

Design and Implementation of a Secure Cloud-Based Storage System

Ashok Sharma ^a, Amrita Pandey ^b

^a *Department of Electrical Engineering, Power Tech Institute, Ujjain.*

^b *Department of Electrical Engineering, Power Tech Institute, Ujjain.*

Abstract

The biggest obstacles to cloud adoption in terms of data are privacy and security. Data security, privacy, and integrity must all be offered by the cloud service. The ability to share data across several businesses is one advantage of CC. To prevent data threats, data repositories must be secured. One of the main advantages of the cloud is the safe storage of data. Because it enables users to securely store important data on a private or public cloud, cloud storage has raised a lot of concerns. When a specific quality of service is requested, cloud storage offers virtualized on-demand storage across a network. The primary obstacle to CC infrastructure is data security in cloud storage. The foundation of a safe, private, and user-friendly inter-cloud data sharing architecture is encryption, which guards against unwanted access to cloud data. Ensuring the security of data being sent between users and the cloud is crucial. To protect the shared data, a number of authentication methods and security strategies have been put forth. These methods seek to preserve data's confidentiality, dependability, and authenticity. Data stored in the cloud is protected by the encryption method. These encryption techniques provide users' identities with integrity and privacy while greatly increasing performance and security level flexibility.

Keywords: Cloud Computing, Storage, Security, CNN.

Introduction

The most recent development in computer science is cloud computing (CC). Numerous options have been made available to small and medium-sized businesses so they can fulfill their goals without having to spend additional money on hardware. A distinct large machine that several clients share to have dedicated resources is the virtualization paradigm used by cloud computing systems (Padhy et al., 2012). In a multi-tenant architecture, a platform provides access to a multitude of computer resources and storage networks. The entire amount of money spent on purchasing, maintaining, and hosting resources is reduced by cloud computing (Chen et al., 2012). The cloud computing network is depicted in Figure 1.1. Low execution times, reduced temporal complexity, and safe access to data on the cloud server are essential prerequisites for cloud computing systems. On the other hand, existing cryptography techniques are not thought to be suitable for cloud storage. The study (Wooten et al., 2012) recommends an efficient two-stage cryptography solution for securely accessing and storing data in the cloud. It incorporates both user authentication methods and encryption. The main solution to the issues with the current authentication methods is the proposal of a one-time password with a two-factor authentication system. The recommended authentication technique's user identification procedure doesn't require any additional processing time or specialized hardware. Second, separate keys are used to individually encrypt two different sections of the plaintext. The user safely accesses the cloud storage by using a unique key. A combination of symmetric and asymmetric encryption methods was created for the security of cloud computing (Mai & Khalil, 2017). The symmetric Blowfish technique should be used to encrypt the single file selected for uploading. Here, the secret key for the Blowfish algorithm was encrypted using the asymmetric RSA technique. Zhonghan et al., (2013) developed a cloud storage security method. Here, files have been securely stored in the cloud using the Third-Party Auditor (TPA) and the AES encryption method. Cloud computing is a networking system that provides easy, dependable, affordable, and straightforward access to information technology resources. This CC service lowers ownership costs and infrastructure overhead. Furthermore, it provides the end-user with improved performance and flexibility (Cadenhead et al., 2012). It provides cloud customers with several benefits, such as resource elasticity, lower service costs, simple online access, etc. Small and large businesses alike are now using cloud computing to expand their partnerships and business dealings with other organizations (Hao & Han, 2011). Cloud computing via the internet enables users to share resources, data, and services. Despite CC's many benefits, users are reluctant to save sensitive or private data on the cloud because it includes government sensitive files, personal health records, and electronic correspondence. Once the data is stored in the cloud's data center, the customers no longer have control over where the data comes from. Sensitive data encryption prior to hosting creates data privacy and confidentiality against Cloud Service Providers (CSPs). The communication overheads associated with the various forms of cloud access make it impractical. Consequently, the cloud necessitates safe methods for maintaining and storing data security and privacy. The CSPs have total authority over the data and are capable of a number of malevolent actions, such as altering, destroying, and copying it. Some control over virtual machines is guaranteed by cloud computing. Because of this lack of management, the information causes security problems.

Need of the study

Accessibility is the primary obstacle in the cloud when data is accessed without authorization. Another obstacle is availability, which requires that the data be consistently accessible to clients without any problems. It has an impact on storage and causes data loss in the cloud. Another obstacle to data correction, management, and security in the cloud is integrity (Achar, 2019). Cloud data storage, also known as Infrastructure as a Service, is a crucial cloud computing service that provides data storage and sharing capabilities for multiple users. However, the expanding privacy and security concerns are a worry for both customers and service providers. According to Shinde and Taur (2015), privacy and security concerns are the main obstacles to cloud adoption. Numerous predictions of penetration into the cloud environment have resulted in enormous gains. There are serious privacy and security concerns with the CSPs hosting the services. By putting security policies and procedures in place, the cloud service provider can guarantee that their infrastructure is safe and that the client's data and applications are protected. According to Shereek, Muda, and Yasin (2014), security is a key consideration for consumers of cloud computing. Since a number of CSPs are not yet prepared to make their infrastructure publicly accessible, it is imperative to estimate the level of security. It might be difficult to manage and create a secure cloud environment. Using appropriate security protocols and tactics is essential to the protection of cloud data. Security requirements for an efficient storage system are defined, and storage and security are interconnected. With inefficient storage space and retrieval costs, fragmentation plays a significant role in the cloud. When a document is fragmented, its secrecy level is not maintained and it is separated into multiple uniform or fixed-size units called partitions. Cloud data security issues result in lost revenue and a damaged reputation. Essential data is shown by the data that customers save in the cloud. For this reason, it is unacceptable when an unauthorized third party violates data. All data must be encrypted before being sent to cloud

storage, and users must exercise caution when putting their information there. This security issue is seen by software engineers as a crucial component of cloud storage services. Designing cloud storage services requires consideration of redundancy, isolation, and dynamic data. Because a user may disable a service after the cooperation agreement expires, management must deactivate or replace cloud service providers. To manage faultless data planning, the software engineer offers a way to use the cloud service. The sharing of physical resources in the CC infrastructure leads to disastrous consequences for data security and privacy. Users are worried about where their data is stored. In order to ensure that cloud data is set up with effective and efficient disaster recovery machinery to ensure ease of data use, laws and regulations must be applicable to information between CC service providers and clients.

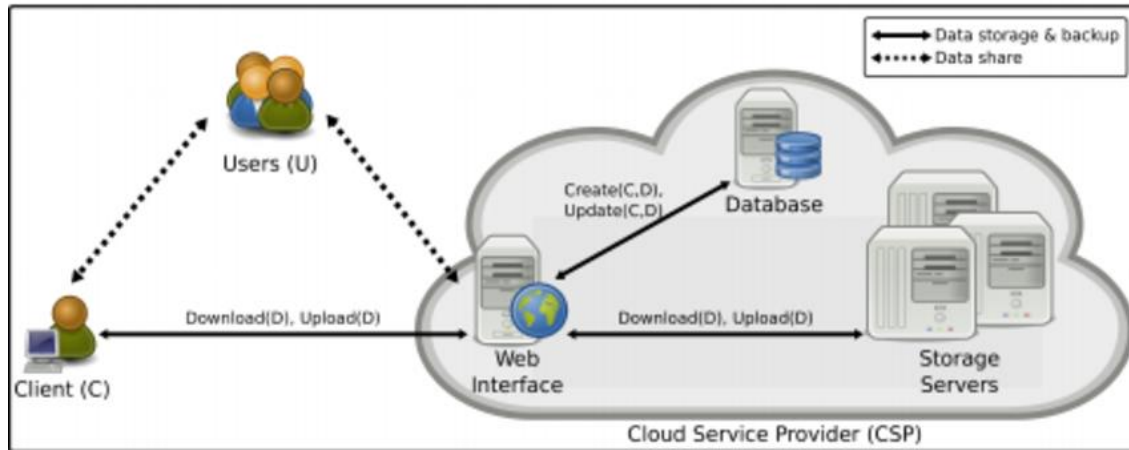


Fig. 1: Architecture of Data Security of Cloud System

Methodology

CC is a method that provides access to information and computer resources from any location with a network. The data that is saved on the cloud must be protected. Security against uncertified attacks must be the primary goal of the encryption algorithm design. However, the most important factors for any cloud computing applications are cost and implementation performance. If an encryption technique were protective but performed slowly, it would be of little benefit. Algorithms for encryption must have comparable security and performance. To address the growing security and privacy risks in the cloud, the traditional AES models ought to be modified. The results section makes it evident that AES is regarded as the most reliable algorithm, providing consumers with reliable encryption, especially when combined with Auto-Encoder-based CNN. In general, the Fernet algorithm makes sure that a message that has been encrypted cannot be read or utilized without the private key. The technique is known as Fernet symmetric encryption, and it offers a straightforward encryption method that uses HMAC for authentication. In addition, the model selects Python as an example environment to employ the suggested encryption methodology. The ciphering utilized in the suggested model was 128 bits. At this level, the training data is first encrypted using the suggested Fernet algorithm, and then it is applied to the data-input images using the proposed CNN and Auto-Encoder.

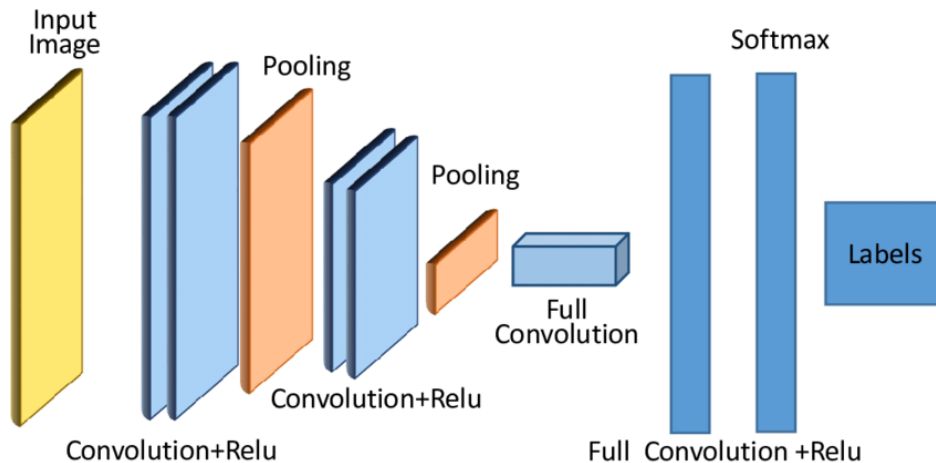


Fig. 2: CNN architecture

The pooling layer continuously reduces the volume of each feature map in order to simply down-sample the data. Furthermore, a single, fully connected layer lead to the output layer. The fully connected layer, a feature vecto that predicts categorization, stores the collective knowledge from all the convolution layers. The activation function of a neuron determines its operational status and helps to normalize the output of each activated neuron. The classifier's activation function is the Rectified Linear Unit, or ReLU.

Experimental Results

The number of epochs shouldn't be decided upon in advance. It is important to track training and validation losses over time and to cease training when the validation loss plateaus or begins to rise. This crucial machine learning approach is referred to as the "early stopping" strategy. It entails setting up an arbitrary number of training epochs and terminating the process when the validation data show that the model's performance has stopped improving.

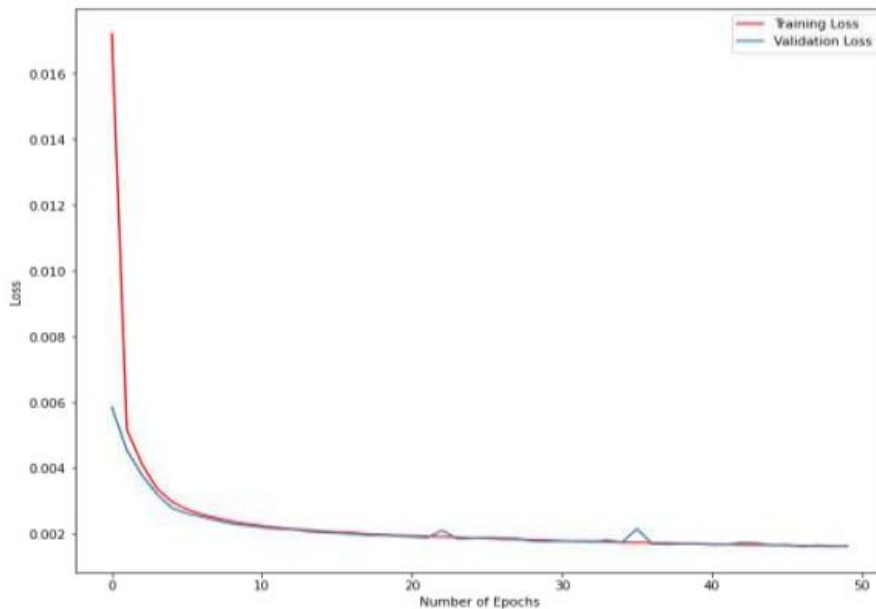


Fig. 3: Epoch-and-Loss Function

Therefore, it can be concluded that when assessing a model's performance, the MAE is either equal to or less than the RMSE, and the MSE is smaller. The study assessed the model's performance based on these two factors, and the model's values are as follows:

MSE	•0.0016165737815238633
MAE	•0.026632327526796448
RMSE	•0.0402066385255453

Fig. 4: Performance Metrics

Figure 4 makes it clear that MSE is lower than MAE and RMSE values. In a similar vein, the RMSE exceeds the MAE. As a result, the CNN-based face-image prediction model does well when datasets are double-level encrypted.

Conclusions

The goal of the study was data security, specifically with regard to the inputs of "facial images" in the cloud atmosphere. The statistical method used in this study was MSE-loss, and the metric values made it evident that the suggested hybrid model was more dependable and effective in protecting data in cloud computing. The suggested model can be regarded as effective since the training level data loss is drastically decreased to zero. This chapter accomplishes the goal of the study concerning performance computation and comparison with existing encryption techniques.

References

- Padhy, R. P., Patra, M. R., & Satapathy, S. C. (2012). Design and implementation of a cloud based rural healthcare information system model. *Univers J Appl Comput Sci Technol*, 2(1), 149-157.
- Chen, Y., Shen, Q., Sun, P., Li, Y., Chen, Z., & Qing, S. (2012, May). Reliable migration module in trusted cloud based on security level-Design and implementation. In *2012 IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum* (2230-2236). IEEE.
- Wooten, R., Klink, R., Sinek, F., Bai, Y., & Sharma, M. (2012, May). Design and implementation of a secure healthcare social cloud system. In *2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (ccgrid 2012)* (p805-810). IEEE.
- Mai, V., & Khalil, I. (2017). Design and implementation of a secure cloud-based billing model for smart meters as an Internet of things using homomorphic cryptography. *Future Generation Computer Systems*, 72, 327-338.
- Zhonghan, C., Diming, Z., Hao, H., & Zhenjiang, Q. (2013, November). Design and Implementation of Data Encryption in cloud based on HDFS. In *1st International Workshop on Cloud Computing and Information Security* (274-277). Atlantis Press.
- Cadenhead, T., Kantarcioglu, M., Khadilkar, V., & Thuraisingham, B. (2012, October). Design and implementation of a cloud-based assured information sharing system. In *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security* (36-50). Berlin, Heidelberg: Springer Berlin Heidelberg.
- Hao, L., & Han, D. (2011, September). The study and design on secure-cloud storage system. In *2011 International Conference on Electrical and Control Engineering* (5126-5129). IEEE.
- Achar, S. (2019). Cloud-based system design. *International Journal of All Research Education and Scientific Methods (IJARESM)*, 7(8), 23-30.