Implementing Location-Based Cryptography on Mobile Application Design to Secure Data in Cloud Storage

Nur Syafiqah Mohd Shamsuddin¹, Sakinah Ali Pitchay*¹,²

¹Faculty of Science & Technology, Universiti Sains Islam Malaysia (USIM), Nilai, 71800, Malaysia
²CyberSecurity and System Research Unit, Islamic Science Institute (ISI), Universiti Sains Islam Malaysia (USIM), Nilai, 71800, Malaysia

*sakinah.ali@usim.edu.my

Abstract. This paper aims to identify security issues and existing solutions for cloud storage protection and to propose a mobile application design for securing data in cloud storage using the location-based cryptographic technique. In the proposed mobile application design, the user is required to perform the encryption before sending the data into the cloud storage. This paper provides a novel technique using location-based cryptography, secret keyword and hash function in order to further enhance the security of data in cloud storage that is currently only using either asymmetric or symmetric encryption algorithm. Asymmetric encryption’s has high security but due to the complexity in its computing, the performance rate is low while symmetric encryption’s performance is much faster as its implementation is easy. However, the attacker can still hack the data in cloud storage when either one of this encryption methods being used alone without any additional security layer. In this paper, location-based cryptography technique used consists of Advanced Encryption Standard (AES) algorithm and location information which are longitude and latitude coordinates. Those coordinates will be employed in the encryption and decryption process as additional security mechanism on top of existing cryptography method by generating supplementary encryption key called geo-lock key. Dynamic Toleration Distance (DTD) protocol will also be implemented with those coordinates to improve its practicality before it will be converted into the geo-lock key. AES algorithm will handle encryption and decryption process using the geo-lock key while secret keyword which defined by the user before starting the process will be used to authenticate the upload and downloading process. Both geo-lock key and secret keyword will be hashed using Secure Hash Algorithm 2 (SHA 2) and stored together with encrypted file in the cloud storage. The purpose of using location information is to ensure the encrypted file can be decrypted at intended location only while hash function is employed to protect the keys when they are stored in cloud storage. As a result, any unauthorized access to the file in cloud storage will not be allowed since each stored file was encrypted by the high performance of AES algorithm together with the decryption’s location restriction and the non-reversible hashed keys. The proposed mobile application design will serve an improvement in protecting stored data at
cloud storage by using AES algorithm with location information as data encryption method and SHA 2 function for hashing the keys.

*Keywords*— Location-based cryptography; coordinates; AES; SHA2; secret keyword.

1. Introduction

Cloud computing emerge as one of the robust computing technologies due to its flexibility and cost reduction [1]. Many companies are already migrated or in the process of migrating to cloud computing, results surge on security issues due to the amassment of digital assets [2]. Cloud storage is the keystone of cloud computing where security of data in cloud is the critical component including the storage security and transmission security [3]. To secure the storage, cloud service protects user’s data by implementing encryption with specific encryption key [4], [5]. Most service keep the encryption key themselves and letting their system see and process user’s data [6], [7]. Conventional encryption used keys that made up of random key-generate by particular algorithm technique. The random generated key however has vulnerability towards some security attack such HTTP-focused brute-force attack [7], [8]. Location-based cryptography is an enhancement of conventional encryption by adding additional security layer which makes use of location information for generate the encryption key [9]. Thus, this paper proposes a mobile system design by implementing an additional layer of security for protecting the data that going to be stored at cloud storage by encrypting the data before upload the file into the cloud storage using user secret keyword and location information as the encryption key. The encryption key will be hashed using secure hash algorithm and stored at the cloud with the encrypted file. Encrypted file can only be decrypted if the hashed location information and secret keyword that being key-in by the decrypter are matched with the hashed location information and secret keyword from the cloud storage.

1.1 Security Issue Associated with Cloud Storage

There are a lot of incidents related to data security in cloud storage history. In March 2009, Google spill of user Document and Spreadsheets with contacts who never have granted access to them [10]. December 2010, Honda customer’s sensitive information was stolen from their cloud service provider [11]. 2012, Dropbox pushed a code change that eliminated the password authentication system. As results, user’s stored data accessible to anyone who wanted to access it [12]. In 2013, more than one billion Yahoo user account experienced data breech [13]. In August 2014, Jennifer Lawrence and other bigger celebrity nude photos leaked online while they use iCloud Service as their personal storage [14]. In April 2016, 93 million voter registration records compromised during the National Electoral Institute of Mexico due to a poorly configured database that made this confidential information publicly available to anyone [13]. Recently issues in December 2017, PayPal customer details was stolen from their subsidiary, TIO Network Inc by unauthorized access to the company’s networks [15].

Based on incidents from [9-12], these four issues are found as the most common challenges in cloud storage that need to be emphasized:

1.1.1 Encryption

Poor implementation when many companies depend on the cloud provider for encrypting data which means that, the cloud provider have control of the encryption key & the cloud provider have a full access the data at any time.
1.1.2 **Key Management**
Most companies store both encryption and decryption key on the same database where the data also being stored. This is not a good practice which it can be detrimental for security.

1.1.3 **Data Loss and Leakage**
Data leakage increases when employees use their personal mobile devices to access and share corporate documents via cloud storage services while all the data are not encrypted during stored at the company cloud storage service. Using personal device can leads to data breech when user accidentally shared the corporate data to outside of the corporate authorize community.

1.1.4 **Multi-tenancy**
An architecture in which a single instance of a software application serves to multiple customers or tenants leads to security, capacity optimization, availability and service challenges [16]. Easier for a hacker to steal the data of all business customers who share the same cloud database.

2. **Existing Solution for Cloud Storage Data Protection**
There are many studies has been carried out to improve data protection in cloud storage. A new method of storing data in cloud storage has been proposed in [17] by partitioning the data into some pieces and the pieces of data later been encrypt using AES and RSA algorithm. After being encrypted, the data is sent to several servers. When the user wish to get back their data, encrypted partitioned data will be downloaded and decrypt back using same technique.

Study in [5] has suggested a new technique to protect the data at cloud by implementing three elements of cryptography which are AES encryption, RSA encryption and MD5 hash function. RSA algorithm used to secure the communication, AES algorithm to secure the file encryption while MD5 used to hash the authentication password. The key is kept in the system database server together with the hashed names of user account.

Work in [18] has proposed another technique of protecting the data in cloud storage by using AES and RSA algorithm. For files encryption, they using AES algorithm while for keys encryption, RSA algorithm has been used. The encrypted files are saved at cloud with both encryption and decryption key in encrypted form.

A study by [19] has proposed a system concept for improving data protection in cloud computing by enhancing the background process of the encryption and decryption. This paper proposed a system which is implementing the combination of RSA and AES encryption in its encrypting process. This system required the used of USB device during the encryption and decryption process. The files will be encrypted right before the upload process to the cloud storage starts. A removable device is required during download process by connecting the device into user's computer. The device then will be used to decrypt the files.

Recent work in [20] has suggest new concept of technique to protect data by implementing the encryption process on the file before it has been uploaded to the cloud. The data is being encrypted using AES algorithm while the encryption key is hashed using MD5 hash function to hash. During
download process, server will hash the keyword and compare with hashed keyword for validation. If the hashed keyword does not match, the decryption process will not be allowed.

Based on existing solutions by [13-16], encryption has been one of the most effectual way to protect stored data in cloud as it store the unreadable form of data at the cloud storage. The reviewed studies focused on implementing encryption technique on the data that going to be stored at the cloud server. However, they are free to decrypt their encrypted data at any place without specific location restriction to perform the decryption process. This will lead to data breaching if there are unauthorized user steal the data from the cloud storage and perform a trial to decrypt the file at anywhere.

3. **Location-based Cryptography**

Cryptography is a secret of writing technique where it enables people to write, store and send sensitive data or information in unreadable or non-understandable language form [20], [21]. Location-based cryptography is a technique that provides an additional layer of security on available encryption structure by implementing the location information into its process [22], [23] using the recipient location information to generate the encryption key [24]. If there are any attempt to decrypt the data at other location, the original information will not been revealed as the encrypted file only can be decrypted if and only if the location of decryption is corresponding to the location that has been set by the sender. Location information that is required for this location-based cryptography process is the coordinate, which are longitude and latitude. Decryption coordinate will be provided by the sender before the encryption process start and later will be converted into an encryption key called geo-lock key through a process called as mapping function and bit-wise XOR.

Location-based cryptography also build from conventional and established cryptographic algorithm techniques either symmetric algorithm, asymmetric algorithm or both of it which also known as hybrid algorithm [22].

3.1 **Asymmetric Algorithm Technique (Public-key Cryptography)**

Asymmetric algorithm which also known as public key cryptography is an algorithm technique that use two type of key to encrypt and decrypt the data. One of the key called as public key is used to encrypt the data which it can be shared with everyone, while the other key called secret key is used to decrypt the encrypted data will be kept secret to the recipient only. [25]. Rivest-Shamir-Adleman Algorithm (RSA) was found as the strongest public key encryption method available in location-based encryption and it is the most technique used by the researchers [17], [19], [26], [27]. The complexity of factoring large prime number in public key encryption process results towards extra strength and extra security of the algorithm [24].

3.2 **Symmetric Algorithm Technique (Private-key Cryptography)**

Symmetric algorithm which also known as private key cryptography is an algorithm technique that use only one key called as secret key in both encryption and decryption process [5]. Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are some of the private key algorithm that widely used due to its fast performance [24], [28]. There were two reasons why symmetric algorithm has a better performance compared to asymmetric algorithm which are speed and vulnerability [25]. Symmetric algorithm is 1000 times faster than asymmetric algorithm because it use a mutual key for both of its encryption and decryption process [29].
3.3 Hybrid Algorithm Technique

Hybrid algorithm technique is a combination of both asymmetric and symmetric technique in a single approach of algorithm process [24]. In encryption, when it come to computational and implementation of the algorithm, it was very fast when using symmetric algorithm to compute but slower when using asymmetric algorithm due to its complexity in its computational [30]. However, symmetric algorithm also has some issue which is how to exchange the secret key securely to each end and keep them unshakable after the exchange [31]. To encounter this issue, asymmetric algorithm is used to encrypt the secret key and perform the key exchange to be sent the other end as asymmetric algorithm offers very high security in its computation [32]. Therefore, a combination of symmetric and asymmetric algorithm called as hybrid algorithm is used. The asymmetric algorithm is used to secure and distribute session keys while the symmetric algorithm is used to encrypt the information.

3.4 Dynamic Toleration Distance (DTD)

Dynamic Toleration Distance was proposed by [33] to overcome the inaccuracy and inconsistent issues in GPS receiver and to increase the practicality. A protocol that use dynamic location of mobile node has been suggested. This protocol which is implemented into the cryptography technique also contribute into very strong algorithm towards attack. The mobile node receiver registers a certain set of coordinates with optional velocity for movement object to apply on the secret key with DTD and estimate the next position. These parameters with type of movement makes this protocol more secure than the static encryption where it is depends only on a position of static nodes and static toleration distance (TD). To implement this protocol, harversine formula are used to calculate the great distance between two points over the earth’s surface.

The calculation of harversine formula are shown as in equation (1).

\[ a = \sin^2(\Delta\varphi/2) + \cos \varphi_1 \cdot \cos \varphi_2 \cdot \sin^2(\Delta\lambda/2) \]
\[ c = 2 \cdot \arcsin \left( \sqrt{a} \right) \]
\[ d = R \cdot c \]

where:
\( \varphi \) is latitude
\( \lambda \) is longitude
\( R \) is earth’s radius, \((\text{mean radius} = 6,371 \text{km})\)
*Note that angles need to be in radians to pass the trigonal functions

In this proposed mobile application design system, the symmetric algorithm will be employed using AES encryption for encryption and decryption process of the original file due to it’s reputation as one of the best encryption algorithm among other symmetric algorithm [4], while the use of DTD protocol is important in the key geo-lock key implementation to increase its practicality in the interval of its decryption of data. This is because, GPS retriever have problem in inaccuracy and inconsistent of retrieving coordinate [33].
4. Proposed system concept

This system proposes a new technique on how to secure file that store in the cloud storage by recommending an additional layer of security in the encryption and decryption process using advance encryption standard, AES [34] and secure hash algorithm 2, SHA 2 [35]. Location information which are longitude and latitude coordinate will be used to generate the geo-lock key as the encryption and decryption key. AES will be appoint as the encryption algorithm for encrypting the original file, while SHA 2 hash function will be employed for hashing the secret keywords, encryption key and decryption key.

The idea of using location information for key generation is to ensure the decryption process will only can be done at the intended location which have been specified before the encryption process. As this system serves to single type of user, user have an ability to decide the location coordinate and the range of toleration distance for decryption process. Therefore, if any trial of stealing the data by unauthorized access on the cloud server will gain no advantages as they cannot decrypt the encrypted data outside the intended location of decryption process. The secret keyword also secured at the user site as it will not to be stored at the cloud server.

The best approach for protecting the data at cloud is to implement encryption before the uploading process and before sending the data to the cloud server. This is to confirm that the file integrity is remain secure and protected in the servers against any authorized access at all time. For the encryption process to begin, the user is required to key in input or auto retrieve his location coordinate to generate the geo-lock key. For decryption process, the user is only allowed to auto retrieve his location before the system process the retrieved location information into geo-lock key. The system then will hashing the geo-lock key and compare it with the hashed geo-lock key which is saved in the cloud with the file. If it is same, then the system will decrypt the file and allow the user to access the original file.

4.1 System Design Use Case Diagram

Figure 1 shows the use case diagram of user’s task to indicate the major task of proposed system. The major tasks of the proposed system are, login into the system, manual key-in or auto retrieving the location information and secret keyword, browsing and selecting files, upload encrypted file and download file.
4.2 System Work Flow

The overall flow of proposes system structure is shown in Figure 2. Figure 3 shows the flow process of the proposed mobile application system for uploading process.

![System Use case diagram](image)

Fig. 1 Use case diagram of the propose system design.

Fig. 2 Overall proposed mobile application system design concept.
The proposed mobile application system will serve to single type of user. Thus, any user can easily create their own account and use this mobile application system to store their private file securely in the cloud storage. User can upload their files after they key-in their secret keyword and decryption location information which is the coordinate for decryption process. User original file will be encrypted using AES algorithm while their keys which are secret keyword and decryption coordinate will be hashed using SHA 2 algorithm. The upload process will ask the user to key-in their intended decryption coordinate and system will process the coordinate given into a geo-lock key before it will be hashed using SHA 2 algorithm. System will encrypt the data based on the geo-lock key produced by key generation process after user input.
The download and decryption process require the user to key-in their secret keyword and let the mobile application system retrieve their current coordinate followed by process it into geo-loco key. When user key-in their secret keyword, the system will hash the inserted keyword and compare it with the saved hashed keyword in the cloud storage to check it similarity. If it is the same, then the system will download the encrypted file from cloud storage.

Fig. 4 Proposed mobile application system flow concept for download file process.
After successfully download the encrypted file, system then will hash the geo-lock key from retrieved coordinate and compare it with the saved hashed geo-lock key from cloud. If it is same, then the system will decrypt the file and allow user to access their original file. Figure 4 shows the flow process of the proposed mobile application system for uploading process.

4.3 System work flow steps

The designed system will contain five main sections as illustrated in Figure 1 use case diagram from previous section which are the login process, location retrieving process, browsing and selecting file, upload process and download process.

4.3.1: Login process: Every single user needs to create an account and login into the system before using the application. The user must create an account by filling up their email and password.
- Enter email
- Enter password

4.3.2: Location retrieving and key-in secret keyword process: Each user needs to fill in the location information for decryption purpose. User must confirm where they want to decrypt and open up their stored data later and provide a secret keyword.
- May select manually by drop down a pin on a map in the application, OR
- Let the device retrieve current location, if user want to decrypt at current location later.
- Key-in secret keyword
- Hashing secret keyword

4.3.3: Browsing and selecting file:
- Browsing file from device
- Select file from device folder

4.3.4: Upload process:
- Confirm the selected file
- Confirm the decryption location information
- Apply DTD on coordinates
- Generate geo-lock key with geo-lock mapping
- Hashing geo-lock key
- Encrypt file
- Upload to cloud server

4.3.5: Download process:
- Browse file from cloud server and select file
- Request to download
- Key-in secret keyword
- Hashing secret keyword
- Hashed secret keyword will be compared with hashed secret keyword in cloud storage
- If same, proceed to download file
- Retrieve current location using mobile device
- System will apply DTD on retrieve location and compute geo-lock key
• Hashing geo-lock key
• Hashed geo-lock will be compare with hashed geo-lock key in cloud storage
• If same, proceed to decrypt file
• If not same, decryption is denied

5. Expected Results
By applying the proposed method which is using the location-based encryption technique, it can be ensured that the data is more secured while it stored at the cloud servers. The data accessibility will be limited only to the owners who have the required parameter which is the correct location information to decrypt the data as the data was encrypted by the same owner. As a result, the proposed design will participate in improving the protection of data at cloud storage by applying the encryption on every file using a location information as the key for decrypting process since the encryption and decryption process will be handled by the user which is the owner of the data. Each encrypted file will be decrypted only by the same encryption and decryption geo-lock key based on the user intended location.

6. Conclusions
This paper highlights several security incidents related to cloud storage that have been occurred in several years. It also describes existing solutions for protecting data in cloud storage. Based on the reviewed studies, encryption has been one of the most effective methods to protect the data at the cloud storage. However, attacker can still hack the data in cloud storage if they used the encryption method only without any additional layer of security mechanism. Thus, this paper recommends an enhanced technique in the mobile application design which implementing location-based cryptography for encrypt data before sending to the cloud storage, secret keyword on handling the upload and download process while hash function for protecting the keys stored at cloud storage. The proposed design using AES algorithm because of its high performance for encrypting and decrypting data together with the location coordinates as supplementary encryption key called geo-lock key. The idea of using location information for key generation is to ensure the decryption process will only can be done at the intended location which have been specified before the encryption process start. This paper is expecting that the proposed system will lead to improve the security and protecting the privacy of cloud storage when the data are stored at the server is encrypted by the high performance of AES algorithm with the decryption’s location restriction and secured encryption keys by non-reversible hashed function. This will ensure the data is remain secured and protected in the server against any unauthorized access at all time.

Acknowledgement
This work was supported in part by the Ministry of Higher Education (MOHE) Malaysia under research grant [USIM/FRGS/FST/055002/50217]. The authors would like to express their gratitude to Universiti Sains Islam Malaysia (USIM) and MOHE for the support and facilities provided.

References
[1] P. Ravi Kumar, P. Herbert Raj, and P. Jelciana, “Exploring Security Issues and Solutions in Cloud Computing Services - A Survey,” Cybernatics Inf. Technol., vol. 17, no. 4, 2017.
[2] O. I. Araoye and K. A. Akintoye, “Security and Reliability Issues in the Deployment of Cloud Computing System,” Oman Chapter Arab. J. Bus. Manag. Rev., vol. 5, no. 2, pp. 1–7, Sep. 2015.
[3] D. W. K. Tse, D. Chen, Q. Liu, F. Wang, and Z. Wei, “Emerging Issues in Cloud Storage
Security: Encryption, Key Management, Data Redundancy, Trust Mechanism,” 2014, pp. 297–310.

[4] F. Gul, A. Amin, and S. Ashraf, “Enhancement of Cloud Computing Security with Secure Data Storage using AES,” 2017.

[5] V. Jaglan, “Proposing Efficient Approach to Improve Integrity Checking in Cloud Data Security,” 2015.

[6] Haibin Zhang, “How secure is your data when it’s stored in the cloud?,”” 2018. [Online]. Available: http://theconversation.com/how-secure-is-your-data-when-its-stored-in-the-cloud-90000. [Accessed: 02-May-2018].

[7] 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.

[8] Joseph Granneman, “Amazon S3 security: Exploiting misconfigurations,” TechTarget, 2011. [Online]. Available: https://searchcloudsecurity.techtarget.com/tip/Amazon-S3-security-Exploiting-misconfigurations. [Accessed: 02-Oct-2018].

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

[10] Jason Kincaid, “Google Privacy Blunder Shares Your Docs Without Permission,” Oath Tech Network, 2009. [Online]. Available: https://techcrunch.com/2009/03/07/huge-google-privacy-blunder-shares-your-docs-without-permission/. [Accessed: 02-Oct-2018].

[11] Fahmida Y. Rashid, “Honda Data Breach Highlights Need to Set Strong Cloud Security Policies,” QuinStreet Inc., 2011. [Online]. Available: http://www.eweek.com/security/honda-data-breach-highlights-need-to-set-strong-cloud-security-policies. [Accessed: 02-Oct-2018].

[12] Dave Shackleford, “Challenges with data protection in the cloud - Information Security Magazine,” TechTarget, 2016.

[13] Contel Bradfort, ”7 Most Infamous Cloud Security Breaches,” StorageCraft Technology Corporation, 2018. [Online]. Available: https://blog.storagecraft.com/7-infamous-cloud-security-breaches/. [Accessed: 02-Oct-2018].

[14] Lee Munson, “Jennifer Lawrence, Rihanna, 98 other celebs’ nude photos leaked online,” Naked Security Sophos Ltd., 2014. [Online]. Available: https://nakedsecurity.sophos.com/2014/09/01/jennifer-lawrence-rihanna-98-other-celebs-nude-photos-leaked-online/. [Accessed: 02-Oct-2018].

[15] Bojana Dobran, “1.6 Million PayPal Customer Details Stolen in Major Data Breach,” Phoenix NAP, 2017. [Online]. Available: https://phoenixnap.com/blog/paypal-customer-details-stolen. [Accessed: 02-Oct-2018].

[16] P. R. Kumar, P. H. Raj, and P. Jelciana, “Exploring Security Issues and Solutions in Cloud Computing Services-A Survey,” Bulg. Acad. Sci. Cybern. Inf. Technol., vol. 17, no. 4, 2017.

[17] C. Adviti and J. Gupta, “Review on Encrypt the text by MD5 and RSA in Client Cloud Approach,” 2016.

[18] Z. Kartit, M. E. L. Marraki, and a Definition, “Applying Encryption Algorithm to Enhance Data Security in Cloud Storage,” IAENG Eng. Lett., vol. 23, no. 4, 2015.

[19] 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), 2015, pp. 201–205.

[20] 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), 2017, pp. 1–6.
[21] N. Rahimi, J. J. Reed, and B. Gupta, “On the Significance of Cryptography as a Service,” *J. Inf. Secur.*, vol. 9, pp. 242–256, 2018.

[22] N. S. M. Shamsuddin and S. A. Pitchay, “Location-based Cryptographic Techniques: Its Protocols and Parameters,” in *RITA 2018*, 2020, pp. 79–86.

[23] Y. Baseri, A. Hafid, and S. Cherkaoui, “Privacy preserving fine-grained location-based access control for mobile cloud,” *Comput. Secur.*, vol. 73, pp. 249–265, 2018.

[24] 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.

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

[26] J. D. D. Nkapkop, J. Y. Effa, A. Toma, F. Cocitoa, and M. Borda, “Chaos-based image encryption using the RSA keys management for an efficient web communication,” in *2016 12th International Symposium on Electronics and Telecommunications, ISETC 2016 - Conference Proceedings*, 2016, pp. 59–62.

[27] J. N. Gaithuru, M. Bakhtiari, M. Salleh, and A. M. Muteb, “A comprehensive literature review of asymmetric key cryptography algorithms for establishment of the existing gap,” *2015 9th Malaysian Softw. Eng. Conf. MySEC 2015*, pp. 236–244, 2016.

[28] K. Seman, M. F. Roslan, A. H. Ab Halim, and M. N. A. Syam Mohd Sayuti, “On selected issues of Boolean function application in symmetric key cryptography against side channel attacks,” *J. Phys. Conf. Ser.*, vol. 1282, p. 012001, 2019.

[29] E. Milanov, “The RSA Algorithm,” 2009.

[30] M. A. Albahar, O. Olawumi, K. Haataja, and P. Toivanen, “Novel Hybrid Encryption Algorithm Based on Aes, RSA, and Twofish for Bluetooth Encryption,” *J. Inf. Secur.*, vol. 9, pp. 168–176, 2018.

[31] M. Patel, “An Optimized Cryptography Algorithm And Key Exchange Method for Small Scale Devices,” *Int. J. Recent Inov. Trends Comput. Commun.*, vol. 3, no. 6, pp. 2605–2611, 2015.

[32] 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.

[33] 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.

[34] F. Information, “Advanced Encryption Standard (AES),” 2001.

[35] P. Kamal, “Security of Password Hashing in Cloud,” *J. Inf. Secur.*, vol. 10, no. 02, pp. 45–68, 2019.