

Assignment#1

1. Describe with an example application how information may be shared securely in the cloud.
- A. Cloud is a fast-growing platform which provides services like infrastructure (IAAS), Software (SAAS) and platform (PAAS) for organizations ranging from small to big. Lack of security features had been a major drawback for cloud services, as confidentiality and integrity authentication are a major concern for industries.

Another problem is defining who and under which circumstances, can gain legal permission to access the data stored on the cloud. Users believe that their information is confidential and protected from everyone just because it belongs to them and ease their property. But they often forget that the space where they store it is not theirs and it function by its own rules. The following are few ways in which cloud data can be shared securely.

1. **Do not house sensitive information on cloud:**

- Always store critical information away from virtual world and read the user argument for the cloud service opted clearly.

2. **Consider passwords very carefully:**

- Almost 90% passwords can be cracked in less than few hours. This shows how important it is to choose your password for cloud service.
- The best way is to use two-step authentication and use alpha-numeric and special characters as passwords with minimum length of 10 characters to make it strong.

3. **Don't forget to use encryption:**

- Encryption is the best way to protect your data on any cloud services. The most easiest way is to zip a file and encrypt it with password.

Application of information shared securely:

iCloud: iCloud is an apple initiative which provides industry standard security technologies and employs strict policies to protect information of its cloud users. Its leading industry by adopting privacy preserving technologies like end to end data encryption.

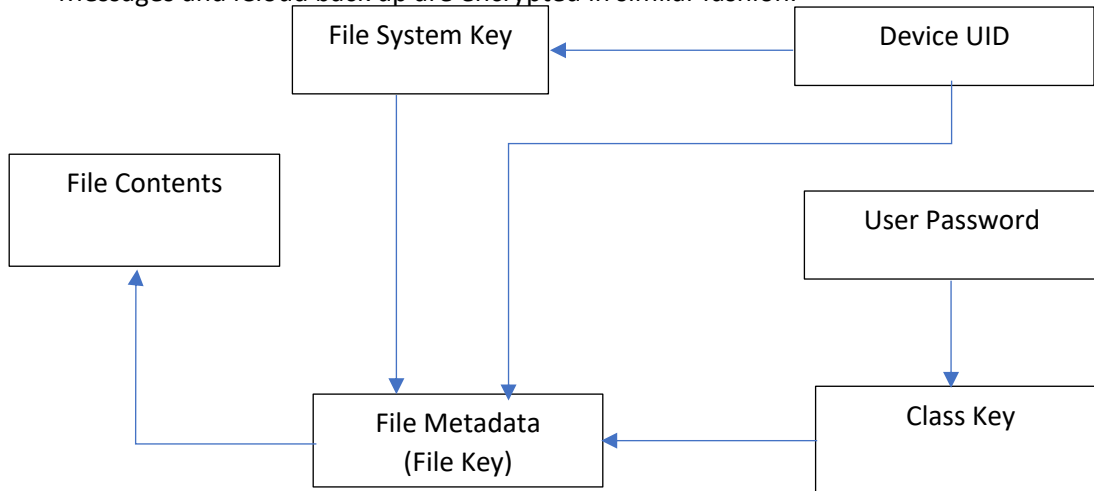
1. **Data Security:**

- iCloud services its customers information while sharing by encrypting in its transit.
- It also stores the user's information in iCloud in an encrypted format using secured tokens.
- Apple users end to encryption which means only the users who uploaded the data r the person the user shred the data with can access.
- Apple end to end encryption uses two factor authentications as a means of additional security measure.

2. **End-to-end encryption data:**

- End to end encryption data provides the data security with a key derived from information unique to the user's device.

- The end to end encryption is used for both transmitted data and stored data on cloud.
The following are some of the data where end to encryption is applied.
 - ➔ Home data ➔ payment information
 - ➔ Health data ➔ Wi-Fi and Siri network information
- Messages and iCloud back up are encrypted in similar fashion.



iCloud File Security Architecture

2. Describe with an example application how SAML and XACML may be extended to the cloud.

A. The application of SAML and XACML may be extended to the cloud using complex resource provisioning model as an example.

- We explore technologies such as XACML and SAML to provide which functionality for the CRP (Complex Resource Provisioning) model policy expression and dynamic security context management.
- The CRP model consists of separate resource reservation allocation and access stages.
- The stages can be further compressed into two stages
 1. Access and 2. Consumption
- Thus, process is controlled by meta scheduling system using Auth.Z policies
- It also uses AAA Auth.Z sequence so that the requestor can send resource access to its requestor.

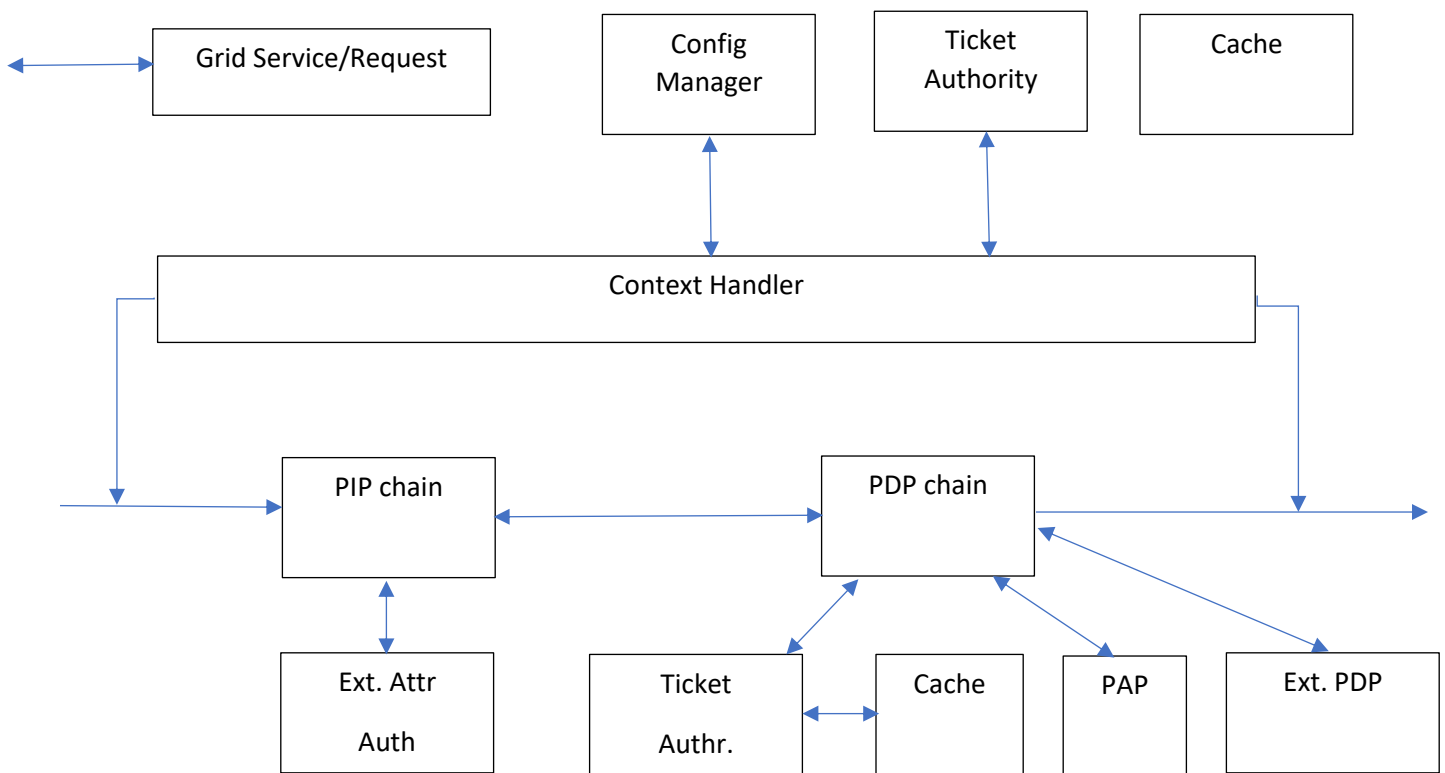
1. Using XACML for policy expression:

- Different CRP scenarios require for both complex and flexible permission management, which can be supported by XACML.
- Hierarchical resources management and policy management are considered very important functionality in CRP security. It is also implemented using XACML.
- XACML provides a policy number and rule combination algorithms for any decision request.

- XACML also provides mechanisms to bind a policy to the resource and handle its domain related security context.

2. **Adding security context management:**

- The semantics of authentication ticket elements is defined in such a way that it allows easy mapping using SAML and XACML.
- The current implementation of gJAF support framework uses SAML and XML based authentication tickets.
- Session management is supported by Auth.Z session management system and triage PDP.
- The framework also uses XACML PDP extension called PDP for general purpose implementation.



Security Context Management in CRP scenarios