Cybersecurity: Handling Sensitive Data in Cloud Architecture

Binoy Kurikaparambil Revi

Independent Researcher, USA
Email: binoyrevi@live.com

Abstract

Before the advancement of cloud applications and cloud storage, sensitive data were stored on isolated systems or servers in encrypted formats. These systems were typically disconnected from external networks and had restricted access. Additionally, a mitigation plan was often implemented to recover data in the event of catastrophic damage. The management of data storage, maintenance, recovery plans, and access control required significant capital investment and ongoing expenses. With modern cloud services, businesses leverage a more secure infrastructure that data centers provide in terms of encryption, security, and access management. Additionally, the recovery plan is now just a matter of a few clicks. While these features and security measures provide many benefits, one significant risk for users and businesses is that any cloud services or data transactions initiated by a user rely on the internet, which means the data is exchanged online. Businesses and users need to design and implement secure data management for handling data related to application use or storage. In various fields, such as medical devices, there are specific standards that dictate who has access to the data and who does not. These standards also define the necessary level of encryption required for data storage. This article explains the risks that are associated with secure data management in a typical cloud application and strategies to safeguard data in domains that handle sensitive data. Data security is highly critical in most applications available today. Cloud services provide all the necessary tools to businesses and users, and it is up to them to utilize these resources wisely and correctly.

Keywords: Cybersecurity, Cloud Security, Data Encryption, Data Transfer, Cloud Apps

Introduction:

Modern cloud service providers offer robust layers of data security, focusing on three key aspects: how data is stored, how it is accessed, and who is allowed to access it. These services employ advanced encryption techniques to protect sensitive information from unauthorized access. Additionally, strict access controls and authentication protocols are implemented to ensure that only authorized users can retrieve or manipulate the data, thereby maintaining the integrity and confidentiality of your information[6].

Applications are designed for adding, viewing, analyzing, and updating data, which is often visible to the user. This means that the encrypted data must be decrypted at some point. It is also crucial to validate the authentication of any application before any data exchange occurs to protect the system against attacks like denial-of-service attacks. Furthermore, data security in transit[1] remains a critical consideration when designing a cloud application.

Related Work:

The paper titled "Data Security in Cloud Computing," authored by A. Albugmi, M. O. Alassafi, R. Walters, and G. Wills, addresses various risks and concerns associated with cloud computing, such as virtualization, storage in public clouds, and shared access or multitenancy. It clearly defines data security in two major states: Data at Rest and Data in Transit, which are the primary focus of the study.

In another paper, "Ensure Data Security in Cloud Storage," authors X. Zhang, H.-T. Du, J.-Q. Chen, Y. Lin, and L.-J. Zeng emphasizes the importance of authority in preventing unauthorized access for users. They also highlight the significance of SSL (Secure Sockets Layer) and TLS (Transport Layer Security) protocols for the secure transmission of data at the transport layer after it has been encrypted at the application layer.

A. Markandey, P. Dhamdhere, and Y. Gajmal discussed data security in cloud computing in their paper titled "Data Access Security in Cloud Computing: A Review." They explored how to achieve data security in cloud storage and proposed a comprehensive cloud storage security strategy. The authors addressed data security in relation to the three primary cloud service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

There are several other papers discussing cloud data security, categorized mainly into two broad areas: the state of the data and the cloud service model.

Risks and Security Concerns Related to Cloud Data Exchange:

There are risks associated with systems, services, and devices that operate on the Internet, and cloud services are no exception[5]. Typically, there are three main components that manage the data in a cloud application or service, each with its own distinct risks. They are:

1. Cloud Infrastructure: This environment is highly controlled from an engineering perspective. Firstly, it effectively restricts access through authorization and user management, meaning that only authorized services, devices, or users can access the cloud infrastructure. Secondly, security updates and patches are usually up-to-date. Thirdly, robust and recommended encryption methods are available. Lastly, data can be distributed or provide high availability. However, cloud infrastructure also has security and performance risks:
    a. Handling Data: If not designed correctly and in accordance with industry standards, data may be exposed to unauthorized entities.
    b. Hiding Business Logic and Intellectual Property: A weak cloud infrastructure architecture can expose business logic or intellectual property to the outside world, potentially harming the business.
    c. Performance Issues: Infrastructure components should be scalable to leverage memory and computing power. However, a faulty design or configuration can lead to overall system performance issues.
2. Communication Channel: Data security is critical when exchanging information over the Internet. The latest version of the transport layer security protocols provides a protective shield for the data being transmitted. However, it is common for systems and software not to be updated to migrate to the latest version of these protocols. This can pose a significant risk to the data exchanged between applications and the cloud.
3. Client Side Application or End Points: Among the three components, this one is most likely to cause data security threats, as it is difficult for the service provider to manage efficiently. In most use cases, the client-side application or endpoint is exposed to users who may not have training in data security. Many tools and techniques are available to enhance data security significantly; however, the most important factor is user training and how users handle data. There are several risks associated with this component, with the major ones outlined below:

a. Data is no longer encrypted: Any data received by the client-side application must be decrypted, or the decrypted data must be presented to the user in a human-readable format at the presentation layer. This is where user authorization becomes important. If the user is not trained to use the endpoint securely, the data could be compromised.
b. Local data storage: Storing or downloading data to local storage can create a serious threat to data security. Unless the device is secure and the user is well trained, this remains a significant risk.

Strategies to Reduce Risks Associated with Cloud Data Exchange:

In the previous section, we analyzed the data security risks. Now, let's examine the strategies for minimizing these risks for each component.

1. Cloud Infrastructure: The design of cloud infrastructure depends on application requirements, security standards, and a security-focused design. This is where data security for Data at Rest (DAR) becomes crucial. Therefore, securing data with multiple layers of security and enhanced encryption is common practice. The cloud infrastructure architecture should guarantee that the data security requirements are met for the Data At Rest(DAR)[1]. Figure 1 shows a typical simple web application.

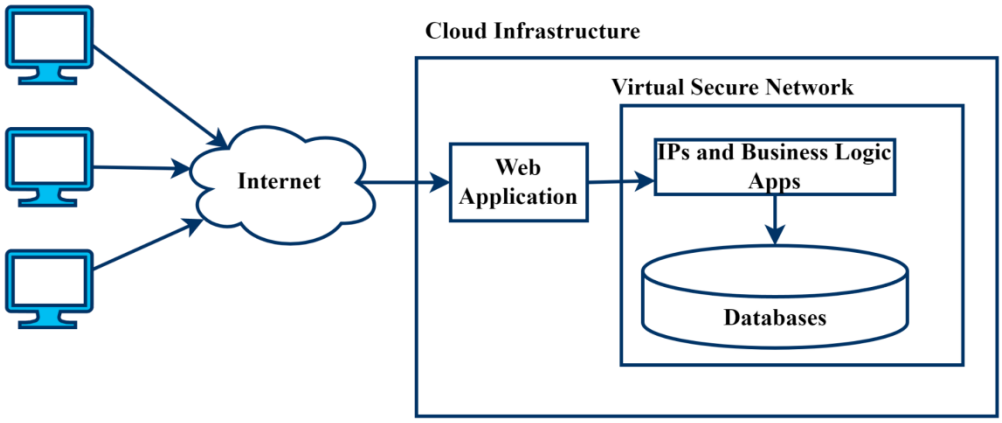

Figure 1: Typical Cloud Web Application

The following strategies may be helpful in designing a better cloud infrastructure.

a. Least Privilege: Only grant users or applications access to cloud resources if really necessary and secure.
b. Use Virtual Secure Network: Secure the IP and business logic applications using a virtual secure network, allowing only designated cloud resources to access these resources according to the design and without external access.
c. Don’t decrypt: Avoid decrypting data at the web application level in the server. If possible, avoid decrypting completely; if unavoidable, perform the decryption within a virtual secure network and use services like a key vault for key preservation. Also, consider encrypting based on domain standards if data encryption is required.

2. Communication Channel: This is the active playground for Data in Transit (DIT)[1]. It is essential to use secure data transmission protocols and strong data encryption to protect information on communication channels. Utilizing the latest version of the Transport Layer Security (TLS) protocol[2], specifically TLS 1.3, is essential to overcome existing vulnerabilities. Despite the TLS

1.3 release in 2018 and widespread awareness of the vulnerabilities associated with previous versions of TLS, many servers have yet to upgrade. Reports indicate that only about 60% of servers have migrated to TLS 1.3. Therefore, it is important to use encrypted data for data transfer over the Internet.

3. Client Side Application or Endpoints: As mentioned in the previous section, managing data security efficiently is the most complex component of this process. However, there are several guidelines that can be followed to ensure that data security remains intact when the client-side application is in the hands of a trained user.
    a. Minimum Information Presentation - The application should display only essential information on the user interface. A good example of this is a patient scan report. In this case, the relevant information is the medical report itself. Therefore, patient details should not be shown, while the report can still be identified using a case number.
    b. Using the standard level of encryption - There are different types and levels of encryption algorithms. The two main types of encryption are symmetric and asymmetric. In symmetric encryption, specifically AES (Advanced Encryption Standard), there are various versions, such as AES-128, AES-192, and AES-256. The choice of encryption algorithms depends on several factors, including the sensitivity of the data, domain-specific standards, the size of the data for each transfer, and the mode of operation. In addition to encryption, it is always recommended to use a Message Authentication Code (MAC) to ensure that the server can verify that the message comes from the expected client. In summary, encryption ensures data integrity, while a message authentication code verifies the authenticity and origin of the message.
    c. Client application or endpoint device Authentication: To ensure the security of the application or device, authentication must be robust to prevent unauthorized access. Two-factor authentication with location tags is widely used across major sectors. If the device needs to function in areas without internet connectivity, it's essential to ensure that authentication remains valid only for a limited period of time in those locations.
    d. Remote Lock and Data wipe: This feature allows devices or applications to be locked remotely and sensitive data to be wiped if the system or device falls into the wrong hands.

Conclusion:

In numerous industrial sectors, such as finance, medical devices, hospital management, and HR services, securely handling data for storing, transmitting, and purging is critical. Data security is a vital aspect of cloud computing and its associated services and applications, as these tools are widely used in these domains to meet business needs effectively. In a typical cloud application that utilizes cloud infrastructure and services over the internet, there are three key components to consider for ensuring data security: Cloud Infrastructure, Communication Channel, and Client-side Application. These components are essential for safeguarding Data At Rest (DAR) and Data In Transit (DIT).

While there is a wide range of tools and services available to enhance the security of Cloud Infrastructure, the effectiveness of these measures largely depends on understanding the sensitivity of the data and the requirements related to security, performance, and scalability. Since data is most likely to be stored in the cloud[3], implementing encryption and managing access for Data At Rest (DAR) is critical for maintaining its security.

The primary communication channel is the Internet, where the Transport Layer Security (TLS) protocol[6] plays a crucial role. It is essential to utilize the latest version of TLS within the system architecture to ensure optimal security.

The client-side application is designed for use by trained users, especially when it deals with critical data or sensitive information. Implementing the correct encryption mechanisms is vital, as this component is responsible for encrypting user input data and decrypting data for user presentation. Additionally, a "Minimum Information Presentation" strategy is essential for applications that handle sensitive information.

In summary, using the right tools and packages with recommended versions, along with a proper design and architecture that prioritizes security, is key to ensuring that cloud applications and systems are designed for data security.

References:

1. A. Albugmi, M. O. Alassafi, R. Walters and G. Wills, "Data security in cloud computing," 2016 Fifth International Conference on Future Generation Communication Technologies (FGCT), London, UK, 2016, pp. 55-59, doi: 10.1109/FGCT.2016.7605062.
2. X. Zhang, H. -t. Du, J. -q. Chen, Y. Lin and L. -j. Zeng, "Ensure Data Security in Cloud Storage," 2011 International Conference on Network Computing and Information Security, Guilin, China, 2011, pp. 284-287, doi: 10.1109/NCIS.2011.64.
3. A. Markandey, P. Dhamdhere and Y. Gajmal, "Data Access Security in Cloud Computing: A Review," 2018 International Conference on Computing, Power and Communication Technologies (GUCON), Greater Noida, India, 2018, pp. 633-636, doi: 10.1109/GUCON.2018.8675033.
4. V. Chang and M. Ramachandran, "Towards Achieving Data Security with the Cloud Computing Adoption Framework," in IEEE Transactions on Services Computing, vol. 9, no. 1, pp. 138-151, 1 Jan.-Feb. 2016, doi: 10.1109/TSC.2015.2491281.
5. R. Velumadhava Rao, K. Selvamani, Data Security Challenges and Its Solutions in Cloud Computing, Procedia Computer Science, Volume 48, 2015, Pages 204-209, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2015.04.171.
6. D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, China, 2012, pp. 647-651, doi: 10.1109/ICCSEE.2012.193.
7. T. V. Sathyanarayana and L. M. I. Sheela, "Data security in cloud computing," 2013 International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), Chennai, India, 2013, pp. 822-827, doi: 10.1109/ICGCE.2013.6823547.