Hybrid Cryptography for Cloud Security: Methodologies and Designs

Chapter · January 2022

DOI: 10.1007/978-981-16-2275-5_7

Sherief Murad
Fayoum University
4 PUBLICATIONS **9** CITATIONS

Kamel H Rahouma
Minia University
82 PUBLICATIONS **180** CITATIONS

Hybrid Cryptography for Cloud Security: Methodologies and Designs

Sherief H. Murad and Kamel Hussein Rahouma

Abstract Cloud computing is a trending information technology applied for storing and accessing information over the Internet. Probably, sensitive information is stored on remote servers that are not managed nor controlled by the customers. Therefore, potential attacks may be launched against stored information from either inside the cloud service provider or outsider attackers. Cryptography is the fundamental mechanism that provides enough level of security to the cloud. Hybrid cryptography endeavors to enhance security and performance by integrating more than one cryptographic algorithm. In our study, we conducted a survey on applied hybrid cryptographic models for data security in the cloud between 2013 and 2020. We have presented the design, the implementation methodology, limitations found, and the suggested applications for each proposal. We finalized this paper with a comparison summary table. We hope to make a scientific contribution to secure the cloud.

Keywords Cloud computing · Information security · Symmetric ciphers · Asymmetric ciphers · Hybrid cryptography

1 Introduction

Cloud computing is considered a new model for hosting and providing IT services through the Internet. It allows access to a shared collection of computational resources with minimal interactions with service providers [1]. Cloud services fall into three main categories: software as a service (SaaS) like Gmail, platform as a service (PaaS) like GoogleApp Engine, and infrastructure as a service (IaaS) like Microsoft Azure [2].

Reducing the implementations and maintenance costs, flexibility and scalable infrastructures, and high availability of well-performance applications have motivated governments and individuals to move their data on the cloud servers. These benefits are limited due to several issues concerning security [3, 4].

S. H. Murad (✉) · K. H. Rahouma
Electrical Engineering Department, Faculty of Engineering, Minia University, Minia, Egypt
e-mail: Sh1547@fayoum.edu.eg

D. A. Magdi et al. (eds.), *Digital Transformation Technology*, Lecture Notes in Networks and Systems 224, https://doi.org/10.1007/978-981-16-2275-5_7

Cryptography or secret writing could be utilized to provide confidentiality, integrity, and availability to the data stored or accessed through the cloud. It transforms plain data into unreadable or encrypted form to the unintended users. Both encryption and decryption take place with an extra input called the key [5]. Mainly, cryptography is divided into symmetric-key cryptography and public-key cryptography [6]. Hybrid cryptography implies that two or more cryptographic mechanisms are blended to enhance security. In this paper, we propose a survey study of cryptographic algorithms applied to secure data on the cloud.

2 Literature Survey

Symmetric or secret-key cryptosystems utilize a single key in both encryption and decryption phases. Communicating parties must share this key via a secure channel before any encryption or decryption. An example of symmetric cryptosystems is the data encryption standard (DES), triple-DES (3DES), blowfish, and advanced encryption standard (AES) [5]. On the contrary, asymmetric or public-key cryptosystems utilize two keys; a publically shared key used in encryption, and the other is kept private for decryption. The public key is sent over the network and not necessarily over a secured channel, but the private key must be kept safe from disclosure. An example of asymmetric cryptosystems is Rivest–Shamir–Adleman (RSA), ElGamal, and digital signature algorithm (DSA) [6].

Symmetric and asymmetric cryptosystems have their advantages and disadvantages. Secret key cryptosystems are fast but suffer the secret key exchanging. Public key cryptosystems are secure and solve the key exchange problem but they are slow. Therefore, in practices, hybrid cryptographic schemes, that is a combination of both, are used to exploit the efficiency of symmetric-key algorithms and the simplicity of asymmetric algorithms [4]. The main objective of this approach is to produce a more secure, better performance, and robust algorithm than applying them individually.

A survey on different security issues related to cloud computing was presented by Nigoti et al. [21]. They focused on solving these issues using hybrid cryptographic algorithms and concluded that DES was easier to implement on the cloud than AES. They used RSA and Diffie-Hellman to generate keys to be utilized with the symmetric ciphers.

Another survey was conducted by Sajjan et al. [22] to analyze multilevel encryption used in cloud data security. After various ciphers have been investigated, they implemented a two-layer encryption algorithm composed of DES and RSA ciphers. Their study concluded that applying multilayer encryption provides more security than single-level models.

A novel proposal by Sinchana and Savithramma [4] has examined different hybrid cryptographic models and emphasized the design, implementation, and features of these models. They have enhanced both security and efficiency via integrating symmetric and asymmetric algorithms.

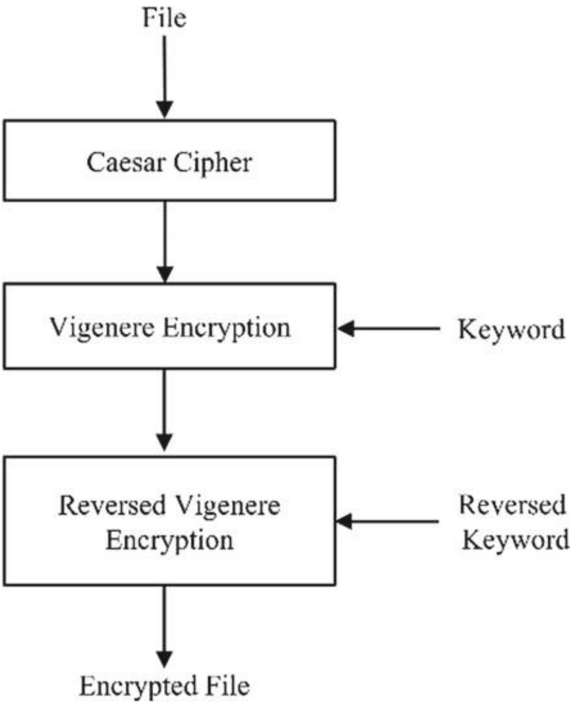
3 Methodology

Hybrid cryptography is mainly categorized into two schemes: The first scheme uses a symmetric algorithm to encrypt data and an asymmetric algorithm to encrypt the secret key. The other scheme performs two layers of symmetric or asymmetric encryption where data is double encrypted by applying either two consecutive symmetric or asymmetric ciphers. Other researchers have applied encryption using symmetric algorithms followed by asymmetric algorithms, both for data encryption, then applied asymmetric algorithms to exchange the secret keys. Many studies used to achieve data security on the cloud as described below:

Sengupta and Jeffrey [7] have proposed a hybrid model to secure cloud infrastructure based on combining Caesar and Vigenere algorithms [5]. In Fig. 1, the plaintext is double encrypted using Caesar cipher. The resulting ciphertext is encrypted using Vigenere cipher with a keyword then encrypted again but with the keyword reversed. The decryption phase is the same as encryption but applied in reversed order.

Vishwanath and Aniket [8] have proposed a hybrid model to enhance data security in the cloud, based on RSA and AES algorithms. As shown in Fig. 2, the data is encrypted using AES then encrypted again using RSA. The system timing is used in the key generation phase.

Fig. 1 Hybrid cryptographic model proposed by Sengupta and Jeffrey



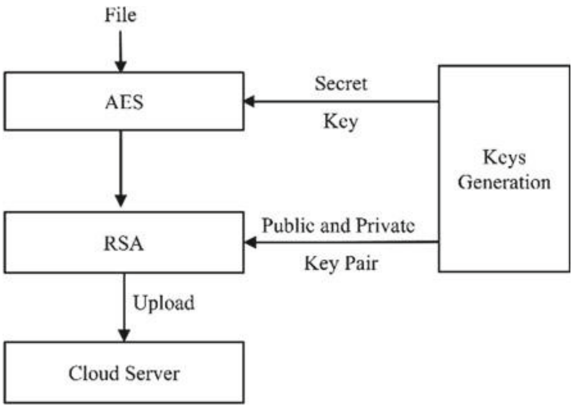


Fig. 2 Hybrid cryptographic model proposed by Vishwanath and Aniket

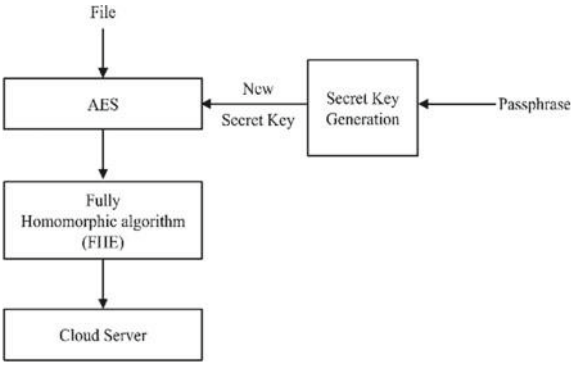


Fig. 3 Hybrid cryptographic model proposed by Atewologun et al.

Atewologun et al. [9] have proposed a hybrid model to provide secure transmission of data on the cloud by using AES and fully homomorphic encryption (FHE) algorithms. As shown described in Fig. 3, the file is firstly encrypted using AES, and the resulting ciphertext is encrypted using FHE cipher. The secret key is derived from a passphrase provided by the sender.

Punam and Aruna [10] proposed a hybrid model to secure cloud storage using AES, blowfish, RC6, and byte rotation algorithm (BRA) ciphers. In Fig. 4, data is split into eight parts, each part is encrypted using a different cipher. Encrypted blocks and secret keys are embedded into an image then uploaded to the cloud using the least significant bit steganography [5, 6, 16].

Adviti and Jyoti [11] have enhanced cloud security using Blowfish and MD5 hybrid model. In Fig. 5, data is encrypted using blowfish cipher, and integrity is provided with message digest 5 (MD5). Finally, encrypted parts and MD are uploaded to the cloud.

Rohini and Sharma [12] have proposed a hybrid model to secure data over the cloud, based on RSA and hashed message authentication code (HMAC) [5] ciphers. As shown in Fig. 6, the data is encrypted using RSA cipher, and the HMAC is

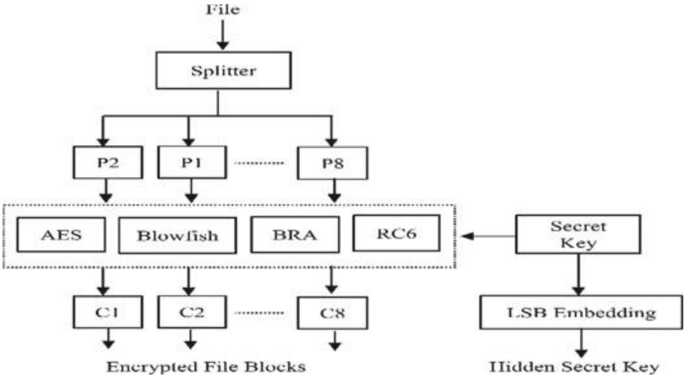


Fig. 4 Hybrid cryptographic model proposed by Punam and Aruna

Fig. 5 Hybrid cryptographic model proposed by Adviti and Jyoti

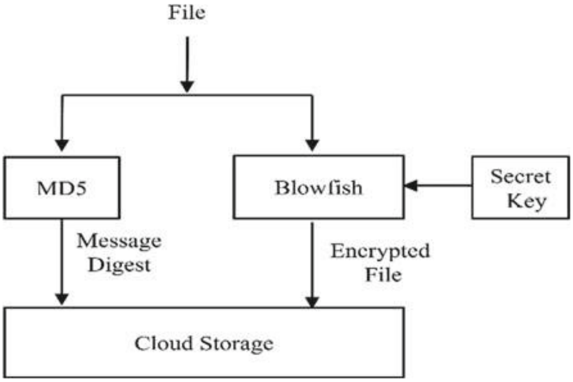
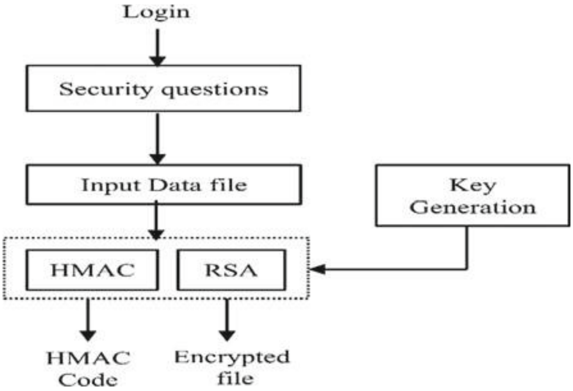


Fig. 6 Hybrid cryptographic model proposed by Rohini and Sharma

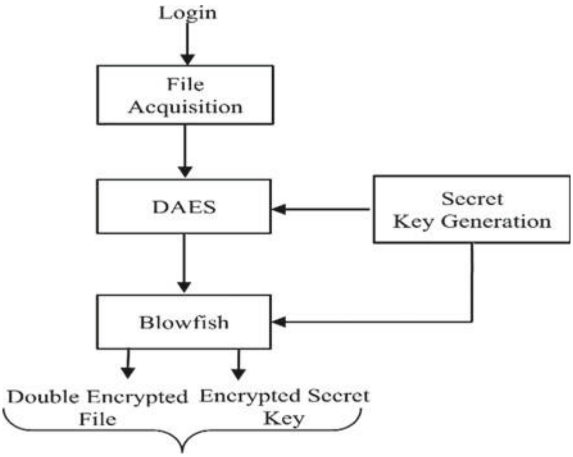


generated to provide integrity. Both message digest and encrypted data are uploaded to the cloud.

Salma et al. [13] have proposed a hybrid model to enhance cloud data security based on blowfish and AES ciphers. As shown in Fig. 7, after a successful login, the uploaded file is twice encrypted using dynamic AES (DAES) then blowfish. Secret keys used are encrypted using blowfish. All encrypted data and keys are uploaded to the cloud.

Sherief et al. [14] have proposed a hybrid model to enhance data security based on blowfish, visual cryptography [15], and steganography. As shown in Fig. 8, data is first encrypted using blowfish followed by visual cryptography, producing two shares. These shares are then embedded into two images using LSB before transmission.

Fig. 7 Hybrid cryptographic model proposed by Salma et al.



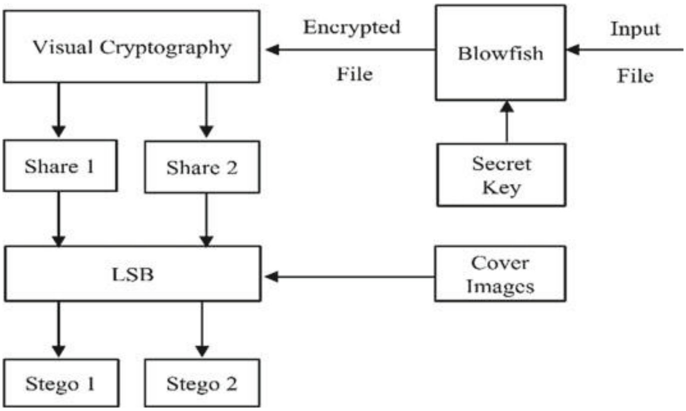


Fig. 8 Hybrid cryptographic model proposed by Sherief et al.

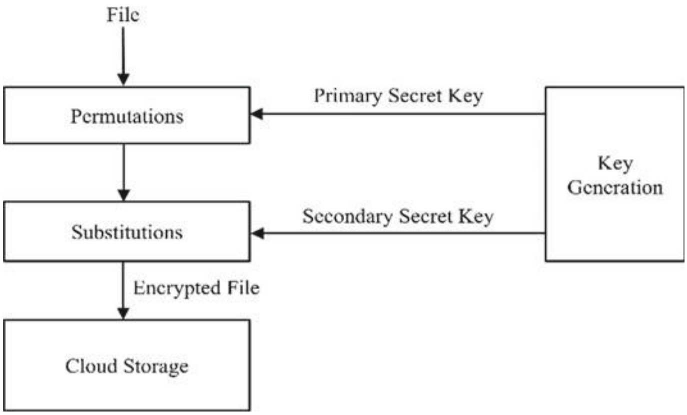


Fig. 9 Hybrid cryptographic model proposed by Shweta and Ashish

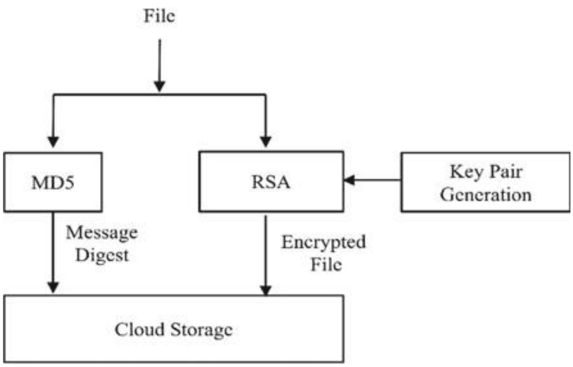
Shweta and Ashish [16] have proposed a hybrid model to secure data on the cloud based on transposition and substitution algorithms. As shown in Fig. 9, the input file is permuted using a primary secret key. Before uploading to the cloud, another encryption is made using substitution cipher with a secondary secret key. The auditor is responsible for generating the secret keys and sharing them between the cloud users.

A proposal to secure robots on the cloud by Huili et al. [17] based on the hybrid of RSA and MD5 ciphers. As shown in Fig. 10, data is first encrypted with RSA cipher. Integrity is achieved via MD5. Finally, the encrypted data and message digest are uploaded to the cloud.

Anuj et al. [18] introduced another hybrid model for cloud storage security consisting of RSA and DES ciphers. As shown in Fig. 11, data is double encrypted using RSA then DES cipher.

Another cloud storage security model was implemented by Shivam et al. [19] consisted of AES, RC4 [6], and DES ciphers. As shown in Fig. 12, the original file

Fig. 10 Hybrid cryptographic model proposed by Huili et al.



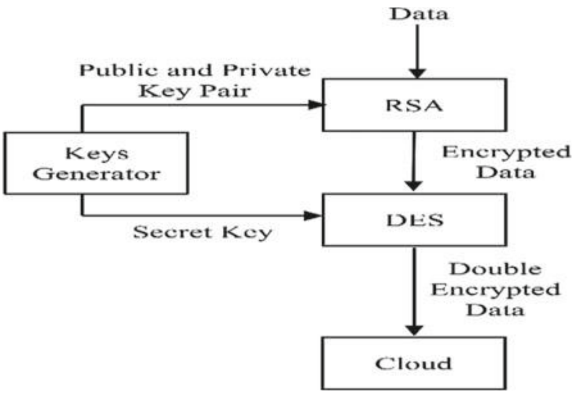


Fig. 11 Hybrid cryptographic model proposed by Anuj et al.

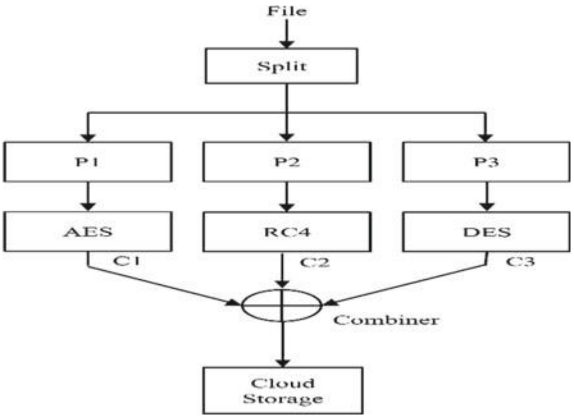


Fig. 12 Hybrid cryptographic model proposed by Shivam et al.

is broken into three equal chunks, and each will be encrypted using a distinct cipher. Finally, encrypted parts are merge and uploaded to the cloud storage server.

A hybrid model consists of AES, 3DES [6], RSA ciphers combined with LSB steganography was presented by Vinay et al. [20]. As shown in Fig. 13, two-layer encryption is achieved via AES then 3DES ciphers. RSA cipher is employed to encrypt secret keys. Finally, both encrypted file and keys are hidden into an image using the LSB insertion method.

4 Comparison Between Proposed Models

A chronological summary of the studied hybrid models proposed from the oldest to the most recent within the period from 2013 to 2020. In Table 1, we have presented a comparison between the proposed models based on hybrid cryptography in terms

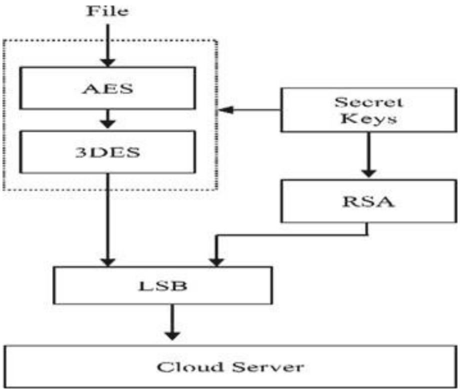


Fig. 13 Hybrid cryptographic model proposed by Vinay et al.

of elements composing the model, features achieved, limitations, and suggested applications for each proposal.

5 Conclusions

After studying all of the trending hybrid cryptographic models, we came up with the conclusion that data security is the most considerable topic related to cloud computing technology. To overcome security limitations, the integration between symmetric and asymmetric cryptosystems is employed. By applying the hybrid of different encryption algorithms such as DES, 3DES, AES, Blowfish, RSA, and SHA, we would try to secure sensitive data on the cloud. Our study also concludes that hybrid cryptography enhances the performance and adds more security levels to the data compared to applying these algorithms individually. All of the examined studies have benefits and some drawbacks. As a future direction, we aim to overcome these drawbacks to enhance security and performance.

Table 1 Summary of the trending studies based on hybrid cryptography

References	Elements	Features achieved	Limitations found	Applications
[7]	Caesar and Vigenere	• More security	• Vigenere key and message must be equal in length • Caesar is not secure	Cloud infrastructure
[8]	AES and RSA	• Confidentiality, integrity, and reliability	• RSA has more computations cost	Cloud storage
[9]	AES and FHE	• Confidentiality, integrity • Malware attack protection	• Not compatible with all cloud services	Cloud storage
[10]	AES, Blowfish, RC6, BRA	• Less delay (multithreading) • Confidentiality, integrity, and authentication	• Secret keys could be compromised or altered	Cloud storage
[11]	Blowfish, MD5	• Confidentiality and integrity	• MD5 is adequately secure • Key distribution issue	Cloud storage
[12]	RSA and HMAC	• Confidentiality and integrity	• RSA takes a long time and a large memory size	Cloud storage
[13]	DAES, and Blowfish	• Brute force and algebraic attack protection	• Key distribution issue • Encryption is slow	File and web servers—social media programs
[14]	Blowfish-Visual Cryptography, LSB	• Very secure • Fingerprint authentication • Robust against steganalysis	• Physical keys distribution • Almost used for documents files	Law enforcement
[16]	Permutation-substitution	• More fast and efficient than asymmetric-Brute-force attack protection	• Key distribution issue • No authentication	Cloud storage

(continued)

Table 1 (continued)

References	Elements	Features achieved	Limitations found	Applications
[17]	RSA and MD5	• Confidentiality, integrity, and authentication	• RSA computations cost • MD5 is adequately secure • RSA is not for large files	Cloud intelligent robot
[18]	RSA and DES	• Provide security to IoT data	• DES is slow and less secure • RSA computations cost • RSA is not for IoT	IoT applications on the cloud
[19]	AES, RC4, and DES	• It is better for bigger file sizes • More efficient compared to AES alone	• RC4 is adequately secure • DES is not secure enough • Key distribution issue	Cloud storage
[20]	AES, 3DES, RSA, and LSB	• Higher security due to double encryption	• Long encryption time • 3DES is very slow	Banking and private sectors

References

1. Badger ML, Grance T, Patt-Corner R, Voas JM (2012) Cloud computing synopsis and recommendations. National Institute of Standards & Technology
2. Kyriazis D, Voulodimos A, Gogouvitis SV, Varvarigou TA (2013) Data intensive storage services for cloud environments. Business Science Reference
3. Singh V, Pandey SK (2020) Cloud computing: vulnerability and threat indications. In: Performance management of integrated systems and its applications in software engineering. Springer, Singapore, pp 11–20
4. Sinchana MK, Savithramma RM (2020) Survey on cloud computing security. In: Innovations in computer science and engineering. Springer, Singapore, pp 1–6
5. Forouzan BA (2007) Cryptography and network security. McGraw-Hill, Inc.
6. Schneier B (2007) Applied cryptography: protocols, algorithms, and source code. C. John Wiley & Sons
7. Sengupta N, Holmes J (2013) Designing of cryptography based security system for cloud computing. In: 2013 international conference on cloud & ubiquitous computing & emerging technologies. IEEE, pp 52–57

8. Mahalle VS, Shahade AK (2014) Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm. In: 2014 International Conference on Power, Automation and Communication (INPAC). IEEE, pp 146–149
9. Olumide A, Alsadoon A, Prasad PWC, Pham L (2015) A hybrid encryption model for secure cloud computing. In: 2015 13th International Conference on ICT and Knowledge Engineering (ICT & Knowledge Engineering 2015). IEEE, pp 24–32
10. Maitri PV, Verma A (2016) Secure file storage in cloud computing using hybrid cryptography algorithm. In: 2016 international conference on wireless communications, signal processing and networking (WiSPNET). IEEE, pp 1635–1638
11. Chauhan A, Gupta J (2017) A novel technique of cloud security based on hybrid encryption by Blowfish and MD5. In: 2017 4th International conference on signal processing, computing and control (ISPCC). IEEE, pp 349–355
12. Sharma T (2018) Proposed hybrid RSA algorithm for cloud computing. In: 2018 2nd international conference on inventive systems and control (ICISC), pp 60–64. IEEE
13. Salma RF, Khaizuran Abdullah R, Darwis H (2018) Enhancing cloud data security using hybrid of advanced encryption standard and blowfish encryption algorithms. In: 2018 2nd East Indonesia Conference on Computer and Information Technology (EIConCIT). IEEE, pp 18–23
14. Murad SH, Gody AM, Barakat TM (2019) Enhanced security of symmetric encryption using combination of steganography with visual cryptography. arXiv preprint arXiv: 1902.11167
15. Naor M, Shamir A (1994) Visual cryptography. In: Workshop on the theory and application of cryptographic techniques. Springer, Berlin, Heidelberg, pp 1–12
16. Kaushik S, Patel A (2019) Secure cloud data using hybrid cryptographic scheme. In: 2019 4th international conference on internet of things: smart innovation and usages (IoT-SIU), pp 1–6. IEEE
17. Cai H, Liu X, Cangelosi A (2019) Security of cloud intelligent robot based on RSA algorithm and digital signature. In: 2019 IEEE symposium series on computational intelligence (SSCI). IEEE, pp 1453–1456
18. Kumar A, Jain V, Yadav A (2020) A new approach for security in cloud data storage for IOT applications using hybrid cryptography technique. In: 2020 international conference on power electronics & IoT applications in renewable energy and its control (PARC), pp 514–517. IEEE
19. Sharma S, Singla K, Rathee G, Saini H (2020) A hybrid cryptographic technique for file storage mechanism over cloud. In: First international conference on sustainable technologies for computational intelligence, pp 241–256. Springer, Singapore
20. Poduval V, Koul A, Rebello D, Bhat K, Wahul RM (2020) Cloud based secure storage of files using hybrid cryptography and image steganography. (IJRTE) Int J Recent Technol Eng 8(6)
21. Nigoti R, Jhuria M, Singh S (2013) A survey of cryptographic algorithms for cloud computing
22. Sajjan RS, Ghorpade V, Dalimbkar V (2016) A survey paper on data security in cloud computing. Int J Comput Sci Eng (IJCSE) 4(4):9–13