electronics

MDPI

Article

Secure Multi-Level Privacy-Protection Scheme for Securing Private Data over 5G-Enabled Hybrid Cloud IoT Networks

Anil Kumar Budati [1,*], Sridhar Reddy Vulapula [2], Syed Bilal Hussian Shah [3], Anas Al-Tirawi [3] and Anil Carie [4]

[1] Department of ECE, KG Reddy College of Engineering & Technology, Hyderabad 501504, India
[2] Department of IT, Vignana Bharathi Institute of Technology, Hyderabad 501301, India; sridhar.vulapula@vbithyd.ac.in
[3] School of Engineering, Computing and Informatics, Dar Al-Hekma University, Jeddah 22246, Saudi Arabia; sshah@dah.edu.sa (S.B.H.S.); atirawi@dah.edu.sa (A.A.-T.)
[4] Department of CSE, SRM University-AP, Amaravathi 522502, India; anilcarie.c@srmap.edu.in
* Correspondence: anilbudati@gmail.com

Abstract: The hybrid cloud is a secure alternative for enterprises to exploit the benefits of cloud computing to overcome the privacy and security concerns of data in IoT networks. However, in hybrid cloud IoT, sensitive items such as keys in the private cloud can become compromised due to internal attacks. Once these keys are compromised, the encrypted data in the public cloud are no longer secure. This work proposes a secure multilevel privacy-protection scheme based on Generative Adversarial Networks (GAN) for hybrid cloud IoT. The scheme secures sensitive information in the private cloud against internal compromises. GAN is used to generate a mask with the input of sensory data-transformation values and a trapdoor key. GAN's effectiveness is thoroughly assessed using Peak Signal-to-Noise Ratio (PSNR), computation time, retrieval time, and storage overhead frameworks. The obtained results reveal that the security scheme being proposed is found to require a negligible storage overhead and a 4% overhead for upload/retrieval compared to the existing works.

Keywords: hybrid cloud; security; multilevel privacy protection; generative adversarial networks

Citation: Budati, A.K.; Vulapula, S.R.; Shah, S.B.H.; Al-Tirawi, A.; Carie, A. Secure Multi-Level Privacy-Protection Scheme for Securing Private Data over 5G-Enabled Hybrid Cloud IoT Networks. *Electronics* **2023**, *12*, 1638. https://doi.org/10.3390/electronics12071638

Academic Editor: Fernando De la Prieta Pintado

Received: 15 February 2023
Revised: 27 March 2023
Accepted: 28 March 2023
Published: 30 March 2023

1. Introduction

Several enterprises are rapidly adopting cloud computing as their sensory data storage and computation platform. Benefits such as on-demand resource availability, affordability, and reliability are the driving factors behind this rapid adoption. The value that cloud computing brings to enterprises is challenged by increasing data compromises and privacy vulnerabilities. Data in the cloud can be leaked, modified, and compromised. Thus, it becomes important to provide security, privacy, and integrity of data to accelerate the adoption of the cloud among enterprises. To this goal, many solutions based on anonymization, randomization, cryptographic transformation, diversification, aggregation, etc. have been proposed. However, a problem in these solutions is scalability and security against data inference attacks. The hybrid cloud is an architectural-level solution proposed to provide a reliable solution ensuring enhanced security and privacy in the cloud. The hybrid cloud has two components—public and private clouds. Data-transformation keys and other sensitive data items are kept in the private cloud. Transformed data and non-sensitive data items are kept in the public cloud. The transformed data items in the public cloud need the keys in the private cloud for restoration, and therefore, the data in the public cloud are secure and private. Many data-transformation solutions have been proposed for hybrid cloud architecture to secure the privacy of data. In most schemes, data-transformation keys and access control parameters are kept in the private cloud, and they assume a completely trusted private cloud. However, when this assumption is broken and data-transformation keys in the private cloud become compromised, the data kept in the public cloud is no longer secure and private. This study addresses this problem

and proposes a multilevel privacy-protection scheme based on Generative Adversarial Networks (GANs). Data-transformation keys are transformed into masks using GAN and stored in the private cloud. These masks are difficult to decipher and, even in the case of leakage, it is not possible to decipher the data-transformation keys hidden in the masks without the cooperation of the data owner and the private cloud. Since mask deciphering is under the joint ownership of the data owner and the private cloud, the data-transformation keys become secure even in the case of a compromise of data in the private cloud.

Self-Organizing Networks (SON) powered by machine-learning technologies are fast emerging as a promising design feature for future mobile networks, as demands for increased service needs and enhanced efficiency are rapidly increasing. Large amounts of real-labeled sample data are needed to train the networks to implement the SON with machine learning as the foundation. The amounts of sample data invariably have a great impact on the effective functioning of the algorithm in these networks. The limited availability of real-labeled data might become a hindrance in the fully fledged implementation of ML-powered SON [1].

Deep-learning techniques, such as convolutional neural networks, are used to create generative modeling approaches such as GANs. These approaches are part of unsupervised learning in ML involving tasks such as automatically finding and learning input data patterns and regularities. These learning models can help in the development of new models learning the patterns of the original dataset. These training generative models of supervised learning problem is resolved by applying the GANs. Conventional cryptographic methods are used to modify the data, as the relevance and utility of these methods cannot be undermined. As an improvement over this, a novel method known as generative coverless information hiding method, which is based on generative adversarial networks, is proposed in the present paper. The main idea of this method is that a generative adversarial network class label is substituted for the information of a secret key as a driver. Confidential data are directly generated and subsequently, with the help of the discriminator, secret information is extracted from the hidden data.

ANs comprise two neural networks, of which one is trained to generate data and the other is trained to identify and put aside fake data from the accurate one. Though the concept of a structure being used to generate data is not new, GANs have yielded significant results in terms of generating images and video. For instance, numerous image-style transformations have been convincingly done with the help of Cycle GAN. Generating human faces using Style GAN serves as an example of the generative model compared with discriminative models that are more widespread. This is often seen on the "This Person Does Not Exist Structures" website.

The novel contributions of this work are (i) a scheme for preserving the security of private/sensitive data in the private cloud. The scheme has two levels of control: the first is with the administrator of the hybrid cloud using GAN, and the second is with the data owner using the Advanced Encryption Standard (AES). The data-transformation parameters are converted into a mask image and are stored in the private cloud, instead of being stored in plain form, as discussed in the existing works. Even if the masked image is leaked, it becomes difficult for attackers to retrieve the transformation parameters due to these two levels of control.

The rest of the paper is ordered in the following manner. Section 2 presents a survey on data-security techniques in the cloud and the accompanying issues. Section 3 discusses a proposed multilevel privacy-protection scheme for securing data in a hybrid cloud. The results of the proposed solution and a comparison with existing works are discussed in detail in Section 4, and Section 5 consists of the conclusion and scope of future work.

2. Related Work

Fabian et al. [1] used cryptographic secret sharing along with attribute-based encryption for secure healthcare data sharing across various departments of the enterprise through the cloud. The data are split into shares using cryptographic secret sharing and distributed

across multiple clouds. The sharing location and access control parameters are kept in the cloud, and this can be compromised. Once the location of a few shares in the cloud is known, data can be reconstructed, and privacy is at stake. Yang et al. [2] proposed a hybrid cryptographic algorithm to preserve the privacy of data in the cloud. The data are split vertically and encrypted before being published to the cloud. The partition information and encryption keys are stored in the cloud. Due to this, the method has a higher security risk in terms of the compromise of partition information and encryption keys. Zhang et al. [3] proposed a privacy-preserving data-security scheme for the hybrid cloud called Cocktail. Data are partitioned using a quasi-identifier partitioning technique. Differential privacy is provided at the data-querying stage. Though retrieval latency is lower in this method, it is completely insecure against the leakage of partition information stored in the cloud. Zhou et al. [4] proposed a data-partition strategy that is independent of applications. The scheme is designed for the hybrid cloud. However, the security of keys and partition information is not considered in this work. Lyu et al. [5] proposed two-stage data perturbation to secure data in the hybrid cloud. The data-perturbation scheme is secure against estimation and independent component analysis attacks. However, the perturbation key is stored in the private cloud without any ciphering; because of this, the scheme is insecure against data-compromise attacks. Chen et al. [6] proposed a data-perturbation scheme to secure data in the cloud. The perturbation involved random sequences of rotation, translation, and noise addition. Due to geometric property preservation, the perturbed data are suitable for data-mining operations. The perturbation sequence stored in the private cloud is insecure against data-compromise attacks. Chen et al. [7] proposed a random projection-based data perturbation to secure data in the cloud but, as in his early work [6], the scheme also did not consider a data compromise in the private cloud. Yuan et al. [8] applied compressed sensing for data perturbation before storage in the cloud. The reconstructed data have marginal error compared to the original data, and the scheme is not suitable for text data. The reconstruction matrix is kept in the private cloud and it is insecure against a data-compromise attack on it. Huang et al. [9] proposed a scheme for securing images in the hybrid cloud. In this scheme, the image is split into blocks and shuffled. The shuffled images are stored in the public cloud and the shuffling information is stored in the private cloud. Even if partial information about the shuffling order is leaked, the entire image can be reconstructed by the attacker. Abbas et al. [10] combined cryptography, steganography, and hashing to ensure data privacy in the hybrid cloud. Data are encrypted with the Rivest–Shamir–Adleman (RSA)/Advanced Encryption Standard (AES), and the encrypted data are hidden in imagery using LSB. Hashing is used to ensure the integrity of the data. However, the mechanism is not scalable, and storing keys in the private cloud with ciphering is insecure. Huang et al. [11] proposed a solution for image data privacy in the hybrid cloud. The image is split into blocks, which are shuffled in a random order. In addition, pixel values are modified using a random one-to-one function. The shuffling order and pixel-mapping function are kept in the cloud, posing a data-leakage issue. Abrishami et al. [12] proposed a hybrid cloud architecture where sensitive tasks are scheduled in the cloud assuming the private cloud is completely trusted. Therefore, security compromises due to internal attacks on the private cloud are not considered in this work. Xu et al. [13] proposed a sensitive data aggregation scheme for securing data in the hybrid cloud. The scheme is more suited to big-data computations. Aggregation rules are stored in the private cloud and, upon leakage of it, the privacy of data in the public cloud is at risk. Li et al. [14] proposed a convergent encryption scheme for the hybrid cloud with support for data de-duplication. However, the security of encryption keys during the compromise of private cloud data is not considered. Saritha et al. [15] enhanced the security of the private cloud and prevented it from unauthorized access using multilevel authentication. However, with authorization control, the scheme is not secure against internal attacks on data. Similarly, Sridhar et al. [16] enhanced the security of the private cloud using hybrid multilevel authentication. This scheme is not able to secure data from insider attacks and virtualization attacks. Udendhran et al. [17] combined homomorphic

encryption combined with user location to secure the data in the cloud. The private cloud just stores the homomorphic keys and, even if leaked, without user location information, the encrypted data stored in the public cloud cannot be deciphered. Nagaty et al. [18] integrated cryptography and access control to secure data in the hybrid cloud. Access control information along with cryptography keys are stored in the private cloud without any security. Quershi et al. [19] developed a secure framework for health record storage based on the hybrid cloud. Keys are stored in the private cloud and, upon leakage of it, the data in the public cloud is at risk. A summary of the surveys is presented in Table 1.

Table 1. Survey summary.

Solution	Summary	Gap
Fabian et al. [1]	Cryptographic secret sharing along with attribute-based encryption	Sharing location and the access control parameters are kept in the cloud, and this can be compromised
Yang et al. [2]	Data are split vertically and encrypted before being published to the cloud	Method has a higher security risk of compromise of partition information and encryption keys
Zhang et al. [3]	Data are partitioned using a quasi-identifier partitioning technique	Approach is completely insecure against leakage of partition information stored in the cloud
Zhou et al. [4]	Data-partition strategy	Security of keys and partition information is not considered in this work
Lyu et al. [5]	Two-stage data perturbation to secure data in the hybrid cloud	Scheme is insecure against data-compromise attacks
Chen et al. [6]	Geometric data-perturbation scheme for securing data	Perturbation sequence stored in the private cloud is insecure against data-compromise attacks
Chen et al. [7]	Random projection-based data perturbation to secure data in the cloud	Approach did not consider data compromise in the cloud
Yuan et al. [8]	Compressed sensing for data perturbation before storing in the cloud	Reconstruction matrix is kept in the private cloud, and it is insecure against data-compromise attacks on it
Huang et al. [9]	Securing images on the hybrid cloud by splitting into blocks and shuffling	Even if partial information on shuffling order is leaked, the entire image can be reconstructed by the attacker
Abbas et al. [10]	Combined cryptography, steganography, and hashing to ensure data privacy in the hybrid cloud	Mechanism is not scalable, and storing the keys in the private cloud with ciphering makes it insecure
Huang et al. [11]	Pixel values are modified using a random one-to-one function	Shuffling order and pixel-mapping functions are kept in the cloud, posing a data-leakage issue
Xu et al. [13]	Sensitive data aggregation scheme	Aggregation rules are stored in the private cloud and upon leakage of it, the privacy of data in the public cloud is at risk
Li et al. [14]	Convergent encryption scheme for the hybrid cloud	Security of encryption keys during the compromise of private cloud data is not considered
Saritha et al. [15]	Multilevel authentication	Scheme is not secure against internal attacks on data
Sridhar et al. [16]	Hybrid multilevel authentication	Scheme is not able to secure data from insider attacks and virtualization attacks
Nagaty et al. [18]	Integrated cryptography and access control to secure data in the hybrid cloud	Access control information along with cryptography keys are stored in the private cloud without any security

From the survey, it can be seen that most solutions based on the hybrid cloud assume a fully trust private cloud and advocate the private cloud to be in the administrative region of an enterprise. Multilevel authentication and intrusion detection has been proposed as a solution to secure access to the private cloud. However, these schemes are not resilient against internal attacks. Based on these observations, this work proposes a defensive mechanism against the leakage of data in the private cloud by internal attackers.

3. Multilevel Privacy-Protection Scheme

The data handling of the proposed multilevel privacy-protection scheme is given in Figure 1. The data owner transforms the files and stores the transformed file in the public cloud. The transformation parameters are usually stored in the private cloud in plain form. However, in the case of an internal attack and a compromise of the transformation parameters, the transformed data in the public cloud is at risk. To secure the transformation parameters, these parameters are stored in a linear array. The data owner also generates a secret symmetric key. The linear array of transformation parameters is encrypted with a secret key provided by the data owner using the Advanced Encryption Standard (AES). The data-transformation parameters are converted to a 2D matrix of size m × n, where m is the number of rows and n is the number of columns. The linear array is converted to a matrix, as most existing deep-learning models only work with images that are a 2D matrix. The 2D matrix is passed to the generator component of the Generative Adversarial Networks (GAN) to be converted into a masked image. The masked image is stored in the private cloud. When the data owner wants to view the data, the masked image is passed to the discriminator component of GAN to retrieve the 2D matrix. The 2D matrix is flattened into a linear array using row major order, and then decrypted using the AES with the secret key belonging to the data owner to obtain the transformation parameters. The transformation parameters are then used to reconstruct the data.

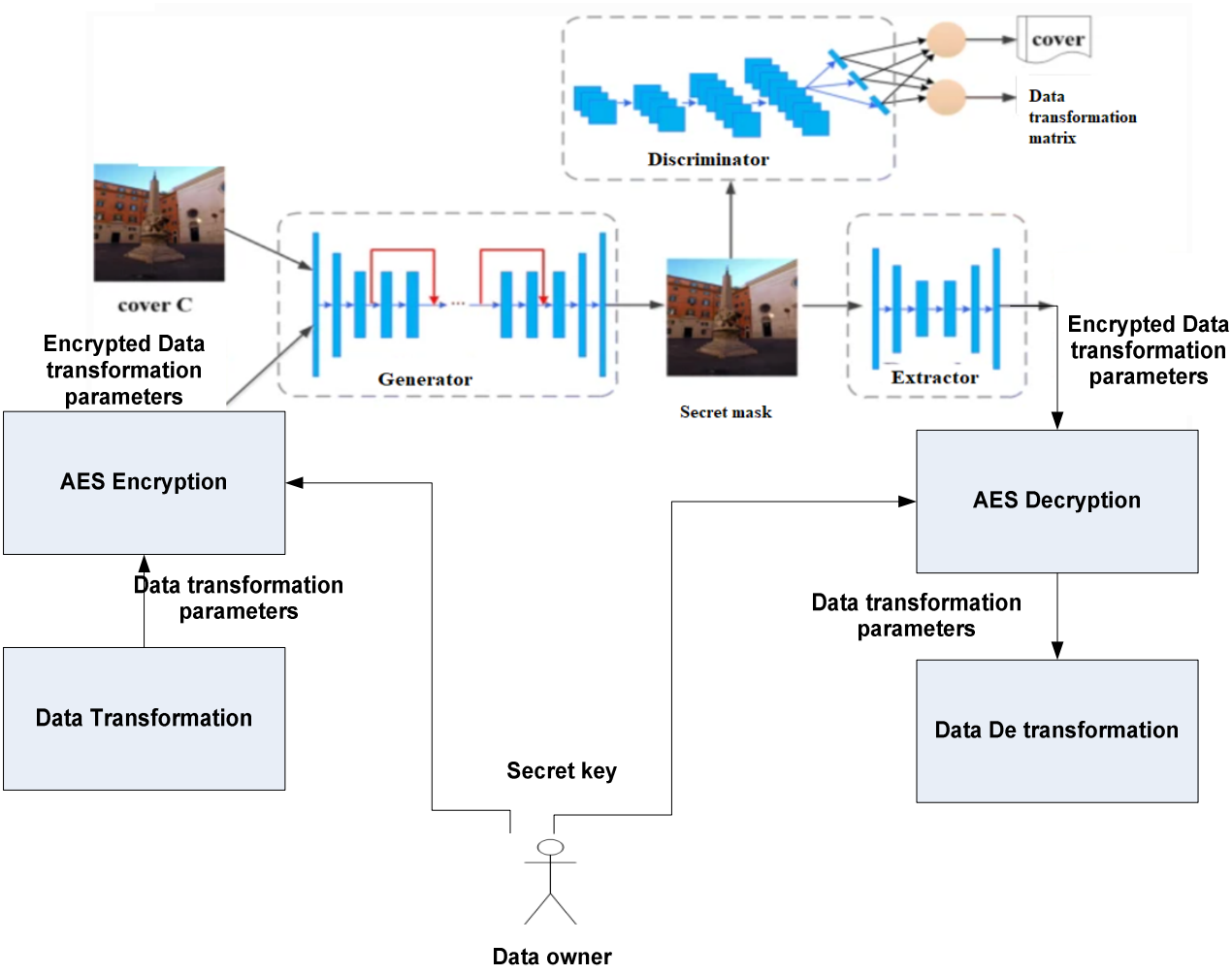

Figure 1. Multilevel privacy-protection architecture.

In this work, GAN is used to transform the secret cover image selected by the data owner according to the encrypted data-transformation matrix to generate a masked image

as shown in Figure 2. This masked image has the encrypted data-transformation matrix embedded as a structural and textural property in the cover image. This masked image is stored in the private cloud, instead of storing the data-transformation parameters in raw form. When the encrypted data-transformation parameters have to be retrieved from the masked image, the data owner selects the masked image. GAN extracts the encrypted data-transformation parameters from the masked image. This encrypted data-transformation matrix is then decrypted with the secret key provided by the owner using AES. The decrypted data-transformation matrices are used to decrypt the files stored in the public cloud. Therefore, the data owner has more control over the data-transformation parameters stored in the private cloud. This method is resilient against data leakages from the private cloud due to internal attacks. From the masked image, it is difficult to retrieve the data-transformation parameters, as the attacker needs to know the GAN model and the secret key of the data owner. Due to two levels of protection, attacks on data due to data compromise in the private cloud are defended in the proposed solution.

$$L_{GAN} = E_{\bar{x}\sim P_g}[D(\bar{x})] - E_{\bar{x}\sim P_r}[D(x)] + \lambda E_{\bar{x}\sim P_x}\left[(\|\nabla_{\bar{x}} D(\bar{x})\|_2 - 1)^2\right] \quad (1)$$

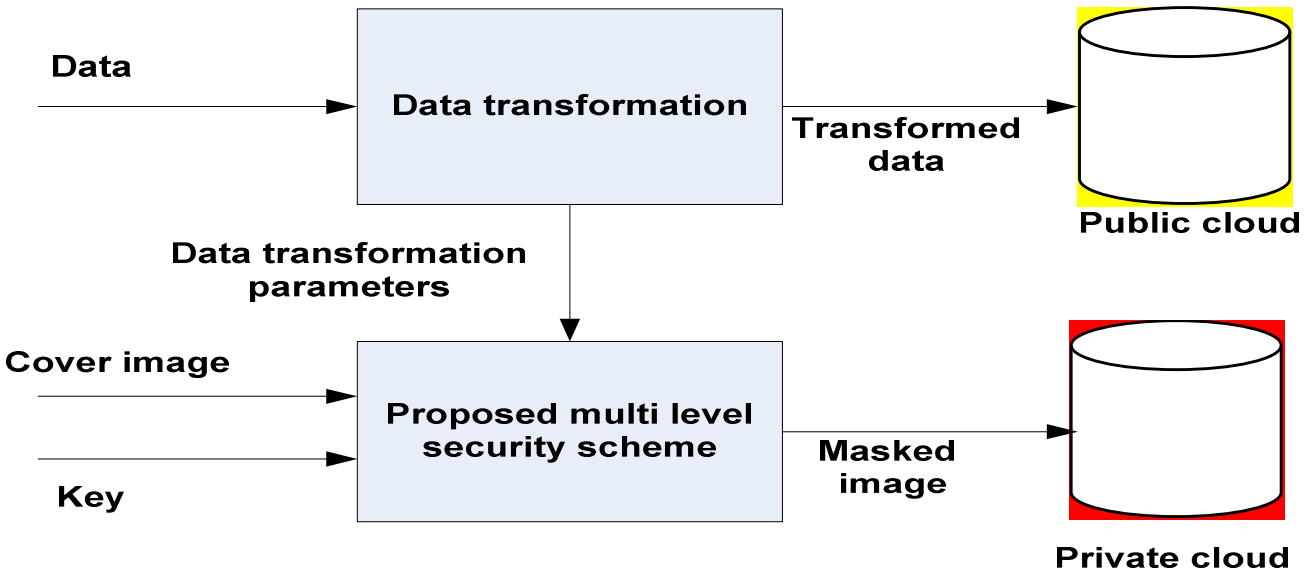

Figure 2. Data distribution in the proposed scheme.

The distribution over V is given as P_r. Figures 3 and 4 depict the GAN configuration in terms of the network used for generative and discriminative purposes in this study. GAN [20] comprises two different networks: one is generative and one is discriminative. The former network creates samples to fool the other network, which tries to determine whether the sample is genuine or has been made by the generative network. With the competition of both these networks, the generative network produces an almost-accurate sample. GAN networks are being used to generate synthetic data because of their capability to adapt to complex distributions. GAN's objective function is given as P_g. The uniform samples over P_r and P_g are given as P_x.

The conventions used in Figures 3 and 4 are given in Table 2.

Generator (G) either synthesizes or modifies the input cover image based on the encrypted data-transformation matrix. The discriminator ascertains whether or not the image consists of any secret embedding. The encrypted data-transformation matrix is extracted from the stegno image. From the encrypted data-transformation matrix, the transformation parameters can be retrieved after AES decryption and used for the decryption of data stored in the public cloud.

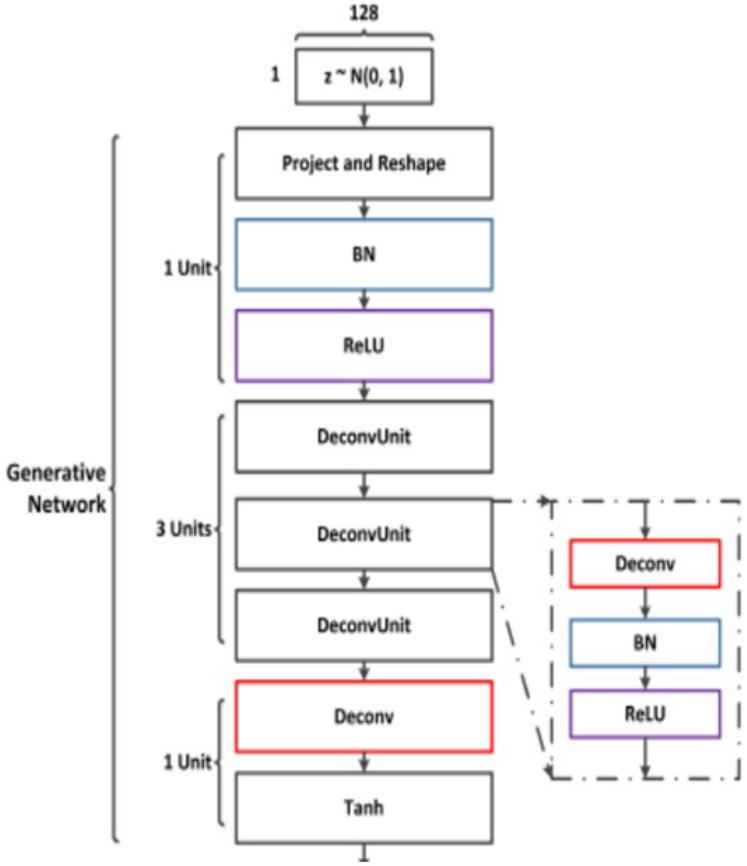

Figure 3. Generative network.

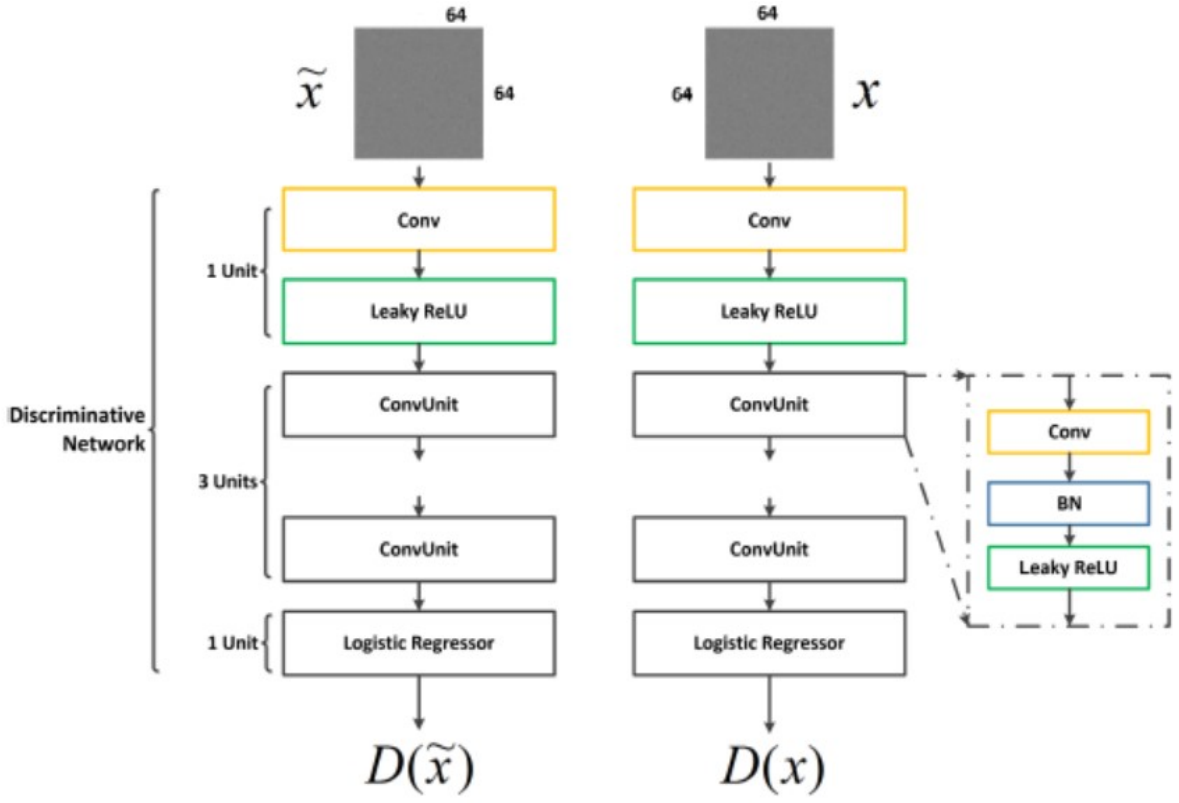

Figure 4. Discriminator network.

Table 2. Conventions used in Figures 3 and 4.

Conv	Convolution with Kernel Size 5 × 5
Deconv	De-convolution
BN	Batch normalization
ReLU	Rectified Linear Unit

4. Results

The proposed multilevel privacy-protection performance is tested using the Arrhythmia dataset in the UCI machine-learning repository [20]. It is measured based on (i) storage overhead, (ii) upload time, (iii) retrieval time, and (iv) security strength. The performance of the solution is compared against combined clustering and the geometric perturbation scheme proposed by Sridhar et al. [21], combined cryptography and steganography proposed by Abbas et al. [10], and the secure data de-duplication scheme proposed by Ma et al. [22]. Geometric data perturbation proposed by Sridhar et al. [21] is used as a data-transformation function in the proposed solution for performance testing.

The performance test was conducted in a hybrid cloud setup with Dropbox as the public cloud and Ubuntu Linux local VM as the private cloud [23,24]. Accounts were created in the Dropbox cloud and used for the storage of data. Upload and download operations were realized using Dropbox python API. The configuration of the machine used for the private cloud was an Intel core i5-8250U CPU@ 1.8 GHZ, 8 GB memory, and 1 TB disk.

The storage overhead in the private cloud is measured as the memory consumed by the private cloud for storing the data-transformation parameters for various data volumes. The result obtained is shown in Table 3.

Table 3. Comparison of storage overhead.

Size (MB)	Storage Overhead (MB)			
	Proposed	Abbas et al. [10]	Ma et al. [22]	Sridhar et al. [16]
20	1.6	1.4	1.9	1.2
40	2.5	2.4	3.5	1.8
60	4.1	4.3	6.1	3.4
80	6.9	7.8	8.1	7.7
100	7.2	8.3	8.4	8.2
Average	4.46	4.84	5.6	4.46

The average storage overhead in the proposed solution is 8% lower compared to Abbas et al. and 16% lower compared to Ma et al. [22]. The storage overhead is the same as that of Sridhar et al. [16].

When compared to the existing models, the storage overhead in the proposed solution is found to be slightly higher is shown in Figure 5. However, this is significantly reduced in the private cloud for higher data volumes, as a larger volume of data-transformation parameter packing is carried out in the same cover image. The higher the amount of data, the larger the storage overhead. In comparison with the three existing models, the proposed model displays a higher storage capacity of 80 MB.

The time consumed for data processing—from the point of its arrival to the point of its storage in the cloud—is shown in Table 4. A remarkable improvement is found in the method proposed compared to the two existing methods while its performance is found to be almost equivalent to Sridhar et al. [16].

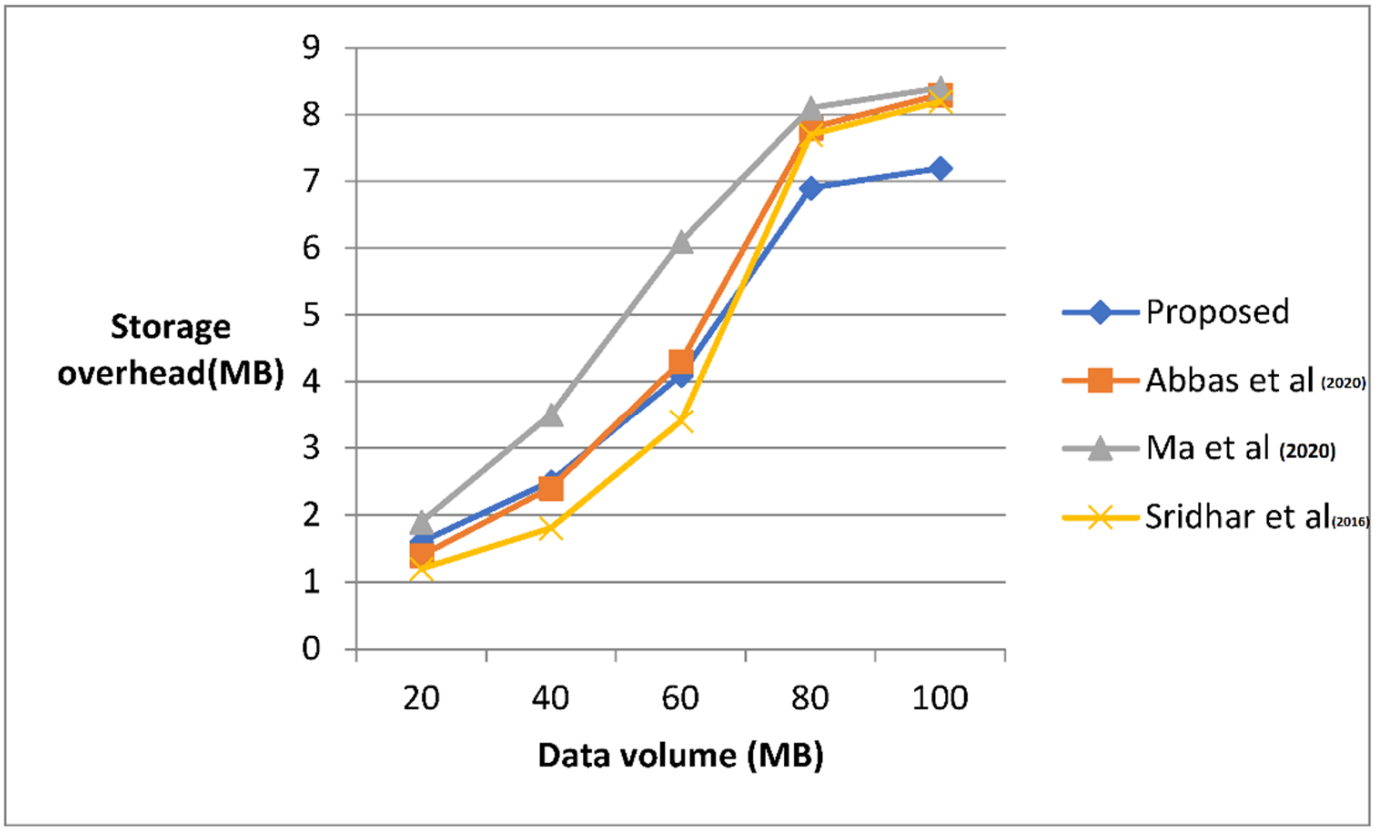

Figure 5. Comparison of storage overhead [10,16,22].

Table 4. Comparison of upload time.

Size (MB)	Computation Time (s)			
	Proposed	**Abbas et al. [10]**	**Ma et al. [22]**	**Sridhar et al. [16]**
20	15	15	18	14
40	21	26	34	20
60	28	48	59	27
80	37	87	110	33
100	39	91	114	38
Average	28	53.4	67	26.4

Compared to the model proposed by Sridhar et al. [16], in the proposed model, the average time taken for uploading is 5% higher, which is because of the AES encryption process of the data-transformation parameters and encoding them to the masked image with the help of GAN and is shown in Figure 6. The uploading time is less when compared to the other three existing methods. Compared to the proposed model, a considerable delay is observed in the uploading of the data in the existing methods: 22% compared to the model proposed by Abbas et al. [10], 32% compared to that of Ma et al. [22], and 5% compared to that of Sridhar et al. [16].

The time taken for data retrieval including the data decryption is measured for various volumes of the data and the result is given in Table 5.

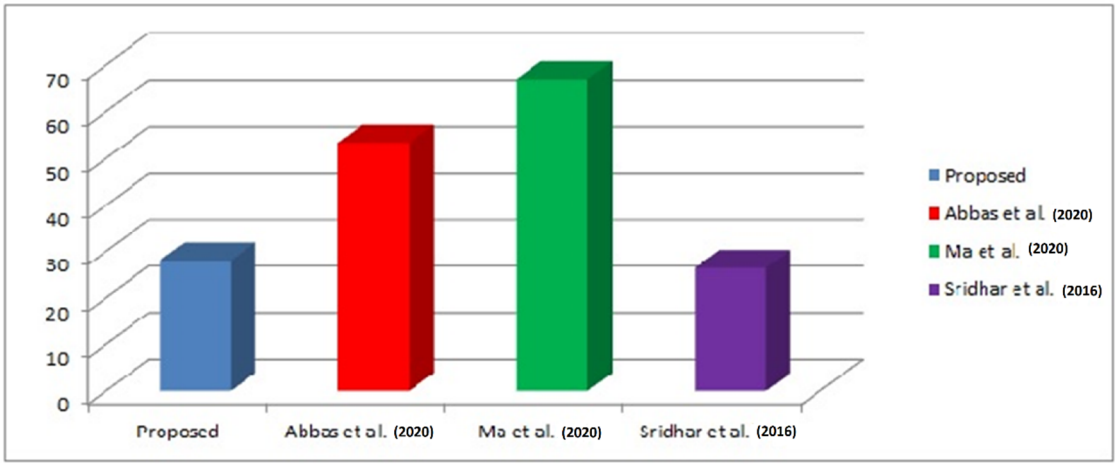

Figure 6. Comparison of average upload time [10,16,22].

Table 5. Comparison of data retrieval time.

Size (MB)	Retrieval Time (sec)			
	Proposed	**Abbas et al. [10]**	**Ma et al. [22]**	**Sridhar et al. [16]**
20	14	14	19	13
40	19	24	35	18
60	25.2	43	61	24
80	34	78	72	33
Average	23.05	39.75	46.75	22

In the proposed method, the time consumed for data retrieval is found to be a mere 4% higher compared to the method proposed by Sridhar et al. [16]. This is slightly higher in the proposed model because of AES decryption, and the reconstruction steps that were followed for data-transformation matrix retrieval. There is not much difference in the data retrieval time between these two models. A notable improvement of 16% and 23% is observed in the average data retrieval time when compared to the two other existing models of Abbas et al. [10] and Ma et al. [22].

The security strength is measured based on the parameter of difficulty in predicting the data-transformation matrix from the masked image. The difficulty level is estimated in terms of a measure called variance of difference (VoD).

Let X_i be a random variable representing the data-transformation matrix value i, X_i' be the estimated result of X_i and difference $D_i = X' - X$. Let the mean of D be $E(D_i)$ and variance be $Var(D_i)$. VOD for column i is $Var(D_i)$. VOD is measured for each column, and the average VOD is given as a privacy measure (pm). A guess is launched every 5 h on the perturbed data and the privacy measure (pm) is measured at 1-h intervals and plotted in Figure 7.

$$pm = \frac{\sum_{i=1}^{N} VOD_i}{N} \tag{2}$$

The VoD value is consistently higher even after spending hours breaking the masked image and obtaining clues about the data-transformation matrix. This is due to the use of GAN in the proposed solution, which modifies the structural property of the image to embed the transformation matrix instead of using Least Significant Bit (LSB)-based methods to hide information.

The embedding capacity is measured against distortion introduced to the cover image by GAN, and the result is given in Figure 8.

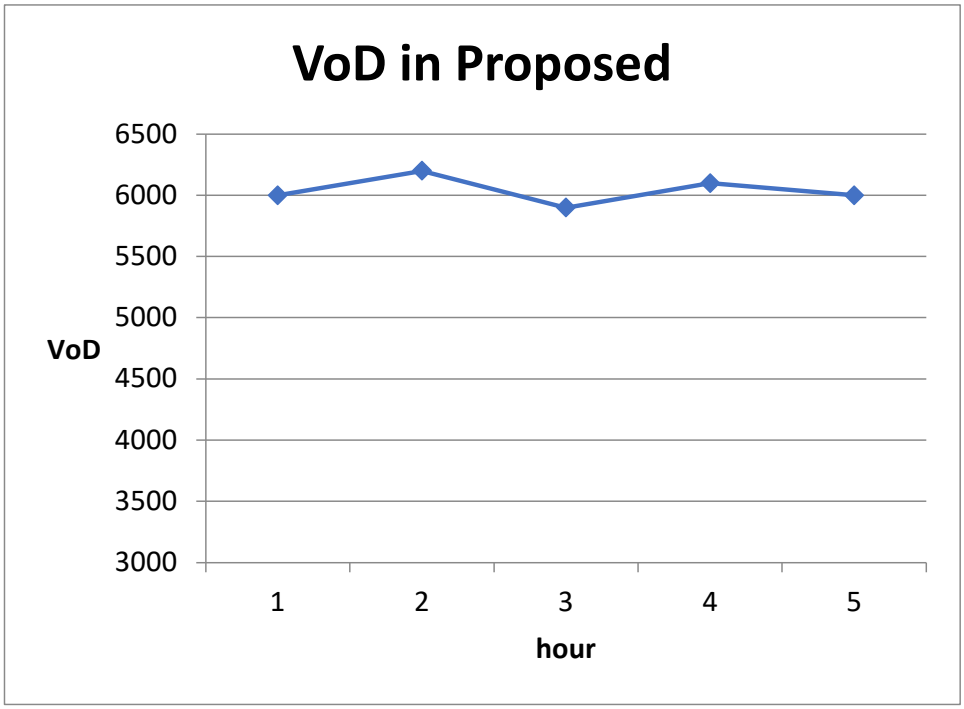

Figure 7. Security strength.

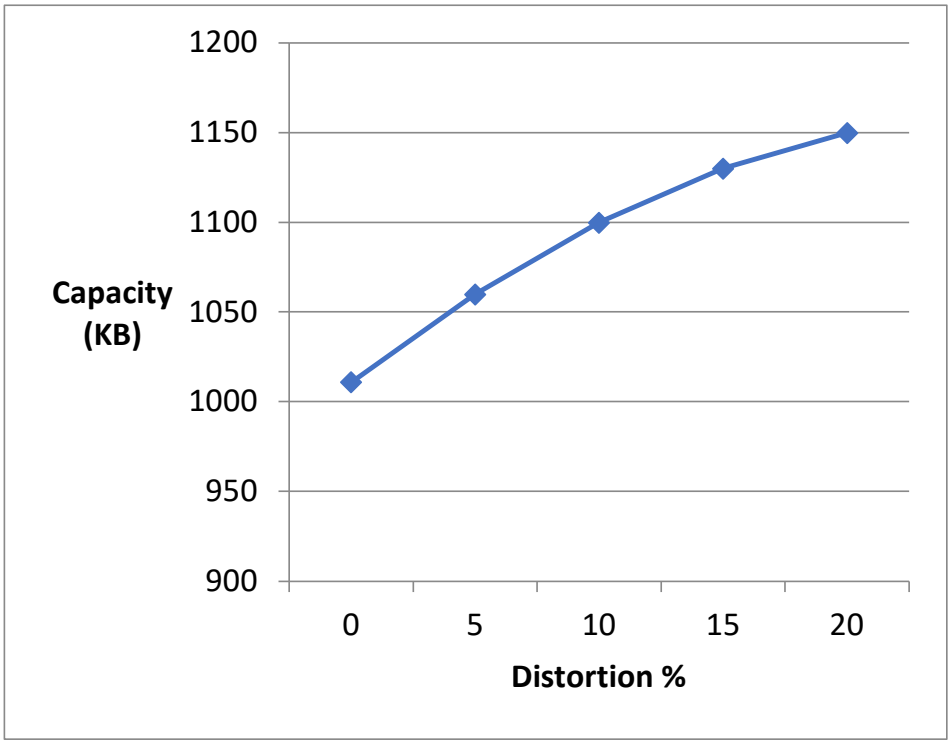

Figure 8. Embedding capacity vs distortion %.

As distortion increases, the embedding capacity also increases. However, higher distortion makes the image become a target for analysis attacks. The peak signal-to-noise ratio is measured between the original cover image and that generated by GAN after embedding. The PSNR is measured for various embedding capacities, and the results are given in Figure 9.

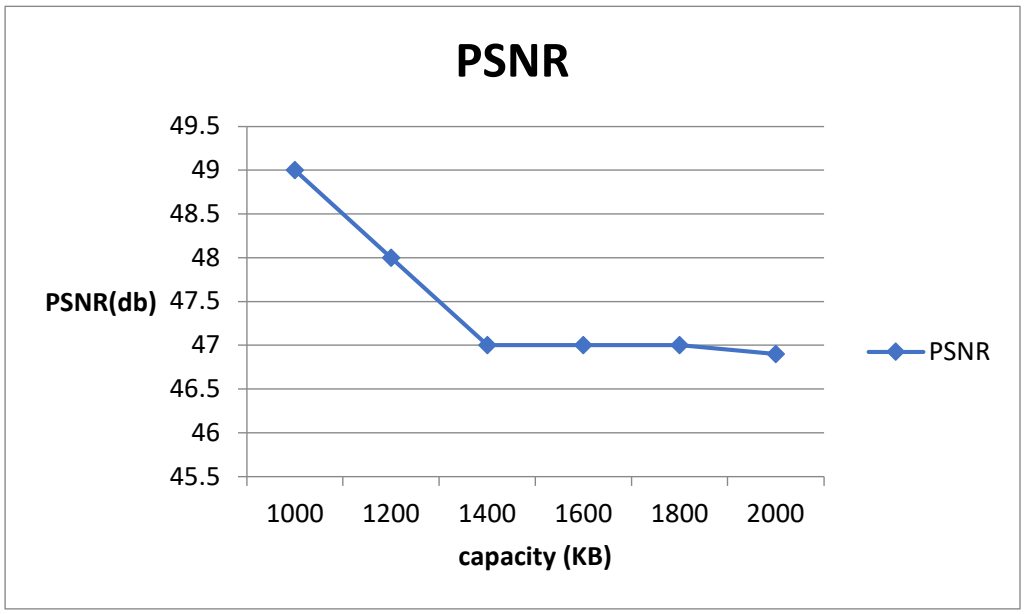

Figure 9. PSNR vs capacity.

The PNSR is consistent and shows a smaller difference even when the embedding capacity is increased. This demonstrates the effectiveness of GAN in generating quality images that are resilient against analysis attacks.

For the same cover image, for different percentages in the key transformation parameters, the difference in structural similarity metric (SSIM) between the cover image and GAN-generated image is calculated, and the result is shown in Figure 10.

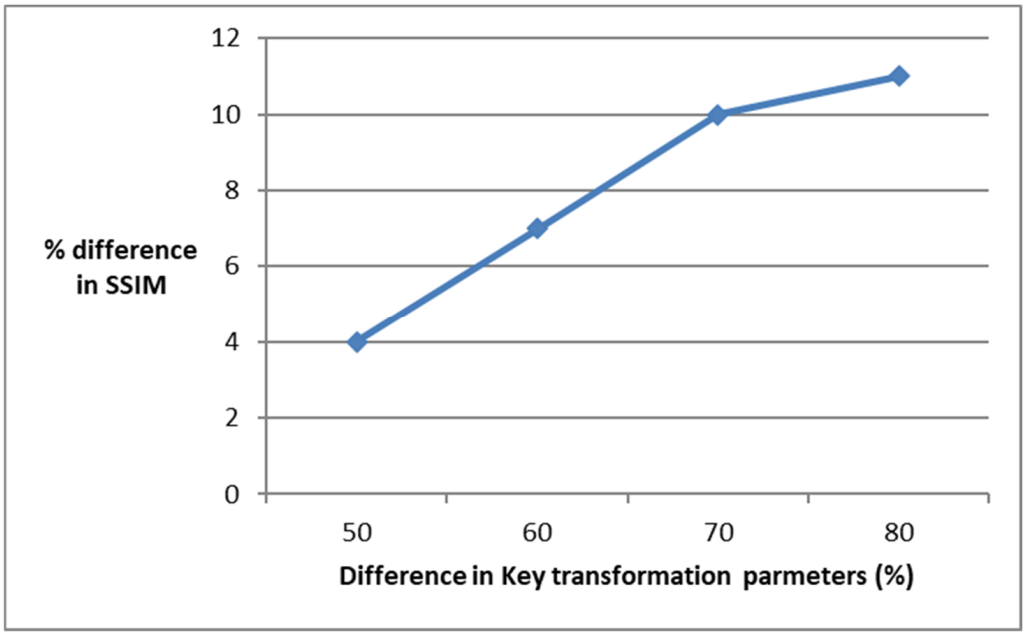

Figure 10. Difference in SSIM.

As seen in Figure 10, even when there is a bigger difference in key transformation parameters, the SSIM difference is low. Hence, it is difficult to know the embedded key transformation parameters from the SSIM.

5. Conclusions

A multilevel privacy-protection scheme for defending a data-compromise attack on the private cloud is proposed in this work. First, data-transformation matrices are encrypted with AES, then encrypted data-transformation matrices are embedded into a cover image using GAN. The two levels securing the data-transformation matrices make the proposed solution robust against data-leakage attacks by insiders. Through performance testing, the cost of the proposed security scheme is found to be a negligible storage overhead and a 4% overhead for upload/retrieval, compared to existing works.

Author Contributions: Conceptualization, A.K.B.; methodology, S.R.V.; software, S.R.V.; validation, S.B.H.S.; formal analysis, A.K.B.; investigation, A.A.-T.; resources, A.C.; data curation, S.R.V.; writing—original draft preparation, A.K.B.; writing—review and editing, S.B.H.S.; visualization, A.A.-T.; supervision, S.R.V.; project administration, A.C.; funding acquisition, A.A.-T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: There is no third party of data is used in this manuscript.

Acknowledgments: The authors wish to express their heartfelt gratitude to Graduate Studies, Business and Scientific Research (GBR) at Dar AI Hekma University, Jeddah, Saudi Arabia.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Fabian, B.; Ermakova, T.; Junghanns, P. Collaborative and secure sharing of healthcare data in multi-clouds. *Inf. Syst.* **2015**, *48*, 132–150. [CrossRef]
2. Yang, J.; Li, J.; Niu, Y. A hybrid solution for privacy preserving medical data sharing in the cloud environment. *Future Gener. Comput. Syst.* **2015**, *43–44*, 7486. [CrossRef]
3. Zhang, H.; Zhou, Z.; Ye, L.; Du, X. Towards Privacy Preserving Publishing of Set-Valued Data on Hybrid Cloud. *IEEE Trans. Cloud Comput.* **2018**, *6*, 316–329. [CrossRef]
4. Zhou, Z.; Zhang, H.; Du, X.; Li, P.; Yu, X. Prometheus: Privacy-Aware Data Retrieval on Hybrid Clouds. In *Proceedings IEEE INFOCOM*; IEEE: Piscataway, NJ, USA, 2013.
5. Lyu, L.; Bezdek, J.C.; Law, Y.W.; He, X.; Palaniswami, M. Privacy-preserving collaborative fuzzy clustering. *Data Knowl. Eng.* **2018**, *116*, 21–41. [CrossRef]
6. Chen, K.; Sun, G.; Liu, L. *Towards Attack-Resilient Geometric Data Perturbation*; Wright State University: Dayton, OH, USA, 2007. [CrossRef]
7. Chen, K.; Liu, L. Geometric data perturbation for privacy preserving outsourced data mining. *Knowl. Inf. Syst.* **2011**, *29*, 657–695. [CrossRef]
8. Yuan, X.; Wang, X.; Wang, C.; Weng, J.; Ren, K. Enabling Secure and Fast Indexing for Privacy-Assured Healthcare Monitoring via Compressive Sensing. *IEEE Trans. Multimed.* **2016**, *18*, 2002–2014. [CrossRef]
9. Huang, X.; Du, X. Efficiently secure data privacy on hybrid cloud. In Proceedings of the 2013 IEEE International Conference on Communications (ICC), Budapest, Hungary, 9–13 June 2013; pp. 1936–1940.
10. Abbas, M.S.; Mahdi, S.S.; Hussien, S.A. Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography. In Proceedings of the 2020 International Conference on Computer Science and Software Engineering (CSASE), Duhok, Iraq, 16–18 April 2020; pp. 123–127.
11. Huang, X.; Du, X. Achieving big data privacy via hybrid cloud. In Proceedings of the 2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 27 April–2 May 2014; pp. 512–517.
12. Abrishami, H.; Rezaeian, A.; Naghibzadeh, M. A novel deadline-constrained scheduling to preserve data privacy in hybrid Cloud. In Proceedings of the 2015 5th International Conference on Computer and Knowledge Engineering (ICCKE), Mashhad, Iran, 29 October 2015; pp. 234–239.
13. Xu, X.; Zhao, X. A Framework for Privacy-Aware Computing on Hybrid Clouds with Mixed-Sensitivity Data. In Proceedings of the 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems, Washington, DC, USA, 24–26 August 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 1344–1349.
14. Li, J.; Li, Y.K.; Chen, X.; Lee, P.P.C.; Lou, W. A Hybrid Cloud Approach for Secure Authorized Deduplication. *IEEE Trans. Parallel Distrib. Syst.* **2015**, *26*, 1206–1216. [CrossRef]
15. Saritha, K.; Subasree, S. Analysis of hybrid cloud approach for private cloud in the de-duplication mechanism. In Proceedings of the 2015 IEEE International Conference on Engineering and Technology (ICETECH), Coimbatore, India, 20 March 2015; pp. 1–3.

16. Sridhar, S.; Smys, S. A hybrid multilevel authentication scheme for private cloud environment. In Proceedings of the 2016 10th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, 7–8 January 2016; pp. 1–5.
17. Udendhran, R. A hybrid approach to enhance data security in cloud storage. In Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing (ICC '17). Association for Computing Machinery, New York, NY, USA, 22–23 March 2017; Article 90. pp. 1–6.
18. Nagaty, K.A. A Secured Hybrid Cloud Architecture for mHealth Care. In *Mobile Health. Springer Series in Bio-/Neuroinformatics*; Adibi, S., Ed.; Springer: Cham, Switzerland, 2015; Volume 5.
19. Qureshi, B.; Koubaa, A.; Al Mhaini, M. A Lightweight and Secure Framework for Hybrid Cloud Based EHR Systems. In Proceedings of the First International Conference, SCITA 2017, Jeddah, Saudi Arabia, 27–29 November 2017; Springer International Publishing: Berlin/Heidelberg, Germany, 2018. [CrossRef]
20. Arrhythmia Data Set. Available online: https://archive.ics.uci.edu/ml/datasets/Arrhythmia (accessed on 12 October 2022).
21. Reddy, V.S.; Rao, B.T. A Combined Clustering and Geometric Data Perturbation Approach for Enriching Privacy Preservation of Healthcare Data in Hybrid Clouds. *Int. J. Intell. Eng. Systems* **2018**, *11*, 201–210. [CrossRef]
22. Ma, X.; Yang, W.; Zhu, Y.; Bai, Z. A Secure and Efficient Data Deduplication Scheme with Dynamic Ownership Management in Cloud Computing. In Proceedings of the 2022 IEEE International Performance, Computing, and Communications Conference (IPCCC), Austin, TX, USA, 11–13 November 2022; pp. 194–201.
23. Hybrid Cloud Networks. Available online: https://www.dropbox.com/ (accessed on 20 October 2022).
24. Hughes, B.; Bothe, S.; Farooq, H.; Imran, A. Generative adversarial learning for machine learning empowered self organizing 5G networks. In Proceedings of the 2019 international conference on computing, networking and communications (ICNC), Honolulu, HI, USA, 18–21 February 2019; pp. 282–286.