02/22/19

Assignment - 1

1. Describe with an example application how information may be shared securely in the cloud.

Ans.

Cloud is a fast growing platform which provides services like infrastructure (IAAS), Software (SAAS) and platform for organizations ranging from small to big. Lack of security features had been a major drawback for cloud services, as confidentiality and integrity authentication is 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 securly.

1. Do not house sensitive information on cloud:

* always store critical information away from virtual world and also read the use agreement 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 also use alphanumeric 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 in 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. It's a leading industry by adopting privacy preserving technologies like end to end data encryption.

1. Data security: *

* iCloud secures its customers information while sharing by encrypting in its transit.

* It also stores the users information in iCloud in an encrypted format using secured tokens.

* Apple uses end to encryption which means only the user who uploaded the data or the person shared the user shared the data with can access.

* Apple end to end encryption uses two factor authentication as a means of additional security measure

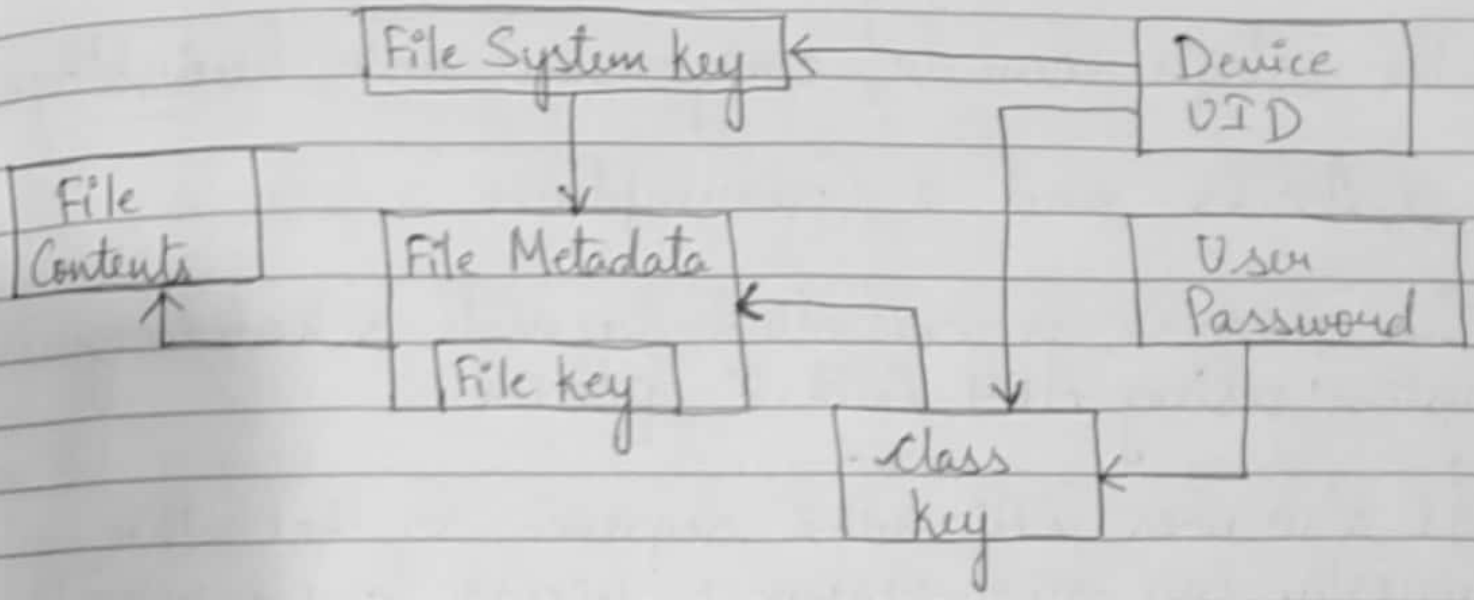
2. End-to-end encryption data:

* End to end encryption data provides the data security with a key derived from information unique to the users 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 → wifi and Siri network information

* Messages and iCloud back up are encrypted in similar fashion.



iCloud file Security Architecture

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

Ans. 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 content management.

* The CRP model consists of seperate resource - reservation, allocation and access stages

* The stages can be further compressed into two stages
1. Access and 2. Consumption

* This process is controlled by meta scheduling system using AVT Auth.Z policies.

* It also uses AAA AuthZ 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.

* Hierarchal 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 particular decision request.

* XACML also provides mechanisms to bind a policy to the resource and handle its domain related security content

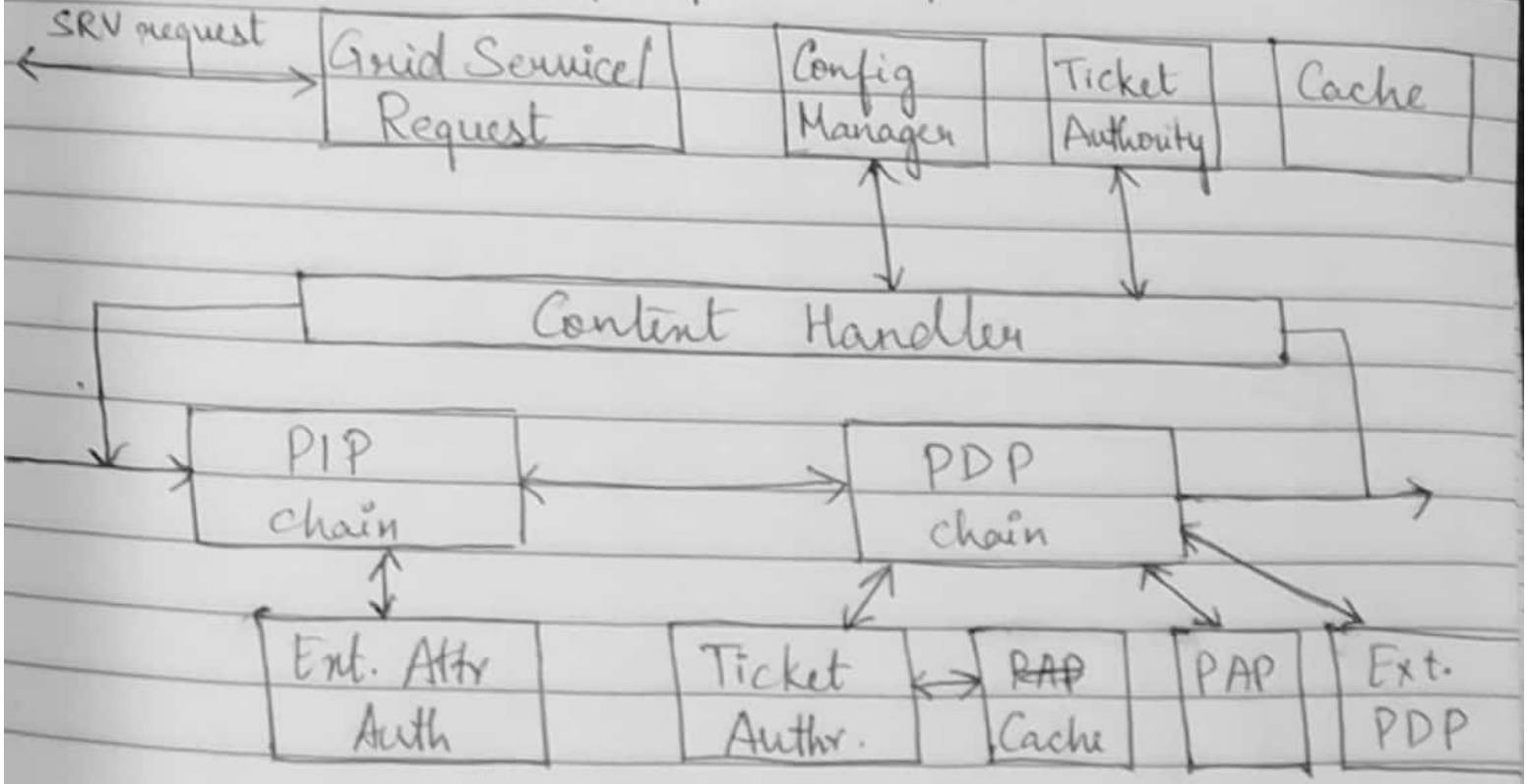
2. Adding security content management :

* 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 authZ session management system and triage PDP

* The framework also uses XACML PDP extension called XOMS PDP for general purpose implementations.



Security Content Management in CRP scenarios.