# A Hybrid Cloud Security Model for Securing Data on Cloud

Pravin Soni[a] and Rahul Malik[a]

[a] *Lovely Professional University, Punjab, India*

**Abstract**

Cloud computing is taken into consideration as one of the famed computing strategies for pooling and offering numerous computing resources on call basis. Cloud computing is now become most important part of the IT enterprise and has turn out to be a beneficial desire for small finances commercial enterprise and organizations. As multiple clients are sharing the same public cloud services, cloud users begin thinking of the security of their important data stored on cloud servers managed by the third party. The main goal of this paper is to provide hybrid security model which provides security to cloud storage during transit and at-rest from unauthorized user by using numerous cryptographic services such as user authentication and authorization using OTP or authenticator application, user access control policy, data confidentiality using hybrid encryption algorithm, integrity control using SHA with DSA algorithm, backup module and monitoring system.

**Keywords 1**

Access Control Policy, Cloud Security, Hybrid Encryption, Monitoring System, User Authorization

## 1. Introduction

Now days, most organizations are migrating to cloud, due to the fact the cloud services are inexpensive and convenient. For organizations, locating sufficient storage area to preserve all of the information they obtained is an actual challenge. Some organizations purchase massive amount of storage drives for storing massive information of organization and yet confronted with problems like 24x7 availability of data, searching, etc [1].

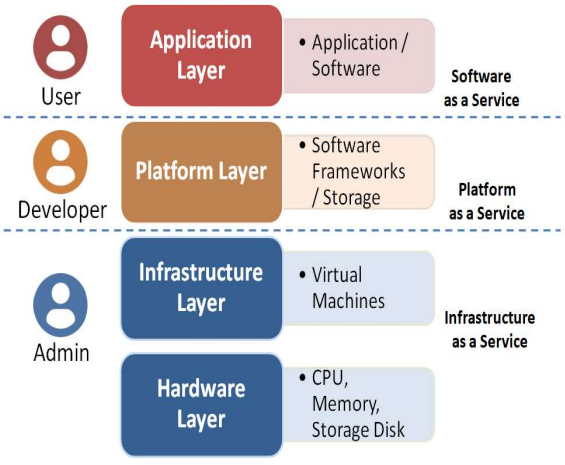


**Figure 1** : Cloud computing layered architecture

WCNC-2021: Workshop on Computer Networks & Communications, May 01, 2021, Chennai, India.
EMAIL: malikvnit@gmail.com (Rahul Malik)
ORCID: 0000-0002-2566-2954 (Rahul Malik)

Cloud Storage is a network based model for storing data wherein the virtual records is saved in logical pools which spans over different servers, and normally owned and controlled by cloud service provider. Cloud provides on demand resources or services to everyone like application, data storage and servers that increases or reduces its resources as peruse with flexibility and cost efficiently. Fig 1 shows the cloud architecture consist of layers like Software as a Service (SaaS): that offers user a numerous software to be utilized on a cloud infrastructure using web browser or API, Platform as a Service(PaaS): that provides platform to developer for implementing various software's frameworks and storage to be consumed by user and Infrastructure as a Service (IaaS): that offers admin to customized hardware on demand in maximum universal segments of cloud [2].

Fig 2 illustrate that cloud service provider deploys there cloud services as public cloud whose services are available to everyone and multiple user data stored at common place, private cloud whose services are private generally developed and utilized by private business organizations and can be accessed only by members of organizations and hybrid cloud which combines the features of public and private cloud [3], [4].

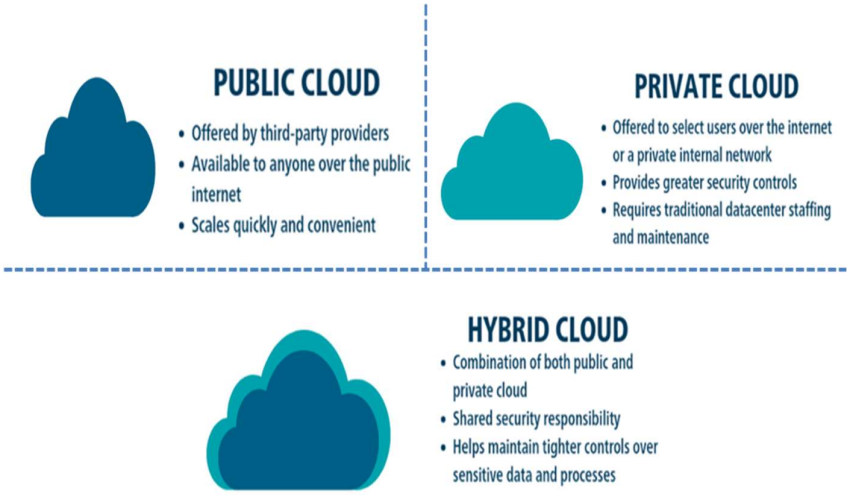


**Figure 2** : Public, Private and Hybrid Cloud [5]

Cloud computing is a preferred approach this is determined and appropriate anywhere as it gives access to the various resources on request of the customers which may be used with much less interaction with the service issuer and with the minimal cost. It is taken into consideration as a dominant era due to the fact it could control the huge quantity of information. Cloud computing is steady and reliable, because of which the companies use this infrastructure without constructing their own. It is an excellent approach for any sized company or enterprise due to its cost-saving technology. It provides huge platform which offers various computing resources as a service like application, frameworks and hardware selection [6].

Although cloud computing has many features and advantages, it also has few limitation too, and security issue is always at the top with highest priority. Cloud services have many security challenges such as integrity control, access control, user identification, resource management and so on. Most cloud service provider stores private and important data of organization or person through some third party vendor by way of utility in public domain. Therefore, the threat of essential data going into unauthorized person or hacker is always there due to the fact cloud offerings are to be had and reachable through all its users. Hence, there may be the maximum opportunity of improper handling of personal records or the personal records can be altered deliberately via hackers or different users of same cloud accidentally. This results in compromised and integrity breach of private information. By thinking about these types of troubles concerning the security of the information, it's always taken into consideration as a challenge in cloud service. Cryptography is extensively accredited technique

for making sure the data safety and provides various services and mechanism which assures confidentiality, integrity control, access control and message authentication [7].

## 2. Literature Review

Mahalle & Shahade, 2014 [8] developed hybrid cryptographic algorithm for cloud systems for providing security to data. There hybrid algorithm is mixture of famous symmetric (AES-128) and asymmetric (RSA-1024) encryption algorithm implemented in eye-OS. The file uploaded by cloud user is first stored in temporary storage where it is encrypted using AES-128 and uploaded to the cloud storage system. The secret key utilized for encryption is encrypted using RSA-1024 using the public key which can be recovered by user only. This model can be utilized for large file size due to fact that only AES is used for data encryption which is considered faster and secure too.

Kiruthika et al., 2015 [9] have reviewed the security challenges encounter in cloud services with various stats also mentioned some key issues in cloud security. Their model provides the solution to this key issues using AES encryption. They have compared various symmetric encryption algorithms like 3DES, DES and RC2 with parameters like encryption speed and throughput. The idea is simply encrypting the data that is stored in cloud storage with AES encryption. The separate application or software will be used for uploading data to cloud which encrypts the data at user side. User need to maintain special software for key management which will be required during data upload and download. Soman & Natarajan, 2017 [6] developed an enhanced hybrid data security algorithm using various algorithms like AES, ECDSA and SHA256 for providing security to data stored inside. These algorithms are arranged appropriately for securely communicating, uploading and downloading data on cloud. The AES Algorithm is used for confidentiality, ECDSA and SHA256 provides authentication and integrity check.

Bindu et al., 2018 [10] developed hybrid cryptography algorithm using 4 symmetric encryption algorithms (AES, RC6, BLOWFISH and BRA) for secure file storage in cloud environment. The file is sliced into 8 equal parts and encrypted using above algorithms simultaneously with multithreading technique. The secret key shared via email which is hidden inside image using LSB technique of stenography. Batra et al., 2018 [11] developed hybrid encryption algorithm using three different symmetric encryption algorithm for secure file storage in cloud. Hybrid encryption uses all three encryption algorithms for providing enhanced security to cloud storage. The data is partitioned into three equal parts and encrypted separately using these three algorithms RC4, DES and AES respectively. The key shared to receiver using Steganography.

L. Kumar & Badal, 2019 [12] reviewed various hybrid cryptographic models and suggested to use AES and FHE which can overcome security issues like data confidentiality, privacy and integrity. The authors also listed and elaborated some major security challenges in cloud which includes Data Confidentiality, Authenticity, Integrity, Authorization, Freshness and Non-repudiation. Zhang et al., 2019 [13] implemented hybrid security model for securing medical patient's data stored in cloud. The authors have modified AES algorithm and named as P-AES which is used in conjunction with RSA to provide privacy and security to medical data stored in cloud. Their hybrid model can only be used for text and doesn't work for securing images and videos.

Viswanath & Krishna, 2020 [14] developed a Hybrid encryption framework containing modules like data slicing, encryption, distribution, uploading, indexing, retrieval and merging. Encryption and decryption in their hybrid framework is done using AES and Fiestel network block wise. The sliced data is encrypted, indexed and stored in multi cloud environment.

The table 1 below provides the brief overview of various security models developed for cloud security.

**Table 1:** Overview of hybrid security models of cloud

| Security Model Studied | Algorithms Used | Gist |
|---|---|---|
| (Mahalle & Shahade, 2014) [8] | RSA and AES | • Every file is encrypted with AES using newly generated key which is stored in encrypted form.<br>• RSA is used for encrypting secret key.<br>• System Supports sharing of file. |
| (Kiruthika et al., 2015) [9] | AES and Key Management Application | • Data on Cloud must be retrieved or uploaded through Application<br>• Application encrypts or decrypts the Data using AES algorithm at user side in conjunction with separate Key management application managed by user. |
| (Soman & Natarajan, 2017) [6] | AES, ECDSA with SHA256 | • System resolves data confidentiality and integrity issue.<br>• The AES Algorithm used for File Encryption.<br>• ECDSA with SHA256 provide message authentication service. |
| (Bindu et al., 2018) [10] | AES, BLOWFISH, RC6, BRA and Steganography | • System provides enhanced security using hybridization.<br>• Data file is sliced in parts and encrypted using these algorithms.<br>• Key sharing is done through image steganography. |
| (Batra et al., 2018) [11] | AES, DES, RC4 and Steganography | • System provides confidentiality to data using hybrid algorithm.<br>• Data file sliced into 3 parts and each part is encrypted once with different algorithm as mentioned.<br>• Secret Key distribution is done through image steganography. |
| (Viswanath & Krishna, 2020) [14] | AES and Feistel Algorithm | • Model distributes data to multi cloud for storage.<br>• Model partitioned data in blocks of 256 bit and then encrypted using hybrid algorithm formed using AES and Feistel algorithm.<br>• Model requires indexing, retrieval and merging modules for smooth working. |
| (Sai Akhil et al., 2020) [15] | AES, CAMELLIA and SERPENT | • Model implemented based on 2 concepts Data Slicing and Hybrid Cryptography.<br>• Input data is sliced in parts, encrypted using mentioned algorithm and stored in different cloud storage buckets. |

## 3. Security Challenges in Cloud Security

Several security issues revolve around cloud security and data security. The cloud service provider faces many security challenges. Thus, cloud security model must be developed considering these security challenges and cryptographic mechanism or services must be incorporated in security model to mitigate and ensure the security in cloud environment.

Table 2 describes the security challenges exist in cloud security and its remedy by using cryptographic services.

**Table 2:** Security Challenges in Cloud with Cryptographic Services as a Solution

| Security Issue | Description | Cryptographic Service or Solution |
|---|---|---|
| Confidentiality, Integrity and Availability (CIA) [16], [17] | CIA assures privacy, accuracy, consistency and guarantees 24x7 availability of data. | • Encryption Decryption<br>• Secure Hash Function with Digital Signature Algorithm.<br>• Backup Module |
| Authentication, Authorization and Access Control (AAAC) [1], [18] | AAAC ensure user identity and access control rules. | • Username Password based authentication.<br>• Authorization using OTP or 2-Factor Authenticator.<br>• Setup of Access Control Policy with Monitoring System. |
| Geographic Physical Location [19] | Ensure safety data where actually data stored | • Must have contractual and jurisdictional control with strong physical security. |
| Data Backup [18], [20] | Ensure availability of data due to any type disasters which occurs due to natural or human-made. | • On-site backup<br>• Cloud Backup |
| Multi-tenancy [20], [21] | Many users' data resides in cloud having same physical location. | • Strong Access Control Policy |

## 4. Proposed Hybrid Security Model for Cloud

### 4.1. Proposed Hybrid Security Model with Techniques

Cloud data security cannot be achieved by merely using hybrid cryptographic algorithm which utilizes hybrid encryption for enhanced cloud data security. The other security issues in cloud security should also be address like user authentication and authorization, data integrity, user access control, and monitoring system [2], [12]. Fig 3 demonstrates the proposed hybrid system for cloud security which involves various techniques to provide complete cloud security solution.

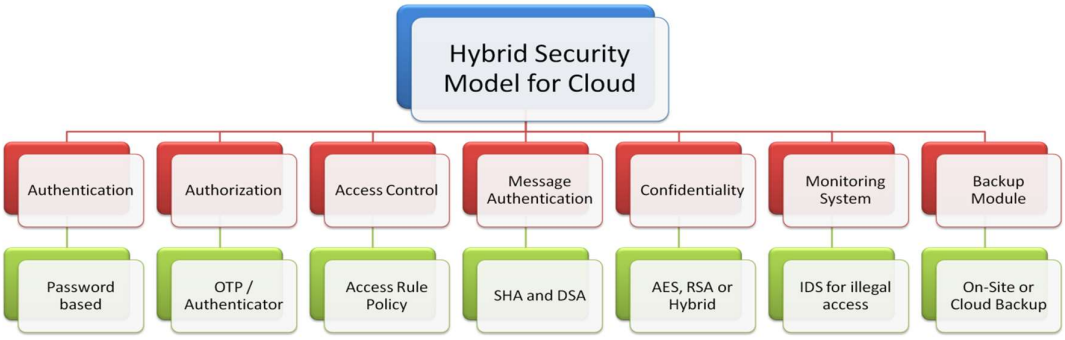


**Figure 3:** Hybrid security model for cloud security with techniques

The proposed hybrid system consist of following module

- User Authentication- The cloud service provider will provide unique username and password to every user. User will provide this information to cloud for authentication to utilize cloud services.
- User Authorization- This module will provide extra safety and will be used in conjunction with authentication module. Cloud will verify user's identity by sending newly created random number as One Time Password (OTP) to users mobile or email which is valid for small time span. Cloud system will provide its services to be utilized only after successful verification of OTP.

Nowadays 2 factor authentication (2FA) application also integrated as authorization service and proved effective for user authorization.

- Access Control- This module gives limits the access rights of user within cloud environment. Cloud service provider creates user access policies definition and enforce to user by which various resources are permitted or not permitted to user as per subscription. This module assures that user always access resource that has been authorized to him as per access policy and unauthorized access to cloud data by any user denied and logged for further action.
- Message Authentication– This module utilizes cryptographic algorithms to assure message integrity and non-repudiation that retrieved data from cloud is correct i.e. no alteration or changes has been done in cloud environment and can verify the identity of data uploader. The SHA256 along with DSA algorithm are used to ensure the integrity of cloud data.
- Confidentiality – This module provide service that assures that data always remain confidentiality during transit and at rest in cloud. This will be achieved by encrypting data using hybrid algorithm for enhanced security which makes data scrambled and impossible to understand by unauthorized person and can be retrieved only by secret key available with authorize user.
- Monitoring System- This module provides service that alerts any illegal activity carried out in cloud environment to service provide and user also. Intrusion detection system always monitors network and system activity and raise alerts in abnormal behaviour arises from user or hacker who wants to obtain private information from cloud.
- Backup Module – This module works internally on scheduled time or on user request for performing backup of cloud data on some other location either on-site (same physical location but different drive) or cloud based (stored in cloud i.e. different geographical location) for disaster management service.

## 4.2. Proposed Hybrid Model Flowchart

Fig 4 shows the flowchart of the proposed hybrid cloud security system which demonstrates how this module communicates with each other during user access to cloud. The monitoring system and backup module always remain active and works in background. The monitoring system module always checks each activity performed in cloud and gives alerts for abnormal activity observed in system module, resource utilization, network traffic or violation of access rules. The backup module takes the backup of cloud data during scheduled time as per configuration. The flowchart can be described in 2 phases as login phase and upload/download phase.

Login Phase: The user attempts to access cloud will always first go to login phase where 3 different module works together to perform security check for ensuring user identity and enforcing access control rules. The authentication module utilizes basic username and password to verify register user followed by authorization module which ensures the user's identity and based on user role the access control module enforces the access policy rules as defined by service provider.

Upload/Download Phase: Cloud always needs that user must be logged in system for user data upload or download request. The data upload request handle by message authentication module which creates digital signature for integrity control and non-repudiation service and then applies encryption algorithm for privacy of data before storing data on cloud. The reverse procedure is followed during download request i.e. data is decrypted first then by message authentication module checks that the digital signature matches (stored in upload request and newly created from downloaded data) for assuring data integrity can also verify the originator of data if required.

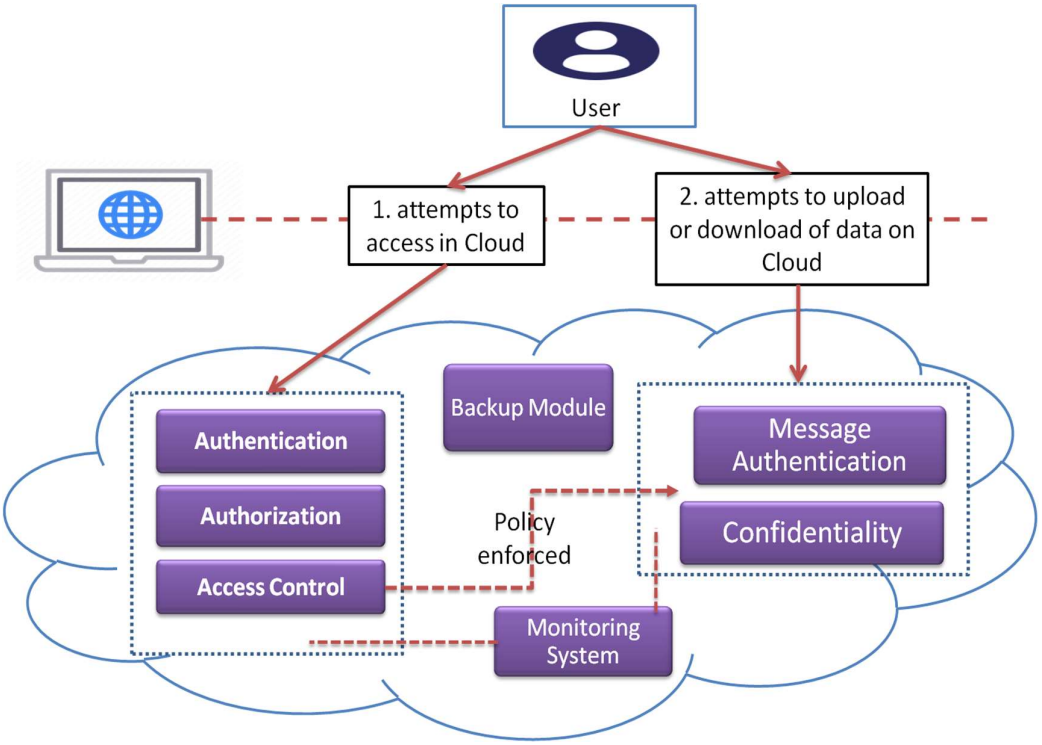


**Figure 4:** Proposed hybrid cloud security system flowchart

## 5. Conclusion

Cloud services around the world increased due to the recent covid-19 pandemic. Security issues in cloud environment still have a huge horizon for companies and hackers that both can workaround and earn rewards. Cloud service providers offer their services on various parameters like hardware selection, resource requirement, pricing, flexibility, support system, etc with some security features. Our proposed hybrid cloud system covers majority of security challenges exist in cloud environment like CIA, AAAC, physical location, data backup and multi-tenancy. The proposed system utilizes and mixes numerous cryptographic mechanism and services to provide enhanced security model for cloud data security such as user authentication and authorization using OTP or authenticator application, user access control policy, data confidentiality using hybrid encryption algorithm, message authentication using SHA with DSA algorithm, backup module and monitoring system.

## 6. References

[1] S. A. Ahmad and A. B. Garko, "Hybrid cryptography algorithms in cloud computing: A review," *15th Int. Conf. Electron. Comput. Comput. ICECCO*, pp. 1–6, 2019, doi: 10.1109/ICECCO48375.2019.9043254.

[2] J. Kumar, "Cloud computing security issues and its challenges: A comprehensive research," *Int. J. Recent Technol. Eng.*, vol. 8, no. 1 Special Issue 4, pp. 10–14, 2019.

[3] Varsha, A. Wadhwa, and S. Gupta, "Study of Security Issues in Cloud Computing," *Int. J. Comput. Sci. Mob. Comput.*, vol. 4, no. 6, pp. 230–234, 2015.

[4] O. Givehchi and J. Jasperneite, "Industrial Automation Services as part of the Cloud : First Experiences," 2013.

[5] K. Singh, "What is the difference between Public, Private and Hybrid Cloud?" [Online]. Available: https://karansinghreen.medium.com/what-is-the-difference-between-public-private-and-hybrid-cloud-a41bba631479. [Accessed: 25-Dec-2020].

[6] V. K. Soman and V. Natarajan, "An enhanced hybrid data security algorithm for cloud," *Int.*

*Conf. Networks Adv. Comput. Technol. NetACT 2017*, pp. 416–419, Jul. 2017, doi: 10.1109/NETACT.2017.8076807.

[7] M. K. Sinchana and R. M. Savithramma, "Survey on Cloud Computing Security," *Lect. Notes Networks Syst.*, vol. 103, pp. 1–6, 2020, doi: 10.1007/978-981-15-2043-3_1.

[8] V. S. Mahalle and A. K. Shahade, "Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm," *2014 Int. Conf. Power, Autom. Commun. INPAC 2014*, no. I, pp. 146–149, 2014, doi: 10.1109/INPAC.2014.6981152.

[9] R. Kiruthika, S. Keerthana, and R. Jeena, "Enhancing Cloud Computing Security using AES Algorithm," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 5, no. 3, pp. 630–635, Mar. 2015.

[10] B. Bindu, L. Kamboj, and P. Luthra, "Secure File Storage in Cloud Computing Using Hybrid Cryptography Algorithm," *Int. J. Adv. Res. Comput. Sci.*, vol. 9, no. 2, pp. 773–776, 2018, doi: 10.26483/ijarcs.v9i2.5916.

[11] M. Batra, P. Dixit, L. Rawat, and R. Khalkar, "Secure File Storage In Cloud Computing Using Hybrid Encryption Algorithm," *Int. J. Comput. Eng. Appl.*, vol. XII, no. VI, pp. 30–36, Jun. 2018.

[12] L. Kumar and N. Badal, "A Review on Hybrid Encryption in Cloud Computing," *Proc. - 2019 4th Int. Conf. Internet Things Smart Innov. Usages, IoT-SIU 2019*, pp. 1–6, 2019, doi: 10.1109/IoT-SIU.2019.8777503.

[13] F. Zhang, Y. Chen, W. Meng, and Q. Wu, "Hybrid Encryption Algorithms for Medical Data Storage Security in Cloud Database," *Int. J. Database Manag. Syst.*, vol. 11, no. 01, pp. 57–73, 2019, doi: 10.5121/ijdms.2019.11104.

[14] G. Viswanath and P. V. Krishna, "Hybrid encryption framework for securing big data storage in multi-cloud environment," *Evol. Intell.*, no. 0123456789, 2020, doi: 10.1007/s12065-020-00404-w.

[15] G. Sai Akhil, G. Kaarthikeyan, D. Aswin, and V. B.S, "DATA SLICING AND HYBRID CRYPTOGRAPHY," *Dogo Rangsang Res. J.*, vol. 10, no. 07, pp. 118–125, 2020.

[16] W. Liu, "Research on cloud computing security problem and strategy," *2012 2nd Int. Conf. Consum. Electron. Commun. Networks, CECNet 2012 - Proc.*, pp. 1216–1219, 2012, doi: 10.1109/CECNet.2012.6202020.

[17] W. Stallings, *Cryptography and Network Security*, Fifth Edit. Prentice Hall Press, USA, 2010.

[18] I. Ahmed, "A brief review: Security issues in cloud computing and their solutions," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 17, no. 6, pp. 2812–2817, 2019, doi: 10.12928/TELKOMNIKA.v17i6.12490.

[19] D. I. G. Amalarethinam and S. E. J. Rajakumari, "A Survey on Security Challenges in Cloud Computing," *J. Phys. Sci.*, vol. 24, pp. 133–141, 2019, doi: 10.1007/s11227-020-03213-1.

[20] P. R. Kumar, P. H. Raj, and P. Jelciana, "Exploring Data Security Issues and Solutions in Cloud Computing," *Procedia Comput. Sci.*, vol. 125, pp. 691–697, 2018, doi: 10.1016/j.procs.2017.12.089.

[21] A. Albugmi, M. O. Alassafi, R. Walters, and G. Wills, "Data security in cloud computing," *5th Int. Conf. Futur. Gener. Commun. Technol. FGCT 2016*, no. October 2017, pp. 55–59, 2016, doi: 10.1109/FGCT.2016.7605062.