JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Security Model for the Cloud, Applying a Hybrid of Cryptography and Steganography

[1]Bokhari Nabil, [2]José Javier Martínez Herráiz

[1]Student of Information and Knowledge Engineering
[2] Professor Doctor of Computer Science
[1] Information and Knowledge Engineering Department
[1] University of Alcala, Madrid, Spain

Abstract: Cloud computing has revolutionized digital business by offering highly cost-effective, scalable, and flexible on-demand services and resources. However, data transmitted and stored in a cloud computing environment are vulnerable to various cybersecurity attacks, including denial of service attacks and SQL injections. Successful attacks in the cloud may lead to massive data loss, theft, or manipulation by unauthorized users. This study leverages the design science research methodology (DSRM) to develop, design, and evaluate a security model to enhance data security and privacy in the cloud. The security model leverages a hybrid of cryptography and steganography to strengthen security in a cloud computing environment. The cryptography algorithms Advanced Encryption Standard (AES) and Rivest Shamir Adleman (RSA) are combined with the least significant bit (LSB) steganographic technique. The combination of cryptography, steganography, data backup, and recovery provides an indomitable and resilient security model for fast-evolving cloud computing.

Key word: cryptography, steganography, security, data privacy, cybersecurity, advanced encryption standard, Rivest Shamir Adleman, least significant bit, encryption, cloud computing, design science research, cyberattacks

1. INTRODUCTION

Cloud computing is a technological advancement that has significantly transformed the world. Businesses can access on-demand cloud products and services on various models, including software, platforms, and infrastructure. Cloud computing is cost-effective, efficient, scalable, and reliable, especially for large-scale data storage. Despite these massive benefits, cloud computing is vulnerable to cybersecurity attacks and threats (Brumfield and Haugli, 2021). According to Thabit et al. (2021), attacks prevalent in a cloud computing environment include Denial of Service (DoS), Zombie, Phishing, and Man-in-the-Middle attacks. The proposed data security model leverages a hybrid of cryptography, steganography, and data backup and recovery to enhance security in cloud computing.

2. BACKGROUND

2.1. CLOUD CYBERSECURITY

Cloud computing security is an issue that has attracted the attention of various stakeholders recently. Several studies have been formulated and executed to investigate various cybersecurity issues related to cloud computing (Golightly et al., 2022). Recent studies have focused on exploring how innovative techniques such as cryptography can enhance security in cloud computing. Experts have experimented with how a hybrid of various symmetrical and asymmetrical encryption algorithms can be effectively used to improve data security and privacy. According to Thabit et al. (2021), combining algorithms such as RSA, AES, and Eclipse IDA can enhance the privacy of data stored in cloud servers. Figure 1 shows the cloud computing service models: IaaS, PaaS, and SaaS (Butt et al., 2020).

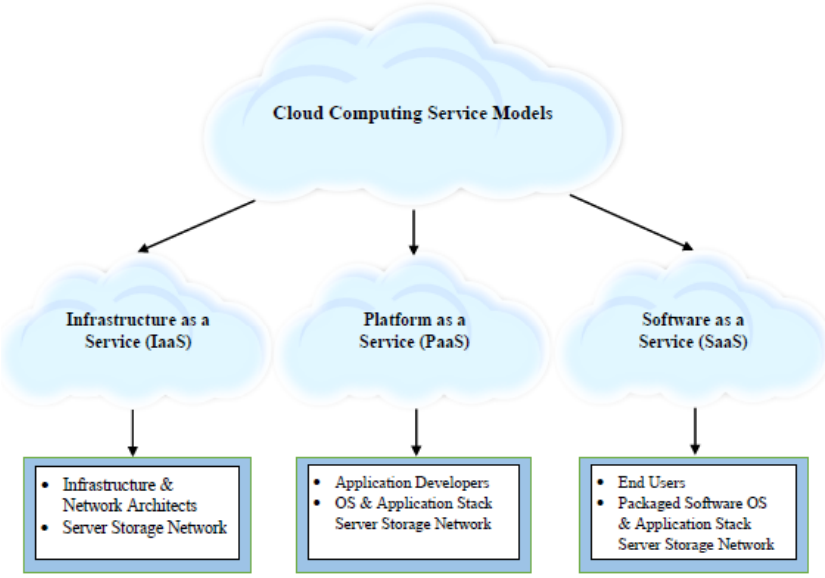

Figure 1. Service models for the cloud (Butt et al., 2020, p.5).

Figure 2 shows the basic security requirements in cloud computing suggested by NIST. NIST emphasizes that confidentiality, availability, and integrity must be the fundamental building blocks of cloud computing.

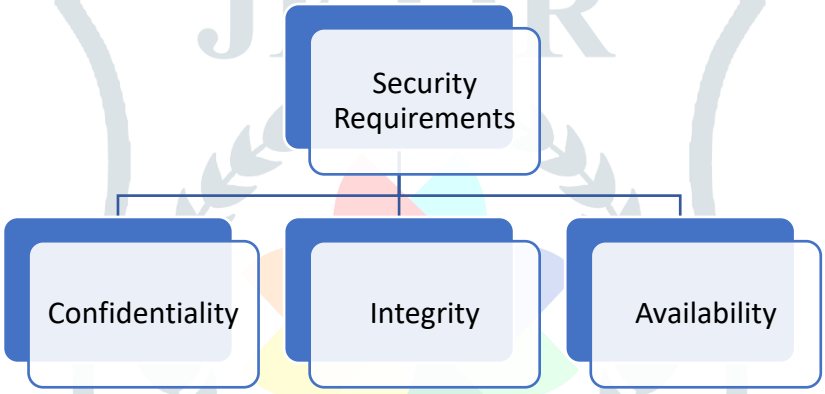

Figure 2. Basic cloud security requirement (Thabit et al., 2021).

2.2. CRYPTOGRAPHY

Cryptography focuses on securing information and communication using encryption and decryption techniques and methods (Adee & Mouratidis, 2022). Sensitive data such as financial transactions and credit cards must be encrypted to enhance their security against unauthorized access (Thabit et al., 2021). Dotson (2019) describes encryption as the silver bullet of data protection. Everyone desires that everything be encrypted for enhanced security, especially in a cloud computing environment. However, the process of encrypting and decrypting is complex because data can be in three states: motion, use, and rest (Dotson, 2019). Encrypting data in use is relatively new and mainly employed in high-security environments. Encrypting data at rest is the most complex. Once data have been encrypted, the encryption and decryption keys must also be secured.

Figure 3 provides an overview of different types of cryptography, including classical and modern. The RSA used in the proposed security model was asymmetrical.

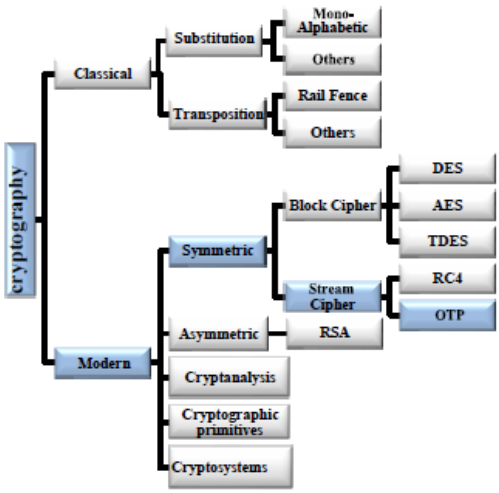

Figure 3. Types of cryptography (Osman et al., 2022, p. 329).

2.2.1. Advanced Encryption Standard (AES)

NIST officialized the Advanced Encryption Algorithm (AES) in 2001. The symmetric block cipher algorithm has 128, 192, and 256 bits, with variable lengths. The algorithm enhanced performance and security is comparable to DES. The encryption key length determines the rounds (Shaheen, 2021). The algorithm runs 14 rounds for 256 bits encryption keys.
Figure 4 shows the AES model for the 128-bit encryption key. The algorithm has ten rounds as indicated.

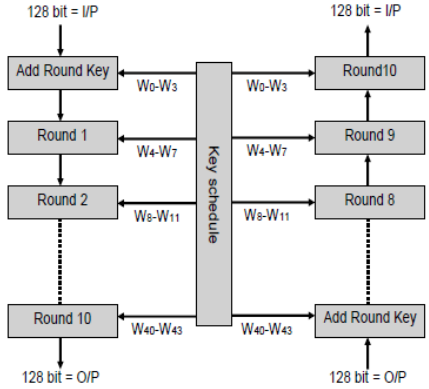

Figure 4. AES model for a 128-bit encryption key (Shaheen, 2021, p. 8).

Figure 5 shows the four steps in each round. The substitute byte is a forward substitution process consisting of a 16*16 S-box to determine the replacement byte.

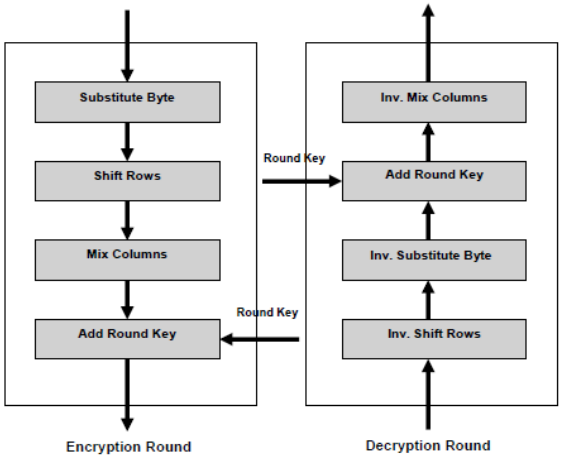

Figure 5. Encryption and decryption rounds (Shaheen, 2021, p. 8)

2.2.2. Rivest Shamir Adleman (RSA)

RSA encryption is based on the principle that any data can be represented as numbers, and large numbers are complex to factorize. As a result, a mathematical process is required to encrypt and decrypt numbers (Wilkinson, 2006).
The keys used were pairs of numbers (e,n) and (d,n), where e is encryption and d is decryption.
Two prime numbers (n) are required in RSA encryption.

Table 1 shows the lowest sample prime numbers selected for the RSA algorithm testing.

Table 1. Prime numbers for the RSA process.

Prime 1	**7**
Prime 2	11
n = prime 1 * prime 2	77
dp = decremented_product	60

The message was encrypted using the following formula:

$$C = M^e \bmod n$$

where M is the message unit and C is the cipher unit (Wilkinson, 2006)

2.3. Steganography

Steganography is the concept of hiding messages during transmission to prevent discovery by the naked eye. Technically, steganography is a primordial form of hidden communication. An effective steganography scheme must meet the parameters of imperceptibility, capacity, and robustness. Imperceptibility means the stego file is not discernible (Hambouz et al., 2019, as cited in Pramanik et al., 2021). Capacity measures the complete secret information, while robustness indicates the impossibility of extracting private information (Duan et al., 2020; Eyssa, Abdelsamie, and Abdelnaiem, 2020, as cited in Pramanik et al., 2021).
Figure 6 shows the process of the steganography system. The final output is the target secret image.

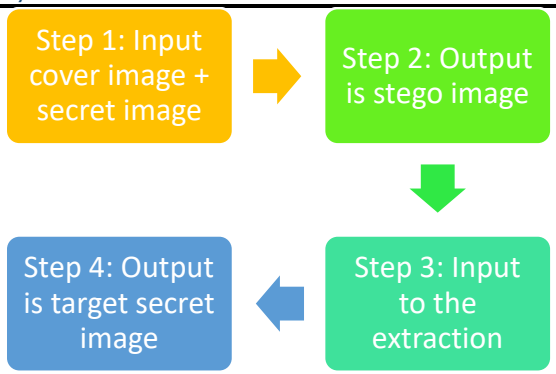

Figure 6. Steganography system process (Pramanik et al., 2021).

According to Pramanik et al. (2021), there are four methods of steganography: image, audio, text, and video. Audio, text, and video hide the secret data in audio, text, and video steganography, respectively (Kuri and Rafi, 2020).

Figure 7 shows the different types of steganography. The proposed security model leveraged the LSB technique designed for spatial domains and images as the cover media.

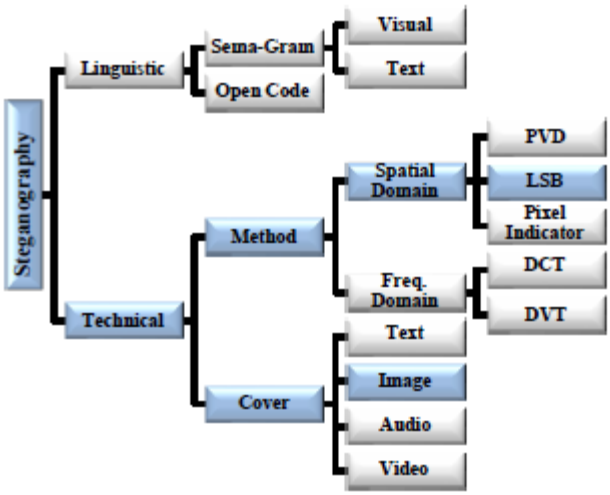

Figure 7. Types of steganography (Osman et al., 2022, p. 329).

Image steganography was applied to design and develop the proposed data security model. The fundamental representation of a digital image is pixels. The least significant bit (LSB) technique is an example of an effective method for executing image steganography. A photo can be binary, greyscale, or color. A greyscale image of 8-bit has two power 8 = 256 shades of grey.
Histogram-based image steganography uses the following 4*4 matrix:
Figure 8 is the 4*4 transformation equation.

$$t_{ij} = f(x) = \begin{cases} \frac{1}{\sqrt{N}} \; if i = 0 \\ \frac{\sqrt{2}}{\sqrt{N}} \cos[(2j+1)i\Pi) \end{cases} /2N] if i > 0$$

(Pramanik et al., 2021, p.12).

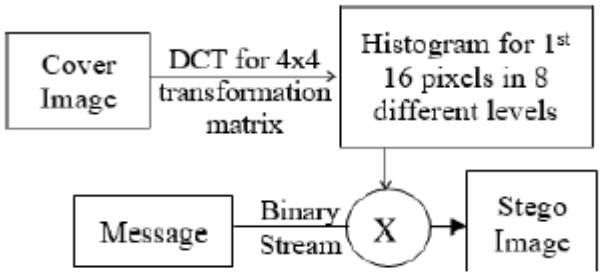

Figure 8. Stego image generation procedure (Pramanik et al., 2021, p. 13).

Figure 8 shows the Stego image generation procedure. The cover image was applied DCT for the 4*4 transformation matrix.

2.4. Research Aim and Objectives

The proposed data security model aimed to enhance privacy and security in cloud computing, leveraging a hybrid of cryptographic algorithms and steganographic techniques. The cryptographic algorithms proposed are the Advanced Encryption Algorithm (AES) and Rivest Shamir Adleman (RSA). The proposed steganography technique is the least significant bit (LSB). The revised DSR methodology was used to design, develop, and evaluate the model (Muntean and Militaru, 2022). The security model secures data using cryptographic algorithms, adds an extra security layer using steganography, and implements backup and data recovery. The study's primary objective was to develop a security model using a hybrid of encryption algorithms and steganography.

3. Related Work

This study was motivated by several recently published studies exploring innovative strategies to enhance security in cloud computing. Most recent studies have examined how a combination of encryption algorithms can be successfully deployed with other methods and techniques (Astuti, Aribowo, and Saputra, 2020). Thabit et al. (2021) provided a comprehensive systematic discussion and critical analysis of various recent studies that have successfully combined cryptography algorithms and techniques to enhance security in the cloud. A hybrid of the RSA algorithm, RSA Digital Signature, and XOR operating algorithms was also found to improve safety in a cloud computing environment (Thabit et al., 2021). A study by Ngnie Sighom, Zhang, and You (2017) explored how top-ranked cloud computing providers, such as Google and Microsoft, use cryptographic algorithms to enhance the security of data transmitted and stored in a cloud computing environment. Timothy and Santra (2017) compared the performance of SHA-512, AES-256, and IDAs in encrypting and decrypting data. Current studies have innovatively combined various algorithms and achieved different security results. However, the findings broadly show that combining multiple cryptographic algorithms and advanced techniques, such as steganography, significantly enhances security in a cloud computing environment.

Recent studies have also explored how machine learning can be deployed to predict, detect, and prevent attacks in cloud computing. Nassif et al. (2021) analyzed 63 studies examining how different machine learning algorithms and techniques can be effectively used to detect and prevent attacks in the cloud. The survey by Nassif et al. (2021) found that data privacy and distributed denial of service attacks (DDoS) are prevalent in a cloud computing environment.

Figure 9 shows the popular hybrid machine learning models that enhance data security in a cloud computing environment.

Hybrid Model	Reference
Linear Regression + Random Forest	A2
SVM + Linear SVM	A11
Random Forest + Linear Regression	A13
KNN + SVM	A37
SVM + Fuzzy C-Means	A38
SVM + Random Forest	A40
ANN + KNN	A46
Neural Network + Naïve Bayes + Decision Tree	A49
SVM+ Neural Network	A54
CNN + LSTM	A57

Figure 9. Hybrid machine learning models (Nassif et al., 2021, p. 20724).

Adee and Mouratidis (2022) reviewed various security models currently used in cloud computing. Their analysis showed the cryptography algorithms, steganographic technique, backup and recovery, and data-sharing techniques used in each model.

Figure 10 shows our review of security models used currently in cloud computing. For instance, the private cloud for SaaS uses AES and LSB video steganography. Visually Imperceptible Hybrid Crypto Steganography (VIHCS) leverages a hybrid of RSA and AES algorithms. The steganography techniques used are LSB and 2D-Discrete Wavelet Transform (2D-DWT-2L) (Adee & Mouratidis, 2022).

Security Model	Cryptographic Algorithms	Steganography Technique	Backup and Recovery	Data Share
The private cloud for software as a service (SaaS)	AES	LSB video technique of steganography	No mention of data backups and recovery	Deliver services to end users in a pay-as-you-go manner
Image-Based Steganography Using Pseudorandom Sequence Generator Function and DCT Coefficients	No clear mention of cryptographic algorithms	LSB Image steganography using pseudo-random sequence function with 2D-DCT	No mention of data backups and recovery	Provide services in a pay-as-you-go manner
The hybrid encryption in Bluetooth innovation and in cloud computing	AES, FHE	Steganography not applied	Maintain data redundancy and security	Bluetooth
Data security in cloud computing using Elliptic Curve Cryptography	ECC	Steganography not applied	No mention of backups and recovery	Data share not specified
Visually Imperceptible Hybrid Crypto Steganography (VIHCS) model	AES, RSA	2D-Discrete Wavelet Transform (2D-DWT-2L) AGA-OPAP with LSB	No clear mention of backups and recovery	Combined cryptosystems with Steganography for data transmission
RGB shuffling method using combined steganography and cryptography	RGB shuffling algorithm and Message Digest 5 (MD5) algorithm	LSB image, video, or audio technique of steganography	Mention of image recovery in one of the phases	No specific mention of data sharing using the model

Figure 10. Review of security models in cloud computing (Adee & Mouratidis, 2022, p. 23).

4. Materials and Methods

4.1. DSR Methodology

The Design Science Research Methodology (DSRM) was applied to design and develop the proposed data security model for cloud computing. The DSR methodology, revised by Peffers et al. (2020), outlines six steps to follow to design, develop, and evaluate an artifact. According to De Sordi (2021), an artifact can be a construct, model, method, or instantiation.

Figure 11 presents an overview of the DSR process followed to design, develop, and evaluate the proposed data security model for cloud computing.

Figure 11. DSR process.

4.2. Defining Functional and Non-Functional Requirements

Functional requirements outline what the data security model will achieve for the users. The unique functional requirement of the model is to enhance data privacy and security in cloud computing using encryption. The model combines RSA and EAS algorithms to strengthen security. The model also adds an extra layer of protection using the LSB technique's image steganography. Non-functional requirements show how the model achieves its functions. The security model will be simple, scalable, and reliable in enhancing security in a cloud computing environment. The functional and non-functional requirements must address the needs and preferences of the unique users of the model. Refer to Figure 12 for the model requirements.

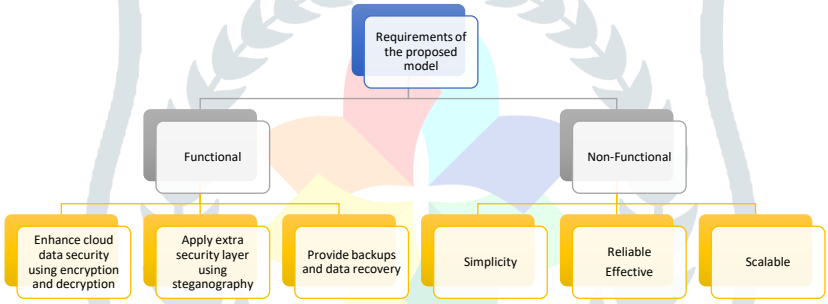

Figure 12. Requirements.

5. Results

5.1. Design and Develop the Model

The security model designed and developed using the DSR methodology enhances privacy and security in a cloud computing environment through the following three steps:

5.2. Step 1: Data Security and Privacy using Cryptography

Firstly, the security model applies AES and RSA cryptographic algorithms to encrypt and decrypt data in the cloud. Data transmitted and stored in the cloud are vulnerable to cyberattacks and threats. Successful attacks may lead to data loss, theft, and manipulation by unauthorized users (Prajapati & Shah, 2020; Butt et al., 2020). The security model generates RSA pair-public and public keys before further encryption by the AES algorithm.

Figure 13 shows the specific process of generating the RSA pair-public and private keys for encryption. The information is further secured using AES algorithm encryption. A third-party critical management service distributes the private keys to decrypt the enciphered message.

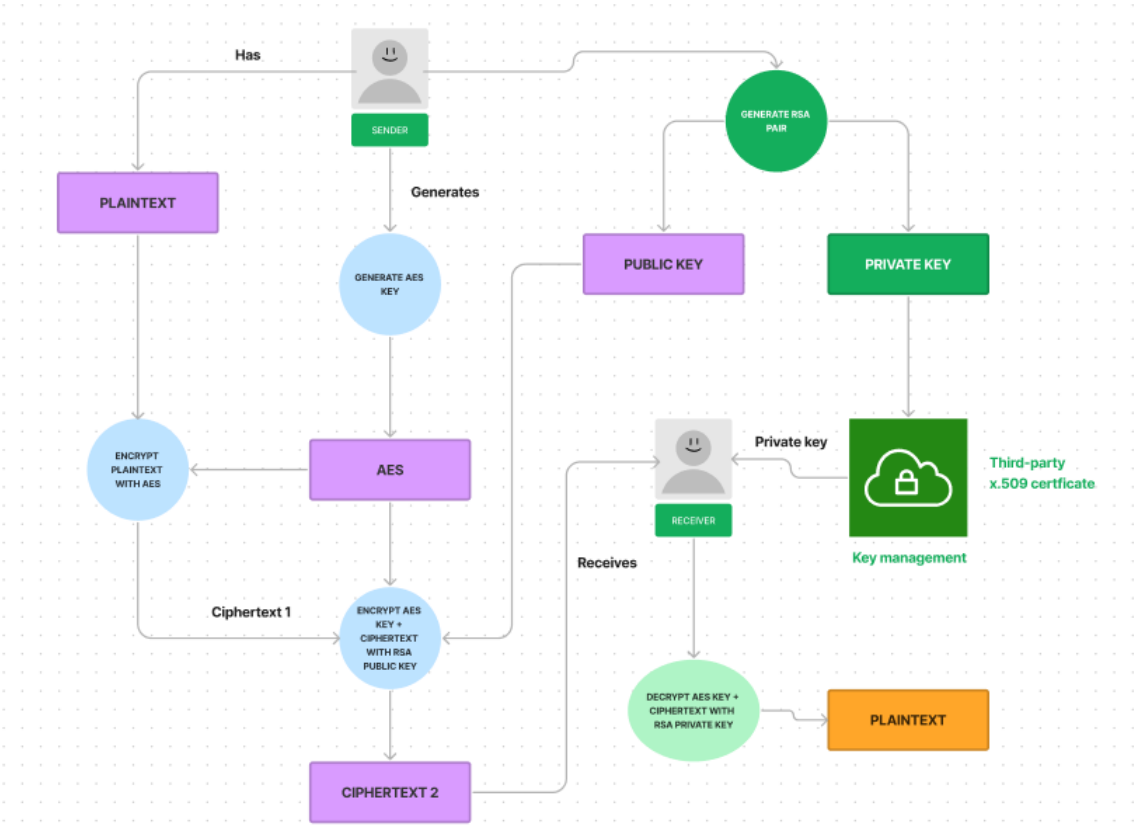

Figure 13. Step 1: Cryptography.

5.3. Step 2: Extra Security Layer with Steganography

Secondly, using steganography, the security model adds an extra layer of security to the encrypted data. The LSB and histogram image steganography techniques are used in this stage.

Figure 14 shows how steganography adds an extra layer of security to the model. LSB steganography is used to reinforce the security of the AES key and the cyphertext encrypted using the RSA pair generated in the previous stage. The LSB method transforms the ciphertext and the AES key into secret messages before transmission in a cloud computing environment.

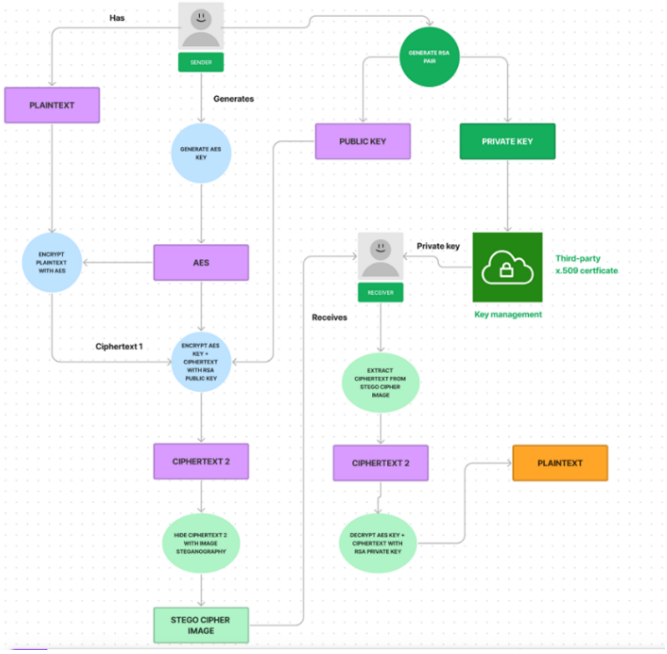

Figure 14. Adding an extra layer using steganography.

5.4. Step 3: Backup and Recovery

The final step of the data security model is backup and recovery. The security model supports incremental, complete, and differentiation backups. The Stego image and ciphertext generated in the previous sections are backed up for more security (Zuo et al., 2021).

Figure 15 shows the entire process of the security model. The security model begins by applying cryptography to generate the RSA pair-public and private keys for encrypting and decrypting data in a cloud computing environment. Encryption is further enhanced using the AES algorithm and steganography. Finally, the Stego image and ciphertext are backed securely in the cloud to improve security and privacy. The combination

of cryptography, steganography, and backup and recovery provides an indomitable security model for the fast-evolving cloud computing environment.

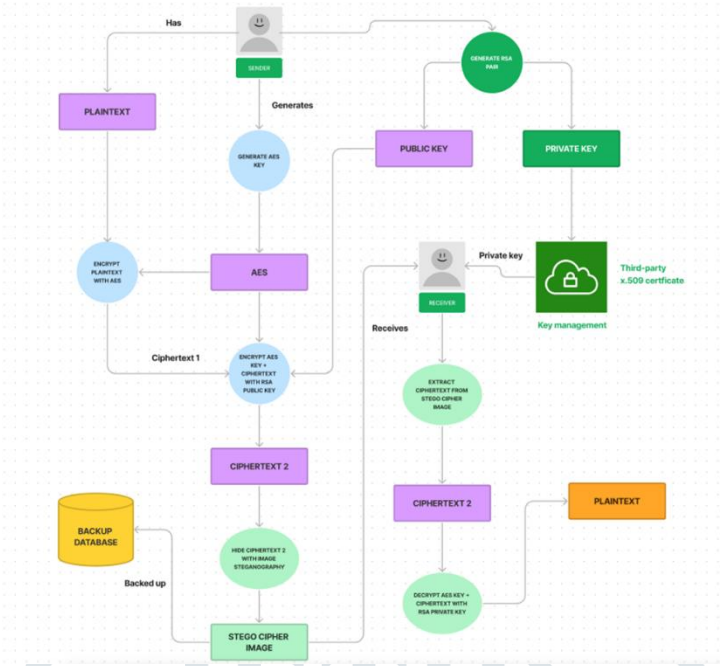

Figure 15. Backup and recovery.

6. Conclusions

The data security model leverages a hybrid of cryptography, steganography, and data backup and recovery to enhance security in a cloud computing environment. The combination of the RSA algorithm, AES algorithm, and LSB technique provides an indomitable security model for the cloud. Adding an extra layer with steganography and backing up the keys and the cyphertext maximize the resilience of data against various cyberattacks, including denial of service attacks and SQL injections. Though the design and development of the security model were successful, this study has a few limitations. Firstly, the design and development stages of the DSR methodology did not involve system users directly. The functional and non-functional requirements of the proposed model are primarily based on an extensive review of related studies. The DSR methodology has also been criticized for lacking critical realism, which should be the fundamental philosophical underpinning of research in information systems.

7. Recommendations for Future Research

The findings of this study showed how a hybrid of cryptography, steganography, and backup and recovery can enhance data security and privacy in a cloud computing environment. Future research should leverage mixed-method research to explore how other cryptographic algorithms and steganography techniques can be combined to enhance security in cloud computing. Combining qualitative and quantitative methods will yield more comprehensive results (Saunders, Lewis, & Thornhill, 2009). Future research also needs to investigate how machine learning, artificial intelligence, and emerging technologies can be leveraged to enhance security in cloud computing. Integrating Python programming in such endeavors will also play a critical role in strengthening cloud cybersecurity. Future studies should also investigate the effectiveness of new algorithms, such as Fully Homomorphic Encryption (FHE), in securing data in a cloud computing model (Pulido-Gaytan et al., 2021).

References

[1] Adee, R; Mouratidis, H. A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. *Sensors* 2022, *22*,1109.

[2] Astuti, N.R.D.P.; Aribowo EANDSaputra, E. Data security improvements on cloud computing using cryptography and steganography. *IOP Conf. Ser. Mater. Sci. Eng.* 2020, *821*, 012041.

[3] Butt, U.A.; Mehmood, M.; Shah, S.B.H.; Amin, R.; Shaukat, M.W.; Raza, S.M.; Suh, D.Y.; Piran, M.J. A review of machine learning algorithms for cloud computing security. *Electronics* 2020, *9*, 1379.

[4] Brumfield, C.; Haugli, B. *Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework*; John Wiley & Sons, Inc.: New York, NY, USA, 2021.

[5] De Sordi, J.O. Theory Development from Artifacts. In *Design Science Research Methodology*; Palgrave Macmillan: Cham, Switzerland, 2021; pp. 79–109.

[6] Dotson, C. *Practical Cloud Security: A Guide for Secure Design and Deployment*; O'Reilly Media: Sebastopol, CA, USA, 2019.

[7] Golightly, L.; Chang, V.; Xu, Q.A.; Gao, X.; Liu, B.S. Adoption of cloud computing as innovation in the organization. *International J. Eng. Bus. Manag.* 2022, *14*, 18479790221093992.

[8] Kuri, J.; Rafi, M. Securing data in Internet of Things (IoT) using cryptography and steganography techniques. *IEEE Trans. Syst. Man Cybern. Syst.* 2020, *50*, 73–80.

[9] Muntean, M.; Militaru, F.D. Design science research framework for performance analysis using machine learning techniques. *Electronics* 2022, *11*, 2504.

[10] Nassif, A.B.; Talib, M.A.; Nasir, Q.; Albadani, H.; Dakalbab, F.M. Machine learning for cloud security: a systematic review. *IEEE Access* 2021, *9*, 20717–20735.
[11] Ngnie Sighom, J.R.; Zhang, P.; You, L. Security enhancement for data migration in the cloud. *Future Internet* 2017, *9*, 23.
[12] Osman, O.M.; Kanona, M.E.A.; Hassan, M.K.; Elkhair, A.A.E.; Mohamed, K.S. Hybrid multistage framework for data manipulation by combining cryptography and steganography. *Bull. Electr. Eng. Inform.* 2022, *11*, 327–335.
[13] Peffers, K.; Tuunanen, T.; Gengler, C.E.; Rossi, M.; Hui, W.; Virtanen, V.; Bragge, J. Design science research process: A model for producing and presenting information systems research. *arXiv* 2020, arXiv:2006.02763.
[14] Pramanik, S.; Ghonge, M.; Ravi, R.; Cengiz, K. *Multidisciplinary Approach to Modern Digital Steganography*; IGI Global: Hershey, PA, USA, 2021.
[15] Pulido-Gaytan, B.; Tchernykh, A.; Cortés-Mendoza, J.M.; Babenko, M.; Radchenko, G.; Avetisyan, A.; Drozdov; AY. Privacy-preserving neural networks with Homomorphic encryption: Challenges and opportunities. *Peer Peer Netw. Appl.* 2021, *14*, 1666–1691.
[16] Saunders, M.; Lewis, P.; Thornhill, A. *Research Methods for Business Students*; Pearson Education: London, UK, 2009.
[17] Shaheen, M. H. *Hybrid Encryption Algorithms over Wireless Communication Channels*; CRC Press: Boca Raton, FL, USA, 2021.
[18] Sreenivasulu, R. R.M-RSA Algorithm. *J. Discret. Math. Sci. Cryptogr.* 2020, *25*, 1–13. https://doi.org/10.1080/09720529.2020.1734292.
[19] Thabit, F.; Alhomdy, S.; Al-Ahdal, A.H.; Jagtap, S. A new lightweight cryptographic algorithm for enhancing data security in cloud computing. *Glob. Transit. Proc.* 2021, *2*, 91–99.
[20] Timothy, D.P.; Santra, A.K. A hybrid Cryptography Algorithm for Cloud Computing Security. In Proceedings of the 2017 International Conference on Microelectronic Devices, Circuits, and Systems (ICMDCS), Vellore, India, 10–12 August 2017; pp. 1–5.
[21] Wilkinson, J. RSA Encryption Algorithm, a Simple Example. By Spreadsheet. 2006.
[22] Zuo, Y.; Kang, Z.; Xu, J.; Chen, Z. BCAS: A blockchain-based ciphertext-policy attribute-based encryption scheme for cloud data security sharing. *Int. J. Distrib. Sens. Netw.* 2021, *17*, 1550147721999616.