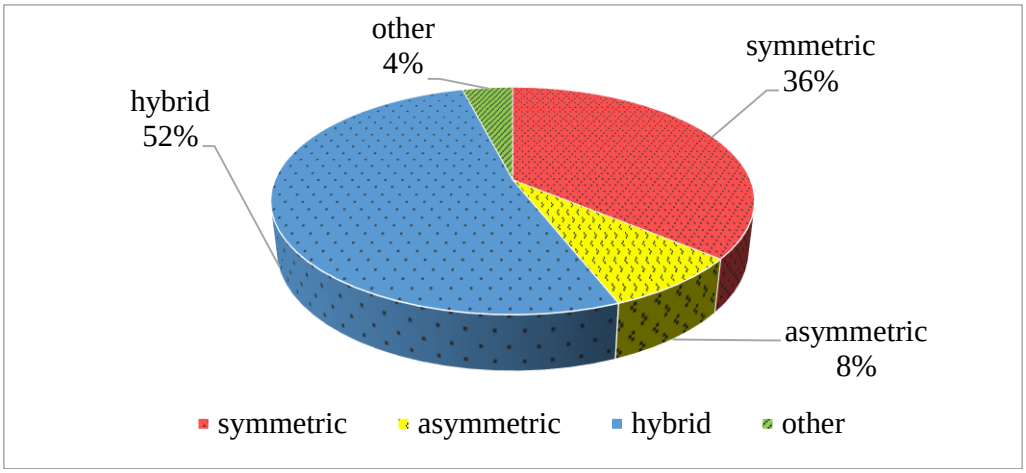

Fig. 1 Percentage of Algorithm Techniques Used in Location based Cryptographic

IV. CONCLUSIONS

Three main algorithms which are asymmetric algorithm, symmetric algorithm and hybrid algorithm have been discussed in this paper and highlights that the majority of the researchers used hybrid algorithm to implement their location-based encryption due to fast symmetric algorithm computation and high security of asymmetric dual keys. The least technique that has been used by researchers is the permutation cipher algorithm which has been found only in one previous work, but having a major drawback as the decrypted image was totally distorted.

ACKNOWLEDGMENT

This work was supported in part by the Ministry of Higher Education (MOHE) Malaysia under research grant [USIM/FRGS/FST/055002/50217].

REFERENCES

[1] L. Scott and D. E. Denning, "A Location Based Encryption Technique and Some of Its Applications," *Inst. Navig. Natl. Tech. Meet.*, no. 1, pp. 734–740, 2003.

[2] A. Al-Fuqaha, O. Al-Ibrahim, and A. Rayes, "Geo-encryption Protocol for Mobile Networks," *Comput. Commun.*, vol. 30, no. 11–12, pp. 2510–2517, 2007.

[3] S. A. Pitchay, W. A. A. Alhiagem, F. Ridzuan, and S. Perumal, "A Proposed Mobile Application Design for Protecting the Data in Cloud Using Enhanced Technique of Encryption," in *International Conference on Information Systems & Security (ICOISS)*, pp. 1–6, 2017.

[4] L. Scott and D. E. Denning, "A Geo-Encryption: Using GPS to Enhance Data Security," Institutional Archive of The Naval Postgraduate School, 2003.

[5] D. Qiu, S. Lo, P. Enge, and D. Boneh, "Geoencryption Using Loran," *Natl. Tech. Meet. Inst. Navig.*, pp. 104–115, 2007.

[6] S. A. Pitchay, W. A. A. Alhiagem, F. Ridzuan, and M. M. Saudi, "A Proposed System Concept on Enhancing the Encryption and Decryption Method for Cloud Computing," in *2015 17th UKSim-AMSS International Conference on Modelling and Simulation (UKSim)*, pp. 201–205, 2015.

[7] A. Khan, "Geo Location Based RSA Encryption Technique," *Int. J. Adv. Comput. Theory Eng.*, vol. 2, no. 2, pp. 17–20, 2013.

[8] A. K. Gupta, A. Srivastava, T. K. Goyal, and K. Gupta, "A Novel Security Approach using Location based RSA Encryption," *Int. J. Mod. Commun. Technol. Res.*, vol. 2, no. 5, pp. 38–42, 2014.

[9] E. Milanov, “The RSA Algorithm,” 2009.
[10] R. Karimi, “Enhancing Security and Confidentiality in Location-based Data Encryption Algorithms,” *Fourth Int. Conf. Appl. Digit. Inf. Web Technol. (ICADIWT 2011)*, pp. 30–35, 2011.
[11] R. Karimi and M. Kalantari, “Enhancing security and confidentiality on mobile devices by location-based data encryption,” in *ICON 2011 - 17th IEEE International Conference on Networks*, pp. 241–245, 2011.
[12] S. B. Sasi, B. K. Abraham, J. James, and R. Jose, “Location Based Encryption using Message Authentication Code in Mobile Networks,” *IJCAT – Int. J. Comput. Technol.*, vol. 1, no. 1, pp. 104–107, 2014.
[13] P. G. Kolapwar, “An Improved Geo-Encryption Algorithm in Location Based Services,” *IJRET Int. J. Res. Eng. Technol.*, vol. 4, no. 5, pp. 547–550, 2015.
[14] H. Pant, V. Kaushik, P. Singhal, and Vishal, “Geo-Encryption to Access The Data Using AES Algorithm,” *Int. J. Eng. Appl. Sci. Technol.*, vol. 1, no. 3, pp. 114–116, 2016.
[15] D. Auti, K. Landage, and S. Chavan, “Location Based Security for Online Transaction,” *Int. J. Innov. esearch Comput. Commun. Eng.*, vol. 4, no. 10, pp. 18660–18664, 2016.
[16] P. Dalvi, M. Patel, C. Dhalpe, A. Chaudhari, and P. S. Gaikwad, “Enhancing Security Using Location And Time,” *Int. J. Adv. Eng. Res. Dev. Sci. J. Impact Factor*, vol. 72, no. 4, pp. 4–6, 2017.
[17] S. S. Kadam, A. Shinde, and H. Durge, “Enhancing Security and Confidentiality for Mobile Device,” *Int. J. Comput. Appl.*, vol. 7, no. 1, pp. 67–69, 2017.
[18] S. Chaudhari, “‘Geo-Encryption Lite’ - A location based Encryption Application for Android,” *Int. J. Comput. Appl.*, vol. 165, no. 4, pp. 13–17, 2017.
[19] A. Deshpande, M. Jagtap, S. Kadam, A. Chechare, and P. Dhade, “Security to Mobile Banking using Location Based Encryption,” *Int. J. Adv. Res. Comput. Eng. Technol.*, vol. 4, no. 11, pp. 4011–4014, 2015.
[20] O. Al-Ibrahim, A. Al-Fuqaha, D. Van Dyk, and N. Akerman, “Mobility Support for Geo-Encryption,” in *2007 IEEE International Conference on Communications*, 2007, pp. 1492–1496.
[21] H.-C. Liao and Y.-H. Chao, “A New Data Encryption Algorithm Based on The Location of Mobile Users,” *Inf. Technol. J.*, vol. 7, no. 1, pp. 63–69, 2008.
[22] H. Hamad and S. Elkourd, “Data Encryption Using The Dynamic Location and Speed of Mobile Node,” *J. Media Commun. Stud.*, vol. 2, no. 3, pp. 67–75, 2010.
[23] A.S. Amin, “Improved Geo-Encryption Protocol for Mobile Networks,” in *7th International Conference on Electrical Engineering ICEENG-7*, vol. 1, pp. 1–4, 2010.
[24] M. S. Abolghasemi, M. M. Sefidab, and R. E. Atani, “Using Location Based Encryption to Improve The Security of Data Access in Cloud Computing,” in *2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 261–265, 2013.
[25] P. G. Kolapwar and P. H. P. Ambulgekar, “Use of Advanced Encryption Standard to Enhance The Performance of Geo Protocol in Location Based Network,” *Int. J. Sci. Res. ISSN (Online Impact Factor*, vol. 3, no. 11, pp. 2888–2890, 2014.
[26] G. Vandana, J. Supriya, P. Priya, P. Sumedha, and Nalawade, “Improve Security of Data Access in Cloud Computing Using Location,” *Int. J. Comput. Sci. Mob. Comput.*, vol. 4, no. 2, pp. 331–340, 2015.
[27] S. Kumar and N. Murthy, “Location Based Security of Data Access in Cloud Computing Using Scheduler,” *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 3, no. 5, pp. 104–111, 2015.
[28] S. Anju and J. Joseph, “Location Based Service Applications to Secure Locations with Dual Encryption,” *ICIIECS 2015 - 2015 IEEE Int. Conf. Innov. Information, Embed. Commun. Syst.*, pp. 1–4, 2015.
[29] P. Reddy, K. R. Sudha, and S. Naidu, “A Modified Location-Dependent Image Encryption for Mobile Information System,” *Int. J. Eng. Sci.*, vol. 2, no. 5, pp. 1060–1065, 2010.