# Understanding the CIA Triad and The Differences Between Authentication and Authorization

BLUF:
This paper discusses the principles of the CIA Triad and information security. This journal also talks about the differences between Authentication and Authorization, highlighting their roles in safeguarding sensitive data.

## Introduction:

In cybersecurity the CIA Triad is used to ensure the security of information systems. The three pillars of the CIA Triad are Confidentiality, Integrity, and Availability. These pillars form the basis of a robust security framework. The framework's goal is to safeguard sensitive data and maintain the overall functionality of digital systems.

## The CIA Triad:

### Confidentiality:

Confidentiality makes sure information is only accessible to certain people that are authorized. Encryption, access controls, and secure communication channels are big components when it comes to confidentiality. Protecting sensitive data from unwanted and unauthorized access is the main goal of confidentiality.

### Availability:

Availability ensures that information and resources are available when needed. Disaster recovery plans and network infrastructure play a role in making sure digital systems remain available even with disruptions like hardware failures or cyber-attacks.

## Authentication vs. Authorization:

### Authentication:

Authentication is the process of verifying the identity of a user, device, or a system. The goal is to make sure people accessing a system are who they claim to be. Authentication methods like passwords and multi-factor authentication are used. Authentication is the first line of defense against unauthorized access.

### Authorization:

Authorization is the process of granting or denying access to specific resources based on the user's permissions. Once the user is verified through authentication, authorization determines the level of access they have within that system. Role-based access control (RBAC) and access control lists (ACLs) are examples of authorization.

Example:
I'll be using a bank's online banking system as an example. Authentication ensures that a user logging in is the legitimate account holder by verifying their username and password. Once that's done, authorization will see whether the user has permission to view account balances, transfer funds, or do any other transactions based on their account type and the privileges they have.

Conclusion:
The CIA Triad is a framework for cybersecurity and emphasizes the importance of confidentiality, integrity, and availability. Understanding the differences between authentication and authorization is crucial when making effective access controls. By appreciating these concepts and using them, organizations can better defend unauthorized access and data breaches, ultimately helping make a secure and resilient information environment.